PRIDA Track 1 (T1)

PRIDA capacity building workshop on IoT and digital services

07/09/2020

Who I am?

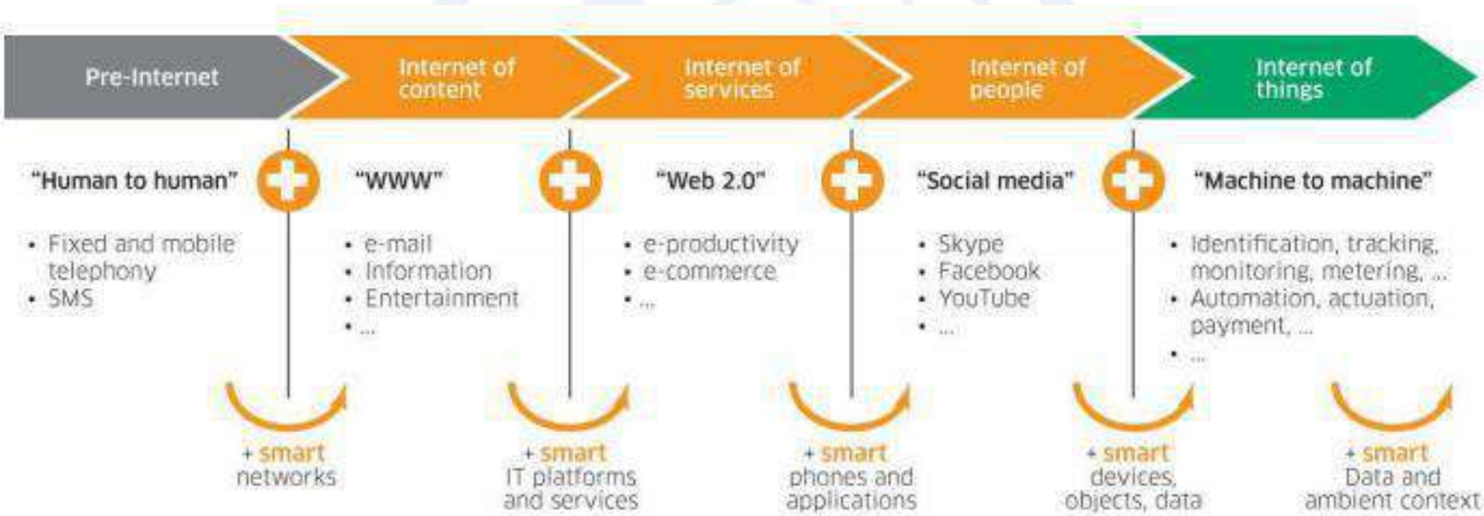
- **Hend Ben Hadji**
- **Ph'D, KAIST (South Korea)**
- Director at Research and Studies Center in Communications (CERT), Tunisia.
- Hend.benhadji@tunsia.gov.tn
- IT Specialist
  - 18 years of experience in IT domain
  - Activites domains :
    - PMO of strategic projects (sectoral projects), Ministry (MTCEN)
    - Responsible of Innovation Program, Ministry (MTCTD)
    - Smart City Program Manager (MTCEN)
    - National focal point of ITU and ATU
    - Member of several international consortia (FP7 PROBE-IT, H2020 GEO-CRADLE, F7 BRAGMA, NIPA-CERT El-Ghazela Smart City, Smart Africa DSNS,…)

Agenda

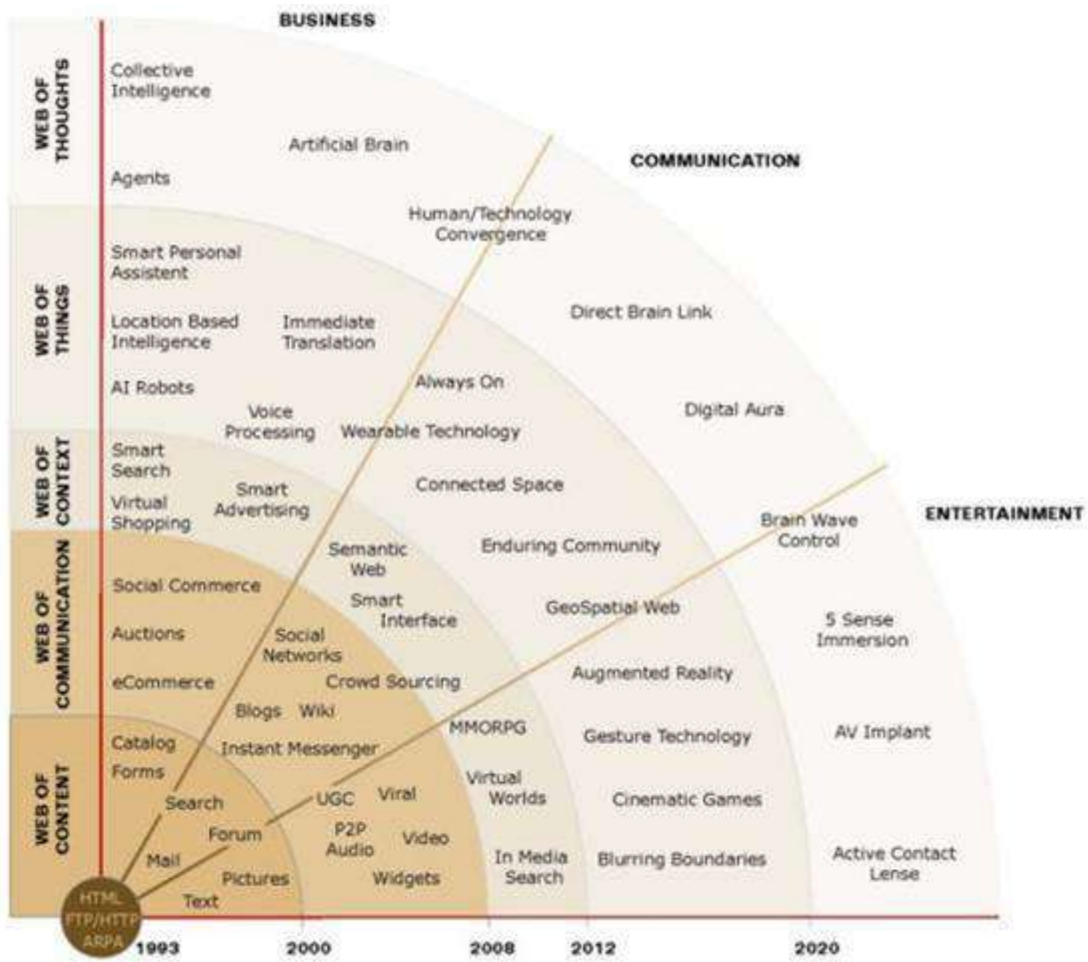
- Part 1: Origin, definitions and motivations
- Part 2: Market, opportunities and challenges
- Part 3: Architecture models and IoT components
- Part 4: IoT value chain, connectivity and business models

Part 1:
Origin, definitions and motivations

Internet evolution

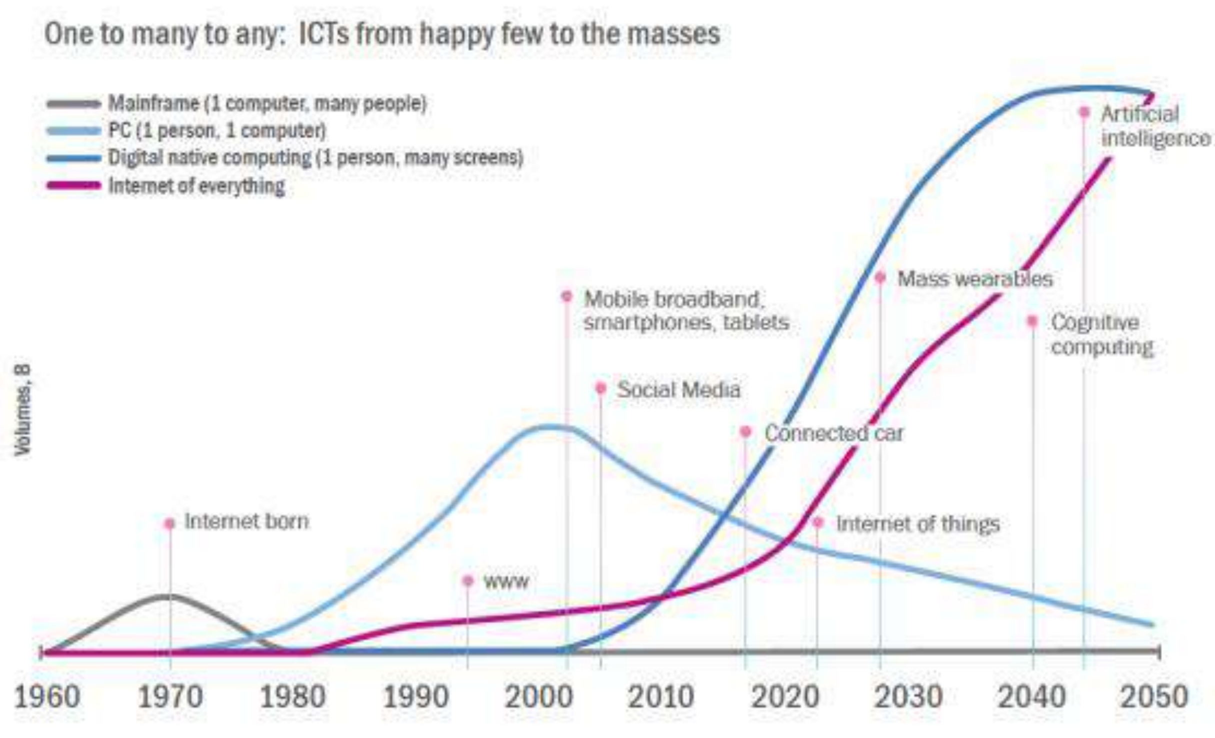


Source: Nokia Insight



Source: https://flatworldbusiness.wordpress.com/flat-education/previously/web-1-0-vs-web-2-0-vs-web-3-0-a-bird-eye-on-the-definition/

History of future



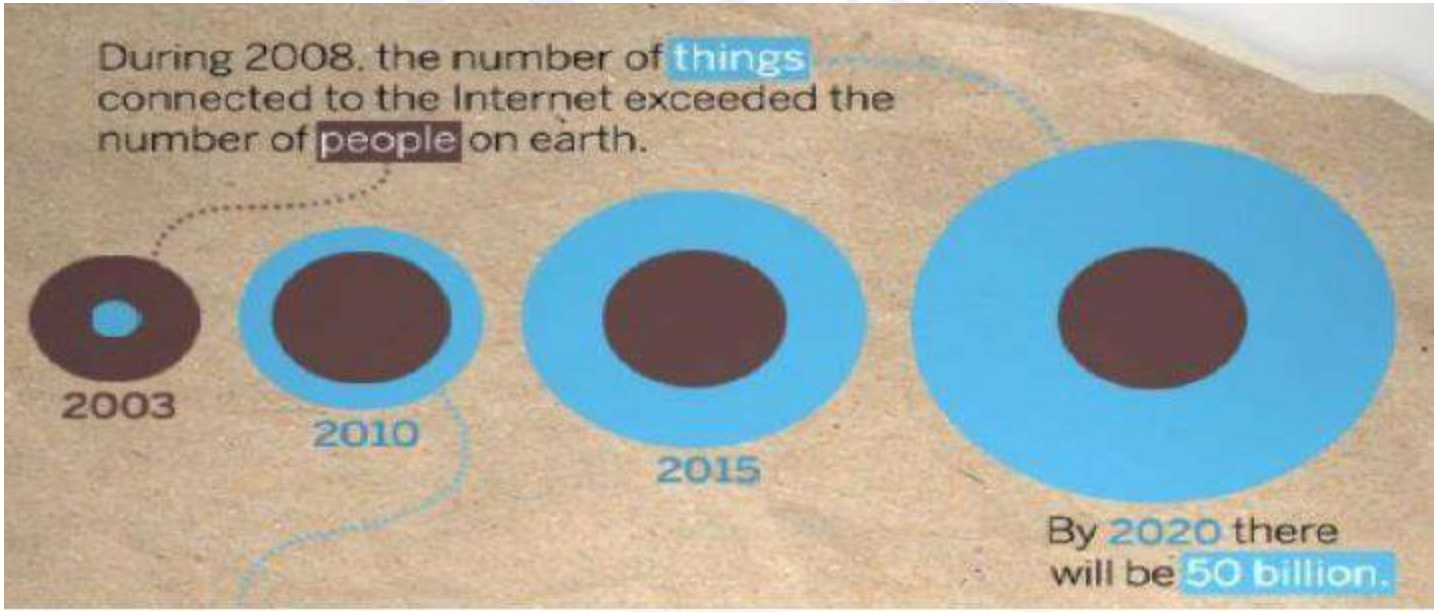
Source: Mario Maniewicz. Digital revolution: Are we ready? 14th Global Symposium for Regulators (GSR)

Origin

- Kevin Ashton: The first to use the term "Internet of Things" in 1999 to describe radio frequency identification (RFID) microchips.

- According to Cisco Internet Business Solutions (IBSG), the Internet of Things was born between 2008 and 2009, when more "things or objects" were connected to the Internet than people.

Origin



Source: Cisco

Origin

- The first IoT application was born at the University of Cambridge in 1991.
- It was a camera fixed into a coffee machine and connected to the university's local network.

- Each IT specialist could know the availability of coffee from his computer.

ITU Definition of IoT

- **Internet of things (IoT)** [ITU-T Y.2060 renamed Y.4000]: “A global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies. »
- **NOTE 1** (from [ITU-T Y.2060 renamed Y.4000]) – From a broad perspective, the IoT can be perceived as a vision with technological and societal implications.
- **NOTE 2** (from [ITU-T Y.2060 renamed Y.4000]) – 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.

IETF Definition of IoT

“The Internet of Things (IoT) refers to devices, that are often constrained in communication and computation capabilities, now becoming more commonly connected to the Internet, and to various services that are built on top of the capabilities these devices jointly provide. It is expected that this development Will usher in more machine-to-machine communication using the Internet with no human user actively involved.”

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

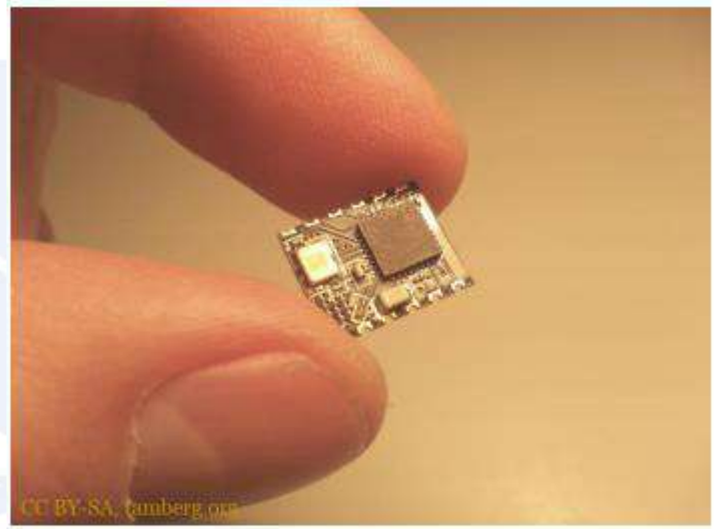
ISO/IEC Definition of IoT

- "It is 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."

Enabling technologies

- **Miniaturization** and **low cost** of electronic components.

RPi zero: 5 dollars



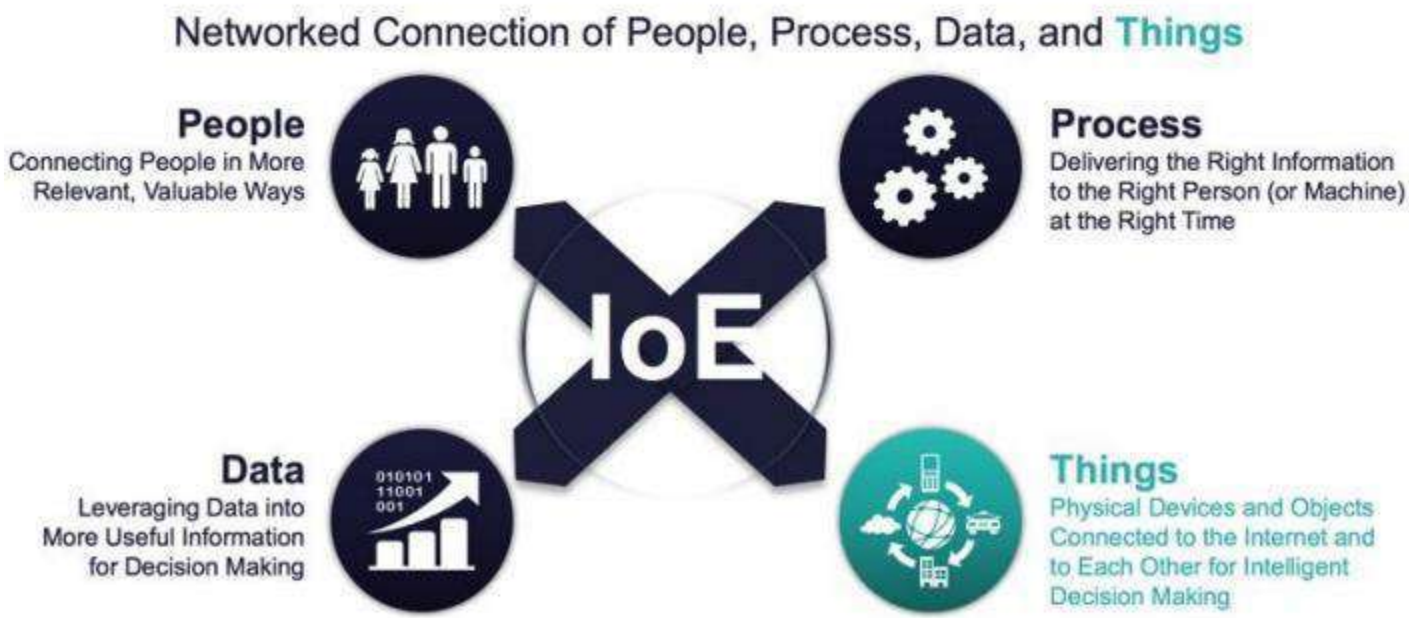
Enabling technologies

- **Ubiquitous connectivity**: variety of wireless connectivity solutions, possibility to connect everything.
- **Communication protocols:** are essential to ensure connectivity between objects and applications. They define the data format, packet size, addressing, routing, etc.
- **Democratization of the Cloud:** The developer does not have to worry about storing data and to invest in hardware and software resources for storage. The Cloud now offers an excellent opportunity for the remote storage of data as well as its processing.
- **Big Data:** offers advanced analysis tools for massive data collected by IoT objects according to their characteristics: volume, speed, variability (form of data: text, audio, video, image).

M2M

- M2M is a subclass of IoT and refers to technologies that enable communication between machines without human intervention.
- Examples include telemetry, traffic control, robotics, and other applications involving device-to-device communications.
- M2M uses a device (sensor) to capture an event (temperature, pollution level, etc.) transmitted via a network (wireless, wired or hybrid) to an application (software) which converts the captured event into meaningful data.

Internet of Every Things



Source : The Internet of Everything | Plutomen Technologies

M2M versus IoT versus IoE

- **M2M:** A device that captures an event and transmits it over the network to an application. The application translates the event into meaningful information.
- **IoT:** A network of uniquely identifiable elements that communicate without human intervntion using IP connectivity.
- **IoE** brings together not only the IoT but also processes, data and people (via smartphones and social networks).

Quizz N°1

What are the fundamental characteristics of IoT ?

Main characteristics of the IoT

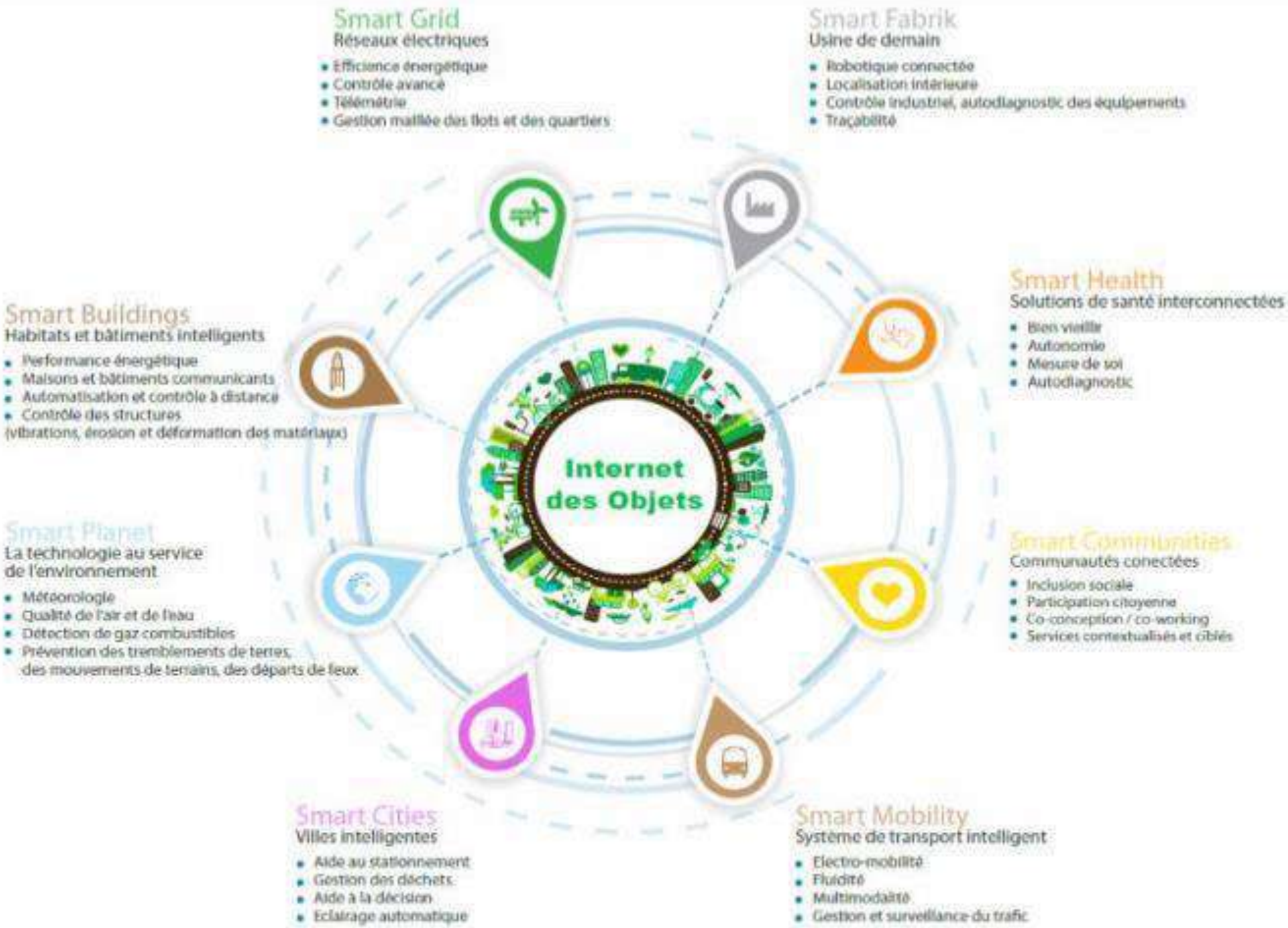
- **Sensing:** Sensors are the main part of the IoT system which are used to perceive changes in the surrounding environment and create data that reveal their status.
- **Intelligence:** Combining sophisticated software algorithms with hardware allow IoT devices to become smart and, consequently, make intelligent decisions in various situations and interact intelligently with other devices.
- **Limited Energy:** Most IoT devices are small and lightweight with limited resources, so they are designed to work with minimal energy consumption.
- **Connectivity:** is the ability to connect various devices with different characteristics and use their information to create novel applications and services.

Main characteristics of the IoT

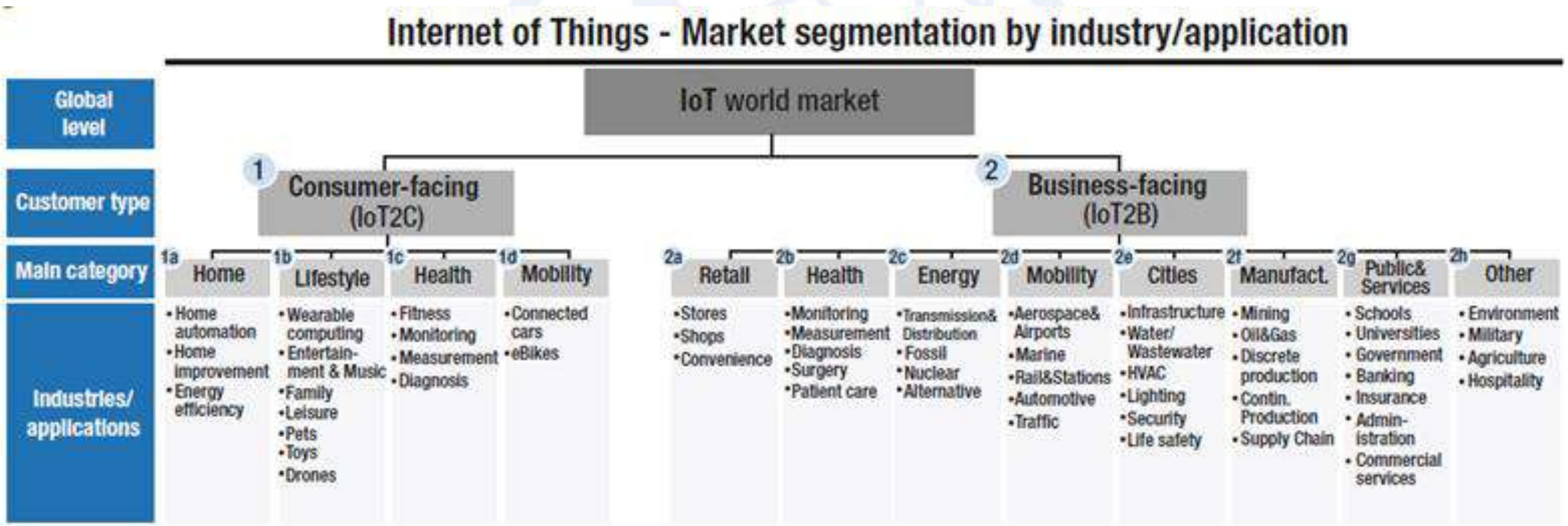
- **Heterogeneity:** The IoT system involves billions of devices with heterogeneous features such as operating systems, platforms, communication protocols and others. These heterogeneous features make the management operation a complex task to perform.
- **Dynamic changes:** The state of devices can change dynamically based on changing conditions and situations, e.g., sleeping and waking up, connected/disconnected acording to the context of devices including localtion and speed.
- **Self-configuring:** the capability of self-configuring enable IoT devices to configure themselves to the uptdate software in association with the device manufacturer without user involvement.
- **Unique Identity:** Within the IoT network, each IoT object is identified and recognized using a unique identifier such as the IP address.

Partie 2: Marché IoT, Opportunités et challenges

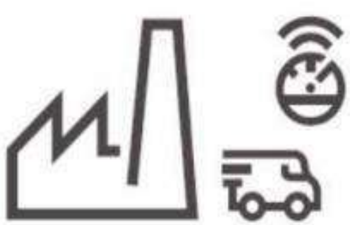
IoT Market


Smart Grid
Réseaux électriques
Efficience énergétique
Contrôle avancé
Télémétrie
Gestion maillée des îlots et des quartiers
Smart Fabrik
Usine de demain
Robotique connectée
Localisation intérieure
Contrôle industriel, autodiagnostic des équipements
Traçabilité
Smart Health
Solutions de santé interconnectées
Bien vieillir
Autonomie
Mesure de soi
Autodiagnostic
Smart Buildings
Habitats et bâtiments intelligents
Performance énergétique
Maisons et bâtiments communicants
Automatisation et contrôle à distance
Contrôle des structures
(vibrations, érosion et déformation des matériaux)
Internet des Objets
Smart Planet
La technologie au service de l'environnement
Météorologie
Qualité de l'air et de l'eau
Détection de gaz combustibles
Prévention des tremblements de terres, des mouvements de terrains, des départs de feux
Smart Communities
Communautés conectées
Inclusion sociale
Participation citoyenne
Co-conception / co-working
Services contextualisés et ciblés
Smart Cities
Villes intelligentes
Aide au stationnement
Gestion des déchets
Aide à la décision
Eclairage automatique
Smart Mobility
Système de transport intelligent
Electro-mobilité
Fluidité
Multimodalité
Gestion et surveillance du trafic

Market segmentation by industry/application



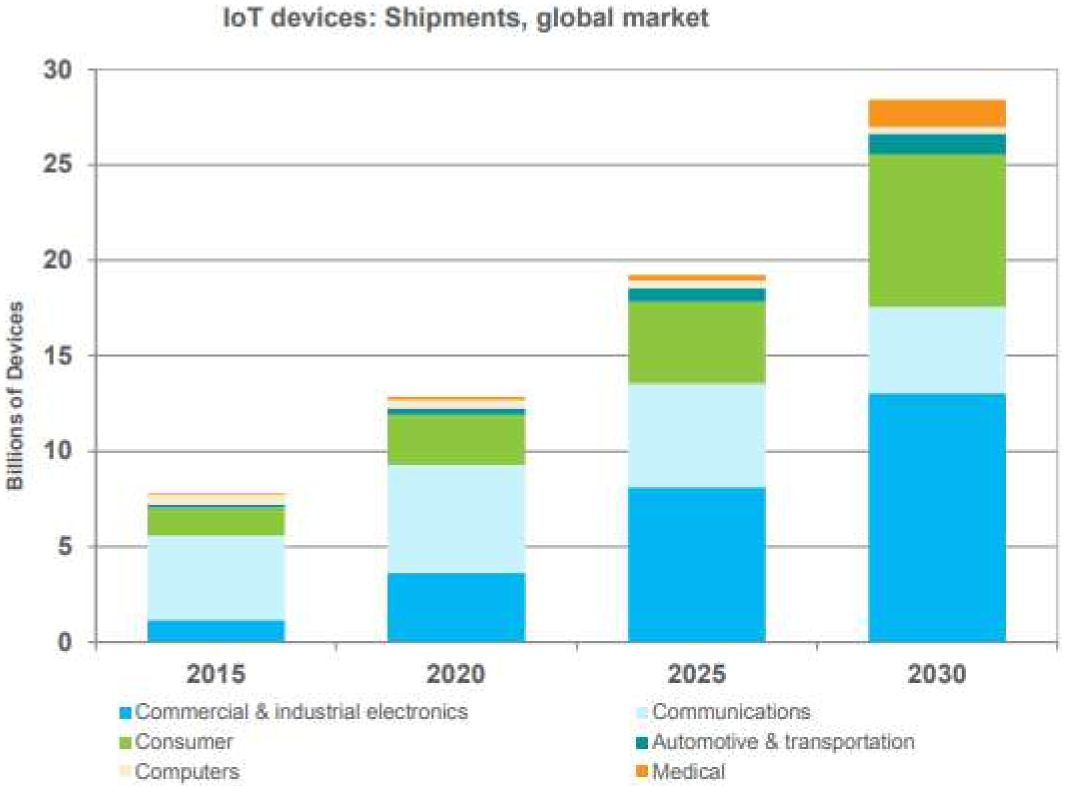
Market segmentation by industry/application

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

Market segmentation by industry/application

- According to IoT analytics, connected objects are classified into 2 categories:
  - **Consumer IoT** are connected objects for the general public. The real value of consumer IoT is in the improved usage it will bring to its user.
  - **Industrial IoT** are a connected objects for industrial use. They are source of new business. Gartner assures that they will be sold less compared those intended for the general public in the years to come, but they will make more money.

IoT Market Growth: Connectable Device Shipments



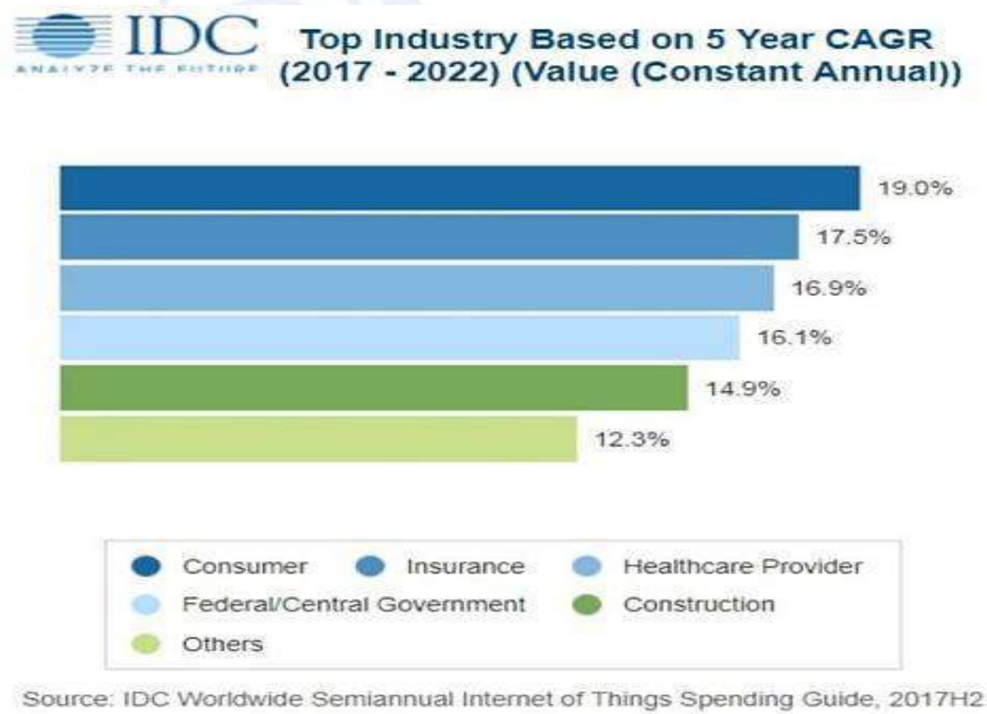
Economic impact of IoT

LPWAN will represent +26% of IoT Market

Source: McKinsey, June 2015

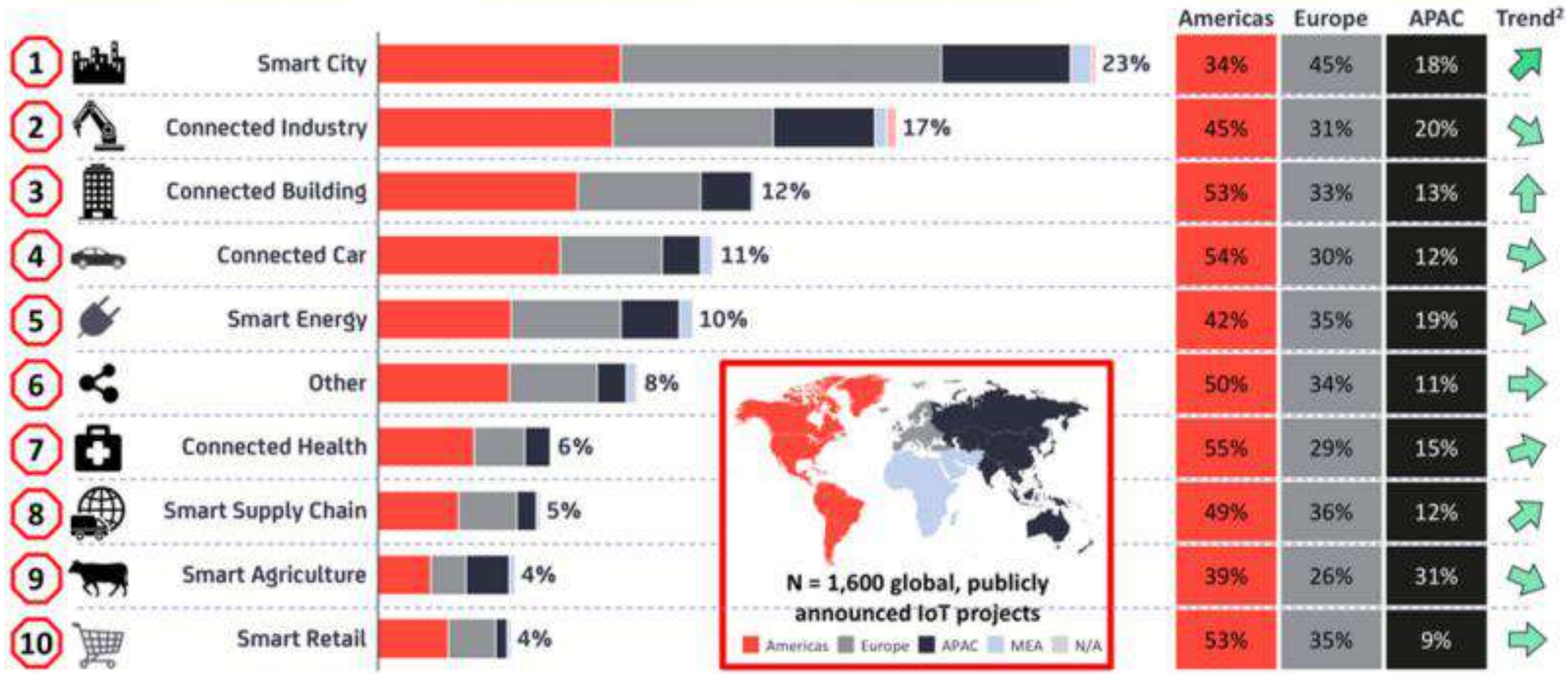
Estimation of IoT expenses

- According to International Data Corporation (IDC), the spending on IoT is expected to reach $ 1.2 trillion in 2022.
- Consumer, insurance, healthcare, government services are expected to be the biggest spending sectors.

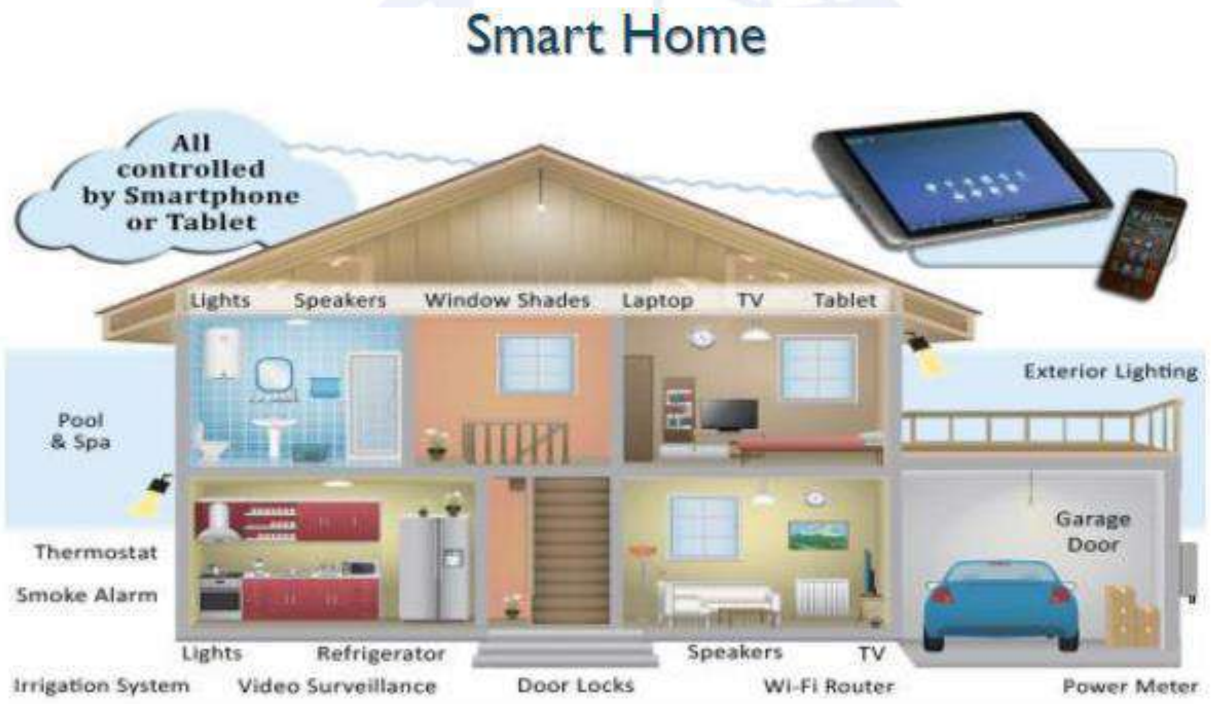


IoT projects share by sector

IoT Segment | **Global market share of IoT projects** | **Details**



Smart home


Smart Home
All controlled by Smartphone or Tablet
Lights
Speakers
Window Shades
Laptop
TV
Tablet
Exterior Lighting
Pool & Spa
Garage Door
Thermostat
Smoke Alarm
Lights
Refrigerator
Speakers
TV
Irrigation System
Video Surveillance
Door Locks
Wi-Fi Router
Power Meter

Smart home


Smart Home Scenario
RDIF tagged Ice Cream
RDIF tagged Cheese Packet
Cloud platform that supports sensing as a service
Ice Cream Manufacturer
Wireless Access Point at Mike's house
Mike
Door Sensor Reader
RFID Reader
Temperature Sensor
Mike's New Refrigerator
Sensor Data Flow
Permission and Access Control Flow

e-Healthcare

E-Healthcare

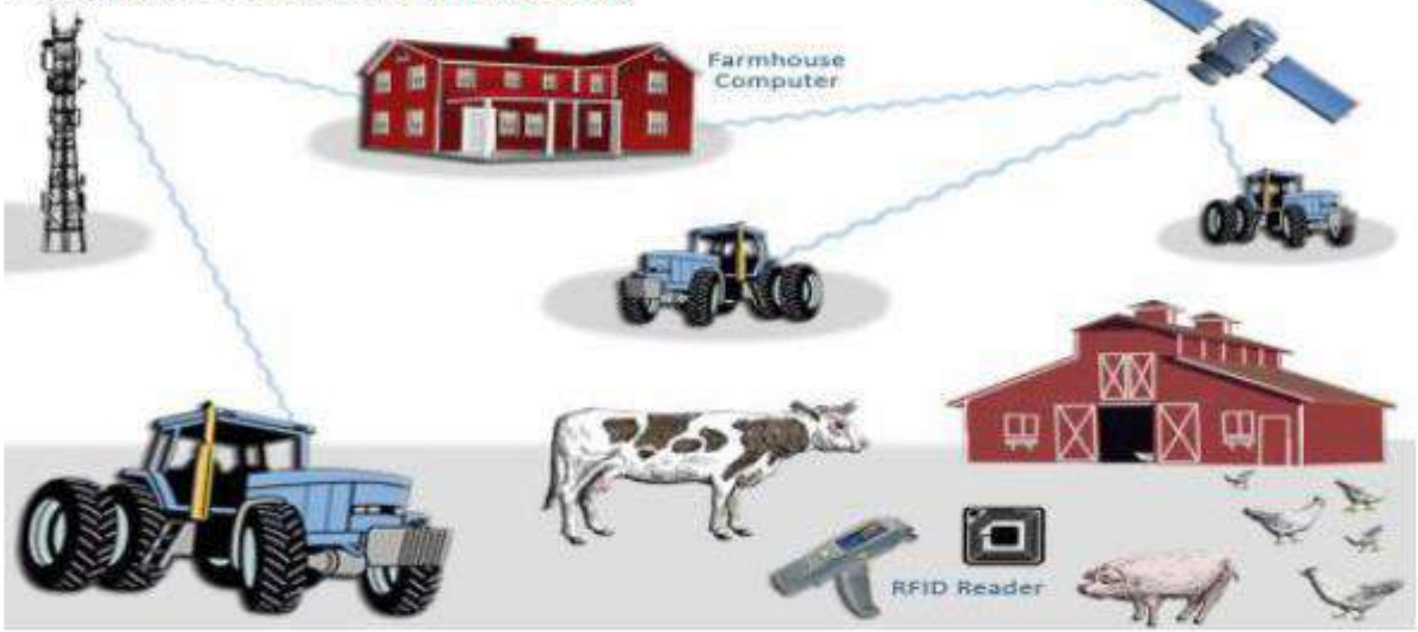
Offer remote health services for baby boomers.
Help them to live independently at their homes instead of nursing homes.

Smart cities

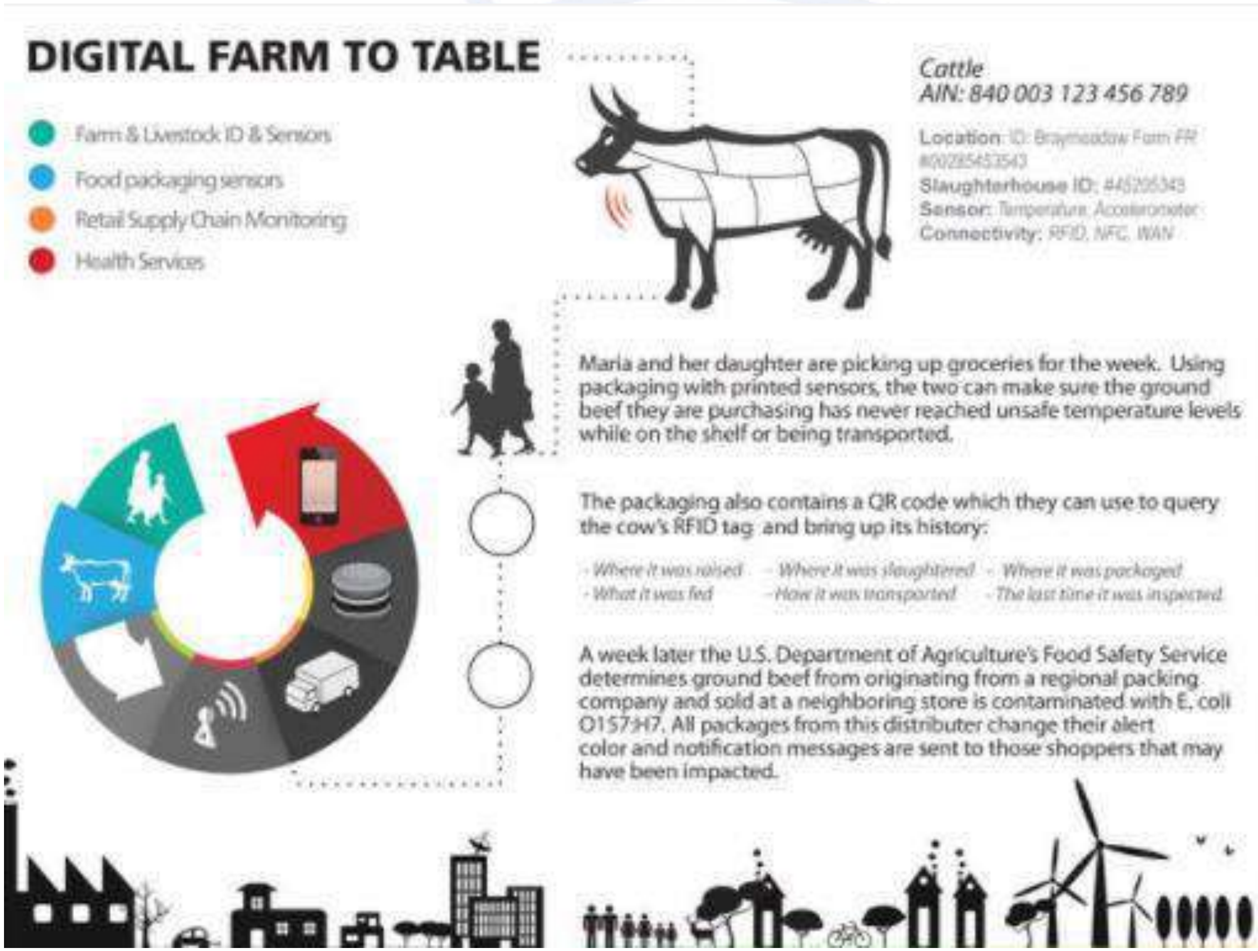
Smart farm

Smart Farms

- Temperature sensors, moisture sensors, etc.
- Sensors to trap and analyze captured insects.
- - Detect when cows are estrus for optimal breeding.



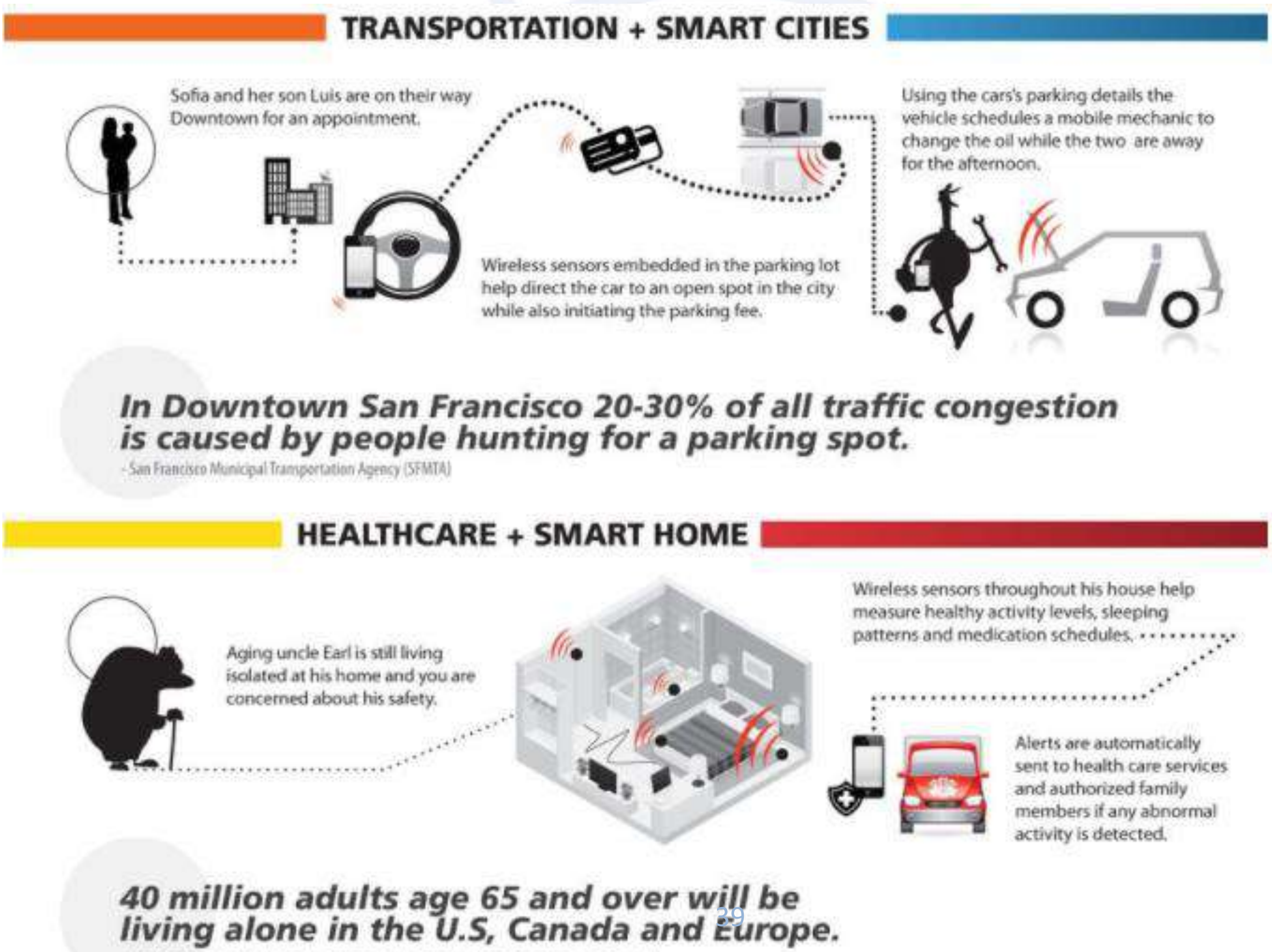
Smart farm



DIGITAL FARM TO TABLE
Farm & Livestock ID & Sensors
Food packaging sensors
Retail Supply Chain Monitoring
Health Services
Cattle
AIN: 840 003 123 456 789
Location: ID: Braymeadow Farm FR
Slaughterhouse ID:
Sensor: Temperature, Accelerometer
Connectivity: RFID, NFC, WAN
Maria and her daughter are picking up groceries for the week. Using packaging with printed sensors, the two can make sure the ground beef they are purchasing has never reached unsafe temperature levels while on the shelf or being transported.
The packaging also contains a QR code which they can use to query the cow's RFID tag and bring up its history:
- Where it was raised
- What it was fed
- Where it was slaughtered
- How it was transported
- Where it was packaged
- The last time it was inspected
A week later the U.S. Department of Agriculture's Food Safety Service determines ground beef from originating from a regional packing company and sold at a neighboring store is contaminated with E. coli O157:H7. All packages from this distributer change their alert color and notification messages are sent to those shoppers that may have been impacted.

Smart building

Other scenarii



Source : https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/

IoT Potential Value / Risk Level by Vertical

Source: OLIVER WYMAN

Challenges

- **Interoperability:** Technological standards in most areas are still fragmented. Continuous fragmentation in the implementation of IoT will decrease the value and increase the cost to the end users. These technologies need to be converged towards a common framework and the standard for IoT devices.
- **Security vulnerabilities:** IoT devices greatly expand the "attack surface," or the amount of potential areas for cybercriminals to penetrate a secure IoT system. Obviously, the consequences of sabotage and denial of service could be far more serious than a compromise of privacy. For instance, Changing the mix ratio of disinfectants at a water treatment plant or stopping the cooling system at a nuclear power plant could potentially place a whole city in immediate danger.
- **Scalability:** Billions of internet-enabled devices get connected in a huge network. The large volume of data obtained from these devices need big data analytics and cloud storage for interpretation of useful data. The system that stores, analyses the data from these IoT devices needs to be scalable.

Challenges

- **Dense and durable off-grid power sources:** Most sensors still need regular battery changes or connection to the grid. It would make a difference if power could be broadcasted wirelessly to such devices from a distance, or if power sources that can last for at least a year can be integrated into the sensors.
- **Regulatory issues:** Existing regulations are not suitable for specific IoT applications. For example, companies are investing heavily in autonomous cars, but the circulation of self-driving cars is not yet allowed as regulatory policies are unclear. Governments often haven't moved with sufficient speed to regulate these new technologies as they become available.
- **Data owner:** A common understanding of property rights among stakeholders should be clearly defined to unlock the full potential of IoT. The question remains open, for example in medical devices implanted in the body of a patient, the question of the right to the data generated, the patient or the manufacturer of the device.

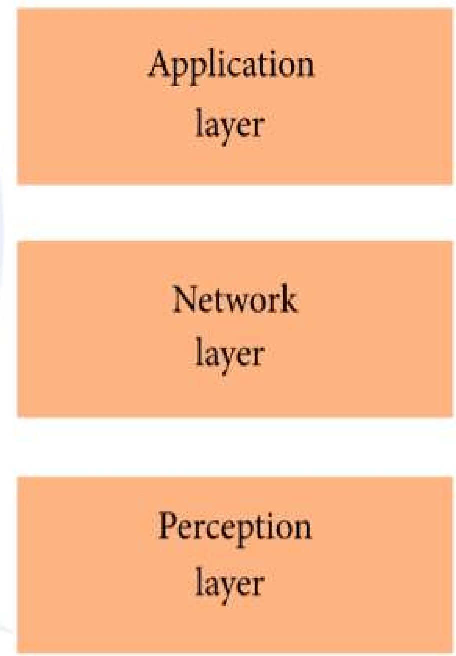
Quizz N°2

1.What are the main sectors that can create economic value in Africa, in your opinion? and Why?

Part 3:
IoT Architecture and components

IoT Architecture: IoT 3 layers model

- The architecture of an IoT solution varies from system to system based on the type of solution to be implemented.
- The most basic architecture is a three-layer architecture:
  - **The perception layer** has sensors and actuators that sense and collect information about the environment.
  - **The network layer** is responsible for connecting, transporting and processing data from sensors and actuators.
  - **The application layer** provides the user with specific services and applications.



IoT Architecture: IoT 4 layers model

Application layer

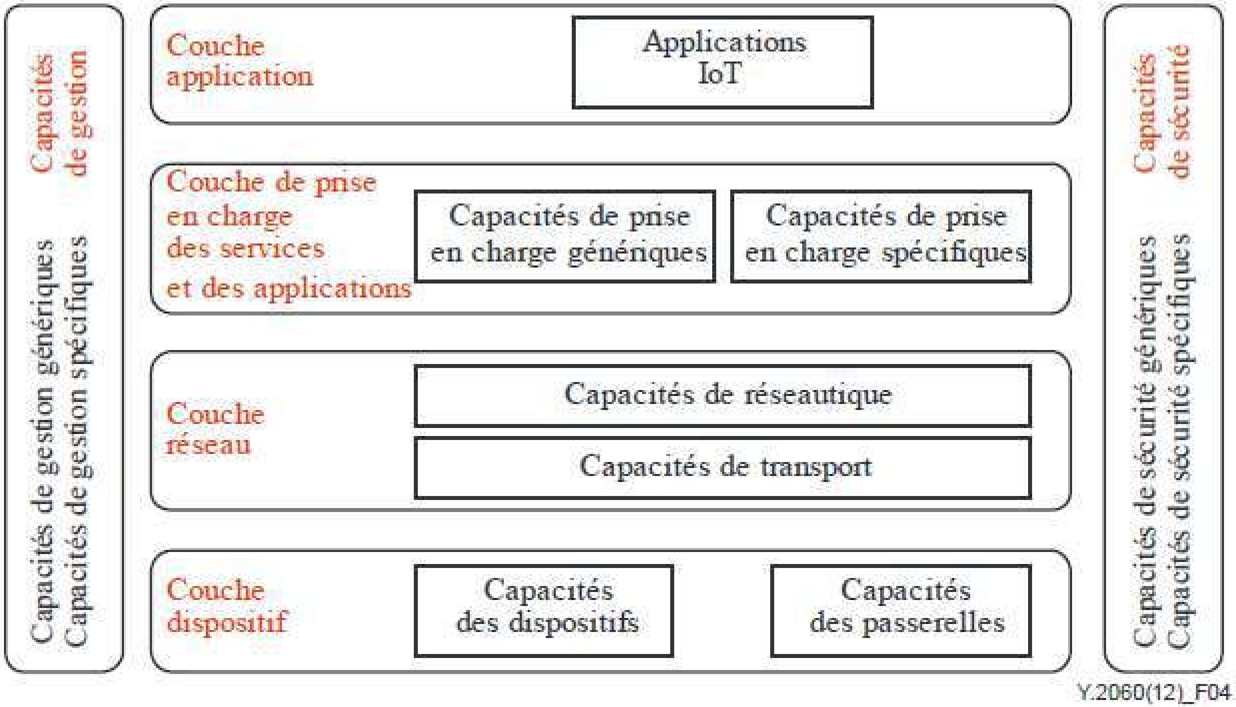
Information processing layer

Network layer

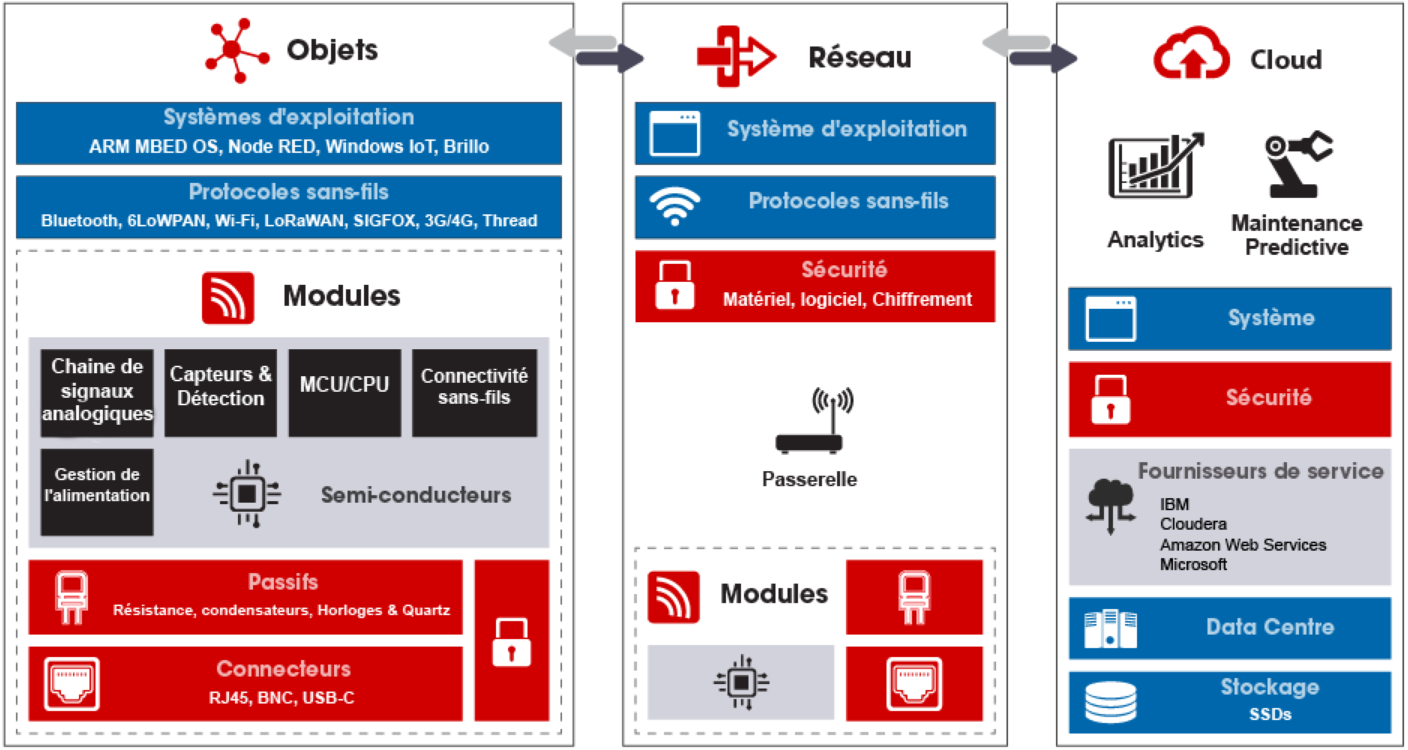
Perception layer

IoT reference model by ITU

- IoT reference model (TU-T Y.2060 recommendation)



Functional architecture of an IoT solution



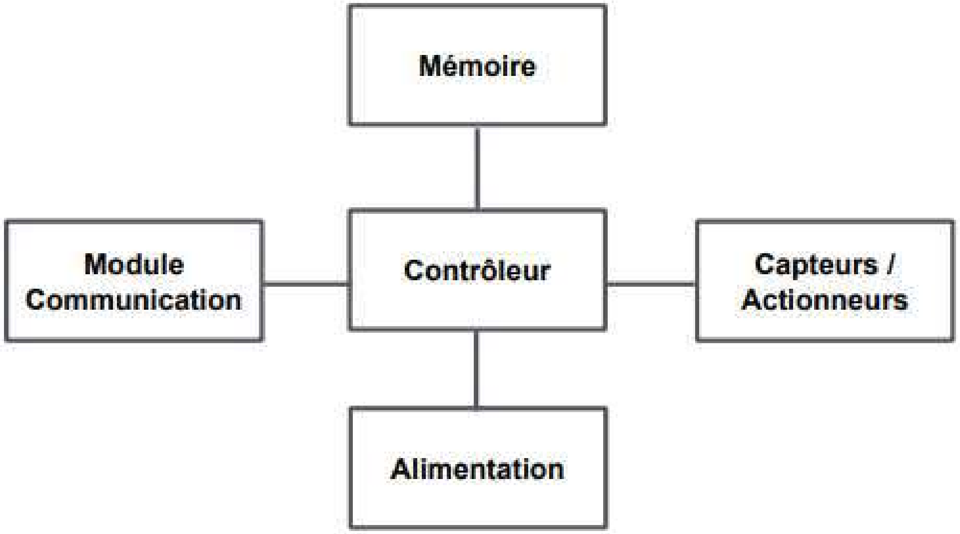
Source : https://fr.rs-online.com/web/generalDisplay.html?id=i/ido-internet-des-objets

IoT solution components

- Typically, an IoT solution is made up of the following components:
  - Sensors/Actuators
  - Gateway
  - Network infrastructure
  - Platforms/Cloud platforms

Level 1: Sensor/Actuator

- Detection unit: Sensor / Actuator
- Processing unit: Controller
- Communication unit: RF module
- Power



Level 1: Sensor/Actuator

- **Sensor:** A device used to detect an event or a physical parameter, such as brightness, temperature, soil moisture, pressure, etc. and provides a corresponding electrical signal.

- IoT sensors are generally small in size, inexpensive, and consume less power.
- Signals produced by a sensor are processed by a microcontroller for interpretation, analysis and decision making.

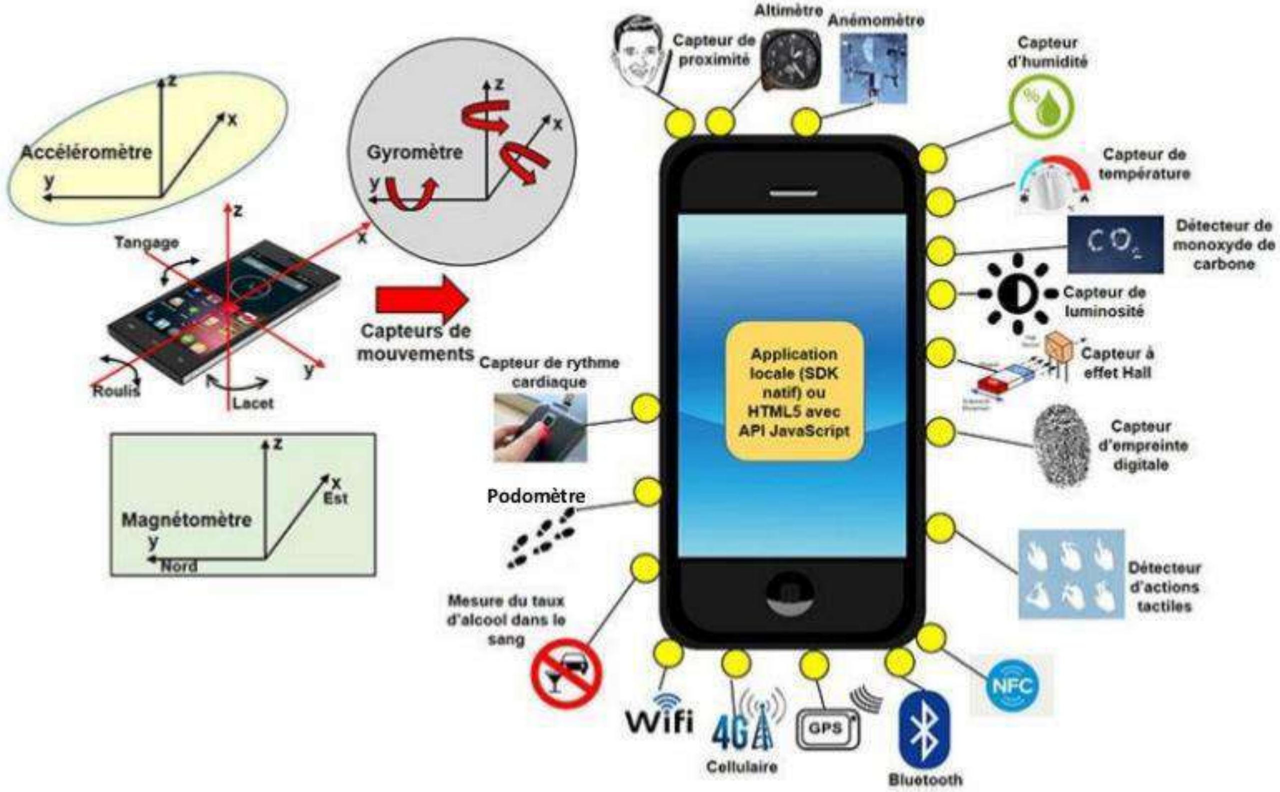
Sensor types	Sensor description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors will generate a signal even when a person is stationary, while a motion sensor will not.	Electric eye, RADAR
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors and measure the force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, bourdon gauge, piezometer

Sensor types	Sensor description	Examples
Pressure	Pressure sensors are related to force sensors and measure the force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter
Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	Microphone, geophone, hydrophone
Humidity	Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector
Radiation	Radiation sensors detect radiations in the environment. Radiation can be sensed by scintillating or ionization detection.	Geiger–Müller counter, scintillator, neutron detector

Sensor types	Sensor description	Examples
Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge
Chemical	Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO2 sensor senses only carbon dioxide).	Breathalyzer, olfactometer, smoke detector
Biosensors	Biosensors detect various biological elements such as organisms, tissues, cells, enzymes, antibodies, and nucleic acids.	Blood glucose biosensor, pulse oximetry, electrocardiograph

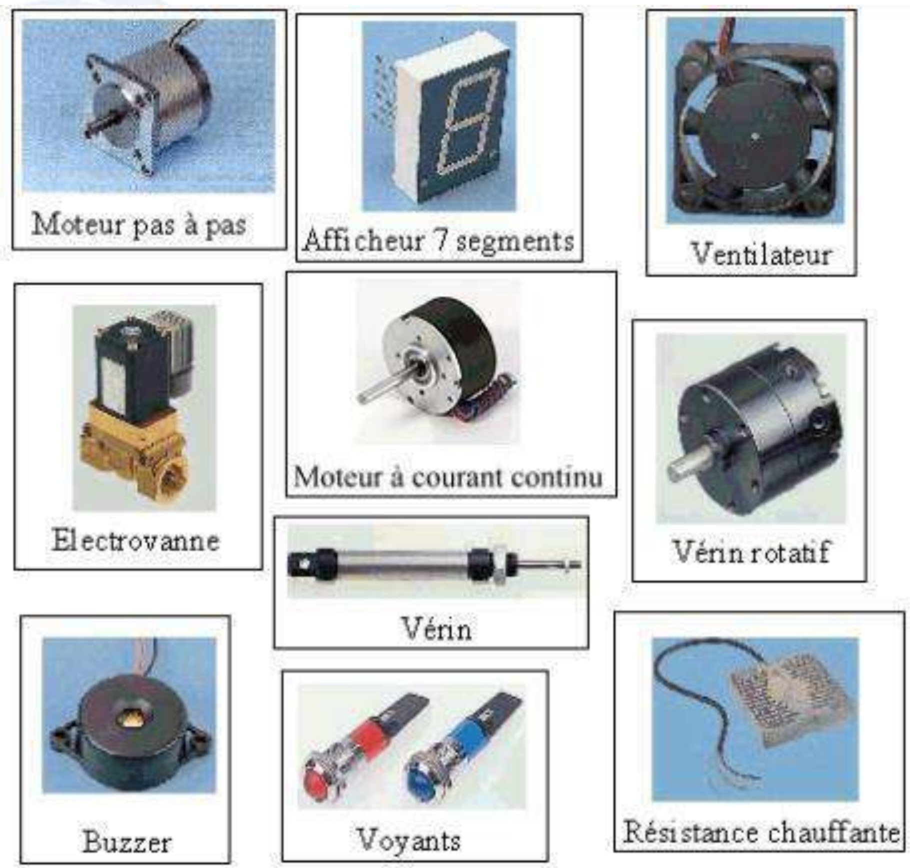
Health sensors

Smart phone sensors



Level 1: Sensor/Actuator

- **Actuator:** a technology complementary to sensors, converts electrical energy into movement or mechanical energy.
- Actuators enable the transformation of the energy received into a physical phenomenon (movement, emission of light, etc.).
- Example: Loudspeakers that convert the electrical signals into wave (acoustic) sounds.



Level 1: Sensor/Actuator

- Actuators, which induce movement, can be classified into 3 categories:
  - **Hydraulic actuators** facilitate mechanical movement by using fluid or hydraulic power.
  - **Pneumatic actuators** use the pressure of compressed air; and
  - **Electric actuators** use electrical energy.

Level 1: Sensor/Actuator

- A microcontroller (µc or MCU) is an integrated and compact circuit that includes a processor, memory, and input and output devices on a single chip.
- The MCU processes the raw data captured by the sensors and extract useful information.

Level 1: Sensor/Actuator

- Examples of microcontrollers

Arduino

- Basé sur un µc Atmega (Single core, 16MHz)
- Connexion simple
- Programmation facile
- Bon choix pour les capteurs

STM32

- Basé sur un µc ARM 32 bits (24-400MHz)
- Bon choix pour les capteurs
- Bon choix pour le traitement local

NodeMCU

- Basé sur le µc ESP8266 (Single core, 80MHz)
- Programmation facile
- Intègre WiFi

Pycom Lopy4

- Basé sur le µc ESP32(Dual core, 160-180MHZ)
- Programmation facile
- Connectivité : WiFi, Bluetooth, Sigfox, LoRa

Source: https://fr.rs-online.com/web/generalDisplay.html?id=i/ido-internet-des-objets

Level 2: Gateway

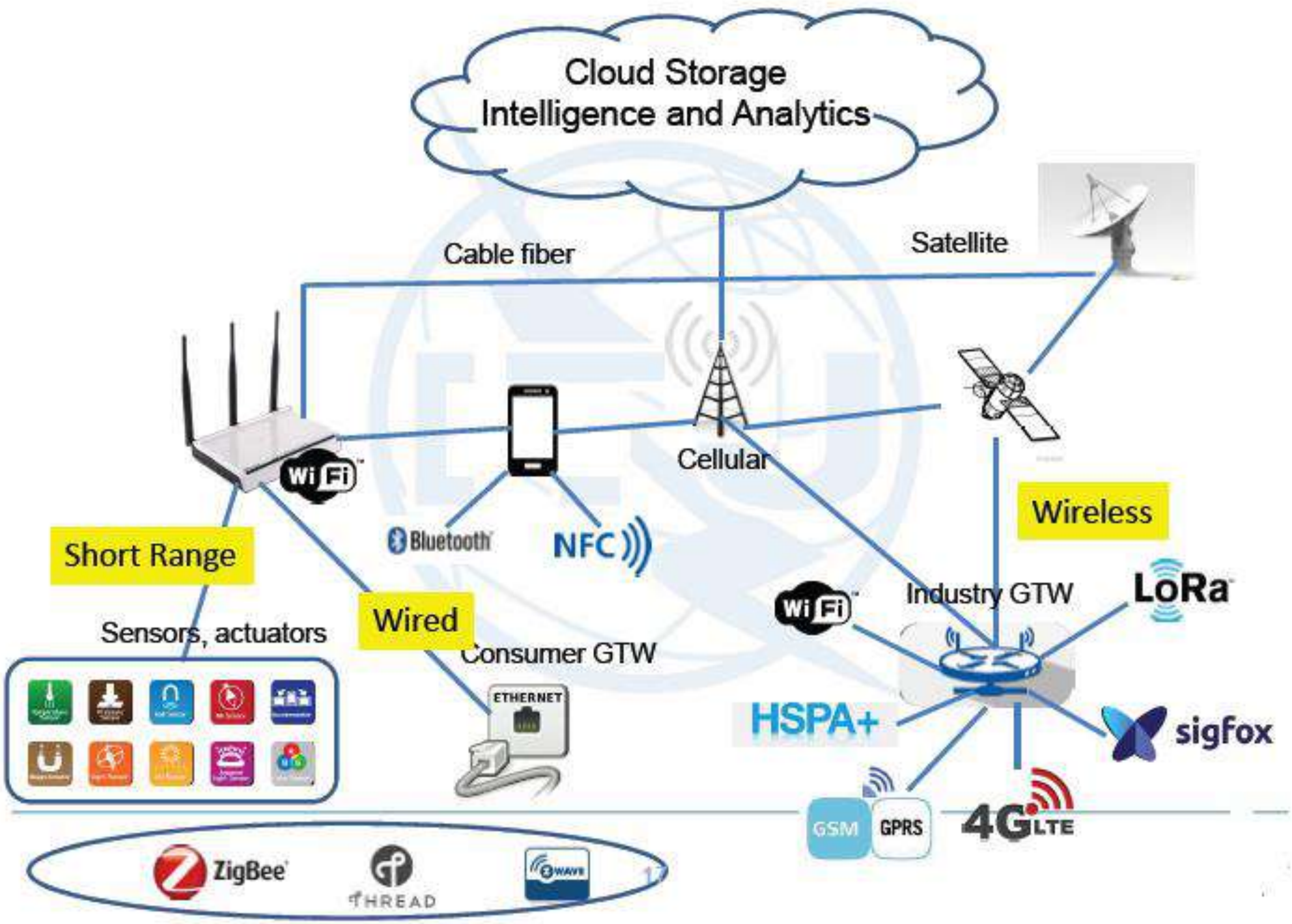
- **A gateway** is a combination of hardware and software components used to connect one network to another.
- Gateways are used to connect sensors or sensor nodes to Internet.
- Gateways are used for data communication by collecting measurements made by sensor nodes and transmitting them to Internet.
- The gateway can perform local processing on the data before relaying them to the Cloud.
- Examples of gateways:

Raspberry Pi

Intel Galileo

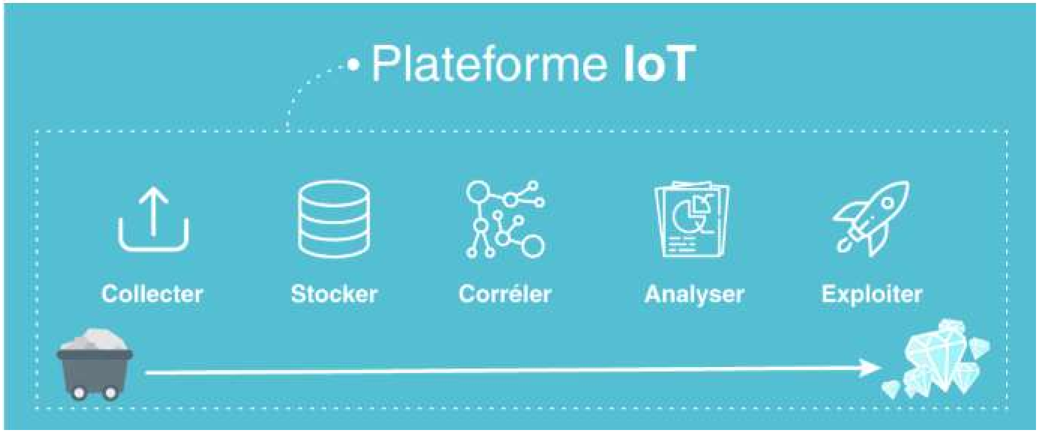
Beaglebone Black

Level 3: Network infrastrucutre



Level 4: IoT Platforms

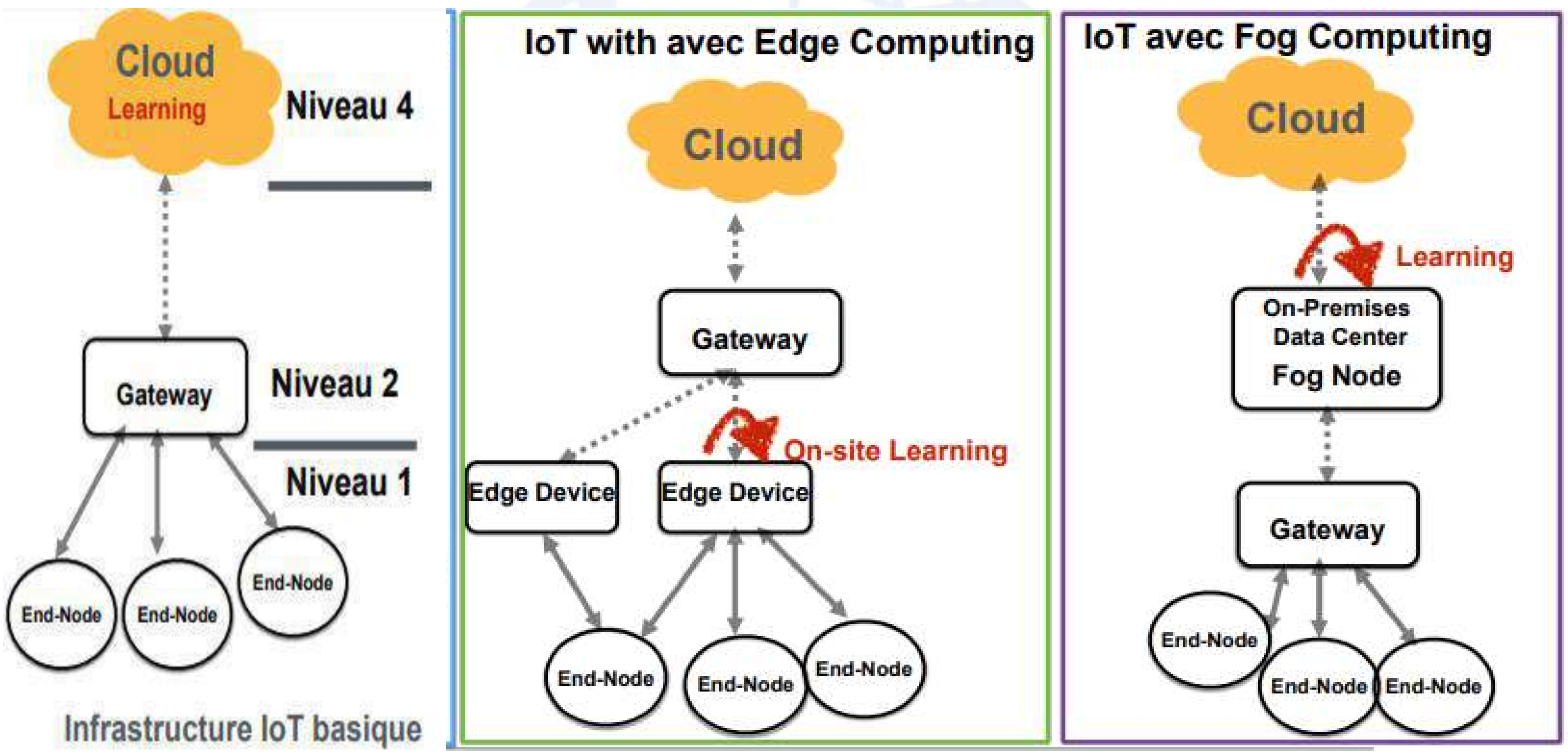
- An IoT platform is a set of services which enables collection, storage, correlation, analysis and exploitation of data.



Level 4 : IoT platforms

- **Cloud computing** refers to storing and retrieving any type of data over the internet. It is a pinnacle of **the IoT platforms evolution**
- 02 Solutions are possible for the implementation of cloud platforms :
  - **Edge Computing:** IoT data processing is done at the end of the network closer to the source of data generation (gateways or intermediate nodes between objects and gateways (Edge device)).
  - **Fog Computing:** allows decentralized computing in between core network core and edge network for data processing to serve the immediate requirements of the end systems.

Cloud Versus Fog Versus Edge



Edge Computing

Benefits of the Edge Architecture

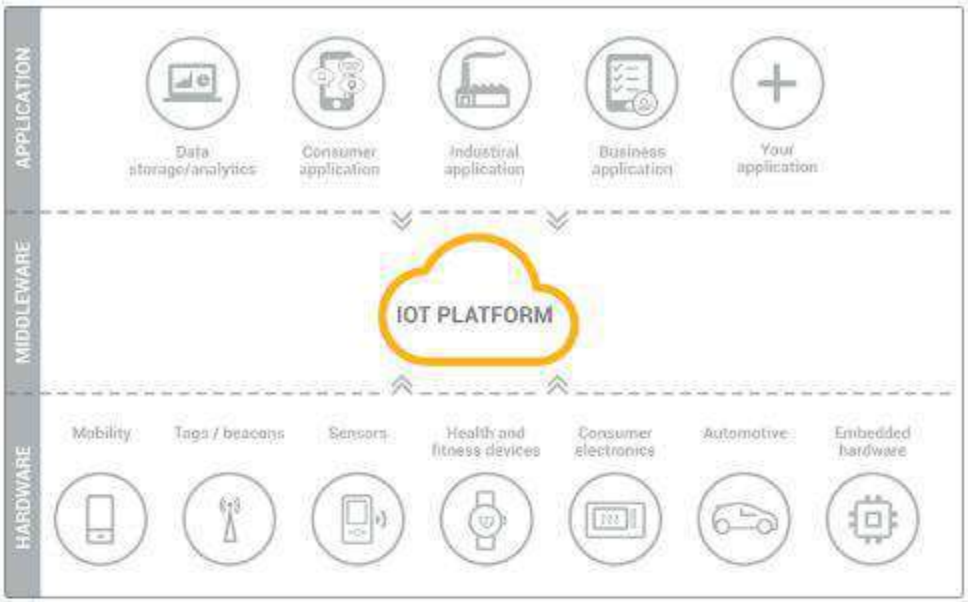
- Reduce the latency times resulting from sending data to the cloud;
- Reduce use of bandwidth, thus saving money and avoiding bottlenecks;
- Rapid analysis and/or fast action *(intelligence shifting to the edge, including real-time decisions)*
- help strengthen security through encryption at the source before relaying data to the cloud.

Level 4 : IoT Platforms

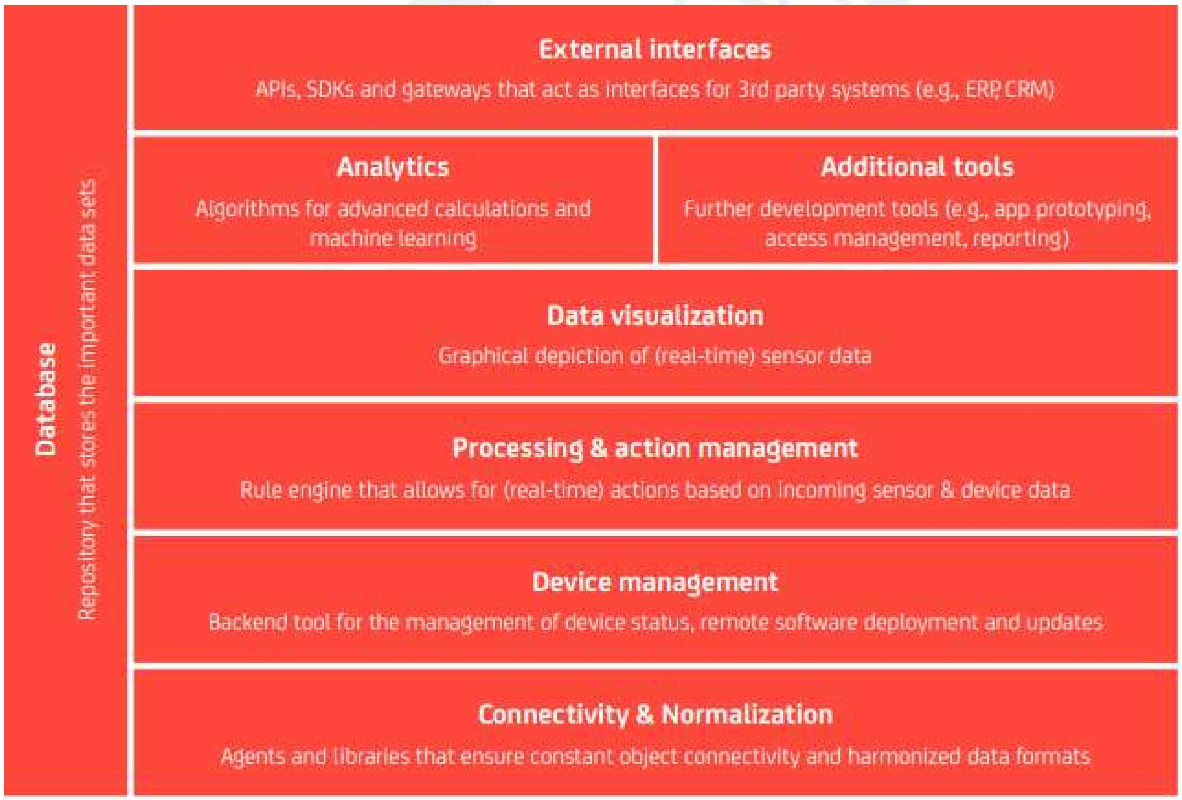
- 3 types of platforms exists:
  - Platforms as a middelware
  - Technological platforms
  - Segment-focused platforms

IoT Platform as a middleware

- IoT platform as a middleware functions as a mediator between the hardware and application layers. Its primary tasks included data collection from the devices over different protocols and network topologies, remote device configuration and control, device management, and firmware updates.



Technological platform



Source : https://iot-analytics.com/product/iot-platforms-white-paper/

Technological platform components

Connectivity and standardisation:

- Provides different protocols and different data formats in a single "software" interface.
- Advanced IoT devices generally provide an API to implement a standardized communication interface with the Platform.
- Very often, software agents must be developed and installed on the hardware in order to allow the IoT platform to establish a stable connection.

Technological platform components

Device management module

- This module ensures that connected objects function correctly and the software and applications are updated.
- Tasks performed in this module include:
  - Device provisioning
  - Remote configuration
  - Management of firmware/software updates, and
  - Troubleshooting.
- The automation of these tasks becomes essential to control costs and reduce manual labor.

Technological platform components

Data storage

- Managing data from different IoT devices brings database requirements to a new level:
  - **Volume.** The amount of data to be stored can be massive.
  - **Variety.** Different devices and different types of sensors produce very different forms of data (structured, unstructured).
  - **Speed.** Many IoT cases require the analysis of data flows to make instant decisions.
  - **Veracity.** In some cases, the sensors produce ambiguous and inaccurate data.

→ **An IoT platform usually comes with a cloud-based database solution.**

Technological platform components

Management of actions and processing

- The data captured by the connectivity and standardization module and stored in the database, comes to life in this module.
- The event-action trigger uses rule-based methods (in the form of IF x THEN y) to enables “smart” actions based on specific sensor data.
  - For example, In a smart home, an action-event trigger can set all lights off when someone leaves the house.
- The technical achievement often comes in the form of an If-this-then-that rule : If the GPS signal indicates that Jason's smart phone is more than 5 m from his house, then turn off all lights. in his house.

Technological platform components

Analytics

- Many IoT use cases go beyond rule-based methods and require complex analytics to get full benefits of IoT data.
- Machine learning methods support the analysis of sensor data, from basic data clustering to deep machine learning.
- In a smart home, for example, machine learning algorithms allow the IoT platform to know which combination of lighting and heating is preferred by the user and at what time of day, taking into account the outdoor weather conditions.

IoT platform components

Visualisation

- The visualization allows users to see patterns and observe trends. It is displayed in different forms, bar or pie charts, 2D or even 3D models.

- The visualization of dashboards is often included in the prototyping tools that an advanced IoT platform provides.

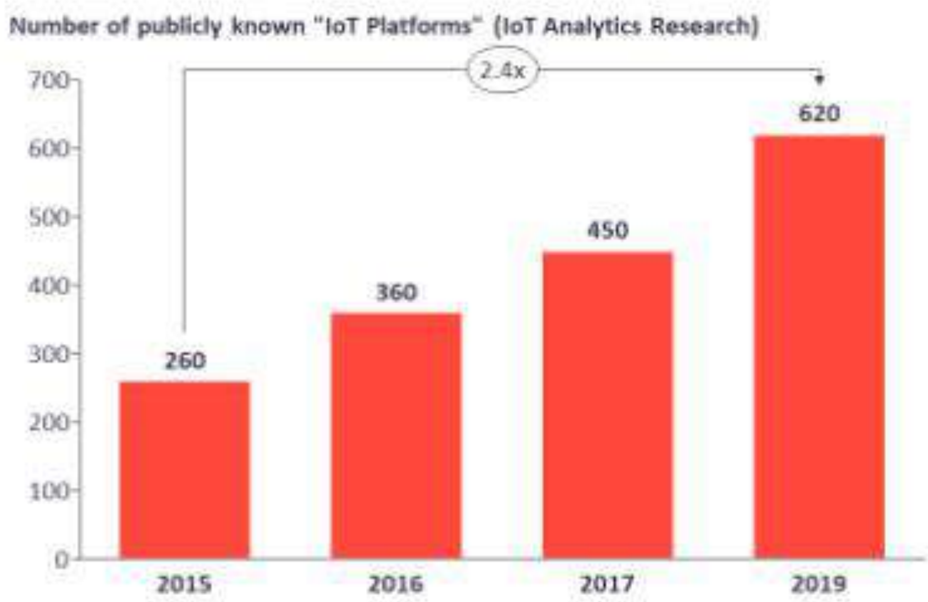
Segment-focused platforms

- **B2C platforms** use minicomputers like the Raspberry Pi or the Arduino. These platforms are often open-source and free to use in their basic version.
- **Smart Home platforms** support home connectivity standards such as WiFi, Zigbee, Z-wave, and Bluetooth. They often support predefined visual applications that allow monitoring and control of devices in the home.
- **Connected car platforms** work with automotive standards and V2V communication protocols. They give special attention to security issues because hacking this platform can cause serious problems. The platforms also integrate telematics services such as fleet management or usage-based insurance.

Segment-focused platforms

- **Smart city platforms.** Smart city use cases like smart parking or connected waste management often rely on low power networks like Wide Area Networks (LPWAN). The platforms are also optimized to work with mapping services (eg, Google maps) and local street information.
- **Industrial IoT platforms** provide special gateways to integrate into SCADA and the automation of existing systems. Strong security is a major concern for companies who fear revealing sensitive data to customers or competitors unintentionally.
- **Other specialized platforms** can be found in segments like smart agriculture, connected health or smart grid.

IoT Platforms Market (2015-2019)



Source: IoT Platforms competitive Landscape & database 2020

IoT Platforms Market (2015-2019)

- 620 IoT platform providers in 2019, compared to 450 in 2017.
- The market is concentrated around a few providers: the top 10 providers held 58% of the market share in 2019, compared to 44% for the top 10 in 2016.
- Industry/manufacturing is the # 1 vertical: 50% of platforms focus on it.

Main IoT platforms

- ThingWorx Industrial
- Microsoft Azure Cloud IoT
- Amazon Web Services IoT
- IBM Watson
- Google Cloud IoT
- Oracle Integrated Cloud for IoT
- SAP Cloud Platform for IoT
- Cisco Jasper Control Center
- GE Predix
- Cisco IoT Cloud

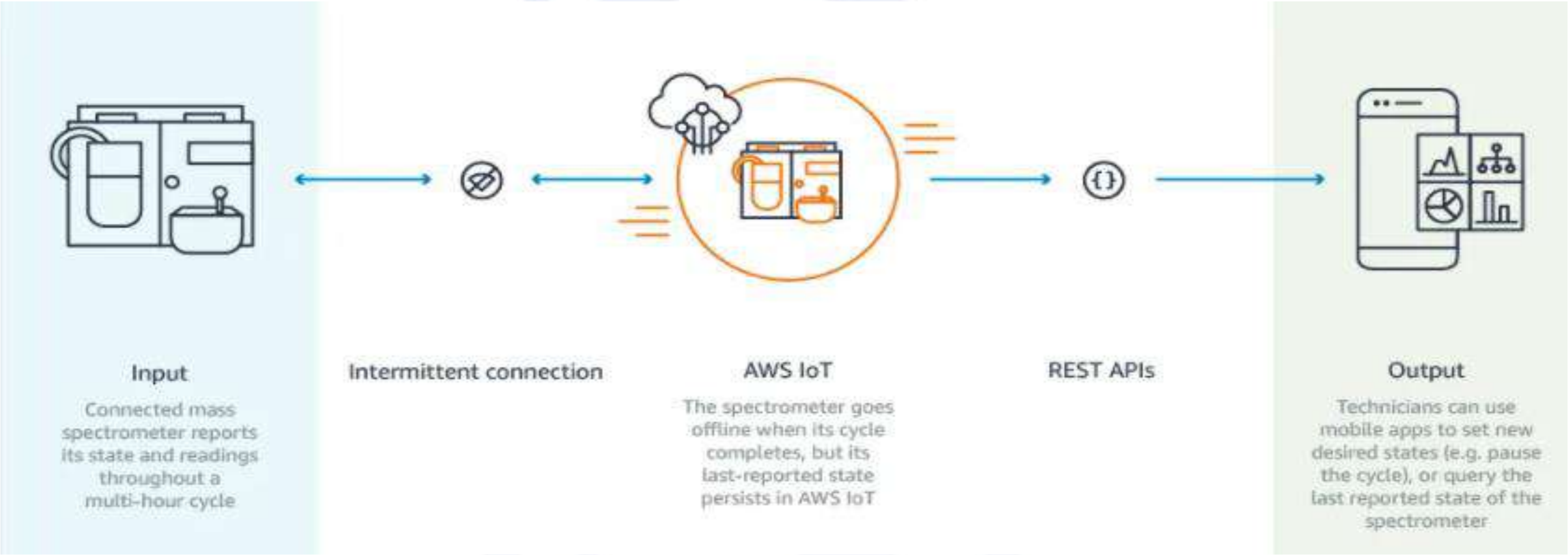
GE Predix Platform

- Predix was designed to target factories. It can directly analyze data from the machine and store. This platform is secure and scalable.
- **Main features:** Provides key performance data; Reduces unplanned downtime; Real-time operational data.

Microsoft Azure IoT Suite

- Microsoft Azure provides multiple services to create IoT solutions. This provides the solutions for a small PoC to Rolling out your ideas.
- **Main features:** Rich Integration with SAP;, Salesforce, Oracle, WebSphere, etc.; Dashboards and visualization; and Real-time streaming.

Amazon AWS Platform



- AWS platform helps developers collect and send data and analyze that information to provide the ability to manage devices.
- **Main features:** Device management; Secure gateway; and Authentication and encryption, etc.

IBM Watson Platform

- IBM Watson Platform providies easy sample apps and interfaces for IoT services, they make it accessible to beginners.
- **Main features :** real-time data exchange, secure Communication, cognitive systems, recently added data sensor and weather data service.

Comparison of IoT platforms

	General Electric (GE)	Microsoft	Amazon	IBM
Platform Name	Predix	IoT Hub	AWS IoT	IBM Watson IoT
Deployment Models	Public, Private, On-Premise	Public	Public	Public
Pricing Models	Subscription, Pay-as-you-go (tiers) # of Services + usage	Subscription – different tiers based on total messages exchanged	Usage-based – messages published and delivered. (messages delivered to other AWS services are free)	Usage-based – Data exchange and analyzed
PaaS Platform	Cloud Foundry	Azure	AWS	IBM Bluemix, Cloud Foundry
Market Place	Extensive	Extensive	Extensive	Extensive
SDK / Languages	Yes	.NET, and UWP, Java, C, NodeJS	C, NodeJS	C#, C, Python, Java, NodeJS
API / API Libraries / Management	Yes	Yes (Extensive, Open)	Yes (Extensive, Open)	Yes
Ingestion Layer	Yes	Yes	Yes	Yes
Identity and Access Management	Yes	Yes	Yes	Yes
Workflow	Yes	Yes	Yes	Yes
Events Processing	Yes	Yes	Yes	Yes
Rules Engine	Yes	Yes	Yes	Yes
Audit	Yes	Yes	Yes	Yes

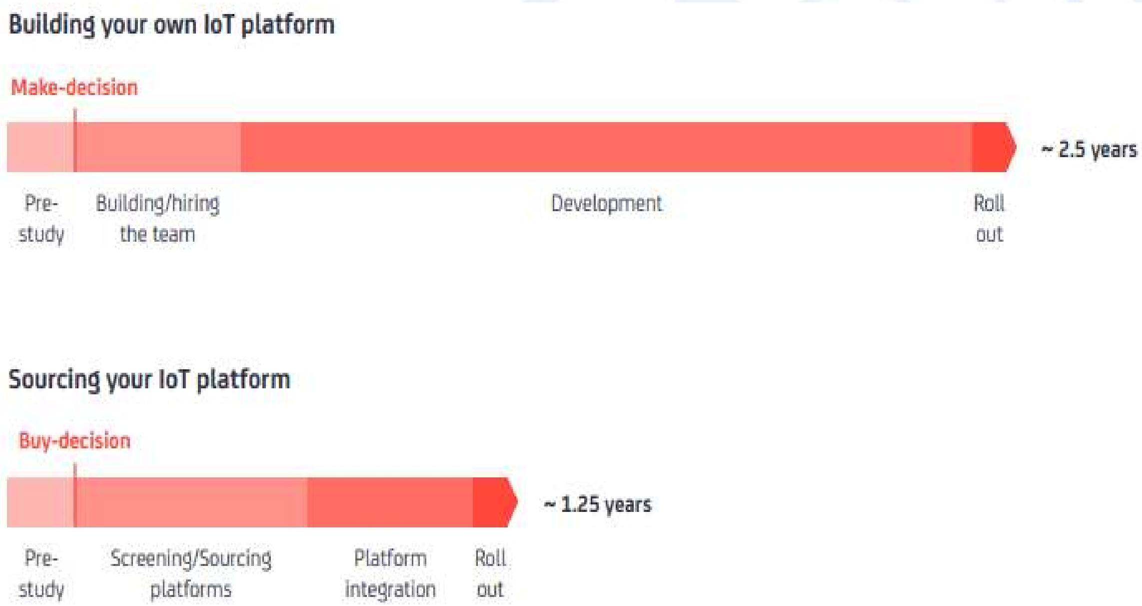
Comparison of IoT platforms

	General Electric (GE)	Microsoft	Amazon	IBM
Platform Name	Predix	IoT Hub	AWS IoT	IBM Watson IoT
CRM / ERP Integration	Manual	Manual	Manual	Manual
Field Service Integrations	ServiceMax	Manual/Partners	Manual/Partners	Manual/Partners
Visualization	Yes	Yes	Yes	Yes
Analytics - Hot Path	Yes	Yes	Yes	Yes
Analytics - Cold Path	Yes	Yes	Yes	Yes
Machine Learning	Yes	Yes/API(managed Service)	Yes	
BigData - Hadoop	Yes	Yes with HDInsight	Yes with Amazon EMR	
Notification and Alerts	Yes	Yes	Yes	
Device Lifecycle Mgmt	Yes	Yes	Yes	Yes
Device Security	Yes	X.509, TLS	X.509	TLS
Device – Device SDK	Yes	Open source SDK	Open SDK	Yes (limits - TBD?)
Device - Protocols	Yes	AMQP, MQTT, HTTP, WebSockets	MQTT, HTTP, Websockets	MQTT, HTTP
Device - Gateways	Yes	Yes	Yes	Yes
Object Storage	Yes	Yes	Yes	Yes

Proprietary platforms versus open source platforms

- 02 types of platforms can be distinguished:
  - **Proprietary platforms** allow the sharing of responsibilities, because the service provider will be responsible for the operational maintenance of all environments.
  - **Open source platforms** require more time and expertise, as they require the development of all services, maintenance of tools, infrastructure and applications.

Which platform to choose?



What you must remember:

- Building your own IoT platform significantly extends project duration
- Internal expertise is scarce and expensive.
- IoT projects are complex - even with an outsourced platform.

Quizz n°3

What are the offers of platform and which dominates the market?

Part 4:
IoT value chain, connectivity and business models

IoT value chain

Devices

- Sensors
- Embedded Chips
- MEMS
- Actuators
- Modules
- SIM Card
- System Design
- Firmware& Drivers
- Interoperability

Connectivity

- Network Equipment
- Connectivity
- Network Service Provider
- Protocols
- Device Provisioning & Configuring

Platform/ Enablement

- IoT Platforms
- Cloud
- Analytics
- Middleware
- Integration with third-party applications
- Testing
- API Development
- Billing

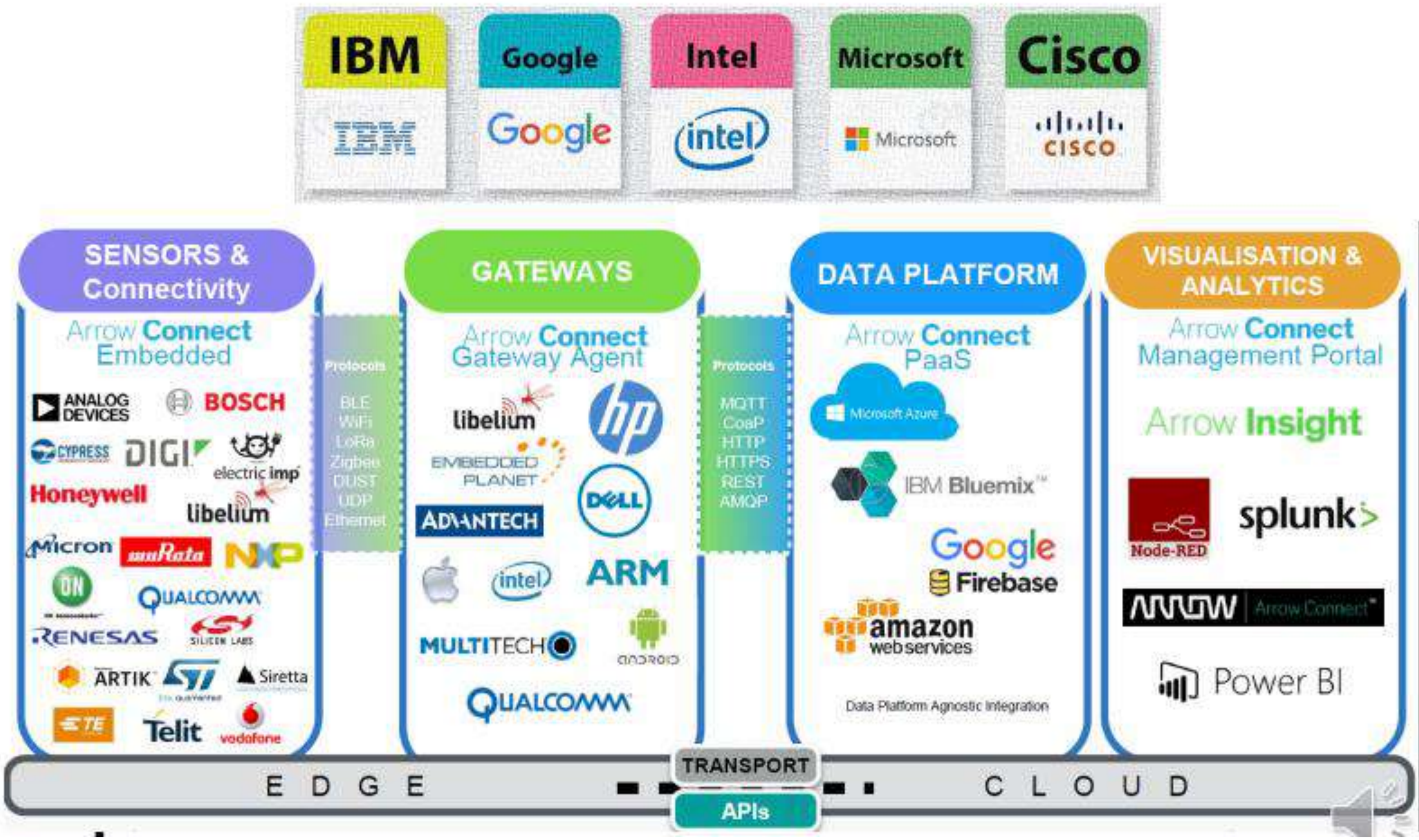
Applications

- Applications Development
- UI/UX Design
- Building Vertical Solutions
- Bundling of Services
- API Development & Management

Managed Services

- Applications Management
- Server Management
- Network Management
- Remote Monitoring
- CRM & Billing
- Customer Care
- Tech Support

Players in IoT ecosystem



Manufacturers of chipsets and modules

- The manufacturers of chipsets and modules produce the sensors and electronic transmitters which, when assembled, will make up the connected objects.
- Examples of manufacturers of electronic chipsets and modules:
  - Texas Instrument,
  - Semtech
  - Silicon Labs
  - Qualcomm
  - Sequans Communications,
  - etc.

Source : https://www.postscapes.com/iot-chips-modules/

Manufacturers of connected objects

- The manufacturer of connected objects refers to the manufacturer of the product. Its mission is to assemble all the components : sensors, chips, modules, antennas, etc. to best meet needs.
- The strategy of object manufacturers is based on:
  - an increase in turnover in the short term, and
  - an improvement in their margin, particularly around **the sale of services**, which is generally more **profitable than the sale of products**.

Servitization strategy

- with increasingly affordable IoT sensors, increasingly reliable connectivity, and increasingly capable IoT software platforms, **“servitization”** are becoming part of the manufacturing strategy in the supply chain, insurance, healthcare, and beyond.

What is servitization?

- The basic idea of servitization is that manufacturers move from a model based on selling assets toward a model in which they offer a service that utilizes those assets.
- **Example: security at home.**
  - **without** servitization: a company selling alarm devices for the house.
  - **with** servitization: a company selling a monthly subscription for a "security solution" (from intrusion detection to intervention), enabled by alarm devices.

Servitization strategy

- The strategy of "**servitization**" of objects offers manufacturers an opportunity to:
  - Generate additional income from services.
  - Allows customers to only pay for what they use.
  - Shifts money from capex to opex.
  - Creates opportunities to build closer relationships between supplier and customer. The connected object should therefore be considered a good tool for customer relationship management and customer loyalty.

Manufacturers of connected objects

- Connected objects are frequently manufactured by startups, but also by subsidiaries of large groups.
- The positioning of new entrants varies according to the sector:
  – they opt for markets where adoption is generally strongest, such as security, energy management or home automation;
  – they avoid markets that require very specific business expertise; and
  – they choose uncompetitive markets.

Manufacturers of connected objects

- Historic manufacturers focus primarily on the sale of objects and move very cautiously on services.
- The new entrants are focusing their strategy primarily on the sale of objects, mobilizing their sales teams on B2B2C distribution to sell larger volumes.
- In the same vein, they usually open free access to their APIs in order to allow third parties to offer services around their objects, to promote adoption and consequently increase the new revenues resulting from them.

Connectivity providers

- Connectivity providers generally refer to telecom operators. They intervene in the IoT market to offer connectivity solutions to objects.
- Some of these players are positioned in different segments:
  - **Service providers** (sometimes end-to-end solutions including the object): They play a more active role in the connected home as they offer a single box solution, with the aim of increasing the monthly bill of their subscribers while maintaining a lowest churn rate.
  - **Connectivity providers:** Their role remains mainly indirect, since a large part of the objects are connected via Wifi / Bluetooth.
  - **Distributors:** They are also present in the distribution of these objects (sport and well-being in particular), in particular smart watch, considered as the second screen of the smartphone.

IoT platform providers

- Platform provider provides the technical tools to collect the data emitted by the objects, process them, and develop business applications and services.
- Platform providers remain few in number (around 640 platforms in 2019).
- It is difficult for them to position themselves in sectors where **object manufacturers propose an end-to-end** (or vertical) approach, **while they provide a horizontal approach** (independent of the object manufacturer).

Dominance of GAFA

- It appears very legitimate to see GAFA positioning themselves in this segment since they benefit from the maturity of their technological solutions.
- Some of them have locked down the home automation, e-health and connected car market:
  - Home automation: Google, Microsoft
  - E-health: Apple, Google
  - Autonomous car: Google, Apple

Dominance of GAFA

- The proliferation of startups, bought by big firms, like the recent acquisition of Withings by Nokia in April 2016, for 170 million US dollars, is a constant in the IoT.

Entreprise	Achetée par	Produit	Sous-secteur
Beats electronic	Apple	Audio grand public	Divertissement
LinX	Apple	Caméra	Tous
Coherent Navigation	Apple	Cartographie	Transports
AuthenTec	Apple	Biométrie	Sécurité
Didi Chuxing	Apple	VTC*	Transports
Revolv	Google	Domotique	Domotique
Lift Labs	Google	Suivi de santé	Santé
Drop Cam	Google	Caméra	Domotique
Sybox Imaging	Google	Cartographie	Transports
Nest Labs	Google	Domotique	Domotique
Oculus VR	Facebook	Réalité virtuelle	Tous
Face.com	Facebook	Reconnaissance faciale	Sécurité
Mobile Data Labs	Microsoft	Cartographie	Transports
N-Trig	Microsoft	Stylo connecté	Tous
Nokia	Microsoft	Terminaux	Tous
Id8 Groups	Microsoft	Domotique	Domotique
Perceptive Pixels	Microsoft	Capteurs	Tous

*Véhicules de transport avec chauffeur. Réalisation : Nicolas Mazzucchi.

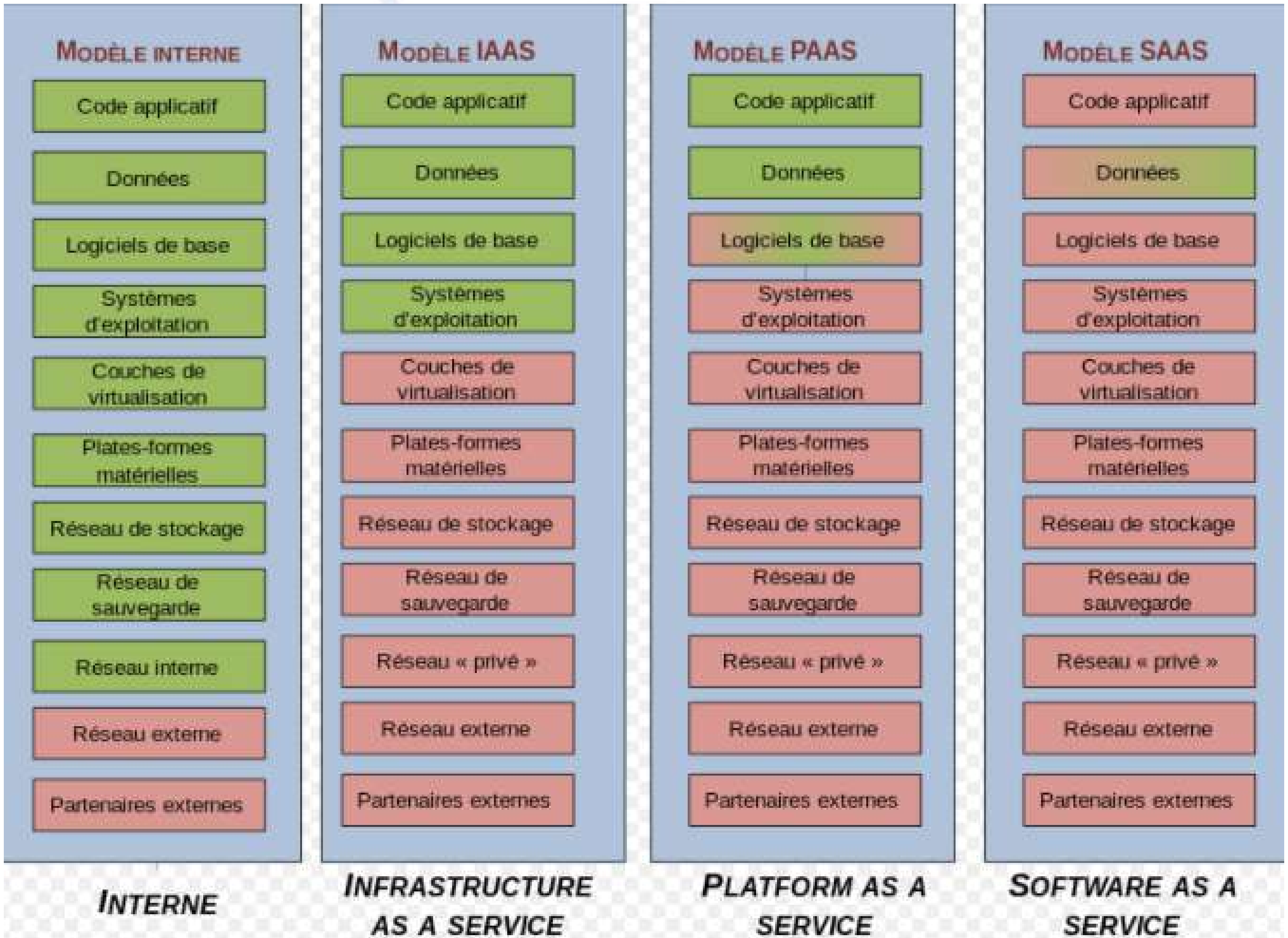
Source : https://www.futuribles.com/fr/groupes/iot-2025/document/vers-une-industrie-integralement-40-2/

Platform providers offers

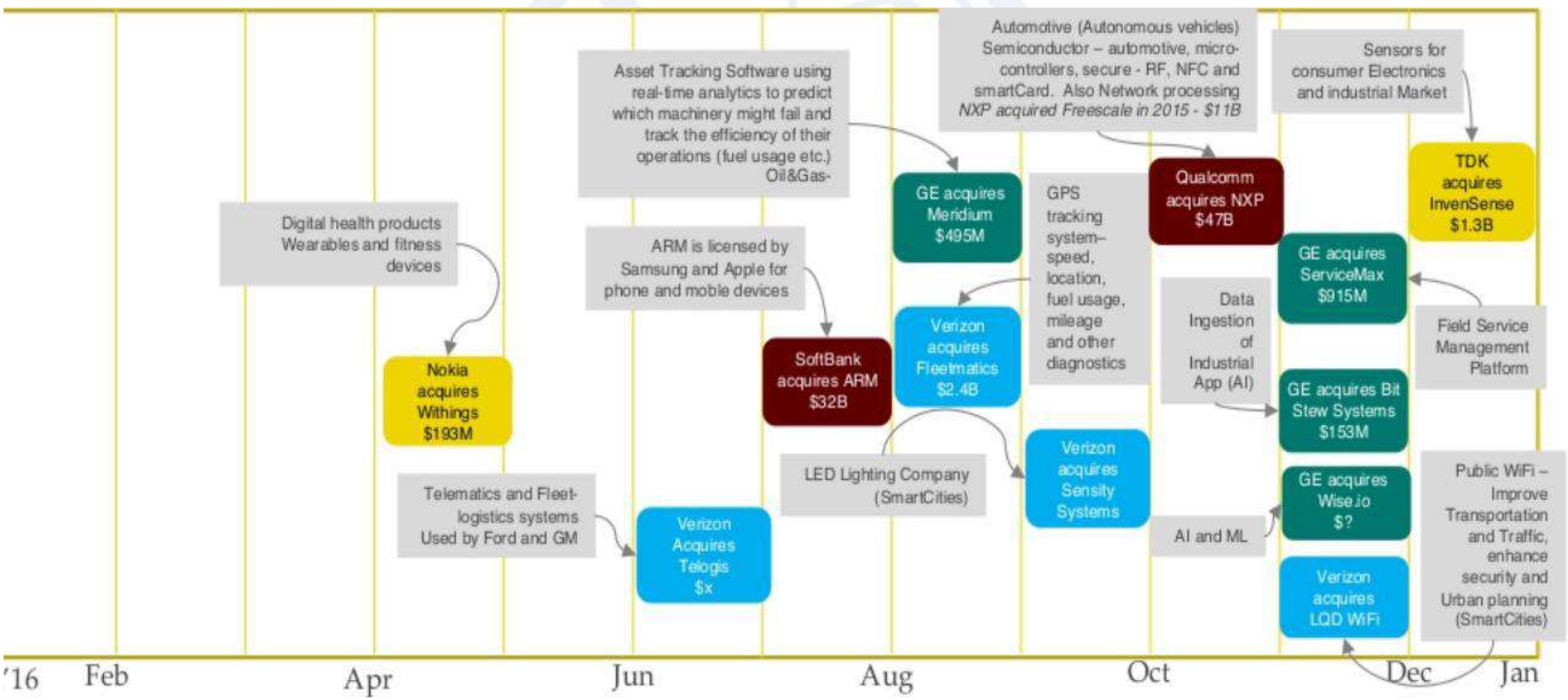
- **3 types of offers are proposed by platform providers:**
  - **Software as a Service (IaaS):** In SaaS, the applications is stored in the cloud and the offer is made in service mode. Whenever a user wants to use the application services, he/she can access to services via a web browser.

    Examples: Salesforce, Google Apps, Citrix GoToMeeting, and Cisco WebEx.
  - **Plateforme as a Service (PaaS):** the cloud providers provide everything to build cloud applications (software, operating system, databases, etc). PaaS offer eliminate the need for buying various software, hardware, hosting. Examples: Microsoft Windows Azure, Force.com and Google App Engine.
  - **Infrastructure as a Service (IaaS):** the cloud providers provide all the infrastructure the user need to build cloud applications. In IaaS mode, the user get services like servers, storage, and data centers to store their applications.

IaaS Versus PaaS versus SaaS



Main buybacks in 2016



Business or service providers

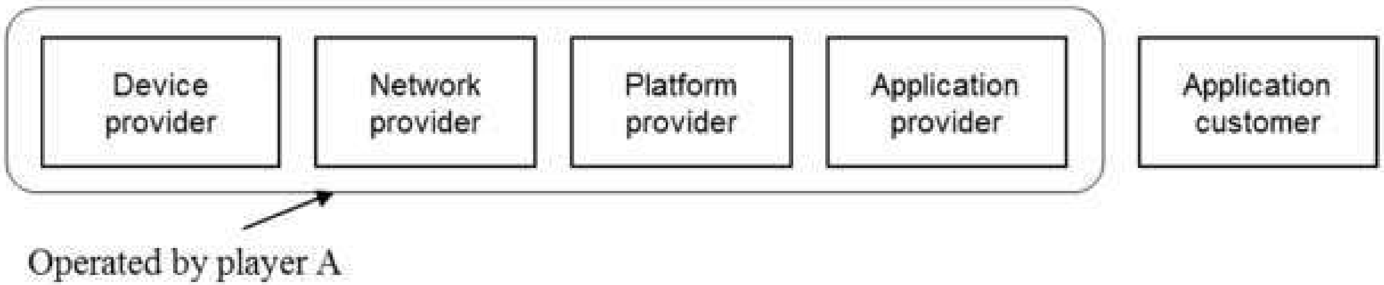
- The service provider delivers the value-added services that take advantage of the data generated by the objects.
  - Examples: Sports or slimming training services or security services.
- The service providers are predominantly the manufacturers themselves given their end-to-end approach.
- Many young start-ups also use data for specific purposes.

Activities model

- Actors in the IoT ecosystem can have a variety of relationships in actual deployments. The diversity of these relationships is presented by business models

UIT Recommandation 2060

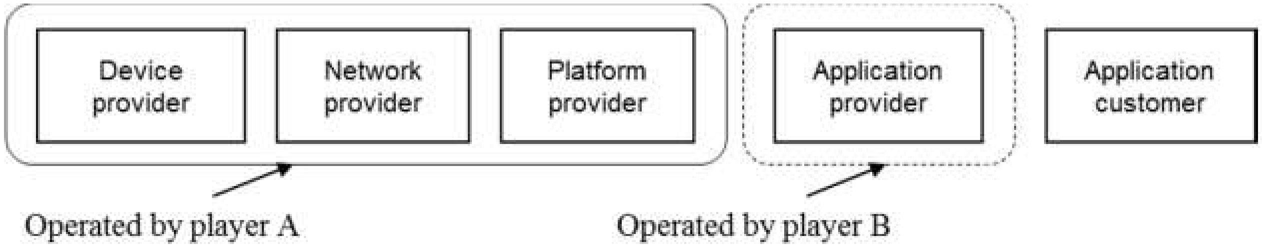
Model 1



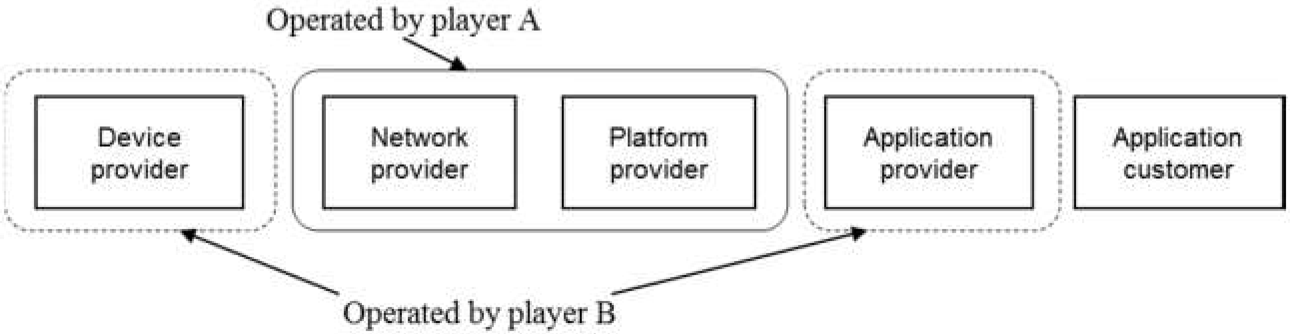
Example : **In general, telecom operators and some vertically integrated businesses (such as smart grid and intelligent transport systems (ITS) businesses) act as player A in model.**

Activities model

Model 2 :

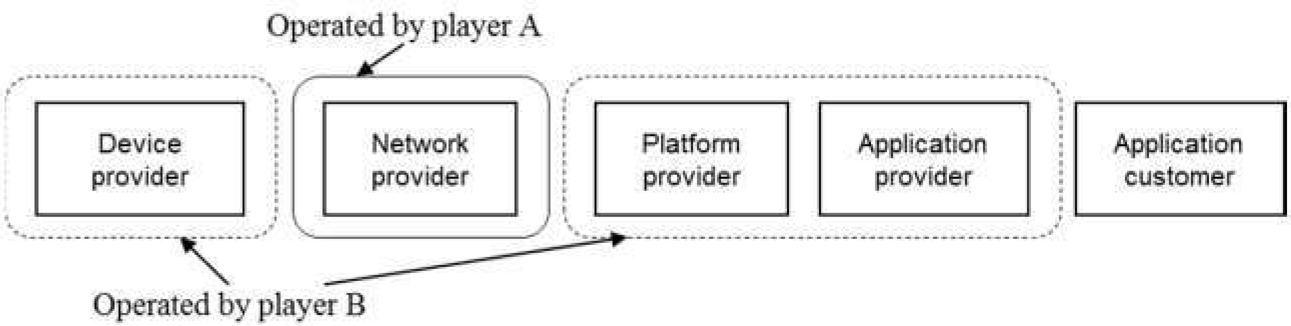


Model 3 :

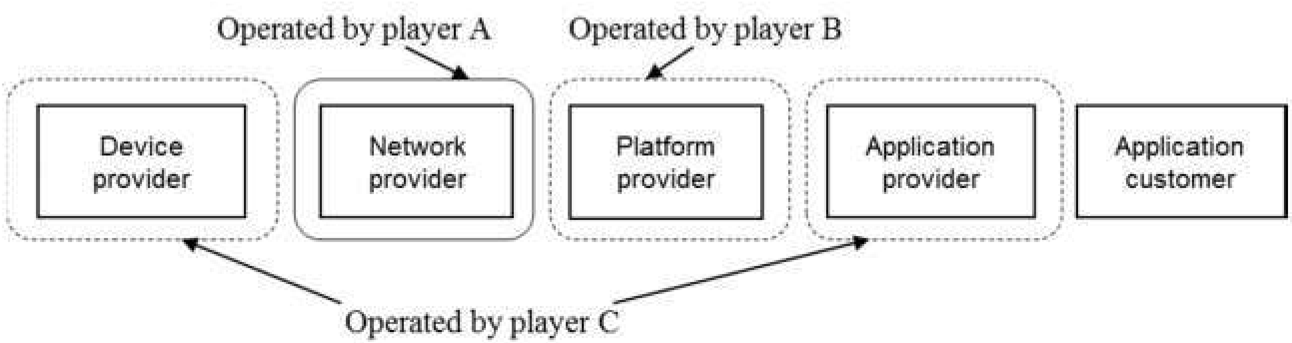


Activities model

Model 4 :



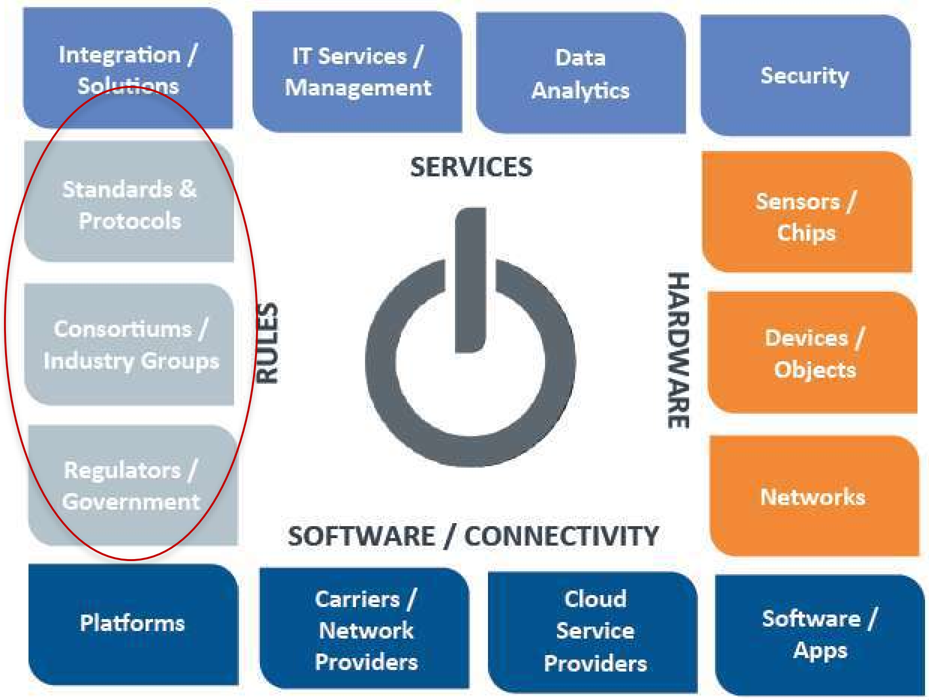
Model 5 :



Quizz N°4

What is the most used business by startups?

Other players in the IoT ecosystem



Thank you!

Structure et standards

Working Group	Reference and title	Scope	Status
WG 3 - IoT Architecture: standardization in the area of IoT vocabulary, architecture, and frameworks	ISO/IEC 20924, Definitions and vocabulary	This draft provides a definition of IoT along with a set of terms and definitions. It represents a terminology foundation for the IoT.	Under development
	ISO/IEC 30141, Internet of Things Reference Architecture (IoT-RA)	This draft specifies general IoT reference architecture defining system characteristics, a conceptual model, a reference model and architecture views of IoT.	Under development
	Technical Report (TR) on IoT Edge Computing	This draft provides basic concepts of IoT edge computing architecture, terminologies, values, characteristics, challenges, use cases and main technologies (including data management, coordination, processing, network functionality, heterogeneous computing, security, hardware / software optimization) of edge computing for IoT systems applications. It is also considered to assist in the identification of potential areas for standardization in edge computing for IoT.	Under development
	ISO/IEC 30147, Methodology for trustworthiness of IoT system / service	This draft provides a methodology to implement and maintain trustworthiness in IoT system/service. The methodology is not targeted to a certain application area of the IoT system/service but for a generic IoT system/ service common to various application areas.	Under development

Structure et standards

WG 4 - IoT Interoperability: standardization in the area of IoT interoperability, connectivity, conformance and testing.	ISO/IEC 21823-1, Interoperability for Internet of Things Systems - Part 1: Framework	This draft provides an overview of interoperability requirements and a framework for interoperability for IoT systems. It aims to enable IoT systems to be built in such a way that all the entities of the IoT ecosystem are able to exchange information and mutually use the information in an efficient way. The goal of this draft is to ensure that all parties involved in developing and using IoT systems have a common understanding of interoperability as it applies within and out of the various entities.	Under development
	ISO/IEC 21823-2, Interoperability for Internet of Things Systems - Part 2: Transport interoperability	This draft presents a conceptual model for network connection interoperability and requirements for interoperable IoT systems to enable information exchange, peer-to-peer connectivity and seamless communication within and out of the IoT systems.	Under development
	ISO/IEC 21823-3, Interoperability for Internet of Things Systems - Part 3: Semantic interoperability	This draft provides a basic concept of semantic interoperability for IoT systems, as described in the facet model of ISO 21823 Part 1. It also describes technologies supporting for semantic interoperability of IoT systems.	Under development

Structure et standards

WG 5 - IoT applications: standardization in the area of IoT applications, platforms, use cases, middleware, tools and implementation guidance.	ISO/IEC TR 22417:2017, IoT use cases	This TR is dedicated to identify IoT scenarios and use cases based on real-world applications and requirements as well as identification of potential areas of standardization to ensure easy operation and interoperability within and out of the IoT ecosystem. It comprises 25 use cases of the IoT applications.	Published

Commissions d'études et objectifs

Study Group	Objective
SG 7 - Wearables	This SG is to study market requirements of smart wearable devices, analyze the current standardization and research activities in this field, and identify standardization gaps.
SG 8 - Trustworthiness	This SG is responsible to propose a definition of trustworthiness. In addition, it is also responsible for investigating related standards and guidelines as well as to identify standardization gaps in the areas of security, privacy, safety, resilience and reliability.
SG 9 - Industrial IoT	This SG is responsible for analyzing market requirements and current standardization activities in the area of IIoT. One of the mission among other of this SG is to perform a comparison of reference architectures and models in the context of IIoT in order to avoid double works in future standardization developments.
SG 11 - Real-Time IoT	This SG is to provide an analysis of market requirements and a status of current standardization activities on real-time IoT. It will identify possible new projects within the area of SC 41.
SG 12 - Aspects of IoT Use Cases including Classification and Verification	The objective of this SG is to build a classification of use cases based on IoT scenarios identified in ISO/IEC TR 22417:2017 - IoT use cases. One of the objective among other of this SG is to propose an improved template for use case presentation as a part of the ISO/IEC 30141 - Reference Architecture.
SG 13 - Reference Architecture and Vocabulary	This SG is responsible for reviewing and analyzing a catalogue of reference architectures and assorted vocabulary, created by JTC 1/SC 41.

Alliances IoT

- AIOTI
- OneM2M
- AllSeen
- Fondation Eclipse
- Consortium Internet industriel (IIC)
- Protocole Internet des objets intelligents (alliance IPSO)
- IoT alliance
- Oasis
- Open Interconnect Consortium (OIC)
- Thread Group
- Alliance ZigBee

Organisations internationales de standardisation

- L'Union Internationale des Télécommunications (UIT) élabore des lignes directrices qui serviraient de référence commune aux autres organisations de standardisation.
- L'Institut des Ingénieurs Electriciens et Electroniciens (IEEE) travaille sur la standardisation des réseaux de communication, des applications sectorielles (smart grid, industrie, agriculture et secteur minier).
- L'Internet Engineering Task Force (IETF) élabore des standards pour les systèmes de communication, notamment pour l'IPv6.

Organisations internationales de standardisations

- OASIS (*Organization for the Advancement of Structured Information Standards*) est un consortium sans but lucratif qui oriente les développements et l'adoption de standards ouverts pour la société de l'information. Les travaux de ce consortium sur l'internet des objets portent sur les technologies de réseau et de messagerie normalisées.
- 3GPP regroupe des organisations de normalisations télécoms produisant des spécifications pour la communication cellulaire par le biais de NarrowBand IoT (NBIoT)

PRIDA Track 1 (T1)

IoT Regulations

08/09/2020

Agenda

- Part 1: IoT Security
- Part 2: Privacy and liability
- Part 3: Standards and Code of practices, certification, and regulation

Introduction

- The number of connected IoT devices has grown rapidly: according to some estimates, the number of IoT devices in operation in 2020 surpassed 20bn.
- Despite the rapid growth of the devices, and the potential benefits they offer, the IoT raises significant security and privacy concerns.
- Regulators should provide legal texts to regulate IoT and protect individuals from breaches.
- Legislators still have a long way to go when it comes to the liability of connected objects or their users

Part 1: IoT Security

IoT Security issues

- IoT can serve as the basis for large-scale attacks on critical infrastructures
- Some targets:
  - National or regional power supply networks
  - Financial and trading system
  - Connected car
  - Industrial system
  - Alarm system
  - Medical equipment
  - Audio and video surveillance

Recent IoT attacks

Botnet Mirai (2016)

- This network of robots infected many IoT devices (old routers and IP cameras), then used them to saturate the DNS server of the DDOS attack).
- The Mirai botnet made part of the internet inaccessible, including some very popular sites: Twitter, Reddit, Netflix, Spotify, The New York Times, CNN, etc.

Challenges of IoT security

- The economy favors weak security
  - Competitive pressures for shorter time to market and cheaper products are pushing many IoT system manufacturers to spend less time and resources on security;
  - Strong security is expensive and it extends the time to market.
- Security is difficult
  - There are no credible means by which suppliers can communicate to consumers the security level of their products;
  - Difficult for consumers to easily understand the security of different IoT systems;
  - Reduced consumer pressure on suppliers;
  - Security is not competitive differentiator.

Challenges of IoT security

- IoT systems are complex and every part must be secure
  - The implementation of enhanced security in IoT systems requires expertise.
  - New players in the IoT ecosystem may have little security experience.
- Security support is not always maintained
  - IoT devices, applications and services require security patches and updates to protect against known vulnerabilities;
  - Supporting IoT system updates is a costly task for IoT service providers.
- Low consumer awareness of IoT security
  - Typically, consumers have limited knowledge of IoT security, which impacts their ability to configure and maintain the security of their IoT systems or to consider security aspects into their shopping habits.

Challenges of IoT security

- Security incidents can be difficult for users to detect or resolve
  - In many cases, the effects of a poorly secured product or services not obvious to the user.
    - Example, a refrigerator can continue to do a good job even if it has been compromised and is part of a botnet carrying out DDoS attacks.
  - Consumers also lack the technical ability, or the user interfaces, to implement the corrections.
  - Users may not know how to patch their devices.
  - Users are contractually prevented from updating or repairing the systems themselves or having them repaired by independent specialists.

Information security

- Information security brings together all the organizational, technological, human and legal means to manage risks and their impacts with regard to the availability of information and its integrity.
- Security of the IoT system can be assessed by employing classical security and risk analysis measures.
- Typical security requirements (Confidentiality, Integrity and Availability, CIA) should be employed in the IoT system.

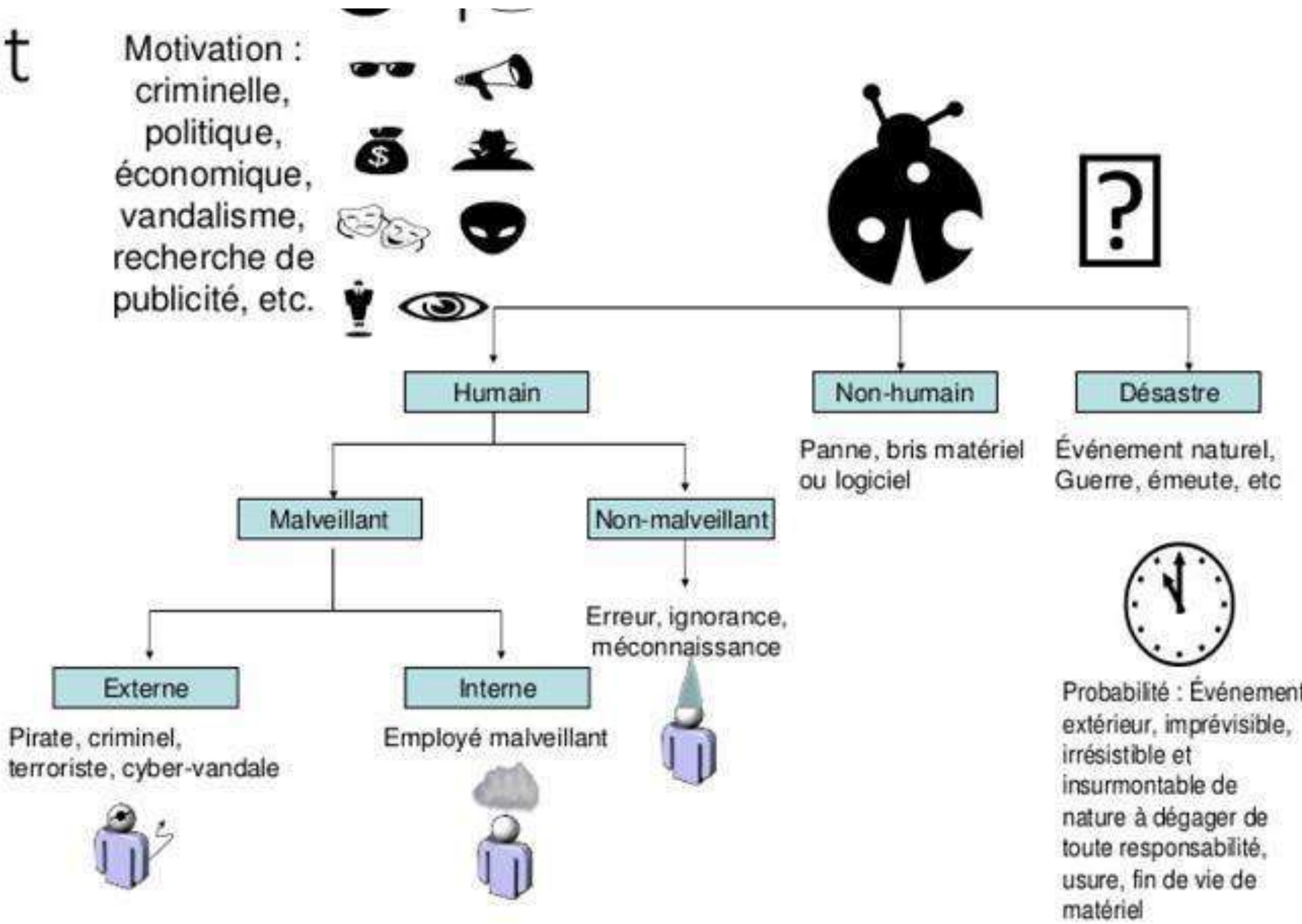
Hackers

- The rise of IoT has made people happy: cybercriminals.
- More and more hackers are relying on the vulnerabilities in connected objects to create a botnet and carry out a large-scale attack.
- Don't turn your IoT system into a sieve

IT security requirements

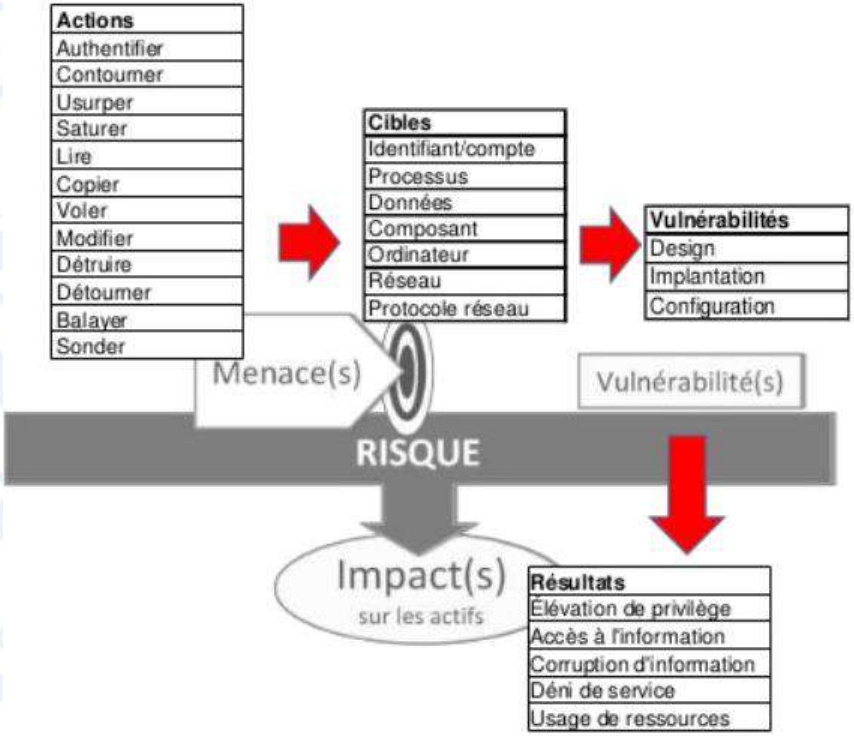
- Confidentiality means exchanging messages between a sender and receiver should be protected against any malicious or unauthenticated user.
- Integrity : is used to guarantee the content of messages exchanged between the sender and receiver is protected against any manipulation by an intruder without the receiver being able to track this manipulation.
- Availability: is used to guarantee that a malicious user is not capable of disrupting or harmfully affecting communication or quality of service provided by IoT devices or communication network.

Agent


Motivation :
criminelle,
politique,
économique,
vandalisme,
recherche de
publicité, etc.
Humain
Non-humain
Désastre
Panne, bris matériel
ou logiciel
Événement naturel,
Guerre, émeute, etc
Malveillant
Non-malveillant
Erreur, ignorance,
méconnaissance
Externe
Interne
Pirate, criminel,
terroriste, cyber-vandale
Employé malveillant
Probabilité : Événement
extérieur, imprévisible,
irrésistible et
insurmontable de
nature à dégager de
toute responsabilité,
usure, fin de vie de
matériel

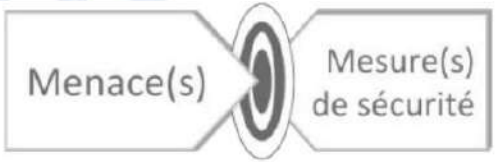
Menaces et mesures de sécurité

- Threat: Potential event, with non-zero probability, likely to undermine IT security.
- A threat exploits one or more vulnerabilities in order to reach a target through an action
- When the attack is successful, it produces an impact on the target (availability, integrity, and confidentiality)



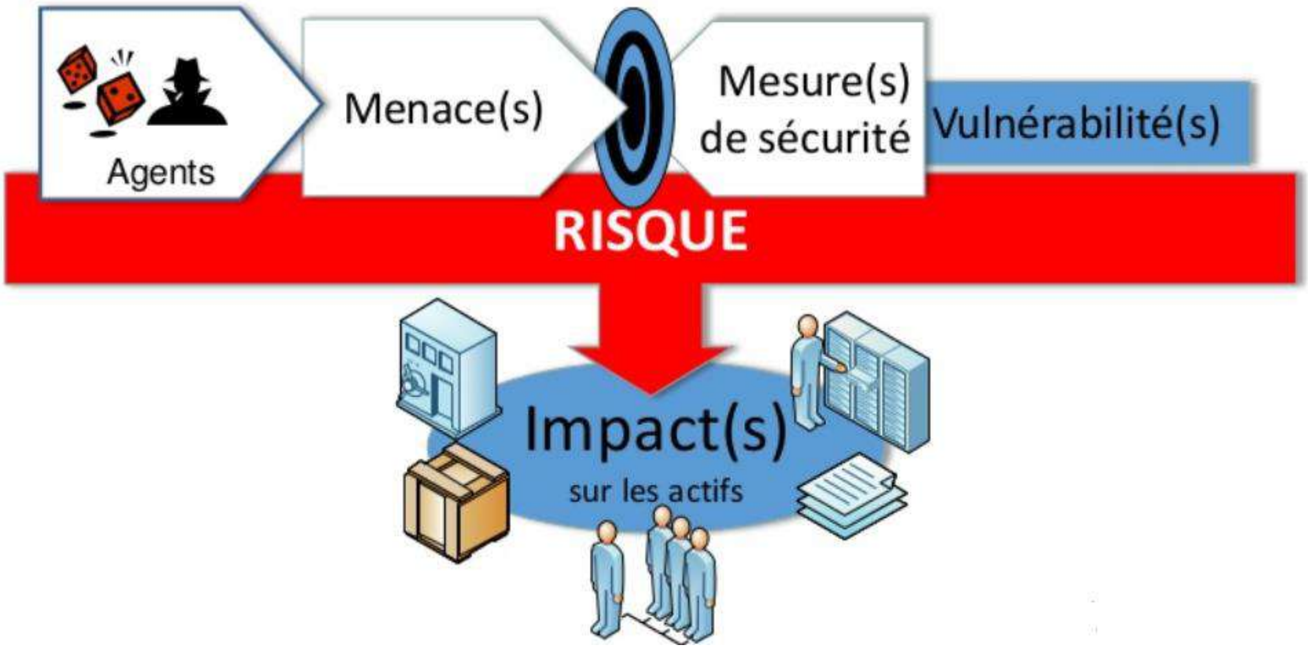
Threats and security measures

- Security measures are implemented to counter one or more threats in order to control, mitigate or eliminate the risks

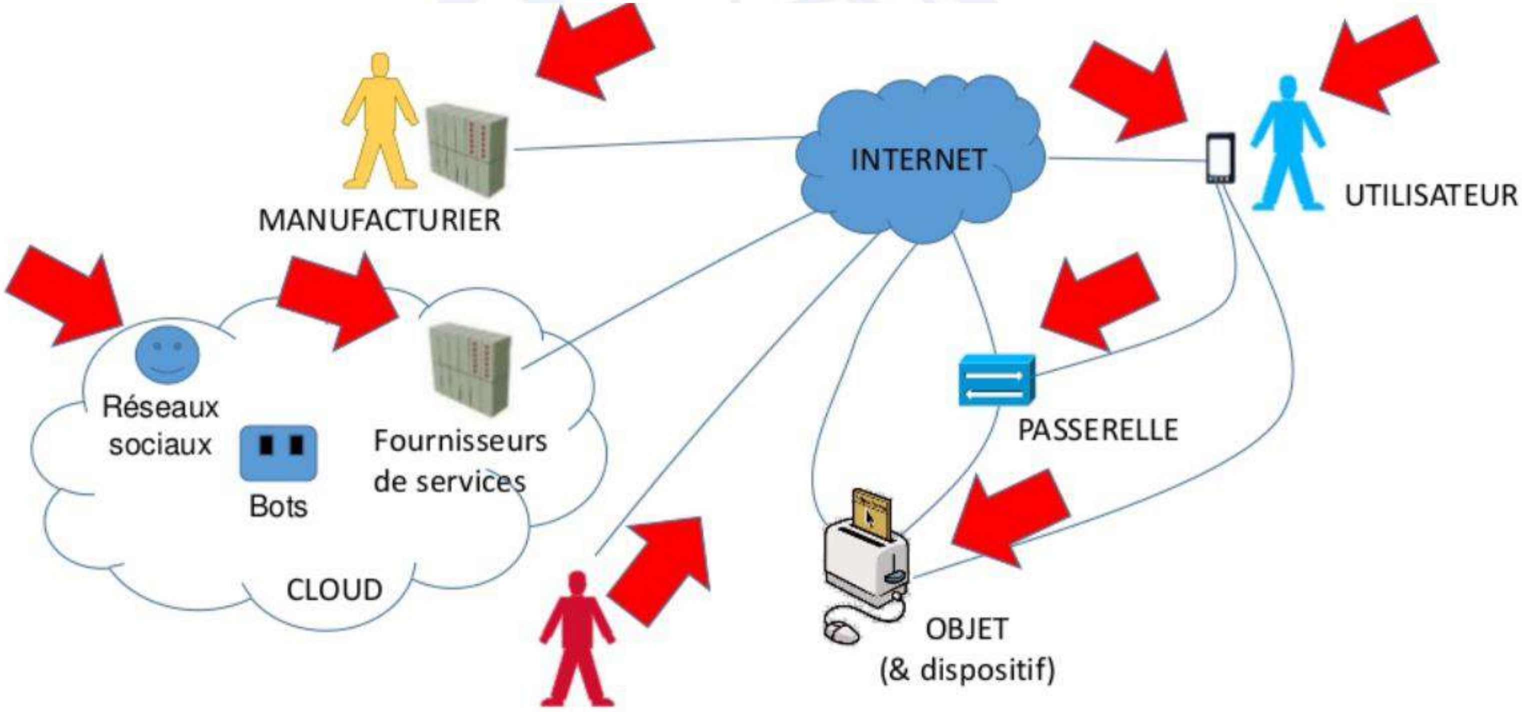


- If, despite the security measure, the threat succeeds in reaching a vulnerable asset, then this attack is successful. It will have an impact on its availability and / or integrity and / or confidentiality of the asset.

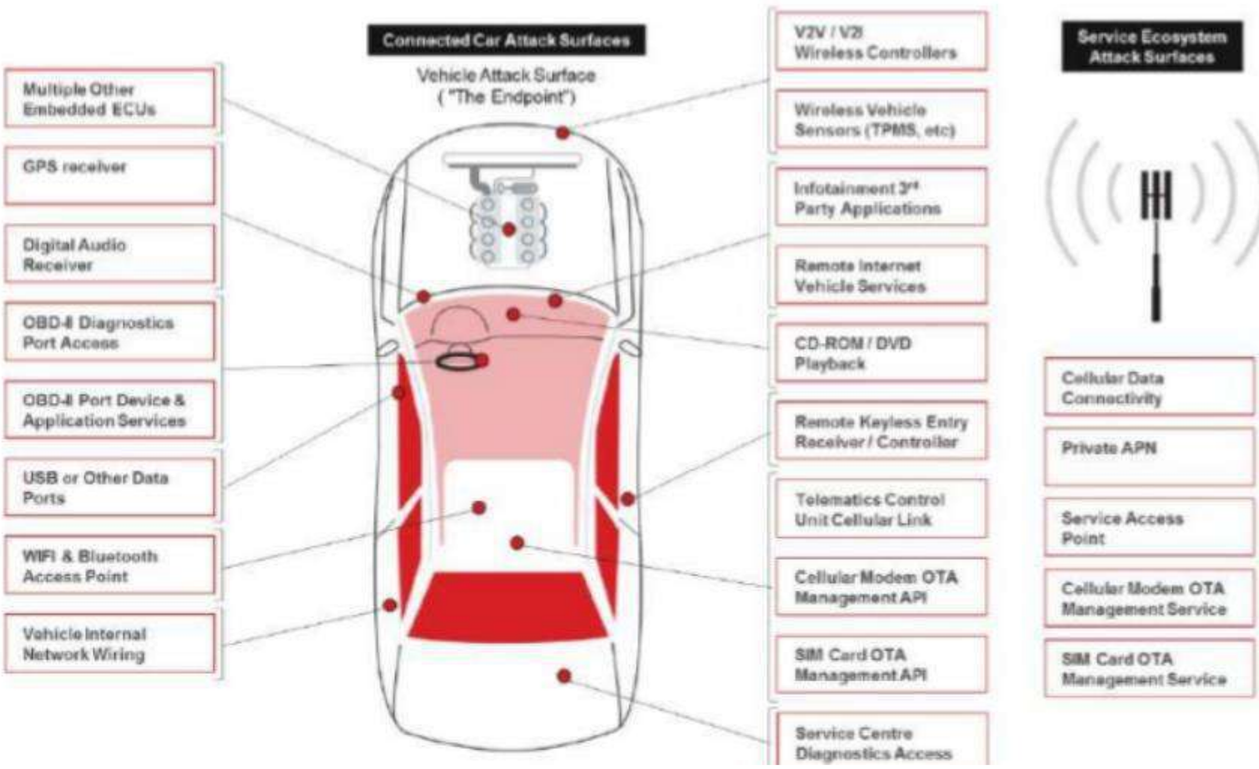
Threats and security measures



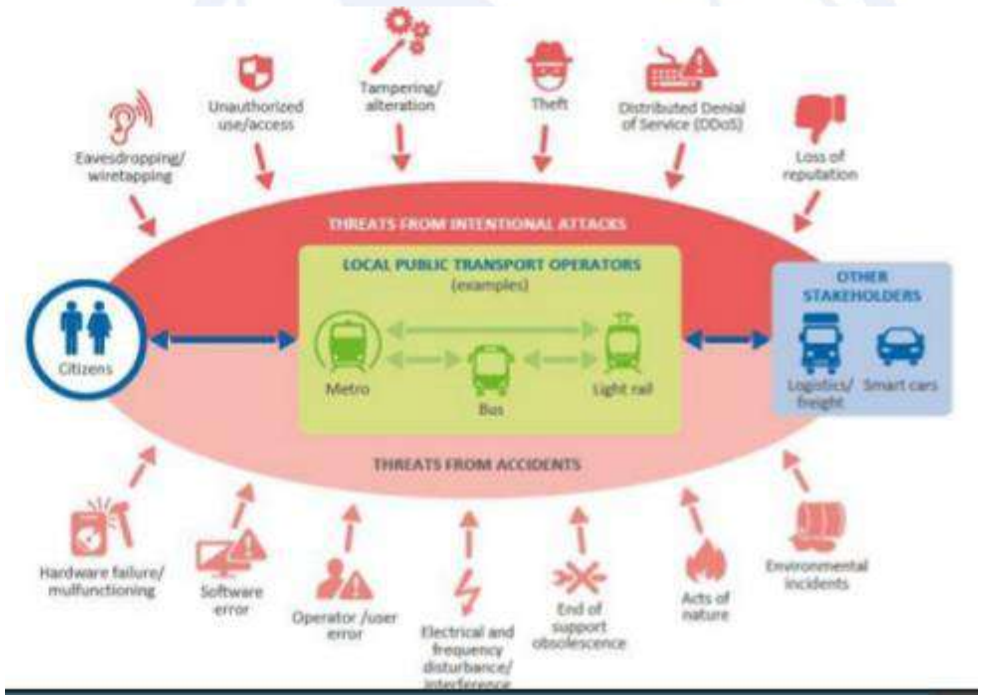
Attack surfaces



Attack surface of the connected car



Attack surface of the intelligent transportation system



Vue générale des menaces

Client Web
- ❑ Code malveillant
- ❑ XSS (*cross site scripting*)

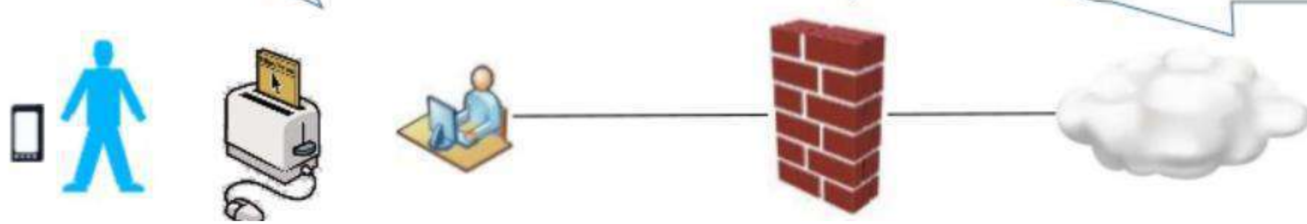
Accès à la ressource Web
- ❑ *Phishing*
- ❑DNS *poisoning*

Infrastructure télécom
- ❑Déni de service

Application & plate-forme
- ❑ Injection SQL
- ❑ Code malveillant
- ❑Déni de service
- ❑Attaque brute sur l'authentification

Infrastructure
- ❑ Code malveillant
- ❑Attaque brute sur l'authentification
- ❑Déni de service

Infrastructure télécom
- ❑Déni de service



Threats at different levels

- Attacks on the entire IoT ecosystem
  - Sensors / devices
  - Network
  - Platforms and services

Security threats to IoT sensors/devices

- **Device capture:** Refers to a device being physically compromised or having its keys lost.
- **Sinkhole attack:** Refers to an attack in which a compromised device attracts communication traffic to form a black hole or introduce selective forwarding.
- **Sybil attack:** Refers to an attack in which a malicious device illegitimately takes on multiple identities.
- **Flooding attack:** A flooding attack is a form of a denial of service (DoS) attack in which an attacker sends a succession of 'hello' packets to a targeted device in an attempt to consume enough of the device's resources to make the device unresponsive to legitimate traffic.

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to IoT sensors/devices

- **Selective forwarding attacks: In** this attack, a compromised node filters randomly received packets and forwards some of them to the next node. If the node filters out (drops) all the packets it receives, it is called a 'blackhole' attack.
- **Wormhole attack**: Wormhole attacks occur when two malicious/compromised nodes advertise having a very short path between them.
- **Impersonation of sensor/device:** his attack happens when an attacker successfully masquerades as the identity of a legitimate sensor/device.

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to IoT gateways

- **Unauthorized access:** Unauthorized access to a gateway can cause the disclosure of sensitive information, data modification, DoS and illicit use of resources.
- **Rogue gateway:** Even if all wireless gateways are secure, it is easy for attackers to deploy a rogue gateway of their own. Once a legitimate device is deceived into connecting to a rogue gateway, confidential connection information can be gathered. .
- **Denial of service attack:** The DoS attack causes a target to significantly slow down or, ideally, stop the services it provides by exhausting the target's memory and/or computing capacity

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to the network

- **Unauthorized access:** Unauthorized access to a wireless sensor network can cause disclosure of sensitive information, data modification, DoS and illicit use of resources.
- **Packet sniffing:** For wireless sensor networks that do not have encryption capabilities it is generally easy for attackers to eavesdrop on network communications.
- **Bluejacking:** This as an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to users of Bluetooth-enabled devices.
- **Bluesnarfing:** This attack results in the unauthorized access of information from a targeted wireless device through a Bluetooth connection, often between phones, desktops, laptops, and personal digital assistants (PDAs).

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to platform/services

- **Profiling:** Exploratory process used to gather information on the platform/services
- **Denial of service:** An attack in which the platform/service is overwhelmed by massive service requests and becomes too busy to respond to legitimate client requests.
- **Arbitrary code execution:** An attack that tries to run malicious code on a platform/service to compromise its resources and to then launch additional attacks.
- **Malicious code execution:** Any part of a software system or script, which is intended to cause undesired effects, security breaches, or damage to a system. Typical example includes viruses, worms, and Trojan horses.

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to platform/services

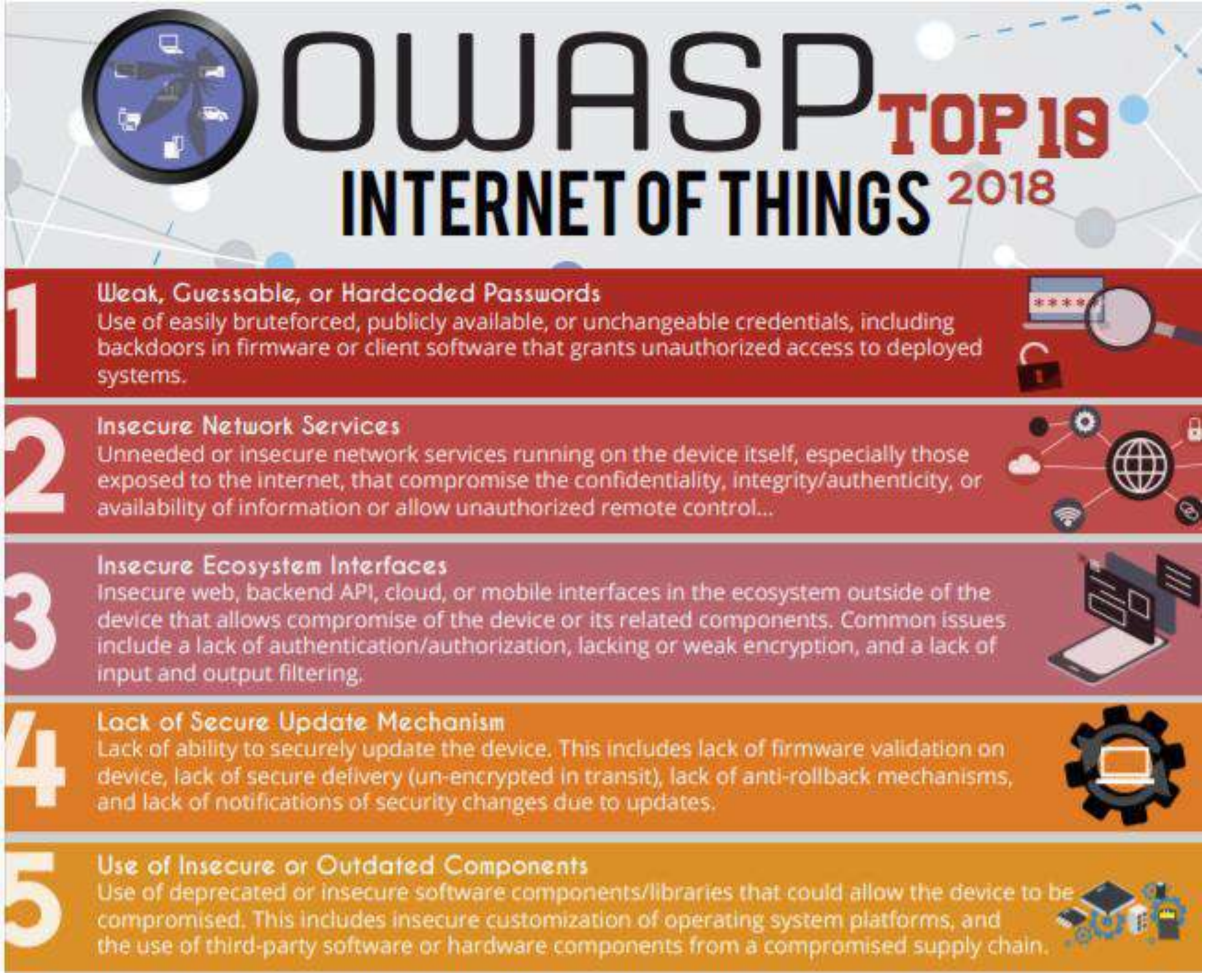
- **Elevation of privileges:** An attack in which code is executed, using a privileged process account, to elevate the attacker's privileges.
- **Structured query language (SQL) injection:** An attack that exploits vulnerabilities in an application's input validation and data access code to run arbitrary commands that inject or extract information.
- **Unauthorized access:** An attack that gains access to a platform/service using someone else's account or another method of access. F
- **Brute force:** An attack that systematically checks all possible keys until a correct one is found.

Source : Rec. UIT-T X.1361 (09/2018)

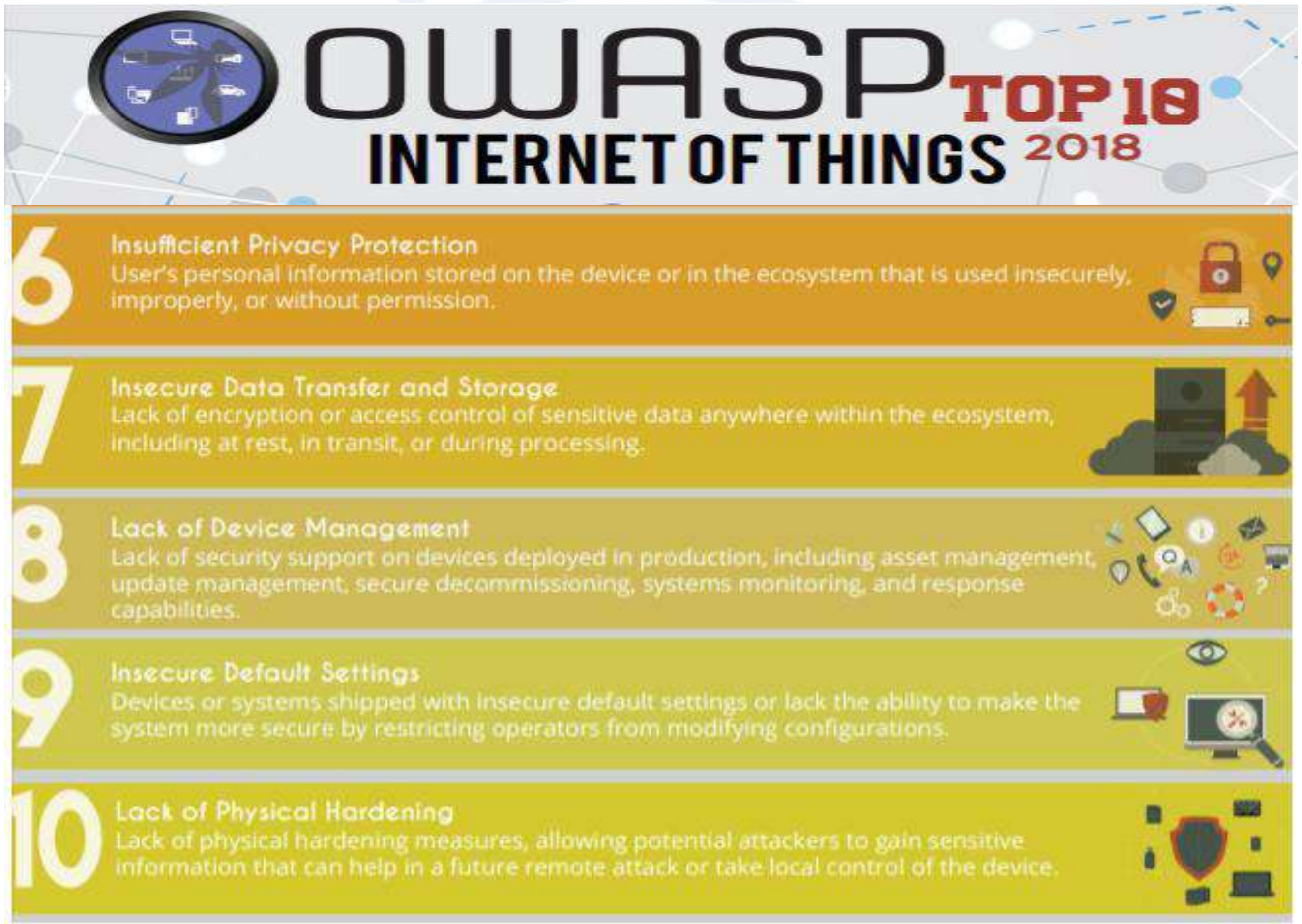
Security threats to platform/services

- **Dictionary attack of usernames/passwords:** An attack that systematically defeats cipher or authentication mechanisms by repeatedly trying passwords, using words in a dictionary.
- **Use of default usernames and passwords/use of weak passwords**: An attack where default usernames and passwords/weak passwords are exploited to gain access to platform/services.
- **Inference attack:** This attack occurs when a user is able to infer protected information from rightfully accessible chunks of information with lower classification

Top 10 Threats (OWASP)



Top 10 Threats (OWASP)



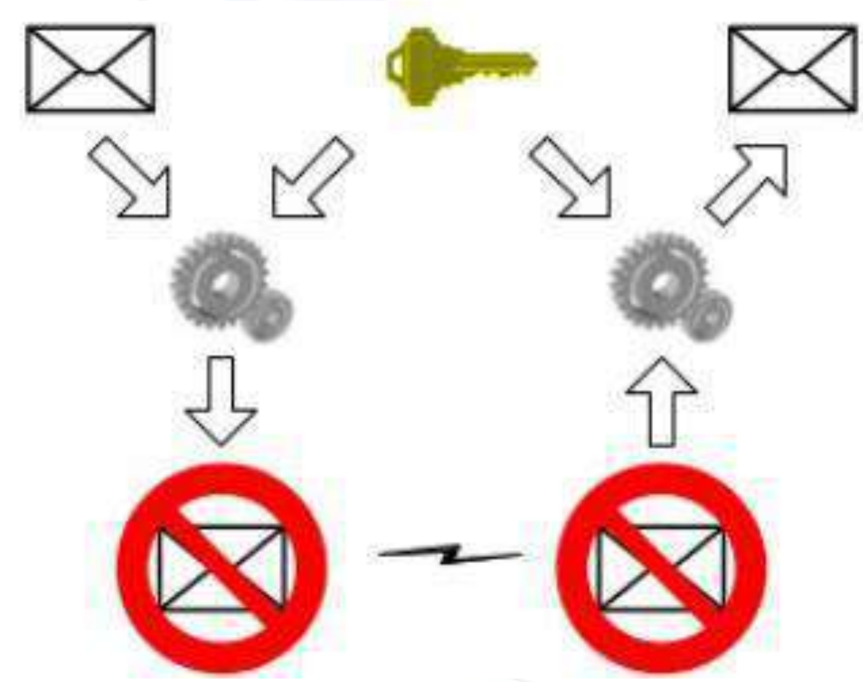
Security measures

- Cryptography solutions are recognised as secure solutions that address all issues related to data security (confidentiality and integrity).

- Cryptography algorithms:
  - Symmetric cryptography algorithms (with secret key): DES, 3DES, AES, RC4, RC4, RC5,…
  - Asymmetric cryptography algorithms (public and private key): RSARSA (encryption and signature), DSA (signature), Diffie-Hellman key exchange protocol (key exchange)
  - Hash function: MD5, SHA-1, ...

Encryption with a secret key

Only one key is used to encrypt and decrypt

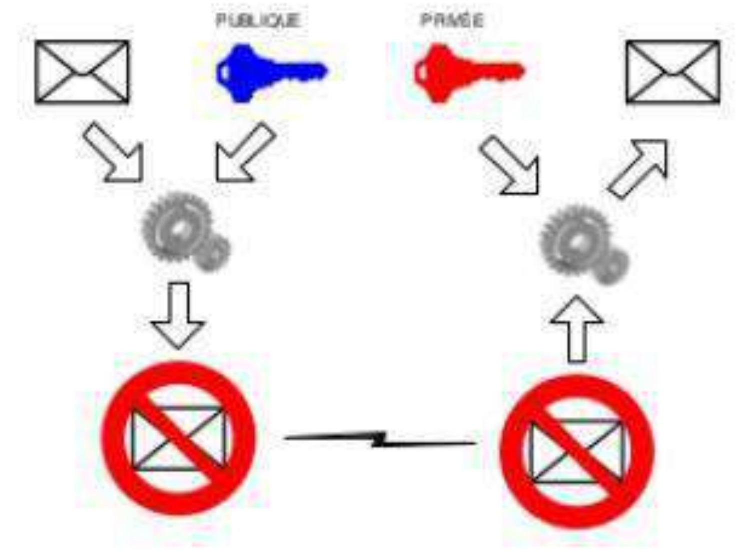


Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

31/3000

Encryption with a private key and a public key

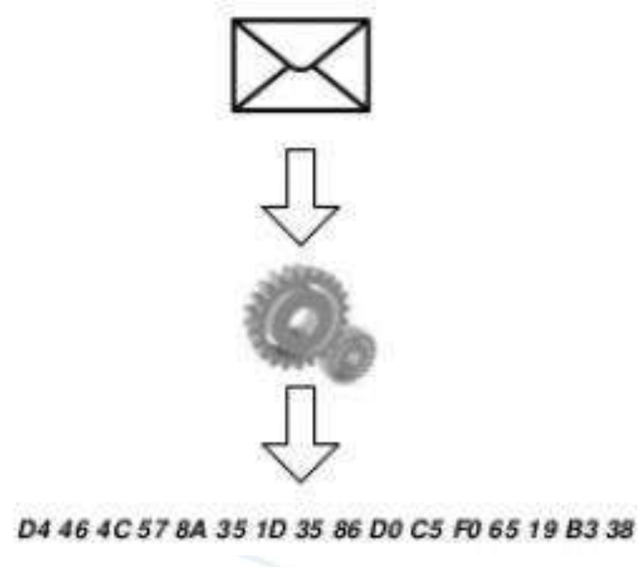
Only one key is used to encrypt and another to decrypt



Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Hash

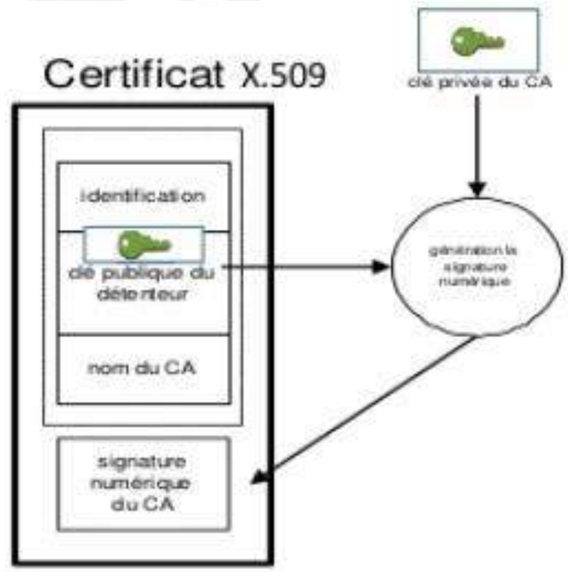
- Not encryption, but a message fingerprint
- One-way operation
- The result is not predictive, 2 different messages will not have the same result
- Used to verify integrity.



Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

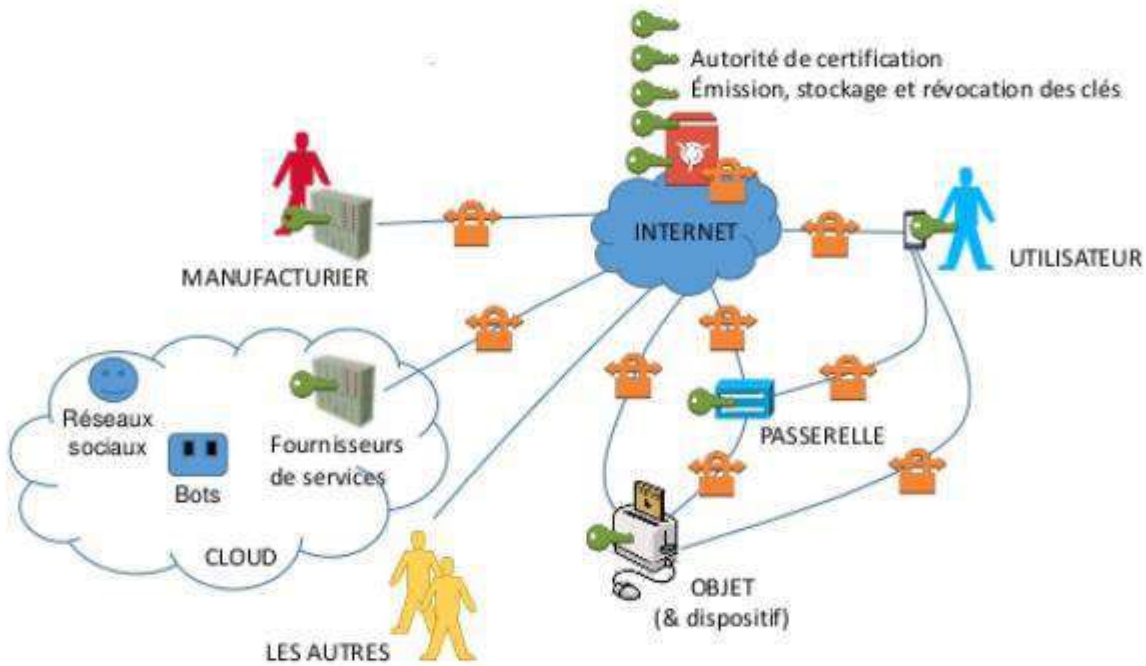
Public key infrastructure (PKI)

Autorité de certification
Émission, stockage
et révocation des clés



Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Encryption, key, and PKI



Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Part 2: Privacy and liability

Democratization of the IoT, a source of privacy threats

- The IoT growth continues to add billions of new sensors and devices to the Internet, generating an enormous amount of data.
  - 44 billion gigabytes of data in 2020, 10 times more than in 2013.
  - 50,000 gigabytes of data created per second in 2020 compared to 100 gigabytes in 1992.
- These data is about people, including their locations, connections, shopping records, financial transactions, pictures, voices, conversations, health state, etc., with or without their consent.
- Democratization of the IoT, a source of privacy threats
  - Lucrative market for criminals => data reselling on the darknet
  - Compromise of personal data via ransomware
  - Abusive corporate espionage

Privacy defintion

- The privacy can be defined as :

‘The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others’.

Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Attack on access control systems

- Hacking of connected locks (home automation) through object or cloud vulnerabilities.

Google Glass

- Google Glasses were not marketed because of the privacy breach.

Attack drones

- Preparation of terrorist operations using drones
  - Detection of critical infrastructure by drones
  - Transport of explosive substances

Baby monitor hacked

Very nice words uttered by a hacker to the attention of a 2 year old girl after taking control of the family baby monitor

Pacemaker hacked

- A pacemaker can be hacked, with potential dangers to the health of patients.

- Le point commun entre un pacemaker et une pompe à insuline ? Ils ont tous deux été piratés
- Pacemaker : possibilité de l'éteindre ou d'envoyer une décharge de 830 volts
- Pompe à insuline : Prise de contrôle via WiFi, possibilité de la transformer en arme létale !

Atteinte aux biens et aux personnes

Privacy threats

- The potential risk of losing control over personal information is defined as a privacy threat.

Identification

- Identification is the threat of relating an identifier (e.g., name, address) with private data about an individual.
- The use of a surveillance camera, in non-security contexts, is an example of such techniques, where customers' behavior is studied for analysis and marketing.
- To address this issue, attribute-based authentication is recommended to minimize the data a device can collect in the IoT and maintain control over the disclosure of data.

Privacy threats

Localization and tracking

- Localization and tracking are the threats of specifying and recording a person’s location through time and space by different means such as cell phone location, Internet traffic or GPS data.
- The availability of massive and complete spatial and spatiotemporal data has led to an increasing interest in using geographic data and incorporating spatial information analysis.

Privacy threats

Profiling

- Profiling is the process of collecting and processing data about individuals' activities and actions over long periods to classify them according to some feature.
- The information is usually collected without permission from users and integrated with other personal data to create a more complete profile.
- Profiling is currently used in a large range of domains, for example, e-commerce, targeted advertising and credit scoring. One of the risks associated with profiling is that personal information may be exposed to other users. Moreover, many users are disturbed by the mere awareness of being watched and tracked.

Privacy threats

Inventory attacks

- Inventory attacks are related to the illegitimate gathering of information about the existence and characteristics of things in a specific place.
- Inventory attacks can usually be performed by using the fingerprint of IoT devices, for instance, their communication speed, reaction time and so on.
- If the promise of the IoT will be fulfilled, all smart things will be addressable over the Internet, opening the opportunity for unauthorized entities to exploit this and create an inventory list of things belonging to a target.
- An inventory attack could be used for profiling individuals, since owning special items disclose private information about the owner.

Privacy threats

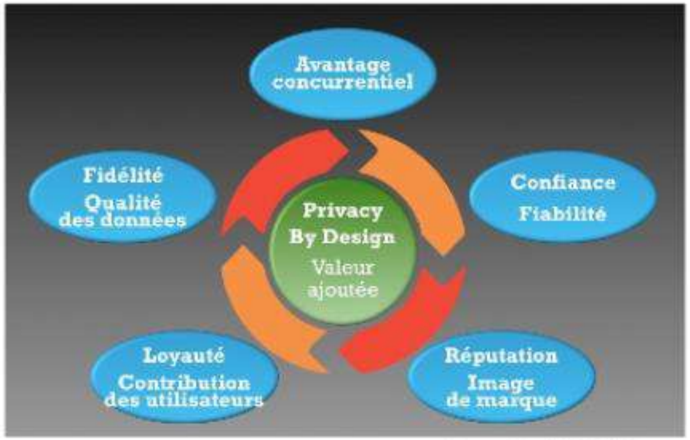
Linkage

- Linkage threat refers to uncontrolled disclosure of information due to combining
- separated data sources and linking different systems. Integrating various types of
- information about the individual reveals new facts which are not expected by the
- owner. The revealed information is considered a privacy breach [41].

Privacy-Preserving Solutions for IoT

Privacy by Design

- It is one of the valuable key to preserving privacy in the IoT environment.
- The IoT customers should have the required features to control their own information and define who can access it.
- Currently, some companies use a sort of agreement that allows certain services to access data as desired. Therefore, built-in tools to preserve user's privacy are required to be built as an essential part of any product.



Privacy-Preserving Solutions for IoT

- Privacy Awareness/informed consent transparency: One of the main problems of privacy violation is the lack of public awareness. IoT users have to be fully aware of how to keep themselves protected against any types of privacy threats. IoT users give their consents about data usage, storage and processing.
- Data Minimization: IoT service providers should employ the concept of data minimization by limiting personal data collection to only what is related to the service they introduce. They also need to retain the data only if they need it for the service.

Privacy-Preserving Solutions for IoT

- Cryptographic Techniques: One of the main solutions to preserve the privacy in IoT devices is employing the appropriate cryptographic technique to encrypt data. However, with limited storage and computation resources in IoT devices, this solution may be difficult to achieve.
- Data anonymization: It is necessary after data collection that all unique identifiers such as social security number and driving license numbers should be removed from data records in such a way that the data can no longer be used to identify natural person.
- Access control: Providing an efficient access control model for the IoT system to enable smart things to provide fine-grained decisions is one of the solutions for preserving the privacy of IoT users.

IoT product liability

- The question of responsibility has become an imperative with the explosion of connected objects.
- Connected objects can make decisions autonomously and without human intervention.
- In case of damage caused by a connected object, a complaint by a third party could result in a dismissal.
- There is no specific legal framework applicable to liability for connected objects or connected robots.

Legal issues

- Object which is dedicated to act alone and under its own responsibility
  - Ex Google Car: What about the responsibility for the accident?
- The connected object performs actions that lead to the issue of liability.

When does the connected car hit the wall?

Legal issues

There is a need to develop a legal framework of responsibility specific to connected objects and legal texts that adapt to the nature of objects and their evolution, and define without a shadow of doubt the responsibility of the user or the manufacturer of a connected objects in case of failure.

The 6 GDPR principles to ensure accountability

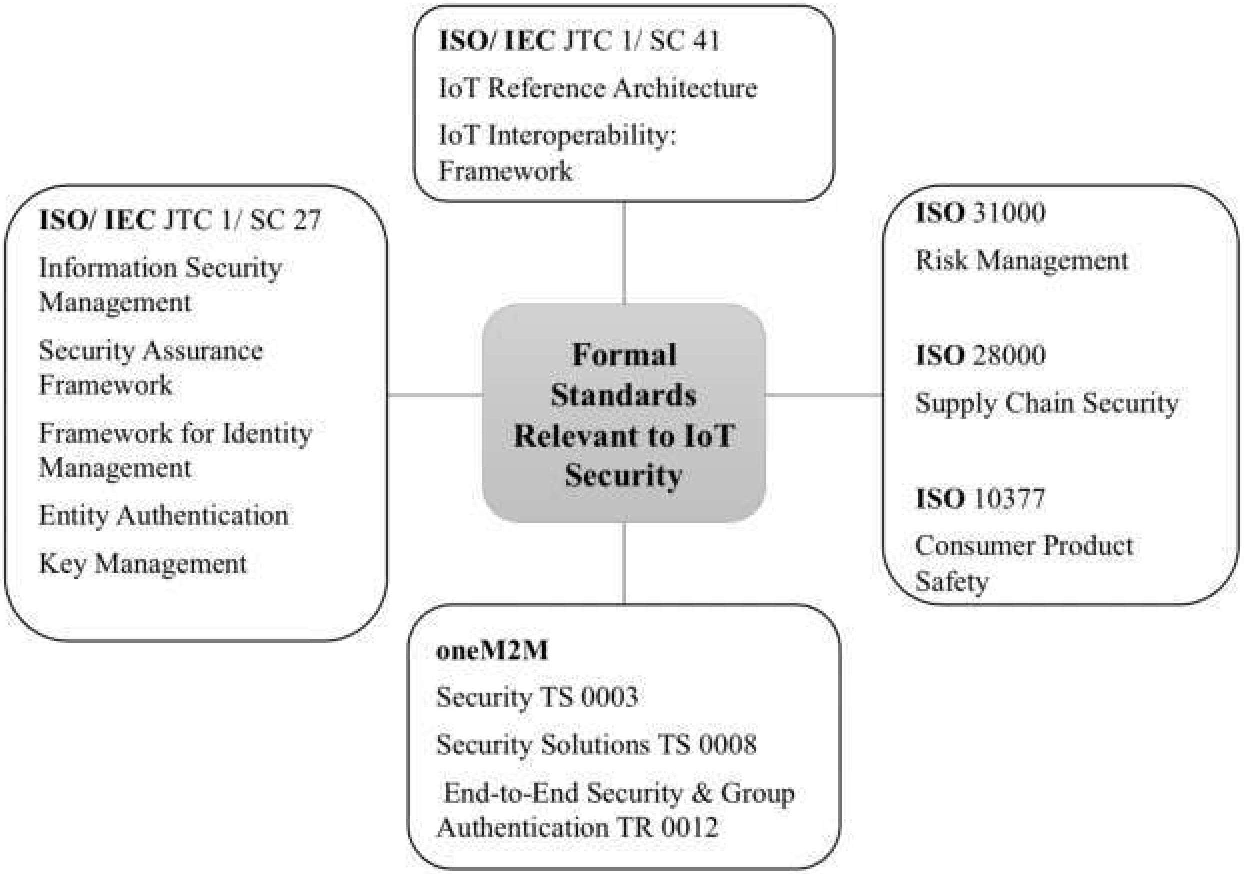
Source : https://gdpr-info.eu/art-5-gdpr/

Part 3:
High-level guidelines for IoT security, Code of practices and Certifications

Standardisation activities relevant to IoT security

- The sustainability of IoT market depends on compliance with standards, codes of practices and certifications.
- Several works carried out by many standardization organizations to compensate the lack of standards.
- 02 types of standards:
  - Formal standards (ISO/IEC, OneM2M, …)
  - De facto standards (OWASP, GSMA, IoTSF, …)

Formal standards relevant to IoT security



Code of practices relevant to IoT security

Industry Association & Guidelines	Compliance Testing	Certification
Open Web Application Security Project (OWASP) Principles of IoT Security IoT Security Guidance	IoT Framework Assessment IoT Testing Guides IoT Testing Methodology	N/A
Online Trust Alliance (OTA) IoT Security & Privacy Trust Framework	Online Trust Audit	Honour Rolls
Cloud Security Alliance (CSA) New Security Guidance for Early Adopters of the IoT Future Proofing the Connected World	Cloud Control Matrix Consensus Assessments Initiative Questionnaire	CSA STAR self-assessment, 3rd party, or continuous monitoring certification
Broadband Internet Technical Advisory Group (BITAG) Internet of Things Security and Privacy Recommendations	N/A	N/A
Open Connectivity Foundation (OCF) Security Specifications	OCF Testing and Certification Program	OCF Certification Mark
GSM Association (GSMA) IoT Security Guidelines for: - Endpoint Ecosystems - Network Operators - Service Ecosystem	IoT Security Assessment Checklist Self-Assessment Scheme	Once IoT Security Assessment is approved, product is listed on GSMA IoT website.
IoT Security Foundation (IoTSF) Connected Consumer Products Best Practice Guidelines Vulnerability Disclosure Best Practice Guidelines	IoT Security Compliance Framework	Best Practice User Mark
Industrial Internet Consortium (IIC) Industrial Internet Security Framework	Security Checklists for Verticals Maturity Models for Industrial Systems	N/A

UK DCMS Code of practices

UK Department for Digital, Culture, Media & Sport (UKDCMS)

- UK DCMS proposed a code of best practices for the security of IoT products consumer and associated services.
- The code identifies that many serious security issues arise from poor security design and poor practices in products design to consumers:
    1. No default password.
    2. Implement a vulnerability disclosure policy.
    3. Keep the software up to date.
    4. Securely store credentials and security sensitive data.

Source : https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

UK DCMS Code of practices

5. Communicate securely.
6. Minimize exposed attack surfaces.
7. Ensure the integrity of the software.
8. Ensure that personal data is protected.
9. Make systems resilient to failure.
10. Monitor system telemetry data.
11. Make it easy for consumers to delete personal data.
12. Facilitate the installation and maintenance of devices.
13. Confirm the input data.

GSMA Security guideline

- According to GSMA, providing secure products and services is a process rather than a goal.
- The GSMA has created a guideline for the benefit of service providers looking to develop new IoT services.
- The guideline allows providers of IoT services and products to self-assess the compliance of their products, services and components with GSMA IoT security guideline.
- The assessment ckecklist allows entities to demonstrate the security measures they have taken to protect their products, services and components from cybersecurity risks.
- Assessment statements can be made by submitting a completed statement to the GSMA.

Source : https://www.gsma.com/iot/iot-security/iot-security-guidelines/

OTA

- Online Trust Alliance (OTA) is a comprehensive set of strategic principles that help secure IoT devices and their data.
- Built on the basis of a collaborative process, this framework provides recommendations that all IoT manufacturers should adopt to improve the security, transparency and communication capabilities of their devices, as well as data privacy issues.

AIOTI Recommendations

- The basic AIOTI requirements for IoT devices include:
  - Security Testing and Certification - Using recognized certifications to assess device security based on the risk level.
  - Security Label - Proven labels such as "energy efficiency label" to classify IoT devices.
  - Predefined and certified security structures - Requirement of identity encryption, access, and communication channels; and requirement for secure storage of keys and data.

AIOTI Recommendations

– **Security Justification** - Explanation of the implementation of security measures related to known hazards in order to define an acceptable level of security risks to any IoT device designer, auditable by an independent third party.
– **Information Exchange** - Sharing of information between manufacturers on incidents and potential vulnerabilities.
– **Defined Functions** - IoT devices should be able to perform documented functions, to make sense of IoT devices and services.
– **Standardization** - Interoperability of components and communication protocols.

IoTSF

- IoT Security Foundation (IoTSF) implemented an IoT Security Compliance Framework aimed at assessing the security of a wide range of IoT devices by adopting a risk-based approach derived from the triad CIA.
- The framework defines 5 classes of conformity. The class of a product is defined on the basis of a requirements checklist. This checklist could be made compulsory by the contracting parties in order to verify compliance with the requirements.

Compliance class	Security objectives		
	Confidentiality	Integrity	Availability
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoTSecurity-Compliance-Framework.pdf

IoT Certification

- Lack of trust marks and certificates that can inform consumers about the security and risks of IoT devices.
- Efforts are underway in various parts of the world to create certification schemes.
- It should be ensured that these schemes are aligned in order to create fair competition conditions for manufacturers.

EU cybersecurity certification framework

- The EU has proposed a certification framework for IoT security products.
- The certificate, recognized by all Member States, allows companies to market their products across borders, and enables buyers to understand the safety features of the product or service.
- This framework provides a comprehensive set of rules, technical requirements, standards and procedures.
- ENISA is in charge of implementing the certification process.
- The use of certification is voluntary at this time.

Legislative policies and regulations

- Two types of regulatory initiatives :
  - Sectoral initiatives, led by industrial players wishing to establish a regulatory framework for their sectoral activities.
  - Interventions by public authorities in areas requiring arbitration between stakeholders (industrialists, civil society, etc.).

GDPR

- The General Data Protection Regulation (GDPR) entered into force on 25 May 2018, it is now the reference text for the protection of personal data for the EU.
- The GDPR aims to strengthen the rights of those concerned by data processing and to increase the liability of companies responsible for processing personal data.
- This regulation applies to any business that processes data relating to EU residents, whether established within or outside the EU.
- Thus GAFAs or any companies that address the European market are affected by this regulation.

GDPR

- The GDPR introduces 3 innovative concepts:
  - Privacy by design, taking into account the protection of privacy from the design of a service or product.
  - Privacy by default, principle of data protection at the highest possible level by default.
  - Accountability, logic of accountability based on self-monitoring of the measures taken to guarantee the compliance of data processing and to prove it.

U.S. IoT Cyber Security Improvement Act

- This legislation defines the security standards applicable to IoT equipment installed on the networks of the US administration.
- It aims to guarantee the protection and the absence of equipment vulnerabilities, the conformity of products with sectoral standards as well as the possibility of applying patches to them.
- Suppliers are prohibited by law from selling equipment whose passwords cannot be changed.
- The legislation would also require US agencies to establish and maintain inventories of IoT devices and to update them every 30 days.

Law no° 327 of California

- California Law n° 327, approved in September 2018, came into effect in January 2020.
- It requires that all connected devices must have "reasonable" security features to prevent unauthorized access, modification, or data exposure.
- In addition, if the device features a password, it must either be unique to that device or force the user to set their own password during initial setup, thus preventing cyberattacks through guessing default passwords.

Law no° 327 of California

- It places liability and responsibility directly on the IoT vendors, no matter where the device was purchased or manufactured, so long as the device is connected to the internet in California.
- Using a "reasonable" security features is no longer an option. If anything goes wrong with the device, it might get to court and manufacturers will bear the burden of proof.
- Therefore, it is highly advisable for manufacturers to take the extra mile and look out for new and advanced cybersecurity solutions.

EU cybersecurity law

- In December 2018, the EU adopted the Cybersecurity Law to strengthen the mandate of the European Agency ENISA to better support Member States fighting against cybersecurity threats and attacks.
- This law establishes a European framework for cybersecurity certification, cybersecurity of online services and consumer devices.
- Certification is voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to meet a specific security need.

Source : https://www.allot.com/blog/new-iot-security-regulations-what-you-need-to-know/

- NIST

NIS Directive

- The Network and Information Systems Security Directive was adopted by the European Parliament on July 6, 2016 and entered into force on August 2016.
- The NIS Directive provides legal measures to increase the general level of cybersecurity in the EU by ensuring:
  - The state of readiness of Member States by requiring them to be appropriately equipped eg. via an IT Security Incident Response Team and a National NIS Authority.
  - Cooperation between all Member States, through the establishing a Cooperation Group, to support and facilitate strategic cooperation and exchange of information between Member States.

- In Europe: data-driven regulation
- In America: Object-Oriented Regulation

Conclusion

- Manufacturers may not have the expertise to use the guidelines and recommendations available.
- The usability of the safety guidelines is a challenge and requires more research.
- Harmonization of IoT security guidelines and recommendations are needed to drive adoption.
- Harmonization needs to be supported by cybersecurity research initiatives.

Thank you!

PRIDA Track 1 (T1)

IoT Security and Regulations

08/09/2020

Agenda

- Part 1: IoT Security
- Part 2: Privacy and liability
- Part 3: Standards, guidelines and certification.

Introduction

- The number of connected IoT devices has grown rapidly: according to some estimates, the number of IoT devices in operation in 2020 surpassed 20bn.
- Despite the rapid growth of the devices, and the potential benefits they offer, the IoT raises significant security and privacy concerns.
- The most significant challenge is to determine whether a self-regulatory regime will be sufficient to address these concerns, or whether comprehensive or sectoral legislation or regulation will be necessary to ensure that the public interest in protecting personal privacy and data security will be addressed, and that adequate remedies will be available in the event of systemic failures.

IoT Security issues

- IoT can serve as the basis for large-scale attacks on critical infrastructures
- Some targets:
  - National or regional power supply networks
  - Financial and trading system
  - Connected car
  - Industrial system
  - Alarm system
  - Medical equipment
  - Audio and video surveillance

Challenges of IoT security

- The economy favors weak security
  - Competitive pressures for shorter time to market and cheaper products are pushing many IoT system manufacturers to spend less time and resources on security;
  - Strong security is expensive and it extends the time to market.
- Security is difficult
  - There are no credible means by which suppliers can communicate to consumers the security level of their products;
  - Difficult for consumers to easily understand the security of different IoT systems;
  - Reduced consumer pressure on suppliers;
  - Security is not competitive differentiator.

Challenges of IoT security

- IoT systems are complex and every part must be secure
  - The implementation of enhanced security in IoT systems requires expertise.
  - New players in the IoT ecosystem may have little security experience.
- Security support is not always maintained
  - IoT devices, applications and services require security patches and updates to protect against known vulnerabilities;
  - Supporting IoT system updates is a costly task for IoT service providers.
- Low consumer awareness of IoT security
  - Typically, consumers have limited knowledge of IoT security, which impacts their ability to configure and maintain the security of their IoT systems or to consider security aspects into their shopping habits.

Challenges of IoT security

- Security incidents can be difficult for users to detect or resolve
  - In many cases, the effects of a poorly secured product or services not obvious to the user.
    - Example, a refrigerator can continue to do a good job even if it has been compromised and is part of a botnet carrying out DDoS attacks.
  - Consumers also lack the technical ability, or the user interfaces, to implement the corrections.
  - Users may not know how to patch their devices.
  - Users are contractually prevented from updating or repairing the systems themselves or having them repaired by independent specialists.

Recent attacks

- In last years, many studies reported that IoT devices have been subject to **ransomware** and **Distributed Denial of Service (DDoS)** attacks.
- **Ransomware attack:**
  - It occurs when hackers use a virus to infect a computer and to encrypt all of its data, making the data inaccessible.
  - The hackers then demand a ransom from the affected computer user to decrypt the data.
  - If the computer user fails to pay the ransom within a certain amount of time, the virus destroys the files.

Recent attacks

- **DDoS attack**
  - It is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
  - The cybercriminal begins a DDoS attack by exploiting the vulnerability of just one device, making it the DDoS "master,"
  - It identifies then other vulnerable devices, networks, and systems.

Recent attacks

WannaCry attack

- In May 2017, hackers targeted computers running the Microsoft Windows OS by encrypting data and subsequently demanding ransom payments.
- The WannaCry attack affected thousands of computers in more than 150 countries.
- One of the more serious effects of the attack was the targeting of **16 hospitals across the UK**, leading to the cancellation of appointments and non-urgent operations at some locations.
- The UK National Health Service stated that the global financial and economic damage caused by WannaCry approached billions of dollars, making it one of the most damaging ransomware incidents in history.

Recent IoT attacks

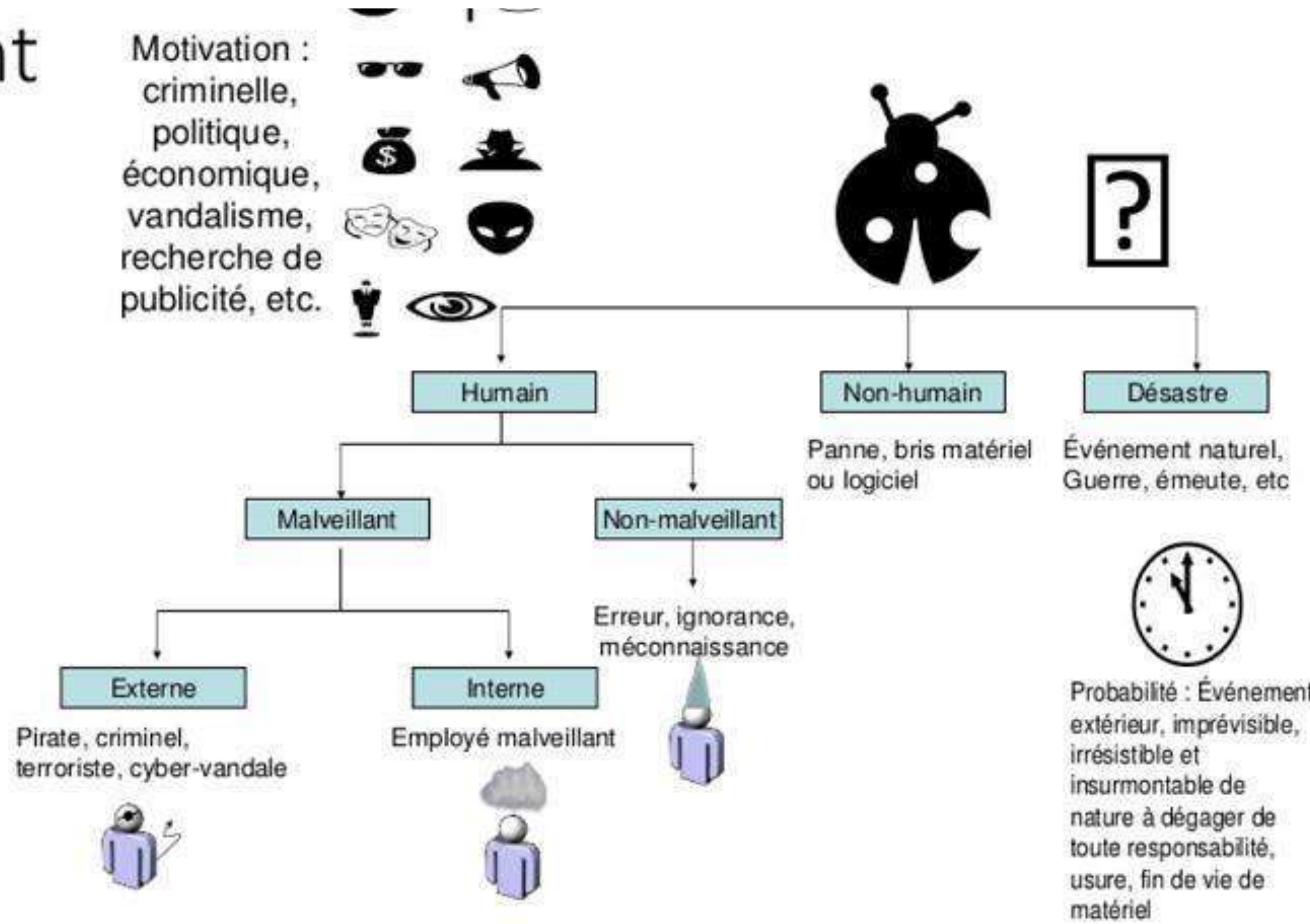
Botnet Mirai (2016)

- A large-scale DDoS attack took place in October 2016 and directly targeted IoT devices.
- The attack affected a large portion of the Internet by infecting a network of computers with **Mirai**, malware meant to bombard a server with so much traffic that it eventually collapses.
- The servers belonged to Dyn, a company that is a major provider of DNS services to other companies
- The attack made part of the internet inaccessible, including some very popular sites: Twitter, Reddit, Netflix, Spotify, The New York Times, CNN, etc.

Hackers

- The rise of IoT has made people happy: cHackers.
- More and more hackers are relying on the vulnerabilities in connected objects to create a botnet and carry out a large-scale attack.

Agent

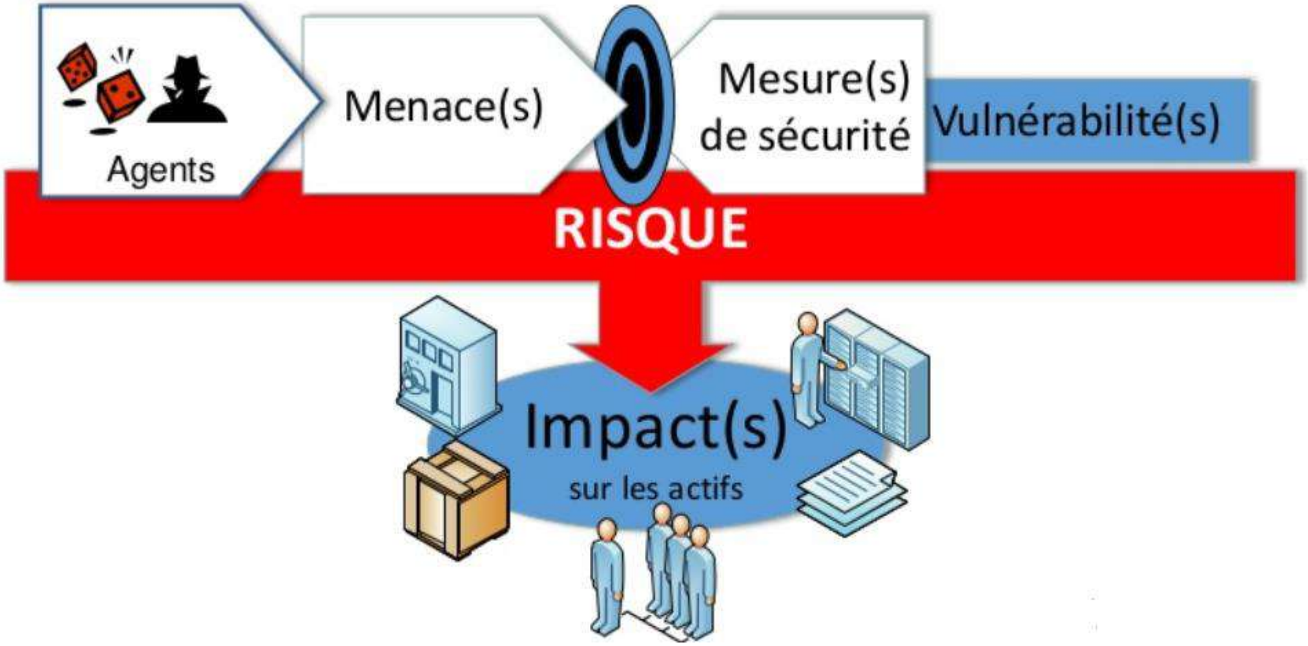


Motivation : criminelle, politique, économique, vandalisme, recherche de publicité, etc.
$
Humain
Non-humain
Désastre
Panne, bris matériel ou logiciel
Événement naturel, Guerre, émeute, etc
Malveillant
Non-malveillant
Erreur, ignorance, méconnaissance
Externe
Interne
Pirate, criminel, terroriste, cyber-vandale
Employé malveillant
Probabilité : Événement extérieur, imprévisible, irrésistible et insurmontable de nature à dégager de toute responsabilité, usure, fin de vie de matériel

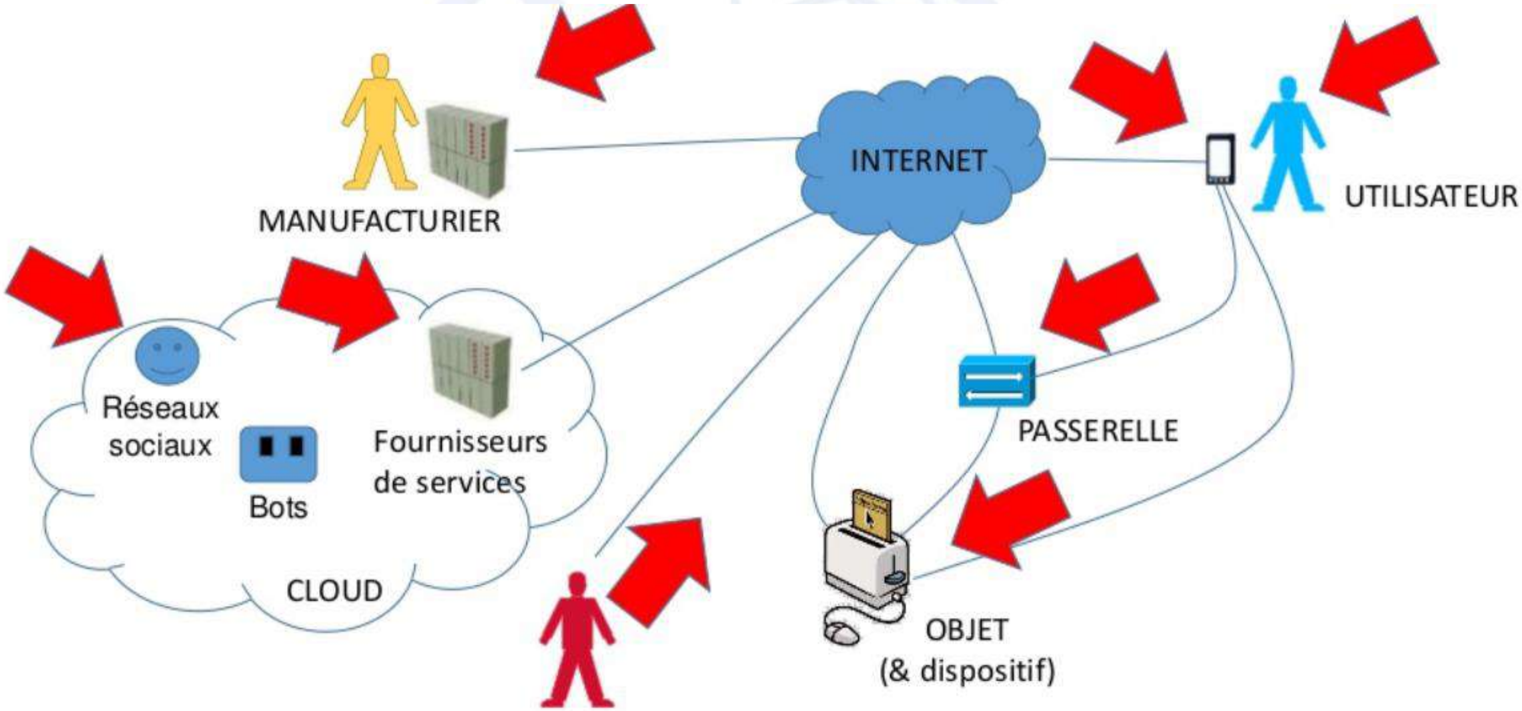
Threats and security measures

- Threat is a potential event likely to undermine security of IT systems. It exploits one or more vulnerabilities in order to reach a target through an action.
- When the attack is successful, it produces an impact on the target (availability, integrity, and confidentiality)
- Security measures are implemented to counter one or more threats in order to control, mitigate or eliminate the risks.
- If, despite the security measure, the threat succeeds in reaching a vulnerable asset, then this attack is successful. It will have an impact on its availability and/or integrity and / or confidentiality of the asset.

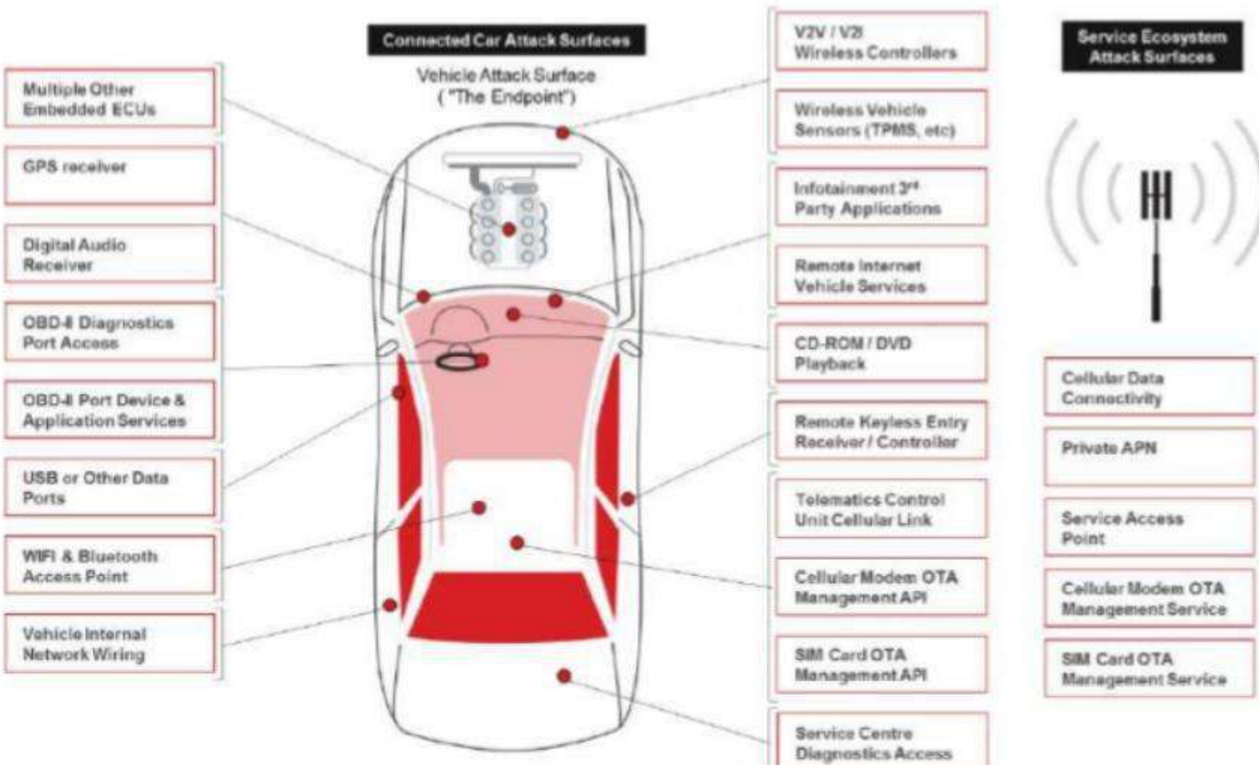
Threats and security measures



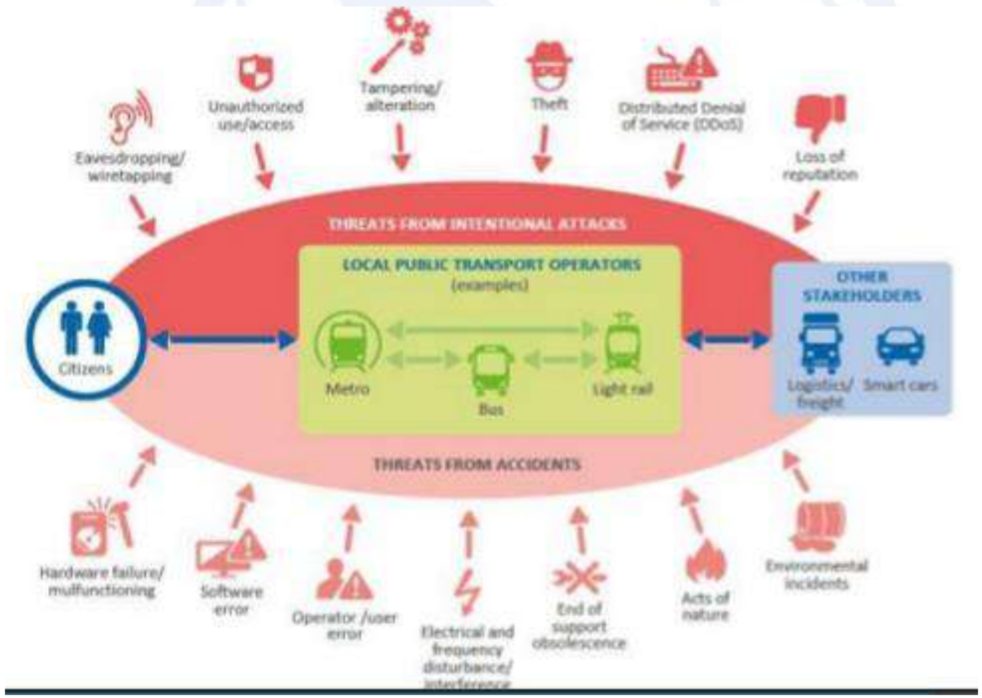
Attack surfaces



Attack surface of the connected car



Attack surface of the intelligent transportation system



Threats at different levels

- Attacks on the entire IoT ecosystem
  - Sensors / devices
  - Network
  - Platforms and services

Security threats to IoT sensors/devices

- **Device capture:** Refers to a device being physically compromised or having its keys lost.
- **Sinkhole attack:** Refers to an attack in which a compromised device attracts communication traffic to form a black hole or introduce selective forwarding.
- **Sybil attack:** Refers to an attack in which a malicious device illegitimately takes on multiple identities.
- **Flooding attack:** A flooding attack is a form of a denial of service (DoS) attack in which an attacker sends a succession of 'hello' packets to a targeted device in an attempt to consume enough of the device's resources to make the device unresponsive to legitimate traffic.

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to IoT sensors/devices

- **Selective forwarding attacks:** In this attack, a compromised node filters randomly received packets and forwards some of them to the next node. If the node filters out (drops) all the packets it receives, it is called a “blackhole” attack.
- **Wormhole attack**: Wormhole attacks occur when two malicious/compromised nodes advertise having a very short path between them.
- **Impersonation of sensor/device:** his attack happens when an attacker successfully masquerades as the identity of a legitimate sensor/device.

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to IoT gateways

- **Unauthorized access:** Unauthorized access to a gateway can cause the disclosure of sensitive information, data modification, DoS and illicit use of resources.
- **Rogue gateway:** Even if all wireless gateways are secure, it is easy for attackers to deploy a rogue gateway of their own. Once a legitimate device is deceived into connecting to a rogue gateway, confidential connection information can be gathered. .
- **Denial of service attack:** The DoS attack causes a target to significantly slow down or, ideally, stop the services it provides by exhausting the target's memory and/or computing capacity

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to the network

- **Unauthorized access:** Unauthorized access to a wireless sensor network can cause disclosure of sensitive information, data modification, DoS and illicit use of resources.
- **Packet sniffing:** For wireless sensor networks that do not have encryption capabilities it is generally easy for attackers to eavesdrop on network communications.
- **Bluejacking:** This as an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to users of Bluetooth-enabled devices.
- **Bluesnarfing:** This attack results in the unauthorized access of information from a targeted wireless device through a Bluetooth connection, often between phones, desktops, laptops, and personal digital assistants (PDAs).

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to platform/services

- **Profiling:** Exploratory process used to gather information on the platform/services
- **Denial of service:** An attack in which the platform/service is overwhelmed by massive service requests and becomes too busy to respond to legitimate client requests.
- **Arbitrary code execution:** An attack that tries to run malicious code on a platform/service to compromise its resources and to then launch additional attacks.
- **Malicious code execution:** Any part of a software system or script, which is intended to cause undesired effects, security breaches, or damage to a system. Typical example includes viruses, worms, and Trojan horses.

Source : Rec. UIT-T X.1361 (09/2018)

Security threats to platform/services

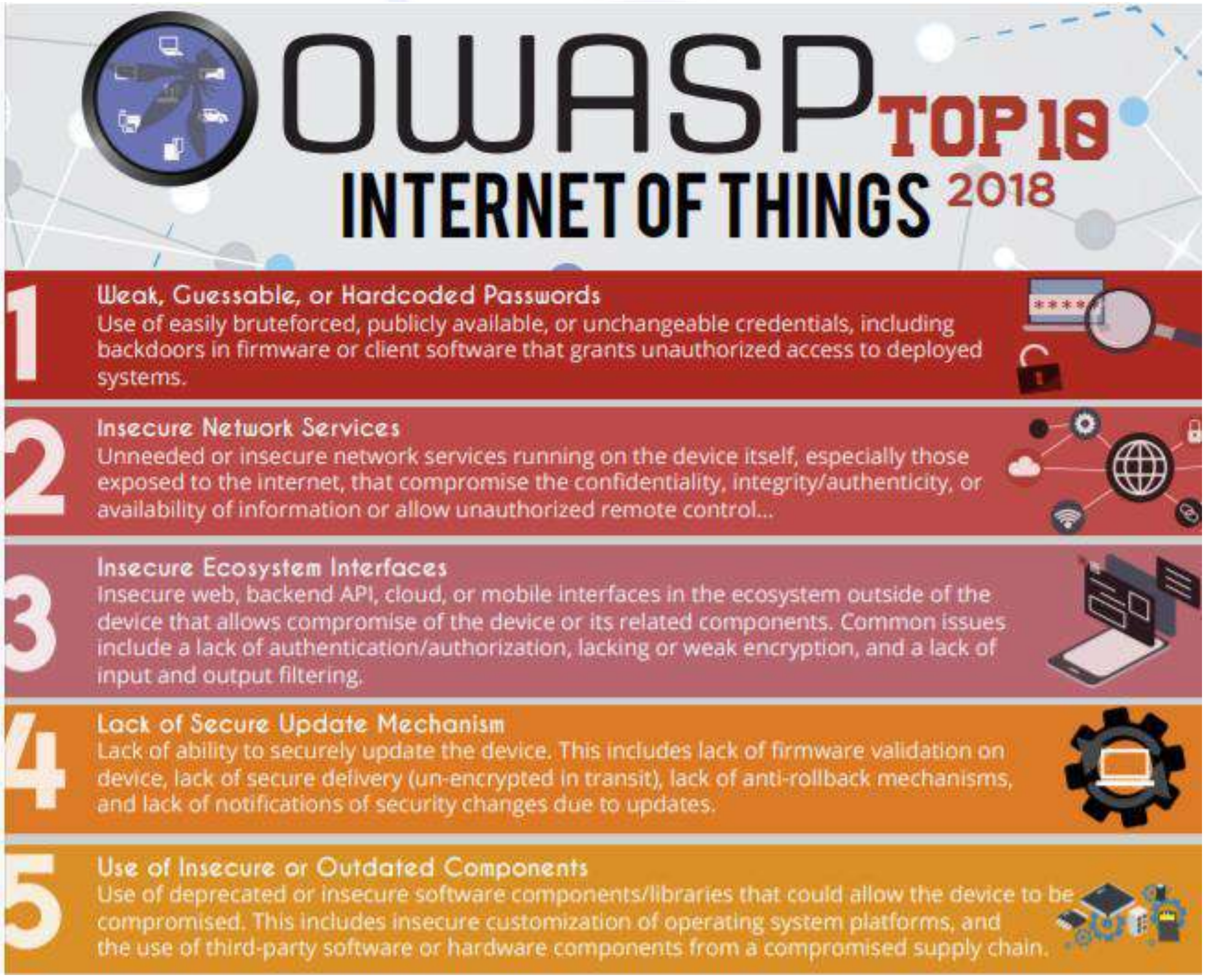
- **Elevation of privileges:** An attack in which code is executed, using a privileged process account, to elevate the attacker's privileges.
- **Structured query language (SQL) injection:** An attack that exploits vulnerabilities in an application's input validation and data access code to run arbitrary commands that inject or extract information.
- **Unauthorized access:** An attack that gains access to a platform/service using someone else's account or another method of access. F
- **Brute force:** An attack that systematically checks all possible keys until a correct one is found.

Source : Rec. UIT-T X.1361 (09/2018)

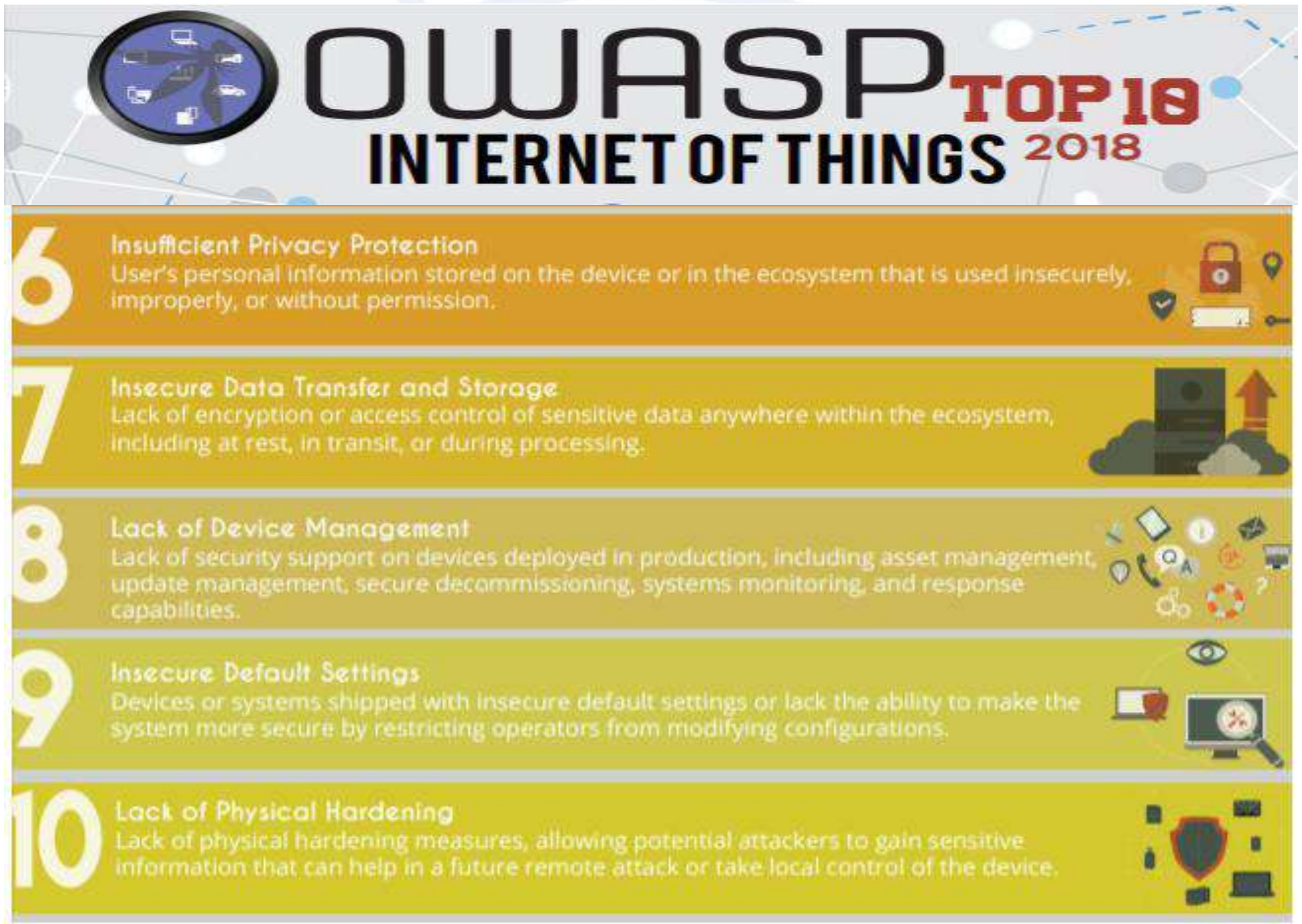
Security threats to platform/services

- **Dictionary attack of usernames/passwords:** An attack that systematically defeats cipher or authentication mechanisms by repeatedly trying passwords, using words in a dictionary.
- **Use of default usernames and passwords/use of weak passwords**: An attack where default usernames and passwords/weak passwords are exploited to gain access to platform/services.
- **Inference attack:** This attack occurs when a user is able to infer protected information from rightfully accessible chunks of information with lower classification

Top 10 Threats (OWASP)



Top 10 Threats (OWASP)



Security measures

- Security of the IoT system can be assessed by employing classical security and risk analysis measures.
- Typical security requirements should be employed in the IoT system:
  - Authentification
  - Confidentiality
  - Integrity
  - Availability
  - Public Key infrastructure

Authentification

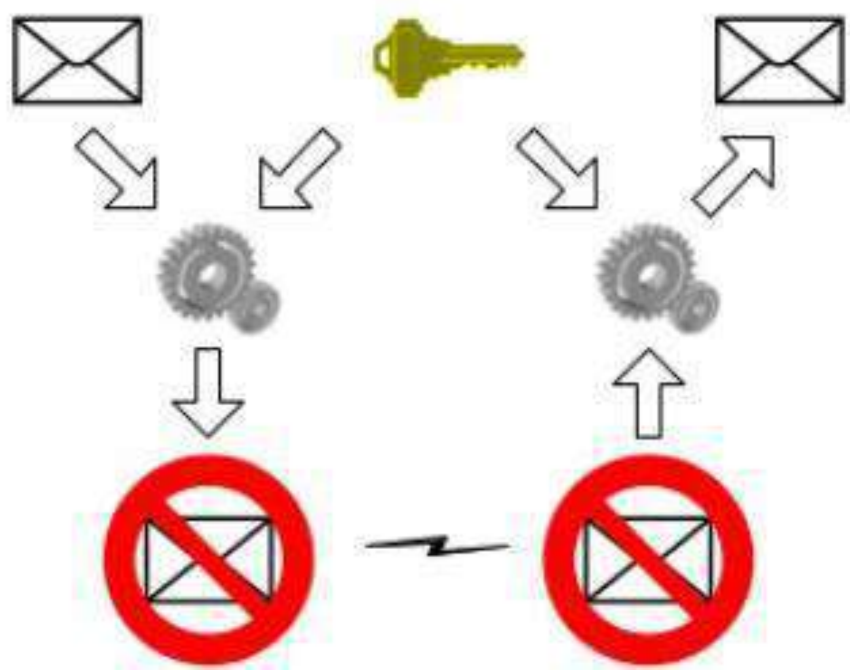
- Many IoT users still use weak and default passwords without any update.
- Manufacturers should ask the customer to update the default one with strong passwords before using the device.

Confidentiality

- Confidentiality is the property whereby information is not disclosed to unauthorized entities.
- Techniques used to ensure confidentiality of data:
  - Data encryption
    - Symmetric encryption algorithms (with secret key): DES, 3DES, AES, RC4, RC4, RC5,…
    - Asymmetric encryption (public and private key): RSA (encryption and signature), DSA (signature), Diffie-Hellman key exchange protocol (key exchange)
    - Hash function: MD5, SHA-1, ...
  - Data Anonymization
  - One way function or hashing
  - …

Encryption with a secret key

Only one key is used to encrypt and decrypt

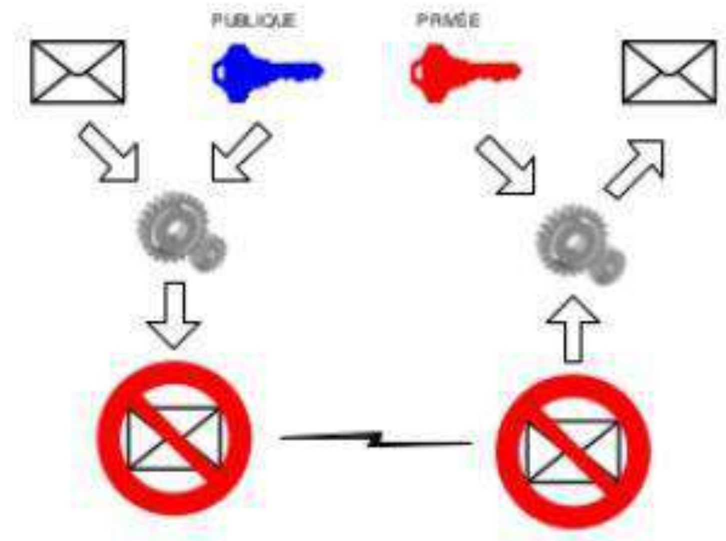


Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

31/3000

Encryption with a private key and a public key

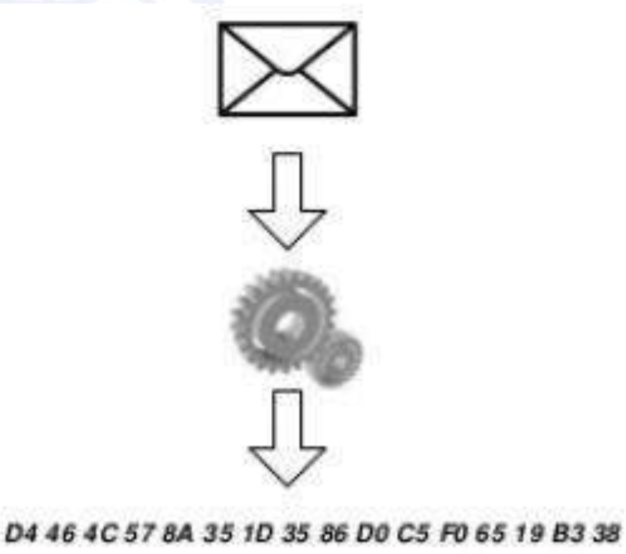
Only one key is used to encrypt and another to decrypt



Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Hash

- Not encryption, but a message fingerprint.
- One-way operation.
- The result is not predictive, 2 different messages will not have the same result.
- Used to verify integrity.



Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Integrity

- Integrity means guaranteeing that data has not been altered since it was created, transmitted or stored.
- Data integrity is very important for IoT systems as the accurate collection of data by sensors is required for the IoT system to function correctly.
- The system should be able to detect any malicious modification.
- Digital signature is a proof of integrity since the hash is protected by the sender's private key

Availability

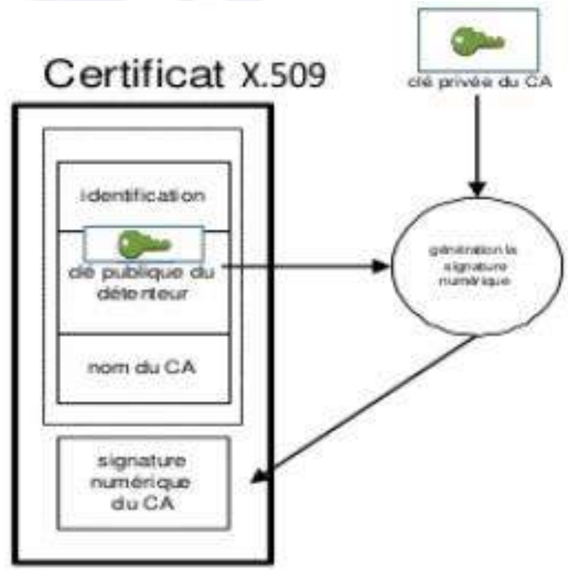
- Availability means that a system needs to be accessible, operational and usable 24/7 or just upon demand by an authorized entity and under all operating conditions.
- Constrained nature of the IoT devices make availability difficult to achieve essentially due to:
  - Mobility
  - Energy limitation
  - Limited connectivity (bandwidth, range, …)
- Classical mechanisms used to ensure high-availability are still valid in an IoT environment (in the cloud side):
  - Load balancing
  - Clustering
  - Duplicating data and systems
  - Automatic and periodic backups
  - Distant data centres
  - Disaster recovery plan
  - …

Public key infrastructure (PKI)

- A **Public Key Infrastructure (PKI) is designed to provide the** trust and the confidence that the used public keys truly belong to the persons (machines) with whom (which) we wish to communicate.
- PKI is built around a data element called **Digital Certificate or** public key certificate which binds a public key to its holder
- Digital Certificate is an **authentication technology that can be** delivered to
  - Persons
  - Organisations
  - Devices
  - Software solutions
- It binds a public key to information about its owner
- Digital certificates can be used for system, network and application authentication
- ITU-T X.509 v3 is the standard of the public key certificates

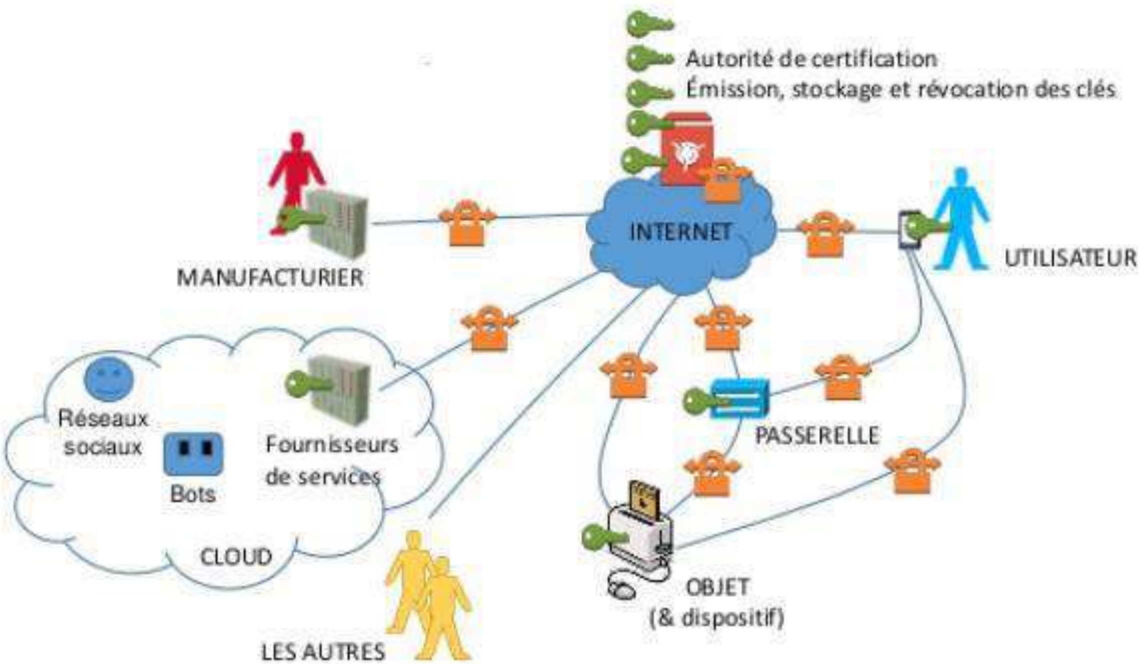
Public key infrastructure (PKI)

Autorité de certification
Émission, stockage
et révocation des clés



Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Encryption, key, and PKI



Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Regulations for IoT security

- Regulations for IoT security should make use of inputs from consumers as well as industry representatives on the rights and responsibilities of consumers and vendors.
- There are only a few legislative efforts aimed at IoT security.

U.S. IoT Cyber Security Improvement Act

- This legislation defines the security standards applicable to IoT equipment installed on the networks of the US administration.
- It aims to guarantee the protection and the absence of equipment vulnerabilities, the conformity of products with sectoral standards as well as the possibility of applying patches to them.
- Suppliers are prohibited by law from selling equipment whose passwords cannot be changed.
- The legislation would also require US agencies to establish and maintain inventories of IoT devices and to update them every 30 days.

Law no° 327 of California

- California Law n° 327, approved in September 2018, came into effect in January 2020.
- It requires that all connected devices must have "reasonable" security features to prevent unauthorized access, modification, or data exposure.
- In addition, if the device features a password, it must either be unique to that device or force the user to set their own password during initial setup, thus preventing cyberattacks through guessing default passwords.

Law no° 327 of California

- It places liability and responsibility directly on the IoT vendors, no matter where the device was purchased or manufactured, so long as the device is connected to the internet in California.
- Using a “reasonable” security features is no longer an option. If anything goes wrong with the device, it might get to court and manufacturers will bear the burden of proof.
- Therefore, it is highly advisable for manufacturers to take the extra mile and look out for new and advanced cybersecurity solutions.

EU cybersecurity law

- In December 2018, the EU adopted the Cybersecurity Law to strengthen the mandate of the European Agency ENISA to better support Member States fighting against cybersecurity threats and attacks.
- This law establishes a European framework for cybersecurity certification, cybersecurity of online services and consumer devices.
- Certification is voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to meet a specific security need.

Source : https://www.allot.com/blog/new-iot-security-regulations-what-you-need-to-know/

NIS Directive

- The Network and Information Systems Security Directive was adopted by the European Parliament on July 6, 2016 and entered into force on August 2016.
- The NIS Directive provides legal measures to increase the general level of cybersecurity in the EU by ensuring:
  - The state of readiness of Member States by requiring them to be appropriately equipped eg. via an IT Security Incident Response Team and a National NIS Authority.
  - Cooperation between all Member States, through the establishing a Cooperation Group, to support and facilitate strategic cooperation and exchange of information between Member States.

Part 2: Privacy and legislation

Privacy and personal data

- The IoT growth continues to add billions of new sensors and devices to the Internet, generating an enormous amount of data.
  - 30 billion gigabytes of data in 2020, 10 times more than in 2013.
  - 50,000 gigabytes of data created per second in 2020 compared to 100 gigabytes in 1992.
- These data is about people, including their locations, connections, shopping records, financial transactions, pictures, voices, conversations, health state, etc., with or without their consent.

Privacy and personal data

- Ability to preclude personal data from being shared or communicated to non authorized entities
- Ability to know what are the sensitive changes performed on your personal data over time.
- **Personal data** refers to data about an individual who can be identified from that data.
- Classification of personal data:
  - Identifiers (SSN, Passport number, Credit card number, …)
  - Quasi-identifiers (Age, Sex, Zip Code, …)
  - Sensitive data (Illness, financial asset, …)
  - General information (Feeling, …)

Source: https://fr.slideshare.net/TactikaComInc/scurit-de-liot-internet-des-objets-formation-dune-journe

Attack on access control systems

- Hacking of connected locks (home automation) through object or cloud vulnerabilities.

Google Glass

- Google Glasses were not marketed because of the privacy breach.
- In the blink of an eye, malicious people can film people without their knowledge and disseminating the footage worldwide via YouTube and social networks.

Baby monitor hacked

Very nice words uttered by a hacker to the attention of a 2 year old girl after taking control of the family baby monitor

Pacemaker hacked

- A pacemaker can be hacked, with potential dangers to the health of patients.

- Le point commun entre un pacemaker et une pompe à insuline ? Ils ont tous deux été piratés
- Pacemaker : possibilité de l'éteindre ou d'envoyer une décharge de 830 volts
- Pompe à insuline : Prise de contrôle via WiFi, possibilité de la transformer en arme létale !

Atteinte aux biens et aux personnes

Liability

- Autonomous car is dedicated to act alone and under its own responsibility
  - Ex Google Car: What about the responsibility for the accident?
- The connected object performs actions that lead to the issue of liability.

IoT product liability

- The question of responsibility has become an imperative with the explosion of connected objects.
- Connected objects can make decisions autonomously and without human intervention.
- In case of damage caused by a connected object, a complaint by a third party could result in a dismissal.

→There is a need to develop a legal framework of responsibility specific to connected objects and legal texts that adapt to the nature of objects and their evolution, and define without a shadow of doubt the responsibility of the user or the manufacturer of a connected objects in case of failure.

Privacy threats

- The potential risk of losing control over personal information is defined as a privacy threat.

Identification

- Identification is the threat of relating an identifier (e.g., name, address) with an individual or private data about him.
- The use of a surveillance camera, in non-security contexts, is an example of such techniques, where customers' behavior is studied for analysis and marketing.
- As facial databases (e.g. from Facebook) become available also to non-governmental parties like marketing platforms, automatic identification of individuals from camera images is already a reality.
- To address this issue, attribute-based authentication is recommended to minimize the data a device can collect and maintain control over the disclosure of data.

Privacy threats

Localization and tracking

- Localization and tracking are the threats of specifying and recording a person's location through time and space by different means such as cell phone location, Internet traffic or GPS data.
- Many concrete privacy violations have been identified related to this threat, e.g. GPS stalking, disclosure of private information such as an illness, or generally the uneasy feeling of being watched.

Privacy threats

Profiling

- Profiling is the process of collecting and processing data about individuals' activities and actions over long periods to classify them according to some feature.
- The information is usually collected without permission from users and integrated with other personal data to create a more complete profile.
- Profiling is currently used in a large range of domains, for example, e-commerce, targeted advertising and credit scoring. One of the risks associated with profiling is that personal information may be exposed to other users. Moreover, many users are disturbed by the mere awareness of being watched and tracked.

Privacy threats

Linkage

- Linkage threat refers to uncontrolled disclosure of information due to combining separated data sources and linking different systems.
- Integrating various types of information about the individual reveals new facts which are not expected by the owner.
- The revealed information is considered a privacy breach.

Privacy-Preserving Solutions for IoT

Privacy by Design

- Security by design is a novel approach suggested by several organizations to implement required security measures in the software and hardware development life cycle and not after detecting a security breach.
- The necessity to adopt security by design becomes essential to protect billions of IoT devices that are poorly secured against common security attacks.
- Security by design aims to protect the security of devices by the manufacturers. Security by design can help the user to understand IoT security requirements and encourages them to make the right decisions to ensure their security and safety.

Privacy-Preserving Solutions for IoT

- Privacy Awareness/informed consent transparency: IoT users have to be fully aware of how to keep themselves protected against any types of privacy threats. IoT users should give their consents about data usage, storage and processing.
- Data Minimization: IoT service providers should employ the concept of data minimization by limiting personal data collection to only what is related to the service they introduce. They also need to retain the data only if they need it for the service.

Privacy-Preserving Solutions for IoT

- Data anonymization consists of removing Personally Identifiable Information (PII) from data sets so that the people whom the data describe remain anonymous.
- According to the National Institute of Standards and Technology (NIST), PII are :
  - National identification number, Social security number, Passport number, Vehicle registration plate number, Driver's license number, Credit card numbers, Home address, Telephone number, Email address, and IP address, Face, fingerprints, or handwriting, Digital identity, Genetic information, Login name, screen name, nickname, …

Privacy legislation

- Privacy legislation tries to define mandatory practices and processes for privacy protection.
- Privacy is recognized as a fundamental human right in the 1948 Universal Declaration of Human Rights and is anchored in the constitutional law of most countries.
- They have been taken by the Organization for Economic Co-operation and Development (OECD), which anticipated trade barriers from the increasingly diverse national privacy legislation.
- Two types of regulatory initiatives :
  - Sectoral initiatives, led by industrial players wishing to establish a regulatory framework for their sectoral activities.
  - Interventions by public authorities in areas requiring arbitration between stakeholders (industrialists, civil society, etc.).

EU GDPR regulation

- The General Data Protection Regulation (GDPR) entered into force on 25 May 2018, it is now the reference text for the protection of personal data for the EU.
- The GDPR aims to strengthen the rights of those concerned by data processing and to increase the liability of companies responsible for processing personal data.
- This regulation applies to any business that processes data relating to EU residents, whether established within or outside the EU.
- Thus GAFAs or any companies that address the European market are affected by this regulation.

EU GDPR regulation

- Experts agree that there are several requirements in the GDPR that may have implications on the IoT industry.
  - Companies must conduct **Data Protection Impact Assessments (DPIAs)** when data processing is likely to result in a high risk to the rights and freedoms of natural persons.
  - Companies dealing with personal data must be **able to identify and deal with security breaches**, in addition to **creating a mandatory notification system in the event of any breaches of personal data**.
  - **Individual's consent be obtained to process their personal data.**
  - Data subjects have a right, at any time, to be informed about **how their personal data is used, where it is stored and to whom it is disclosed**

The 6 GDPR principles

Source : https://gdpr-info.eu/art-5-gdpr/

US Regulation

- Data protection in the US is "sectorial" covering specific areas of data protection (e.g., health care) rather than personal data protection in general as in the EU.
- US Federal Trade Commission's privacy and security recommendations are based on the **Fair Information Practice Principles (FIPPs):**
  - **Choice and notice** states that entities that collect data should give users the option to choose what they reveal and notify users when their personal information is being recorded.
  - **Purpose specification and use limitation** states that entities collecting data must clearly state the purpose to the authority that permits the collection of those data.
  - **Data minimization s**uggests that a company can collect only the data required for a specific purpose and delete that data after the intended use.
  - **Security and accountability s**tates that entities that collect and store data are accountable and must deploy security systems to avoid any unauthorized access, modification, deletion, or use of the data.

Reinforcing regulatory power

- Many data-protection laws contain mechanisms for risk assessment and mitigation, including privacy impact assessments and data protection by design.
- Perfect compliance in a complex IoT system will likely be impossible, but the increasingly strong accountability of data-protection laws might encourage regulators to use their powers to promote a more privacy-aware IoT.
- Also, trends are toward increased regulatory powers; for example, for many breaches of GDPR, regulators can impose penalties up to the greater of €20 million or 4 % global annual turnover. The prospect of severe penalties combined with high regulatory uncertainty could have a chilling effect on the IoT.

Part 3:
High-level guidelines, Code of practices and Certifications

Standardisation activities relevant to IoT security

- While numerous standards exist in the IoT domain, **IoT security has not been standardized significantly until now**.
- Several sets of initiatives IoT were proposed to compensate the lack of standards. The initiatives came from:
  - **IoT-focused groups** formed by SDO, such as ETSI, ITU and IETF;
  - **Professional bodies** such as the Industrial Internet Consortium (IIC), the IoT Security Foundation (IoTSF), and the Cloud Security Alliance.
  - **Governmental initiatives** such as NIST, ENISA, and the Alliance for IoT Innovation (AIOTI).
  - **Alliances** focused on networking standards, such as GSMA.

Standards relevant to IoT security

Formal Standards Relevant to IoT Security

ISO/ IEC JTC 1/ SC 41
- IoT Reference Architecture
- IoT Interoperability: Framework

ISO/ IEC JTC 1/ SC 27
- Information Security Management
- Security Assurance Framework
- Framework for Identity Management
- Entity Authentication
- Key Management

ISO 31000
- Risk Management

ISO 28000
- Supply Chain Security

ISO 10377
- Consumer Product Safety

oneM2M
- Security TS 0003
- Security Solutions TS 0008
- End-to-End Security & Group Authentication TR 0012

Code of practices relevant to IoT security

Industry Association & Guidelines	Compliance Testing	Certification
Open Web Application Security Project (OWASP) Principles of IoT Security IoT Security Guidance	IoT Framework Assessment IoT Testing Guides IoT Testing Methodology	N/A
Online Trust Alliance (OTA) IoT Security & Privacy Trust Framework	Online Trust Audit	Honour Rolls
Cloud Security Alliance (CSA) New Security Guidance for Early Adopters of the IoT Future Proofing the Connected World	Cloud Control Matrix Consensus Assessments Initiative Questionnaire	CSA STAR self-assessment, 3rd party, or continuous monitoring certification
Broadband Internet Technical Advisory Group (BITAG) Internet of Things Security and Privacy Recommendations	N/A	N/A
Open Connectivity Foundation (OCF) Security Specifications	OCF Testing and Certification Program	OCF Certification Mark
GSM Association (GSMA) IoT Security Guidelines for: - Endpoint Ecosystems - Network Operators - Service Ecosystem	IoT Security Assessment Checklist Self-Assessment Scheme	Once IoT Security Assessment is approved, product is listed on GSMA IoT website.
IoT Security Foundation (IoTSF) Connected Consumer Products Best Practice Guidelines Vulnerability Disclosure Best Practice Guidelines	IoT Security Compliance Framework	Best Practice User Mark
Industrial Internet Consortium (IIC) Industrial Internet Security Framework	Security Checklists for Verticals Maturity Models for Industrial Systems	N/A

GSMA Security guideline

- The GSMA has created a guideline for the benefit of service providers who are looking to develop new IoT services.
- The guideline allows providers of IoT services and products to self-assess the compliance of their products, services and components with GSMA IoT security guideline.
- The assessment ckecklist allows entities to demonstrate the security measures they have taken to protect their products, services and components from cybersecurity risks.
- Assessment statements can be made by submitting a completed statement to the GSMA.
- According to GSMA, providing secure products and services is a process rather than a goal.

Source : https://www.gsma.com/iot/iot-security/iot-security-guidelines/

OTA

- **Online Trust Alliance (OTA)** is a comprehensive set of strategic principles that help secure IoT devices and their data.
- It is built on the basis of a collaborative process.
- The framework provides recommendations that all IoT manufacturers should adopt to improve the security, transparency and communication capabilities of their devices, as well as data privacy issues.

AIOTI Recommandations

- The basic AIOTI (Alliance for IoT Innovation) requirements for IoT devices include:
  - Testing and Certifying security - Using proven certifications to assess device security based on the asses risk risk level.
  - Security Labels - Proven labels such as "energy efficiency label" of appliances in order to classify the IoT devices.
  - Preset and certified security structures – Encryption Requirement for identities, access, communication channels, and secure storage of keys and data.

AIOTI Recommendations

- **Security Rational** - Explanation of implementation of security measures related to well understood hazards in order to define an acceptable level of security risks from any IoT device designer, auditable by an independent third party.
- **Information Exchange** - Sharing of information between manufacturers about incidents and potential vulnerabilities.
- **Defined Functions** - IoT devices should be able to perform documented functions, to make sense of IoT devices and services.
- **Standardization** - Interoperability of components and communication protocols.

IoTSF Security compliance framework

- **IoT Security Foundation (IoTSF)** implemented an IoT Security Compliance Framework aimed at assessing the security of a wide range of IoT devices by adopting a risk-based approach derived from the triad CIA.
- The framework defines 5 classes of conformity. The class of a product is defined on the basis of a requirements checklist. This checklist could be made compulsory by the contracting parties in order to verify compliance with the requirements.

Compliance class	Security objectives		
	Confidentiality	Integrity	Availability
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoTSecurity-Compliance-Framework.pdf

IoT Certification

- Lack of trust marks and certificates that can inform consumers about the security and risks of IoT devices.
- Efforts are underway in various parts of the world to create certification schemes.
- It should be ensured that these schemes are aligned in order to create fair competition conditions for manufacturers.

EU cybersecurity certification framework

- The EU has proposed a certification framework for IoT security products.
- The certificate, recognized by all Member States, allows companies to market their products across borders, and enables buyers to understand the safety features of the product or service.
- This framework provides a comprehensive set of rules, technical requirements, standards and procedures.
- ENISA is in charge of implementing the certification process.
- The use of certification is voluntary at this time.

Conclusion

- Manufacturers may not have the expertise to use the guidelines and recommendations available.
- The usability of the safety guidelines is a challenge and requires more research.
- Harmonization of IoT security guidelines and recommendations are needed to drive adoption.
- Harmonization needs to be supported by cybersecurity research initiatives.

Thank you!

PRIDA Track 1 (T1)

Spectrum and IoT Technologies

09/09/2020

Agenda

- Part 1: Short-range technologies
- Part 2: Spectrum and mobile & satellite technologies
- Part 3: IoT protocols
- Part 4: Standardization activities
- Part 5: Roaming

Part 3: IoT Protocols

TCP/IP Model

- IoT uses existing Internet protocols and introduces new ones.

Current Internet Protocols	Protocol Level TCP/IP Model	Expected IOT Protocls
HTTP FTP,SMTP,IMAP	Application	MQTT COAP,AMQP
TCP and UDP	Transport	UDP and TCP
IPv4 and IPv6	Networking	IPv6 and IPv4
Ethernet,Wi-Fi, GSM	Data Link	Ethernet,Wi-Fi, GSM, LTE-M, Lora, SigFox

TCP/IP Model

- The IoT application allows connected objects to send their data to a web server or a cloud platform.
- The Transport layer enables communication and protects data as it flows between layers.
- The Network layer allows individual devices to communicate with the router.

IoT protocol stack

Application Protocol		DDS	CoAP	AMPQ	MQTT	MQTT-NS	XMPP	HTTP REST
			DTLS					TLS
Service Discovery		mDNS				DNS-SD		
Infrastructure Protocols	Routing Protocol	RPL						
	Network Layer	6LoWPAN				IPv4/IPv6		
	Link Layer	IEEE 802.15.4						
	Physical Layer	LTE-A	EPCglobal		IEEE 802.15.4		Z-Wave	
Influential protocol		IEEE 1888.3, IPSec			IEEE 1905.1			

Application layer protocols

- The protocols of the application layer allow transmission of commands from user applications to actuators of connected objects.
- The classic web infrastructure is not suitable for the majority of IoT applications that use constrained resources (small microcontrollers, limited RAM memory, limited power, etc.)
- Application protocols that use a limited number of small messages are used for IoT applications, and are classified into 3 families:
  - Web transfer protocol: Web REST, COAP
  - Messaging protocol: MQTT, XMPP and AMQ.
  - Network protocol: Websocket

Web REST services

- Web REST (Representational State Transfer) is a based on a client/server web architecture that allows to manage, identify, and manipulate resources.
- Sensors, actuators and control systems in general can be represented as resources and thus can provide their services through a RESTful web service.
- The importance of REST stems from the simplicity of the communication and the fact that it is comprehensive: any web service can be realized with the REST architecture.
- REST is supported by all M2M Cloud platforms.

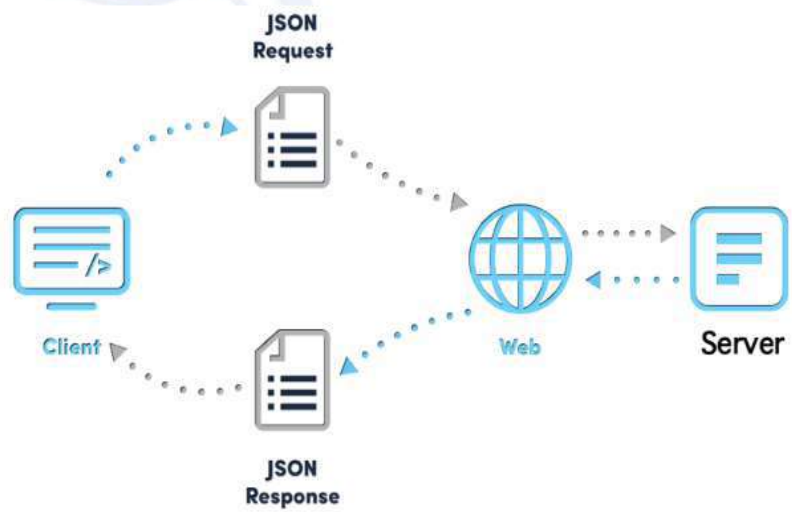
Web REST services

- Web REST is an application programming interface that uses HTTP requests with the {GET, PUT, POST, DELETE} methods to request a web service.

Méthode	Action
«GET»	Cette méthode récupère la représentation de l'information correspondant à la ressource identifiée par la requête URI.
«POST»	Cette méthode demande le traitement de la représentation jointe à la ressource identifiée par la requête URI. Normalement cela aboutit à la création d'une nouvelle ressource ou de sa mise à jour.
«PUT»	Cette méthode demande que la ressource identifiée par la requête URI soit mise à jour avec la représentation jointe. Le format de la représentation est spécifié par le type de media et le codage contenu dans l'option Content-Format, si fournie.
«DELETE»	Cette méthode demande que la ressource identifiée par la requete URI soit supprimée.

Web REST services

- Each resource is defined by a unique URI (Uniform Resource Identifier).
- REST uses several formats to represent resources: Text, JSON, XML. JSON is the most used format.

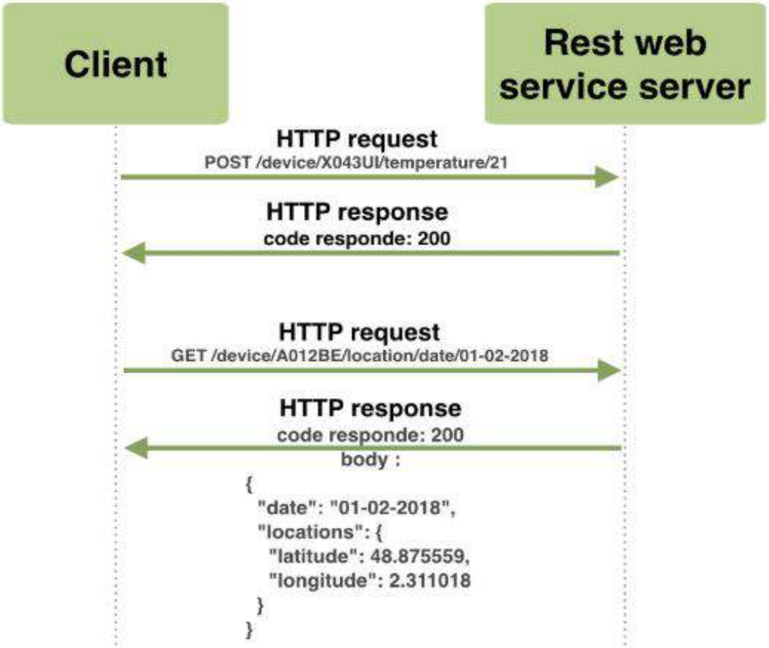


Source: Pietro Manzoni. Intro to MQTT. Workshop on Rapid Prototyping of IoT for Science (smr3268) – January 2019

Web REST services

URI	Méthode	Signification
/device/:device/temperature/:temperature	POST	Effectuer un POST en spécifiant, pour l'objet `:device`, une nouvelle valeur de température `:temperature` en °C
/device/:device/location/date/:date	GET	Effectuer un GET pour obtenir la position GPS d'un objet `:device` à une date donnée `:date`

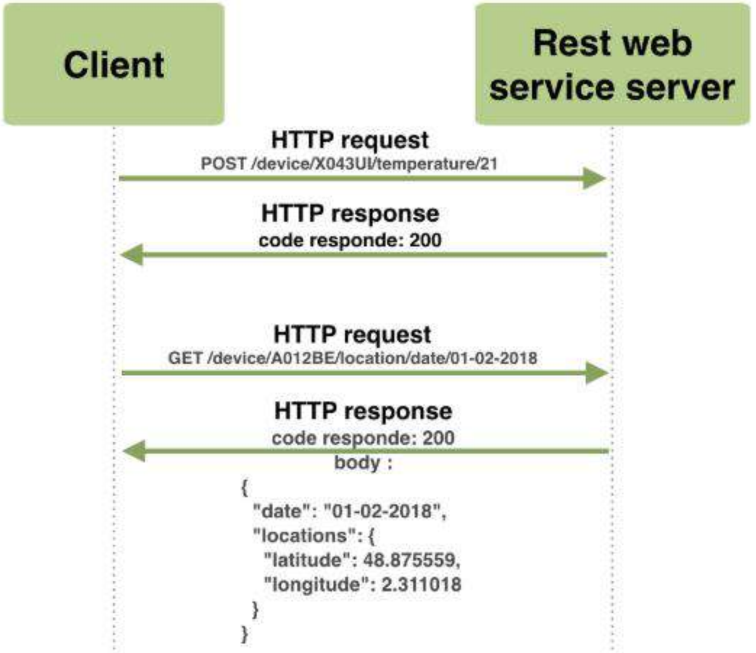
- The client sends a POST request to indicate to the server a new temperature value of 21 ° C, for the object X043UI.
- The server responds with a code of 200 to indicate that everything is OK.
- The client sends a GET request to request the location of the object A012BE on the date of 01-02-2018.
- The server responds by sending the coordinates.



Source: https://blog.engineering.publicissapient.fr/2018/04/16/internet-des-objets-quels-protocoles-applicatifs-utiliser-1-2/

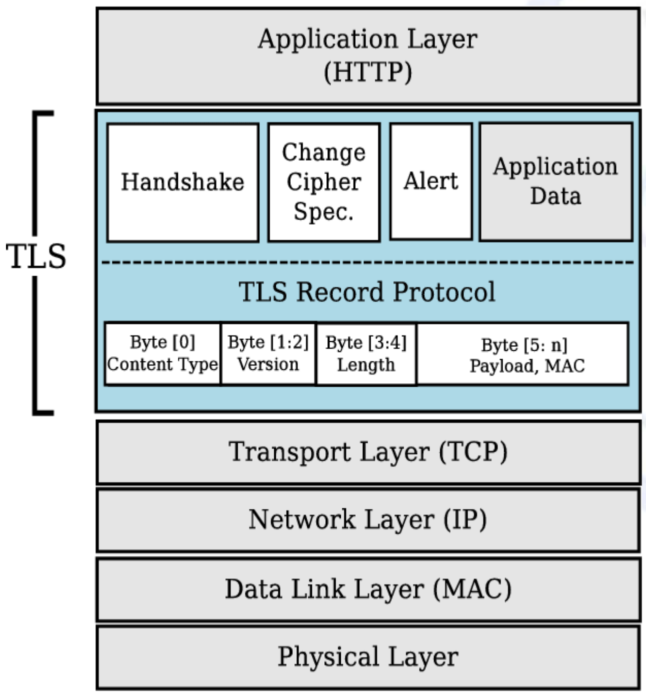
Web REST services

- The server adds a three-digit HTTP response code to indicate the status of the response in the following form:
  - 2xx indicates successful processing of the customer's request (example: 200 for OK)
  - 3xx redirects the client to another link
  - 4xx indicates a fault in the client's request (example: 404 for Not Found)
  - 5xx indicates an error on the server side (example: 500 for Internal Server Error)



Source: https://blog.engineering.publicissapient.fr/2018/04/16/internet-des-objets-quels-protocoles-applicatifs-utiliser-1-2/

TLS

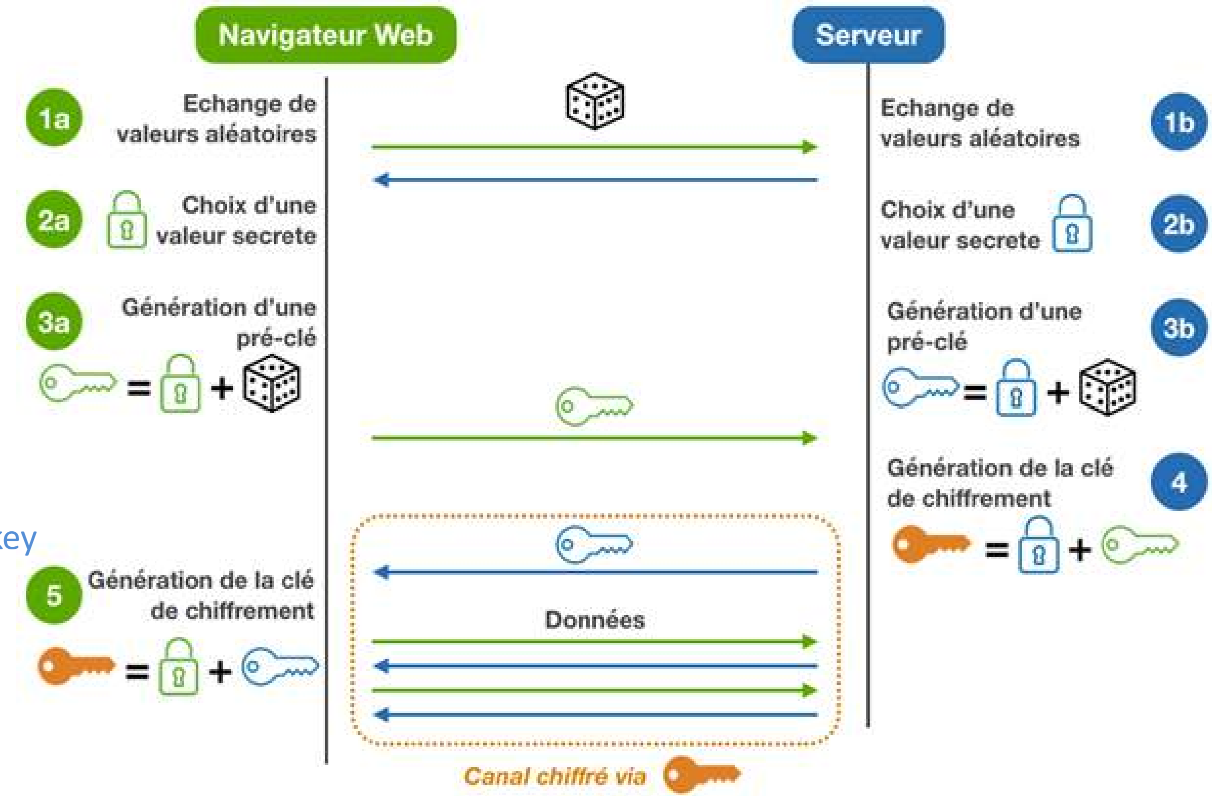


- The messages exchanged through TLS are called records and are encapsulated in datagrams.
- There are four types of records:
  - Handshake messages.
  - Alert type messages provide errors and their severity: warning or fatal.
  - Change Cipher Spec type messages indicate the change of cryptographic suites in the exchanges.
  - Application data messages correspond to crypted and compressed data.

TLS

5 Steps:

- Random value exchange
- Choice of a secret value
- Generation of a pre-key
- Generating the encryption key



CoAP

IETF Standard – RFC 7252

- IETF CoAP (Constrained Application Protocol) is a web protocol based on a client / server architecture.
- CoAP is a lightweight version of REST designed for UDP communications. It is intended for use on low power electronic devices.
- CoAP requests are equivalent to those of HTTP: a client sends a request to a server to request a service from a resource, identified by URI.
- HTTP is based on the TCP / IP suite while CoAP is based on UDP / IPv6 / 6LoWPAN.

Source: http://www.efort.com/r_tutoriels/COAP_EFORT.pdf

CoAP

- CoAP uses the HTTP {GET, PUT, POST, DELETE} methods.
- CoAP uses URIs to identify resources
- CoAP messages are smaller (4 bytes) than HTTP messages (variable).
- CoAP uses four types of messages:
  - Confirmable (CON): Message sent with a request for receipt acknowledgment.
  - Non-Confirmable (NO): Message sent without request for receipt acknowledgment.
  - Acknowledgment (ACK): Receipt acknowledgment of the CON message type.
  - Reset (RST): Receipt acknowledgment of a message that cannot be used.

CoAP

- The client (object) sends a CoAP request, on a resource identified by a URI, to the server by specifying: the type of message (CON, NON), the identifier of the message (mid) and an action (POST, GET, PUT , DELETE).
- The meaning of the response code is as follows:
  - 2.xx : the request was correctly received and processed
  - 4.xx : an error was encountered by the customer
  - 5.xx : the server is not able to process the request

CoAP response versus HTTP code

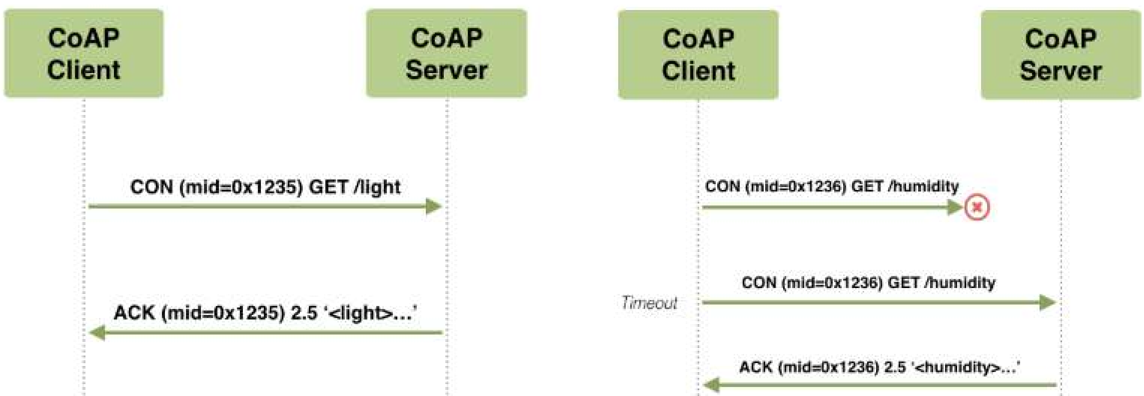
CoAP Status Code	Description
2.01	Created
2.02	Deleted
2.03	Valid
2.04	Changed
2.05	Content
2.31	Continue
4.00	Bad Request
4.01	Unauthorized
4.02	Bad Option
4.03	Forbidden
4.04	Not Found
4.05	Method Not Allowed
4.06	Not Acceptable
4.08	Request Entity Incomplete
4.12	Precondition Failed
4.13	Request Entity Too Large
4.15	Unsupported Content-Format
5.00	Internal Server Error
5.01	Not Implemented
5.02	Bad Gateway
5.03	Service Unavailable
5.04	Gateway Timeout
5.05	Proxying Not Supported

HTTP Status Code	Description
1xx	Informational
2xx	Successful 200 – OK 201 – Created 202 – Accepted 204 – No Content
3xx	Redirection 301 - Moved Permanently 305 - Use Proxy 307 - Temporary Redirect
4xx	Client Error 400 – Bad Request 401 – Unauthorized 403 – Forbidden 404 - Not Found 405 – Method Not Found 408 – Request Timeout
5xx	500 – Internal Server Error 501 – Not Implemented 503 – Service Unavailable 504 - Gateway Timeout

Only mostly used HTTP Status Codes are listed here

CoAP

- If the request type is CON then the server returns a response which contains : the message type ACK, the same mid as that of the request, a response code (2.xx, 4.xx or 5.xx), and a representation of the resource.



Source: https://blog.engineering.publicissapient.fr/2018/04/16/internet-des-objets-quels-protocoles-applicatifs-utiliser-1-2/

DTLS

- CoAP cannot use SSL/TLS to provide security (as this requires the TCP transport layer).
- The DTLS (Datagram Transport Layer Security) standard, which operates over UDP, can be used, and this provides the same assurances as TLS.
- DTLS provides a layer of security for applications using datagram-based protocols like CoAP.
- DTLS-enabled CoAP devices will typically support ECC and AES or RSA and AES.

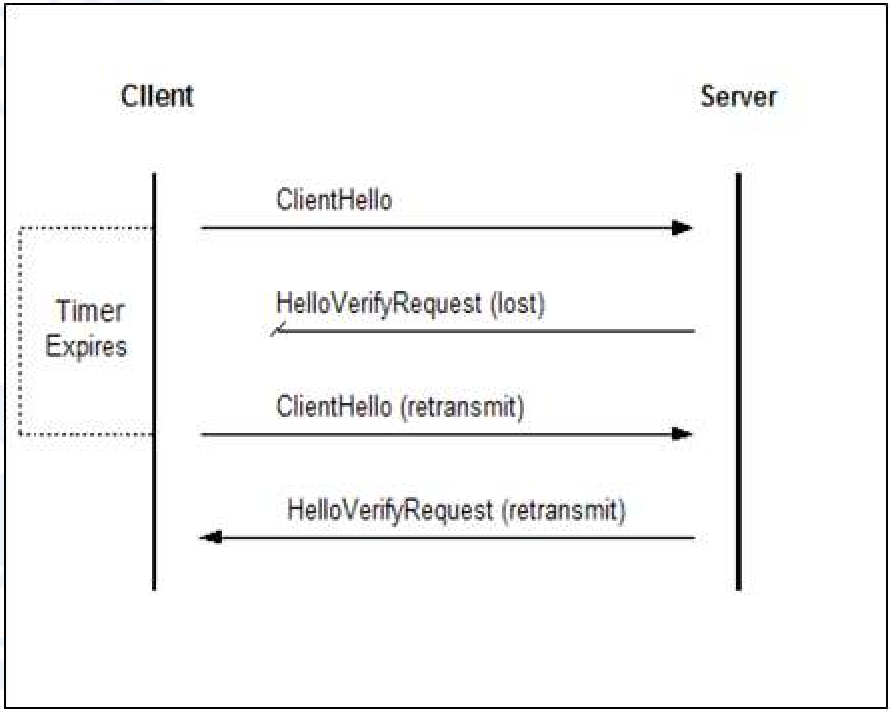
DTLS

DTLS uses a simple retransmission timer:

- The client expects to see the HelloVerifyRequest message from the server.

- If the timer expires, the client knows that ClientHello or HelloVerifyRequest has been lost

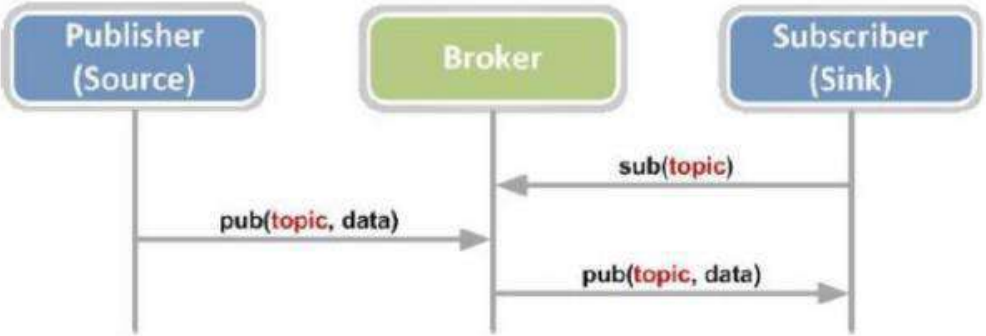
- Retransmits.



MQTT

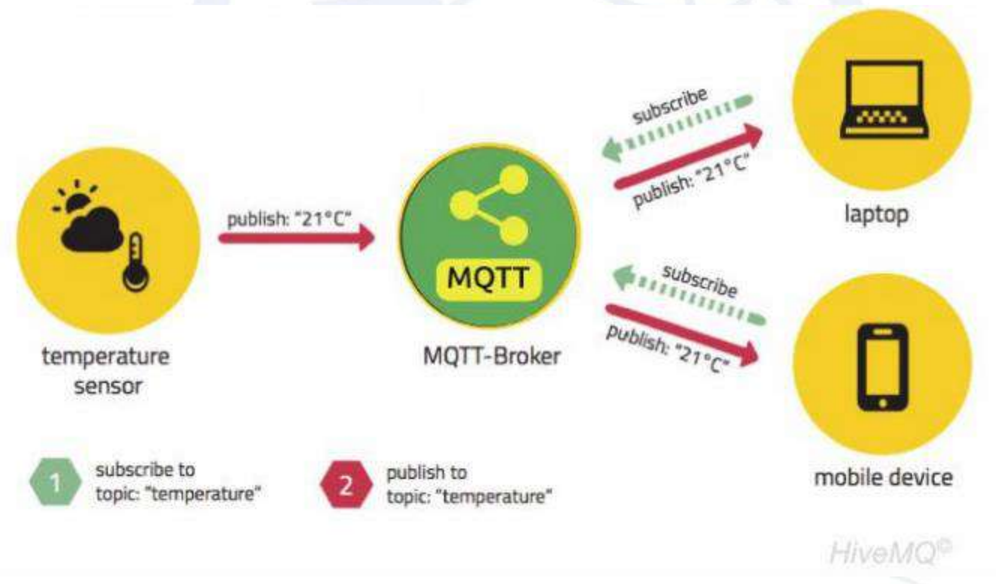
- MQTT (Message Queuing Telemetry Transport) is a messaging protocol based on the publish / subscribe approach.
- The publish/subscribe approach classifies messages by categories (topics) to which recipients subscribe (subscriber).
- The client who sends a message (topic) is named publisher, the one who receives the message is named subscriber.

- An element of the network called a broker, known to the publisher and the subscriber, filters the messages received and distributes them.
- MQTT is based on the TCP / IP protocol.



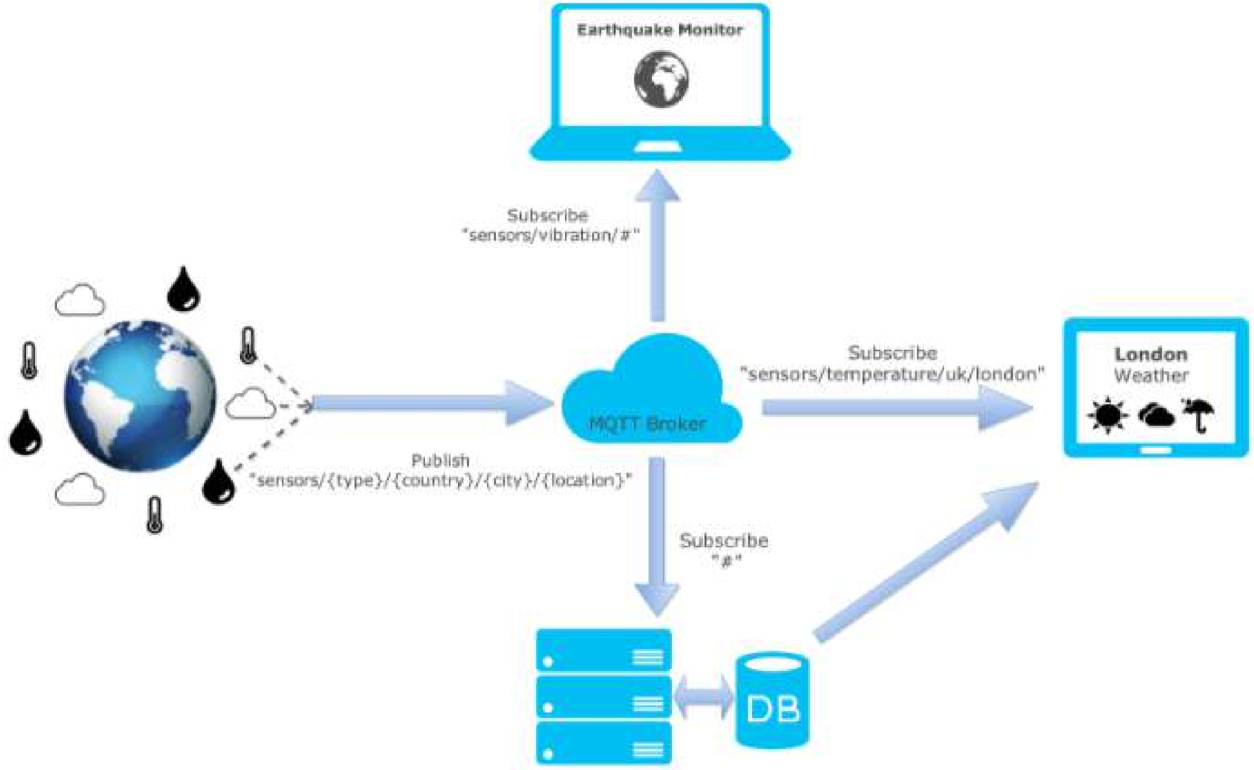
Source : Antonio Linan Colina et al. Internet of Things in 5 days-v1.1 2016

MQTT



publish: "21°C"
subscribe
publish: "21°C"
subscribe
publish: "21°C"
MQTT
temperature sensor
MQTT-Broker
laptop
mobile device
1
subscribe to topic: "temperature"
2
publish to topic: "temperature"
HiveMQ©

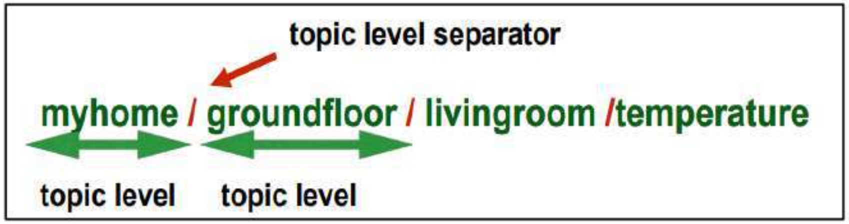
MQTT



Source: https://zoetrope.io/tech-blog/brief-practical-introduction-mqtt-protocol-and-its-application-iot/

MQTT

- MQTT topics are structured in a hierarchical approach.
- The topics can be generic: possibility of making subscriptions to topics which are not yet defined.
- "+": Corresponds to a given level
- "#": Corresponds to the whole tree structure



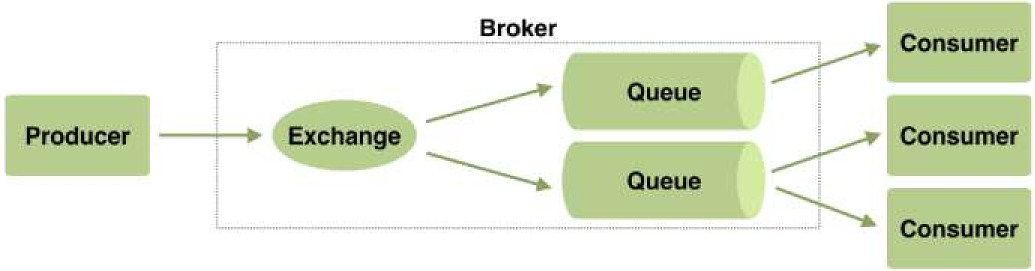
- Exemple:
  - The subscription to the topic house# covers :
    - house/room1/main-light
    - house/room1/alarm
    - house/garage/main-light
    - house/main-door
  - The subscription to the topic house/+/main-light covers :
    - house/room1/main-light
    - house/room2/main-light
    - house/garage/main-light

MQTT

- MQTT is a protocol suitable for IoT networks because it meets the following needs:
  - Suitable for low bandwidth networks;
  - Ideal for use by wireless networks thanks to the limited number of small messages;
  - Low energy consumption because the publication and consumption of messages is fast;
  - Requires few calculation and memory resources;
  - Transmits a message to multiple entities in a single TCP connection.

AMQP

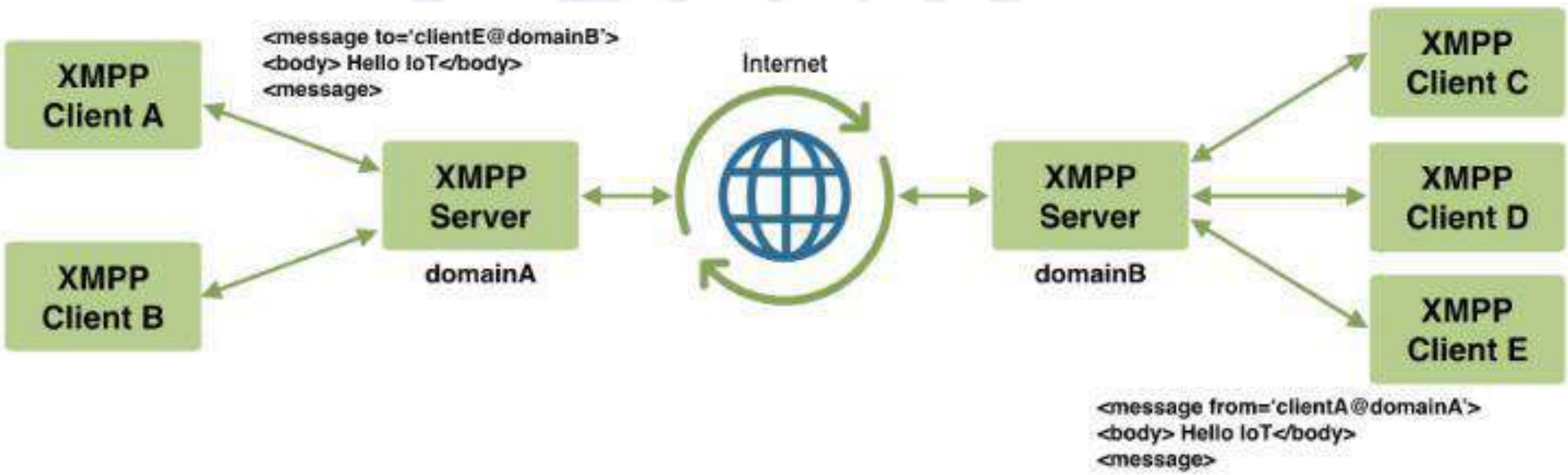
- AMQP protocol is based on the same functionning principle of MQTT, however theconcept of publisher/subscriber is replaced by producer/consumer.
- AMQP ensures the routing of messages from a producer to several topics. Thus, the same message can be consumed by different consumers via several topics.



XMPP

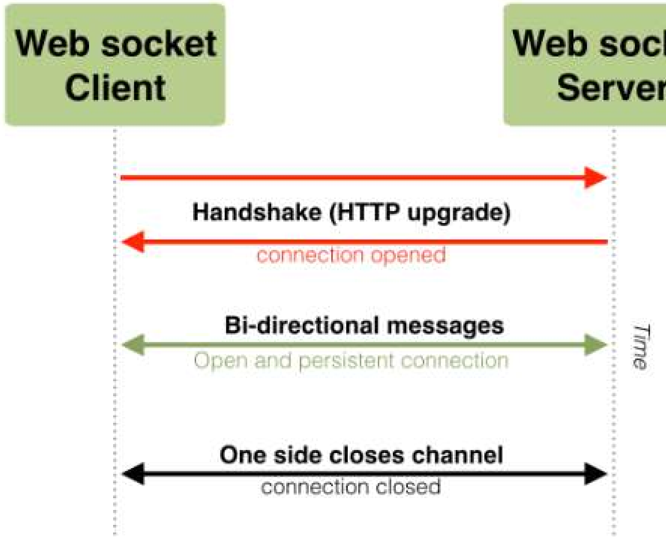
- XMPP (Extensible Messaging and Presence Protocol), is originally an instant messaging protocol used, in particular, in the Jabber and Google Talk services.
- XMPP is based on a client / server architecture and the exchange of data in XML format.
- Communication between two clients is asynchronous and is carried out through XMPP servers.

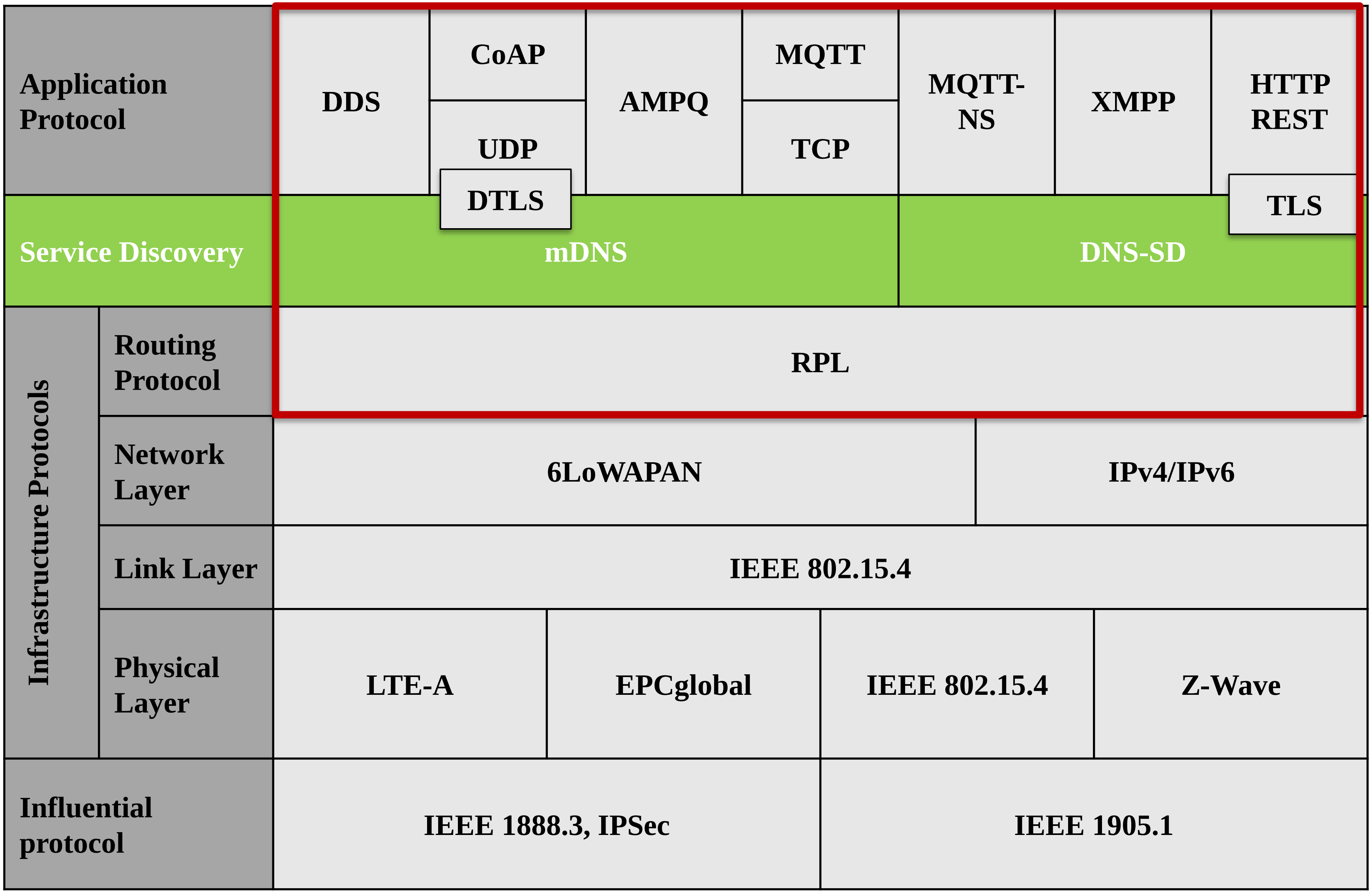
Fonctionnement du protocole XMPP



Websocket

- The Websocket protocol enables a full-duplex communication channel to be established with a single TCP connection between a client and a server.
- The three main phases of the channel's life:
  - the connection phase called "Handshake" initiated by the customer
  - the bidirectional message exchange phase
  - the closing phase of the channel initiated by one of the two parties




Application Protocol
DDS
CoAP
UDP
DTLS
AMPQ
MQTT
TCP
MQTT-NS
XMPP
HTTP REST
TLS
Service Discovery
mDNS
DNS-SD
Infrastructure Protocols
Routing Protocol
RPL
Network Layer
6LoWAPAN
IPv4/IPv6
Link Layer
IEEE 802.15.4
Physical Layer
LTE-A
EPCglobal
IEEE 802.15.4
Z-Wave
Influential protocol
IEEE 1888.3, IPSec
IEEE 1905.1

Service discovery

- An increasing number of devices are connected to TCP/IP networks, all these devices and devices must be correctly configured.
- Configuring the network settings (eg, IP address, netmask, etc.) of a device is a tedious task, as many devices do not have an appropriate user interface to do it comfortably.
- And as the number of devices in a network increases, configuring each device separately is no longer practical.
- Hence the need for automatic configuration of network devices and automatic discovery of network services. In recent years, the industry has developed a variety of different technologies and specifications to address this issue.

- Solution = ZeroConf Network

ZeroConf nework

- Zero-configuration networking or Zeroconf is the generic name for a set of protocols that automatically create an IP network that can be used without any particular configuration or dedicated servers.
- Without Zeroconf one has to set up special services, such as DNS and DHCP, and configure the network parameters of each device manually, which is difficult or practically impossible in the case of deployment of thousands of devices (case of smart metering)
- Zeroconf protocols provide at least the following functionalities:
  - dynamic allocation of IP address without DHCP server => AutoIP
  - resolution of names and IP addresses without DNS server => mDNS
  - search for services without directory => DNS SD

Multicast Domain Name System mDNS

- The mDNS protocol is intended to resolve host names to IP addresses in small networks that do not have a local DNS server.
- The mDNS service can be contacted using UDP requests on port 5353.

DNS-SD

- Problem: A temperature sensor that is programmed to send an alert via email, it must search for a host (which can send an email) then it sends a DNS SD request seeking for the smtp service (port 25).
- DNS Service Discovery hosts (devices) publish services giving details of the services they offer :
  - the type of service,
  - the domain name,
  - optional configuration parameters.
- A register of existing types of service (not exhaustive) is updated and published by DNS-SD.org.
- The types of services are recorded informally on a first come, first served basis.
- DNS-SD uses mDNS to publish or request services available on the network

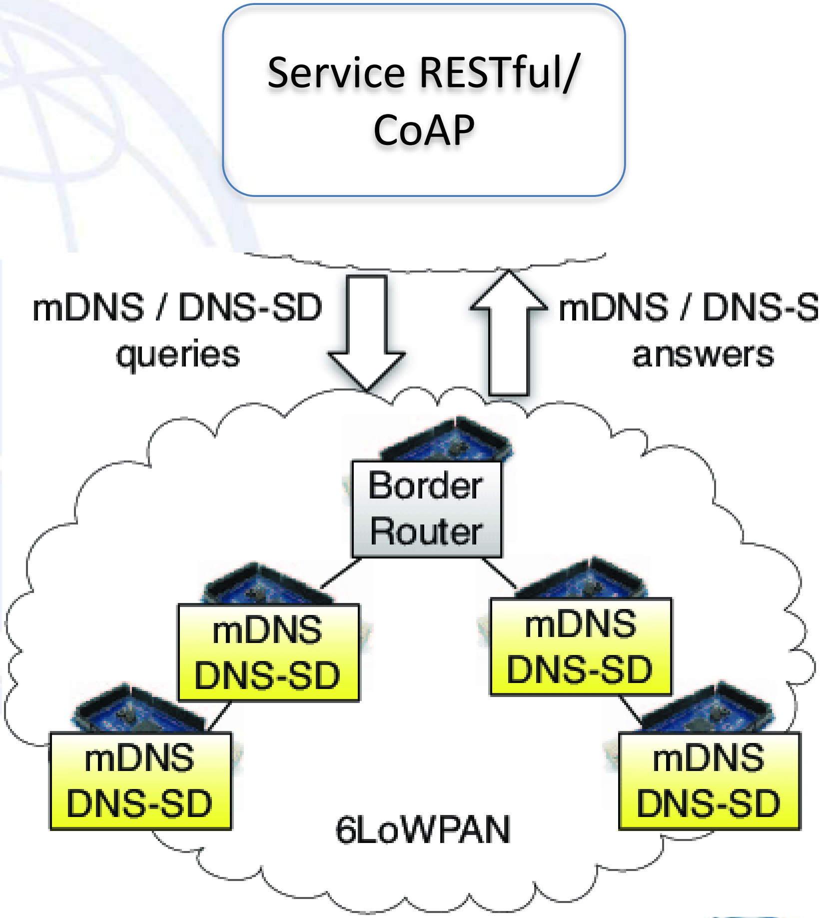
DNS-SD

- DNS-SD should work:
  - With or without a DHCP server: Self-con figured local link addresses
  - With or without DNS server: mDNS (multicast DNS)

- Example request: Service: <instance>. <service>. <domain>
  - Instance: Friendly-name for the service
  - Service: Protocol name (Rp, ssh) followed by _tcp or _udp
  - Domain: the DNS domain (local or other)

mDNS- DNS DS: Strong points

- There is no need for administration or configuration.
- Can operate where no infrastructure exists.
- Can operate with infrastructure failures.



TCP

- TCP (Transmission Control Protocol) is used for the majority of Internet connections.
- It provides host-to-host communication, dividing large data sets into individual packets, and resending and reassembling the packets as needed.
- TCP is not a good option for communication in low power environments because it has a large overhead due to being a connection oriented protocol.

TCP

- The connection is established by a three-step handshaking:
  - establishing the connection;
  - data transfers;
  - end of the connection.
- Connection termination uses four-step handshaking.

TCP Segment

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">Port Source 2 octets</td><td colspan="16">Port destination 2 octets</td></tr>
<tr><td colspan="32">Numéro de séquence</td></tr>
<tr><td colspan="32">Numéro d'acquittement</td></tr>
<tr><td colspan="4">Taille de l'en-tête</td><td colspan="3">Réservé</td><td>ECN / NS</td><td>CWR</td><td>ECE</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="16">Fenêtre</td></tr>
<tr><td colspan="16">Somme de contrôle</td><td colspan="16">Pointeur de données urgentes</td></tr>
<tr><td colspan="22">Options</td><td colspan="10">Remplissage</td></tr>
<tr><td colspan="32">Données</td></tr>
</table>

- **Port source :** numéro du port source
- **Port destination** : numéro du port destination
- **Numéro de séquence :** numéro de séquence du premier octet de ce segment
- **Numéro d'acquittement** : numéro de séquence du prochain octet attendu
- **Taille de l'en-tête :** longueur de l'en-tête (les options font partie de l'en-tête)
- **Indicateurs ou *Flags***
- **Fenêtre** : taille de fenêtre demandée, c'est-à-dire le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception
- **Somme de contrôle** : somme de contrôle calculée sur l'ensemble de l'en-tête TCP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP)
- **Pointeur de données urgentes :** position relative des dernières données urgentes
- **Options :** facultatives
- **Remplissage :** zéros ajoutés pour aligner les champs suivants du paquet sur 32 bits, si nécessaire
- Données : séquences d'octets transmis par l'application

UDP

- The User Datagram Protocol (UDP) is one of the main transport protocols used by the Internet.
- The UDP protocol ensures data transmission in unconnected mode. It is therefore unreliable (no guarantee of protection, order of arrival, or possible duplication of datagrams).
- UDP protocol is useful for real-time applications such as VoIP, online gaming, IoT, etc.

UDP datagram

- The UDP header contains the following fields:
  - Source port: indicates which port send the datagram
  - Destination port: indicates to which port the datagram should be sent
  - Length: indicates the total length (expressed in bytes) of the UDP segment (header and data). The minimum length is therefore 8 bytes (size of the header)
  - Control source: to ensure the integrity of the received packet when it is different from zero. It is calculated on the entire UDP header and data, but also on a pseudo header (extracted from the IP header)

Port Source (16 bits)	Port Destination (16 bits)
Longueur (16 bits)	Somme de contrôle (16 bits)
Données (longueur variable)	

IPv6

- The IPv6 protocol was developed in the 1990s as a successor to IPv4, whose addressing capacities are insufficient today.
- IPv6 became an official standard of the IETF in 1998.
- The main feature of IPv6 is that it uses a 128-bit address format instead of 32-bit in IPv4.

IPv6

340

trillion trillion trillion

Adresses IPv6 Possible!

IPv6

- This protocol provides an address space of nearly 4.3 billion IP addresses. However, the exponential growth of the Internet and connected objects has gradually exhausted IPv4 addresses.
- In addition to providing more space and allowing more objects to connect to the Internet, IPv6 has other benefits, such as enhanced security, simplified configuration and processing.

IP address

X:X:X:X:X:X:X:X/n

- X = 4 positions hexadécimales: X = hhhh oú h = [0 – 9, a – f]
- n = longueur de préfixe en décimale

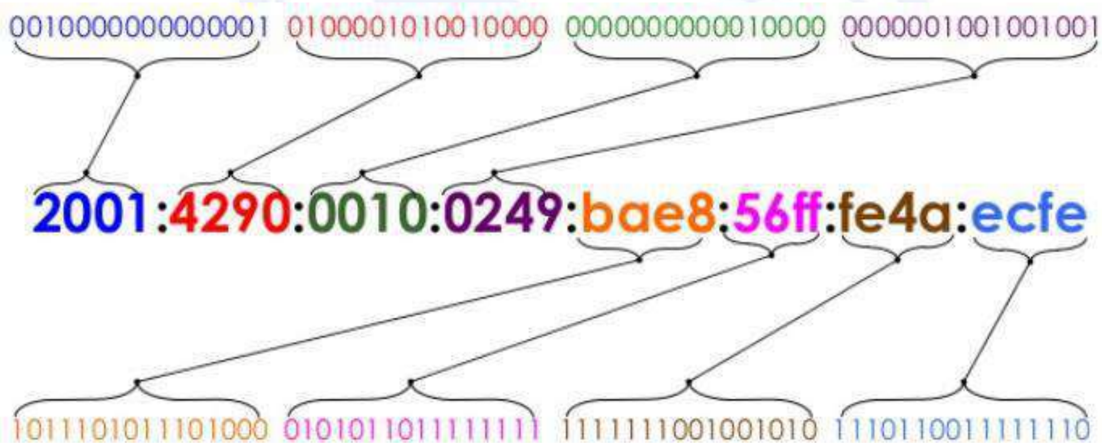
hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh/n

IP address

0010000000000001 0100001010010000
0000000000010000 0000001001001001
1011101011101000 0101011011111111
1111111001001010 1110110011111110

128 bits

IP address



0010000000000001
0100001010010000
0000000000010000
0000001001001001
2001:4290:0010:0249:bae8:56ff:fe4a:ecfe
1011101011101000
0101011011111111
1111111001001010
1110110011111110

IPv6

- It becomes imperative that African network operators begin the transition to IPv6 as soon as possible to ensure that they can continue to communicate with IPv4 and IPv6 networks in other regions.
- This is the only way to guarantee for all Internet users the possibility of free access to the Internet from Africa and to ensure that Africa remains a major player in the growth of the Internet at the level global.

RPL

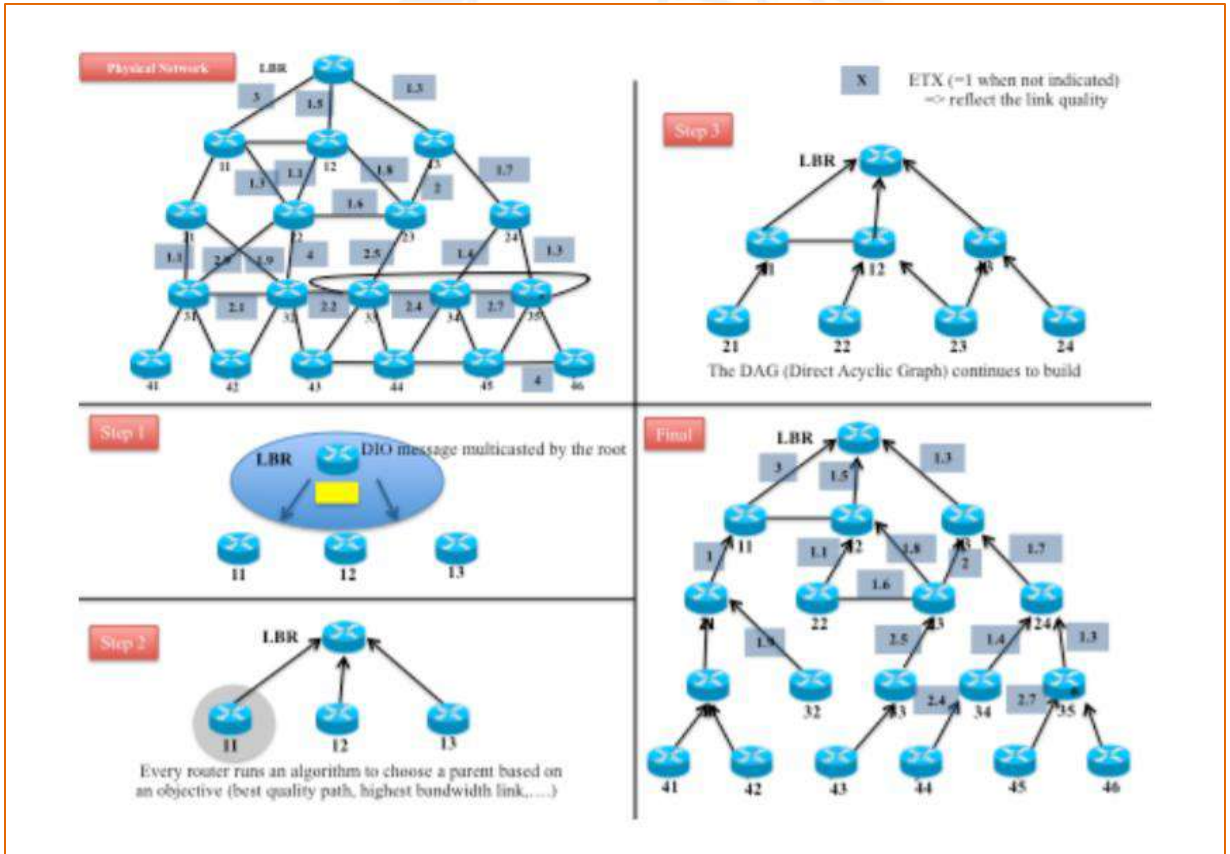
- One of the challenges of the IoT is the routing of IP packets. Objects have limited electrical resources and are often connected by poor quality radio links. Traditional routing protocols are not very suitable for this situation.
- The IETF ROLL working group produced an "official" protocol, RPL (Routing Protocol for LLNs (where an LLN is a Low power and Lossy Network), a network where even routers have little power and where packets get lost on the way).

RPL

- RPL is a routing protocol which constructs routes. It uses the Trickle algorithm (based on graph theory to distribute information on routes and routers.
- To optimize routes, RPL is configured with a function called OF (Objective Function).
- Different networks can use different OFs (one that looks for the shortest path, one that tries not to use machines that do not have connection as a router, etc.)

http://www.cse.chalmers.se/edu/year/2019/course/DAT300/PAPERS/rpl.pdf

RPL



Physical Network
LBR
Step 3
ETX (=1 when not indicated)
=> reflect the link quality
The DAG (Direct Acyclic Graph) continues to build
Step 1
DIO message multicasted by the root
Step 2
Every router runs an algorithm to choose a parent based on an objective (best quality path, highest bandwidth link,….)
Final

6LoWPAN

IETF Standard – RFC 4944 : 6LoWPAN (2007)

- 6LoWPAN (IPv6 Low Power Wireless Personal Area Network) is a combination of two protocols: Internet Protocol version (IPv6) and Low-Power Wireless Personal Network (LPWPAN).
- 6LoWPAN was designed to allow IPv6 to integrate constrained devices and the 802.15.4 networks that interconnect them.
- IPv6 packets have fixed-size headers of 40 bytes: size not suitable for IEEE 802.15.4 networks.
- 6LoWPAN allows 802.15.4 objects to communicate over IPv6 networks so that the end-to-end connection is addressable and a router can be used for routing tasks.

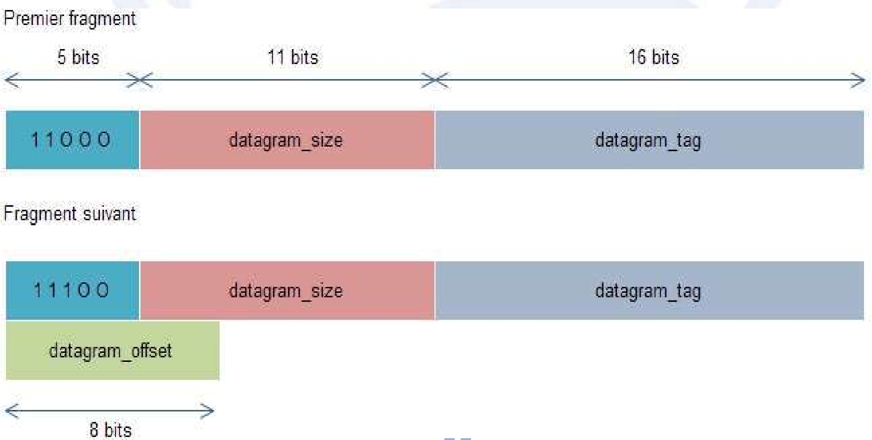
6LoWPAN

- 6LoWPAN is an adaptation layer that resides between the data link layer and the network layer. It performs the following functions:
  - Packet fragmentation and regrouping
  - Header compression
  - Routing
- The 6LowPan standard does not provide any security functions in addition to those potentially implemented at the level of 802.15.4 and IP V6.

6LoWPAN

Fragmentation and reassembly

- Each fragment is preceded by a header (4 or 5 bytes) which contains:
  - 5 bits: used to identify that this is a fragment.
  - 8 bits: position of the fragment in the IP packet
  - 11 bits: size of the IP packet before fragmentation;
  - 16 bits: identifier common to all the fragments of the same IP packet;



6LoWPAN

Routing

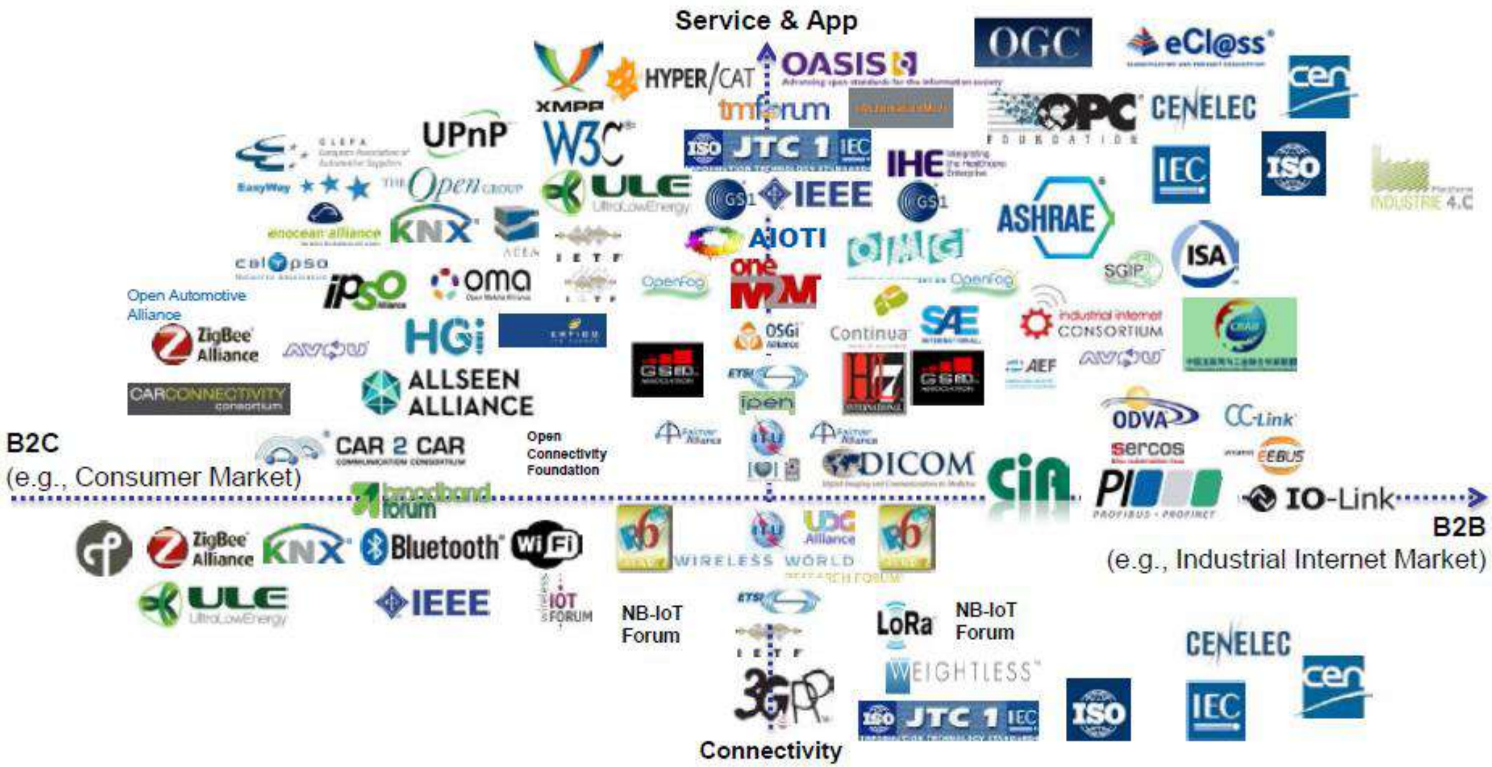
- The RFC 49443 specification defines the IPv6 header compression mechanism for LowPAN networks.
- The use of the LOWPAN_IPHC compression algorithm is recommended by the 6LoWPAN group.
- The IPHC IPv6 header, resulting from the compression, integrates the following information:
  - quality of service,
  - the next headers,
  - the number of jumps, and
  - compressed source/destination addresses.

Part 4 : Standardisation activities

Standardisation activities

- Several international initiatives seek to create a a global architecture framework for IoT in order to:
- avoid the fragmentation of the IoT ecosystem,
- develop intersectoral standards for technologies used by all sectors, and
- ensure interoperability between connected objects, systems and applications.

SDO and IoT alliances landscape



Source : https://tel.archives-ouvertes.fr/tel-02180889/document

ITU-T activities

Development and implementation of standards → ITU-T Study Group 20

Research & pre-standardization work → Focus Group on **Data Processing Management (FG-DPM)**

U4SSC

Open platform for knowledge sharing & Forward looking research → United for Smart Sustainable Cities (U4SSC)

Source : https://www.itu.int/net4/ITU-T/landscape#?topic=0&workgroup=1&searchValue=&page=1&sort=Revelance

ITU-T activities

- ITU has been tasked to study the standardization needs of IoT technologies with a focus on the applications of smart cities and communities.
- The areas of interest include semantics, Big Data, recommendations on networks supporting IoT applications, identification, security and privacy, etc.
- ITU has also defined reference architectures for different applications (transport security, disaster surveillance and preparedness, e-health, smart manufacturing and industrial IoT, and smart agriculture).

ITU-T SG 20 : Questions

WP1/20	Questions
Q1/20	End to end connectivity, networks, interoperability, infrastructures and Big Data aspects related to IoT and SC&C
Q2/20	Requirements, capabilities, and use cases across verticals
Q3/20	Architectures, management, protocols and Quality of Service
Q4/20	e/Smart services, applications and supporting platforms
WP2/20	
Q5/20	Research and emerging technologies, terminology and definitions
Q6/20	Security, privacy, trust and identification
Q7/20	Evaluation and assessment of Smart Sustainable Cities and Communities

FG-DPM Structures

- Duration of FG-DPM (03/2017 -07/2019)
  - WG1 - Use Cases, Requirements and Applications/Services
  - WG2 - DPM Framework, Architectures and Core Components
  - WG3 - Data sharing, Interoperability and Blockchain
  - WG4 - Security, Privacy and Trust including Governance
  - WG5 - Data Economy, commercialization, and monetization

ITU-T activities: IoT et Smart cities

- IoT-GSI - Internet of Things Global Standards Initiative
- JCA-IoT - Joint Coordination Activity on Internet of Things
- ITU-T Focus Group on the M2M service layer
- ITU-T Study Group 2 - Numbering, naming, addressing
- ITU-T Study Group 11 - Testing architecture for tag-based identification
- ITU-T Study Group 13 - NGN requirements and architecture for applications and services using tag-based identification
- ITU-T Study Group 16 - Requirements and architecture for multimedia information access triggered by tag-based identification
- ITU-T Study Group 17 - Security and privacy of tag-based applications
- ITU-R - Global management of the radio-frequency spectrum

ISO/IEC JTC 1/SC 41

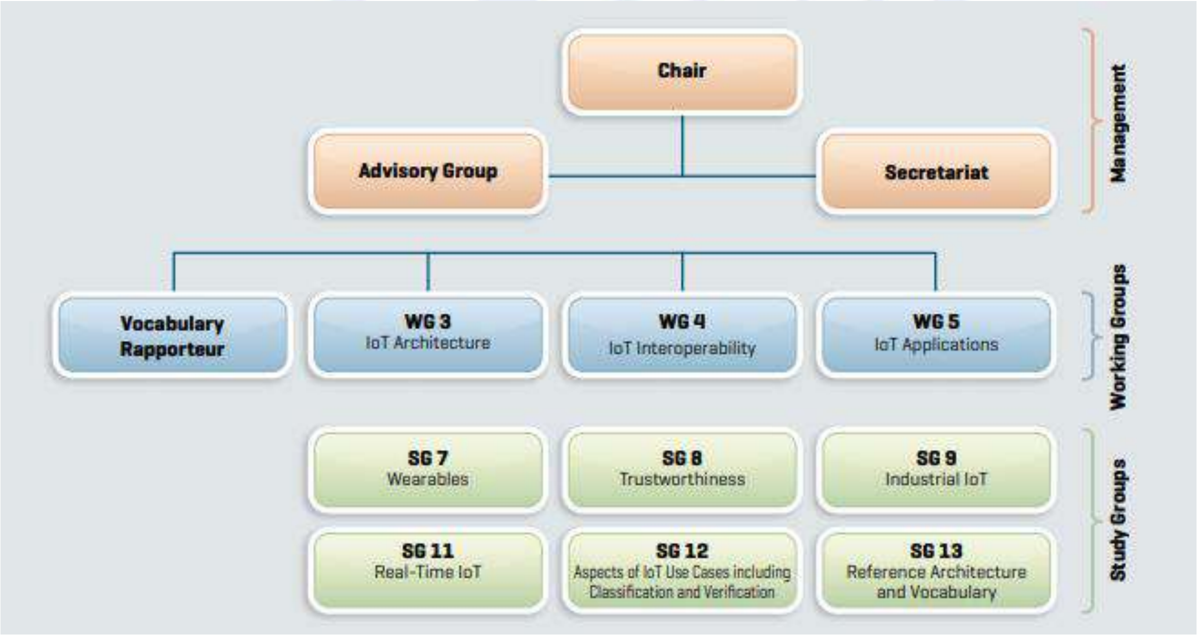
- ISO/IEC JTC 1/SC 41 is the IoT and related technologies subcommittee, it aims to:
  - Be a think tank and a source of proposals for the standardization program in the field of IoT and related technologies (sensor networks and wearables).
  - Provide guidance to JTC 1, IEC, ISO and other entities that develop IoT related applications.

Collaboration domains

- ISO / IEC JTC 1 / SC 41 has a number of links with various technical committees within ISO, IEC as well as with other SDOs that are active in IoT standardization and technologies.

SDOs	Main area(s) of collaboration
AIM - Advancing Identification Matters	AIDC (RFID, barcodes, RTLS, NFC)
GS1 - Global Standards One	Identification systems; Automatic data capture technologies; Data sharing
IEEE IMS TC 9 - Sensor Technology	Sensor Networks; Actuators
IEEE P.1931.1	ROOF computing
IIC - Industrial Internet Consortium	Architecture; Connectivity; Interoperability; Testing; Security; Edge Computing; Use cases
ITU-T - International Telecommunication Union's Telecommunication Standardization Sector	All
OCF - Open Connectivity Foundation	Data model; Architecture; Interoperability; Security
OGC - Open Geospatial Consortium	Geospatial information

Structure


Chair
Advisory Group
Secretariat
Management
Vocabulary Rapporteur
WG 3
IoT Architecture
WG 4
IoT Interoperability
WG 5
IoT Applications
Working Groups
SG 7
Wearables
SG 8
Trustworthiness
SG 9
Industrial IoT
SG 11
Real-Time IoT
SG 12
Aspects of IoT Use Cases including Classification and Verification
SG 13
Reference Architecture and Vocabulary
Study Groups

IEEE

- The Institute of Electrical and Electronic Engineers (IEEE) develops standards for connectivity.
- It plays an important role in defining the physical and data link layers to ensure interoperability between devices.
- Wireless LAN (IEEE 802.11 family) is a practical standard for many IoT applications.
- However, for constrained IoT devices, IEEE proposed the IEEE 802.15.4 standard intended for wireless networks of the LR WPAN family (Low Rate Wireless Personal Area Network).

IETF

- The Internet Engineering Task Force (IETF) develops standards for communication systems.
- IETF has been active in creating specific standards for LPWAN technologies.
- The IPv6 Working Group for LPWAN (6LoWPAN) worked on optimizing IETF protocols for Low Power Wide Area Networks like SigFox or LoRA.
- The work of the IETF has resulted in a protocol stack that enables the implementation of interoperable IoT.

ETSI

- Within ETSI, the M2M Technical Committee was launched with the aim of filling the IoT standardization gaps.
- Its objectives are to standardize the integration of sensors, naming and numbring, location, QoS, security, management, applications and hardware interfaces.
- The ETSI Technical Committee on Cybersecurity (TC CYBER) has released in June 2020 ETSI EN 303 645, a standard for cybersecurity in the Internet of Things that establishes a security baseline for internet-connected consumer products and provides a basis for future IoT certification schemes.

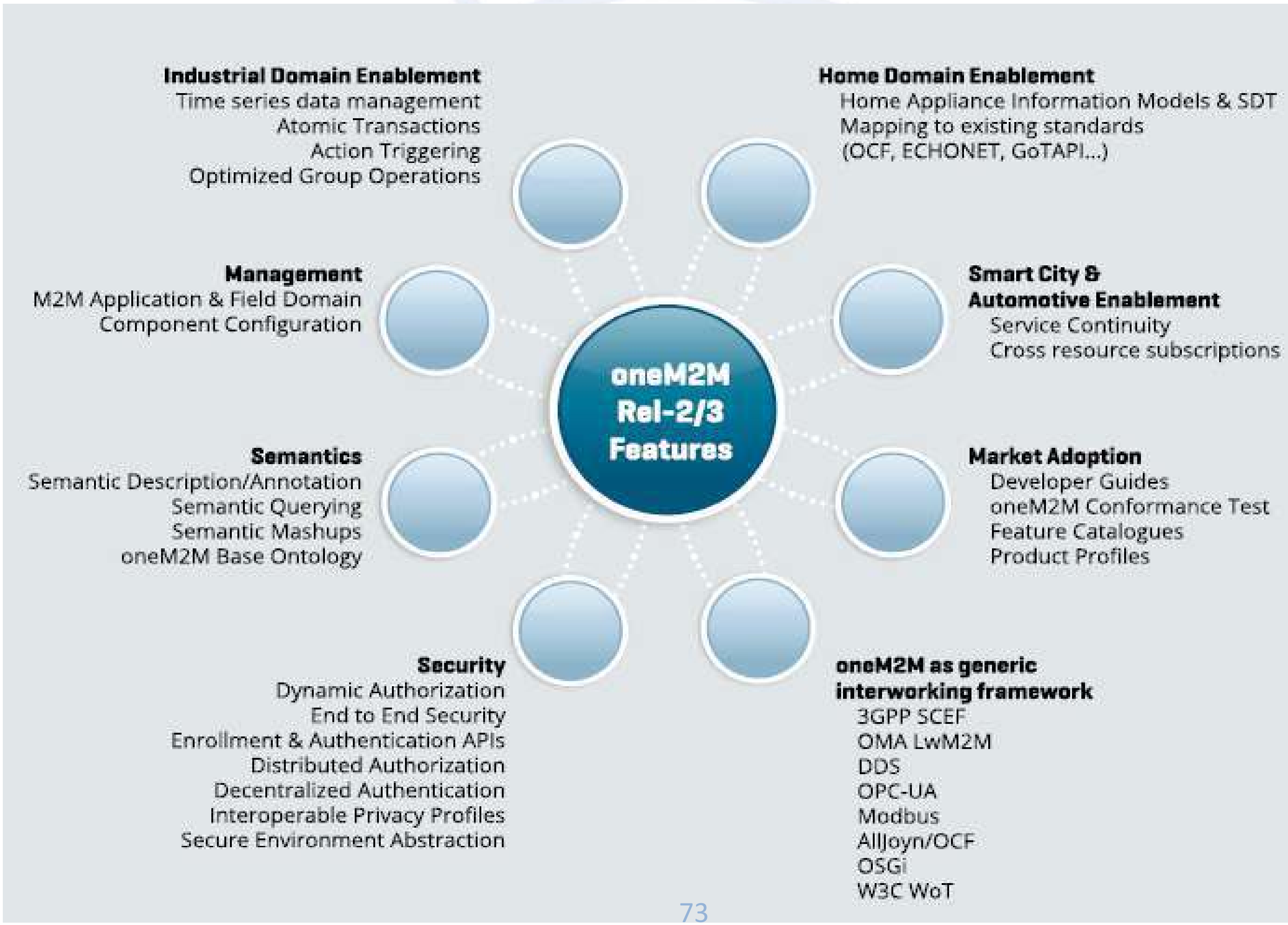
OneM2M

- The oneM2M consortium is composed of various SDOs around the world: American organizations (ATIS and TIA), Europe (ETS), and several Asian organizations: Japan (ARIB and TTC), China (CCSA), Korea (TTA), and India (TSDSI).
- These organizations formed the oneM2M consortium in 2013 to work together on the proposal of a global standard for M2M and IoT.
- oneM2M consortium provides specifications for APIs, architecture, interoperability, security and certification of devices and applications.

OneM2M

- oneM2M released a service layered architecture for IoT devices to interact and exchange data transparently.
- The oneM2M specification considers the IoT network is structured into three service layers: application, common services and network service layer.
- oneM2M provides a comprehensive set of guidelines, numbering formats, links to the most popular IoT protocols and APIs.
- It also provides a mechanism allowing devices other than oneM2M to work with a oneM2M network.

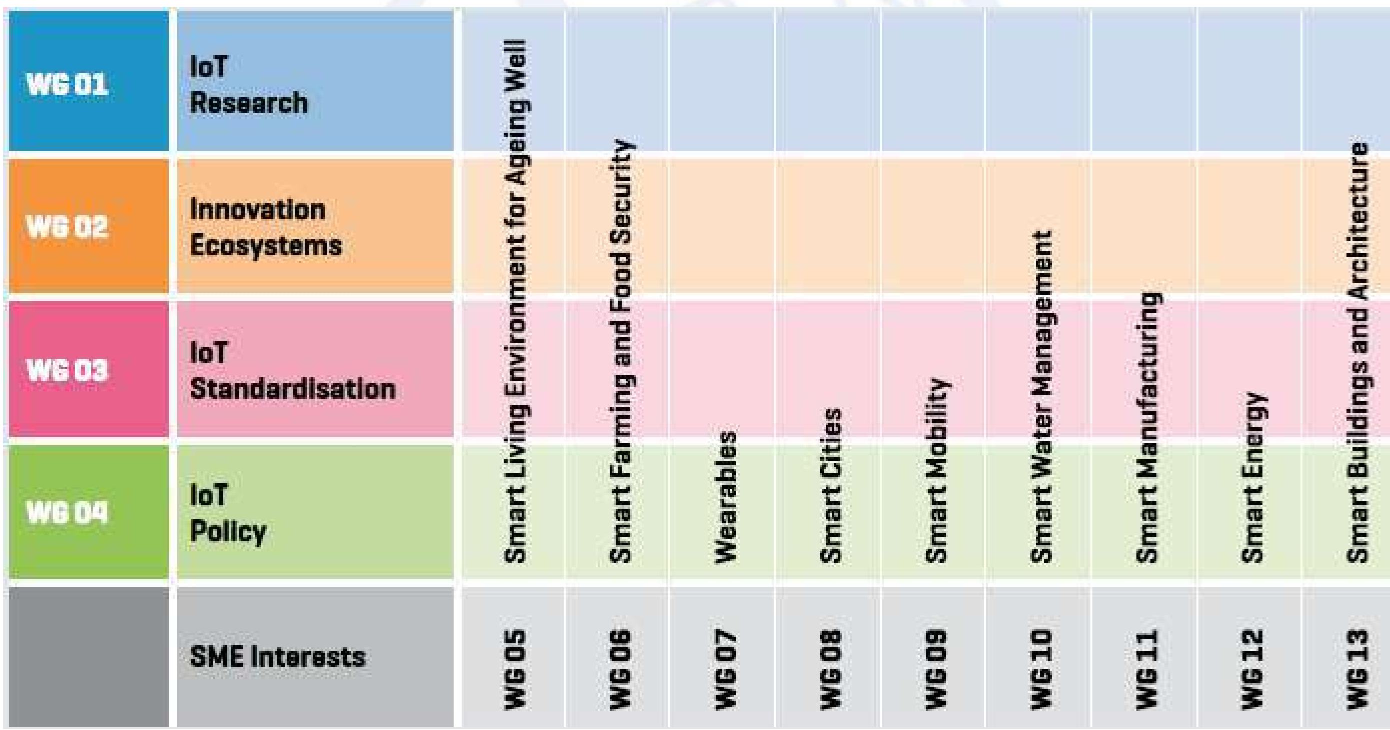
OneM2M


Industrial Domain Enablement
Time series data management
Atomic Transactions
Action Triggering
Optimized Group Operations
Home Domain Enablement
Home Appliance Information Models & SDT
Mapping to existing standards
(OCF, ECHONET, GoTAPI...)
Management
M2M Application & Field Domain
Component Configuration
oneM2M
Rel-2/3
Features
Smart City &
Automotive Enablement
Service Continuity
Cross resource subscriptions
Semantics
Semantic Description/Annotation
Semantic Querying
Semantic Mashups
oneM2M Base Ontology
Market Adoption
Developer Guides
oneM2M Conformance Test
Feature Catalogues
Product Profiles
Security
Dynamic Authorization
End to End Security
Enrollment & Authentication APIs
Distributed Authorization
Decentralized Authentication
Interoperable Privacy Profiles
Secure Environment Abstraction
oneM2M as generic
interworking framework
3GPP SCEF
OMA LwM2M
DDS
OPC-UA
Modbus
AllJoyn/OCF
OSGi
W3C WoT

AIOTI

- Alliance for Internet of Things Innovation (AIOTI) was created in 2015 to develop and support cooperation between IoT stakeholders in Europe.
- Over 200 organizations are members of AIOTI.
- AIOTI is made up of 13 WGs working on IoT standardization activities and conducting research in related fields.
- WG 3, chaired by ETSI, is working on IoT standardization. The main deliverables of this WG are:
  - IoT Landscape which provides insight into SDOs involved in IoT standardization.
  - High Level IoT Architecture (HLA), known as AIOTI HLA
  - Recommendations on semantic interoperability of the IoT.

AIOTI


WG 01
IoT Research
WG 02
Innovation Ecosystems
WG 03
IoT Standardisation
WG 04
IoT Policy
SME Interests
Smart Living Environment for Ageing Well
Smart Farming and Food Security
Wearables
Smart Cities
Smart Mobility
Smart Water Management
Smart Manufacturing
Smart Energy
Smart Buildings and Architecture
WG 05
WG 06
WG 07
WG 08
WG 09
WG 10
WG 11
WG 12
WG 13

3GPP

- 3GPP est une coopération entre organismes de normalisation en télécommunications tels que : UIT, ETSI, ARIB/TTC (Japon), CCSA (Chine), ATIS (Amérique du Nord) et TTA (Corée du Sud).
- 3GPP assure la maintenance et le développement de spécifications techniques pour les normes :
  – GSM (GPRS, EDGE, UMTS, LTE et LTE advanced)
  – 3GPP PSS (packet switched streaming) qui traite des services audio/vidéo, dont la télévision, sur réseau mobile.
  – 3GPP iMB (integrated mobile broadcast) qui traite de la diffusion de la télévision sur les cellules radio des services mobiles 3G.

GS1

- Global Standards 1 (GS1) est un organisme mondial actif dans le domaine de la normalisation des méthodes de codage utilisées dans la chaîne logistique.

- L'objectif de GS1 est d'établir des normes d'identification, de capture et de partage de données, visant ainsi toute la chaîne de distribution du producteur au consommateur.

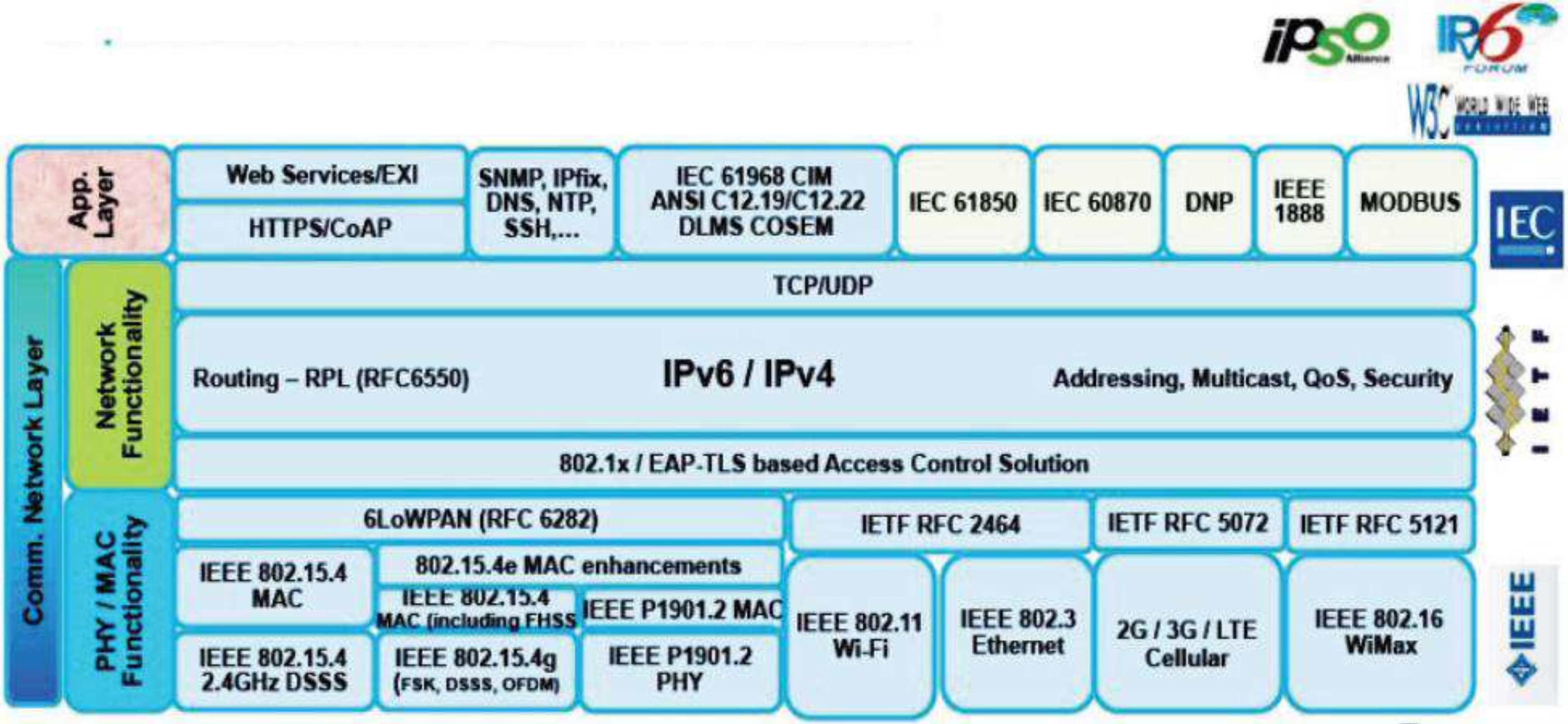
OASIS

- OASIS : IBM a développé les protocoles MQTT et sa variante MQTT pour réseau de capteurs (MQTT-SN) conçu pour être exploités sur TCP/IP, à l'exception du mode MQTT-SN de faible puissance et temps réel conçu pour des échanges locaux et opérant sur UDP.

Examples of standards

Emetteur	Norme / standard	Définition
UIT	UIT-T Y.2060	Concept IoT
	UIT-T Y.2061	Interface machine-application
IEEE	IEEE 802.15.4	Couche liaison
	6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
	CoAP	Constrained Application Protocol
IETF	RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks
GS1	ONS	Object Naming Service
	EPC	Electronic Product Code
OASIS	MQTT	Message Queue Telemetry Transport
	AMQP	Advanced Message Queuing Protocol
	DDS	Data Diffusion Service

Standards reference model



Part 5: Roaming et regulations

Roaming concept

- Le Roaming is a service offered by telecommunications operators that allows mobile phone users to call and be called in a foreign country.

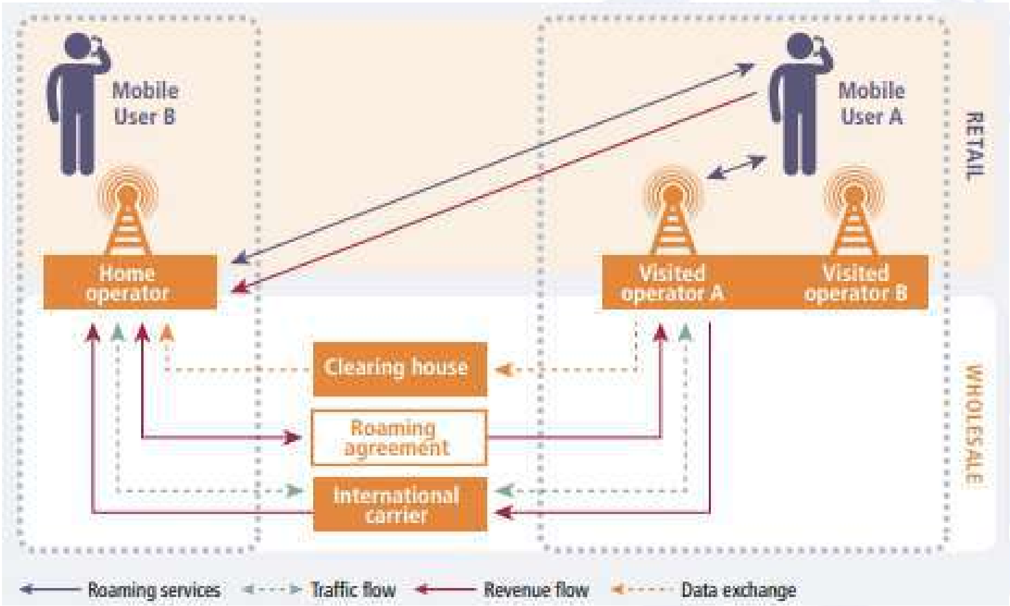
Source: International roaming explained, GSMA

Definition

ITU Definition –T D.97

- International mobile roaming (IMR) is a service (voice, SMS/multimedia messaging service (MMS), data) that subscribers to post-paid or prepaid mobile services purchases from a mobile operator in their home country, that is, from the 'home operator'.
- It allows subscribers the convenience to continue to use their national mobile phone numbers to access voice, short message service (SMS), and data services while visiting another country, by accessing a mobile operator's network in the visited country, that is, the network of the 'visited operator' – with all arrangements made by their home operator.

IMR Concept



- Inbound roaming , refers to the roaming of foreign customers
- Outbound roaming, refers to roaming from abroad.

Source: International roaming explained, GSMA

IMR Concept

- There are 3 types of roaming:
  - National
  - Regional
  - International

Roaming service

- The realization of the roaming service requires the implementation of a structure which must allow the inter-connectivity of the partner networks and guarantee a good quality of service for the roamers.
- This structure is as follows:
  - Connectivity between mobile networks: establishment of signaling systems (SS7, SIGTRAN or MEDIATER) and interconnection.
  - Agreement (bilateral or unilateral): This agreement mainly concerns the interconnection of the two networks, the tariffs/prices, the data format as well as the mechanism which governs the exchange of these data.
  - Test: These are tests to verify interoperability and quality of service
  - Roaming service: The services offered depend on the capacities of the mobile network, the list of services specified in the agreement, the type of subscription, etc.

IMR Challenges

- Bi/multilateral agreements and regional initiatives
- IMR Price/Tariff
- Market competition
- Consumer Protection

Source : ITU IMR Strategic Guidelines, 2018

Bi/multilateral agreements

- The agreement covers the technical aspects and commercial components necessary to activate the IMR service.
- The agreement mainly concerns the interconnection of the two networks, the setting of tariffs/prices, the data format as well as the mechanism which governs the exchange of this data.
- The proliferation of agreements between operators allows subscribers to continue using their mobile phones in almost all countries on the planet.
- This is a great asset for frequent travelers or professionals who travel extensively, but can be very costly.

IMR tariffs

- The IMR wholesale and retail tariffs are the prices charged for the IMR service, namely:
  - IMR wholesale tariffs are the prices charged by the visited operator to the home operator to allow subscribers of the home operator to use the visited operator's network;
  - IMR retail tariffs are the prices that the originating operator charges its subscribers for using IMR services.

IMR tariffs

- The regulation of retail or wholesale rates for IMR could follow at least one of the principles :
  - Benchmarking: This is based on the comparison of relevant retail rates or wholesale rates/costs considering international best practices and experiences (where such benchmarking is available).
  - Retail minus: IMR wholesale rates are estimated from references to relevant retail prices, subtracting a percentage.
  - Cost oriented: Calculating the wholesale cost of IMR by identifying relevant IMR provisioning costs including any reasonable rate of return at a level, which promotes investment and innovation. Care must be taken to ensure that artificial and non-related costs are not included in such an analysis.

IMR tariffs

- If a Member State considers a cost-oriented approach, at a minimum, the following elements should be considered when estimating competitive and affordable IMR rates:
  - local access, origination, and termination costs;
  - International termination costs, international gateways costs;
  - Local transport costs;
  - International transport costs;
  - roaming specific charges, including contract, billing and signaling charges; and
  - retail specific charges, including invoicing and international processing costs .

Market competition & consumer protection

Market competition

- If the high cost of roaming retains in our countries, this could lead to:
  - Increased and more frequent use of local SIMs to the detriment of roaming, thus resulting into a significant loss of operators' income.
  - More increased use of OTTs services (Skype, Viber, Facebook…) in replacement of roaming.

Consumer potection

- National regulatory authorities are encouraged to promote transparency in the information provided to customers ()the tariffs of international roaming providers and the roaming services.

Benefits of regional roaming

- Solve the problem of the high price of roaming services
  - Through the elimination of all surcharges and costs on international communications
  - The setting of ceiling tariffs driven by a regulatory approach
  - Based on a study on the roaming cost value chain
  - By following ITU-T D. recommendations (D.98 & D97)
- Determine the rights and duties of the players (operators, regulators, service providers, consumers) involved in regional roaming.
- Offer an alternative to the use of OTTs services
- Constitute an internal market for mobile communication services where national tariffs and community roaming tariffs converge.

Experiences in regional roaming: EU

- An initiative to limit roaming tariffs has been led by the EU.
- In June 2007: the EU established a regulation of the European Commission "N ° EC 717/2007", defining "Eurotariff"; it concerns the setting of a maximum price for international mobile calls in the EU when the subscriber is in roaming mode.
- Objectives sought:
  - Put an end to the opacity of tariffs and to the agreements between operators to maintain high prices to the detriment of consumers, and institute a “Eurotariff”;
  - Set, at the community level, maximum charges per minute (pricecap) for the retail price as well as for the wholesale price;
  - Reflect as accurately as possible the actual costs of provided services.

Experiences in regional roaming: EU

- Roaming the pricing in Europe for European operators also leaves leeway for operators to compete with prices below the maximum prices.
- The Eurotariff has experienced significant reductions since its implementation in 2010.
- In June 2017: The EU implemented a new roaming regulation, requiring the removal of roaming charges in all 28 member states, including the UK.

Experiences in regional roaming: SADC Zone

The Southern African Development Community (SADC)

- In 2007: the ministers responsible for postal telecommunications expressed their will to set up a roaming service.
- In 2009: establishment of a multidisciplinary working group.
- In 2014: launch of the roaming project in three (3) phases.
- As of June 15, 2016: 7 out of 15 SADC MS were implementing roaming routes on the basis of reciprocity.

→ Observation: the project initiated in 2007 and took about 10 years for realization.

Experiences in regional roaming: CAE

The East African Community (EAC)

- In May 2014: the Heads of State recognized the high cost of roaming, they decided to set up a One Network Area (ONA) free of charge for calls received while roaming.
- In 2014: Rwanda and Uganda set up an One Network Area.
- June 2015: Communications regulators develop the roadmap.
- In 2016: roaming is effective in the area.

Experiences in regional roaming: ECOWAS

The Economic Community of West African States (ECOWAS)

- In 2005: Heads of State and Government called on mobile phone operators to sign roaming agreements.
- In May 2016: ECOWAS launched a feasibility study for the establishment of a free roaming service in West Africa.
- In 2017: 7 countries out of 15 namely, Guinea, Senegal, Sierra Leone, Togo, Burkina Faso, Mali and Ivory Coast signed a MoU (Abidjan Protocol 2016) on the implementation of Free roaming.

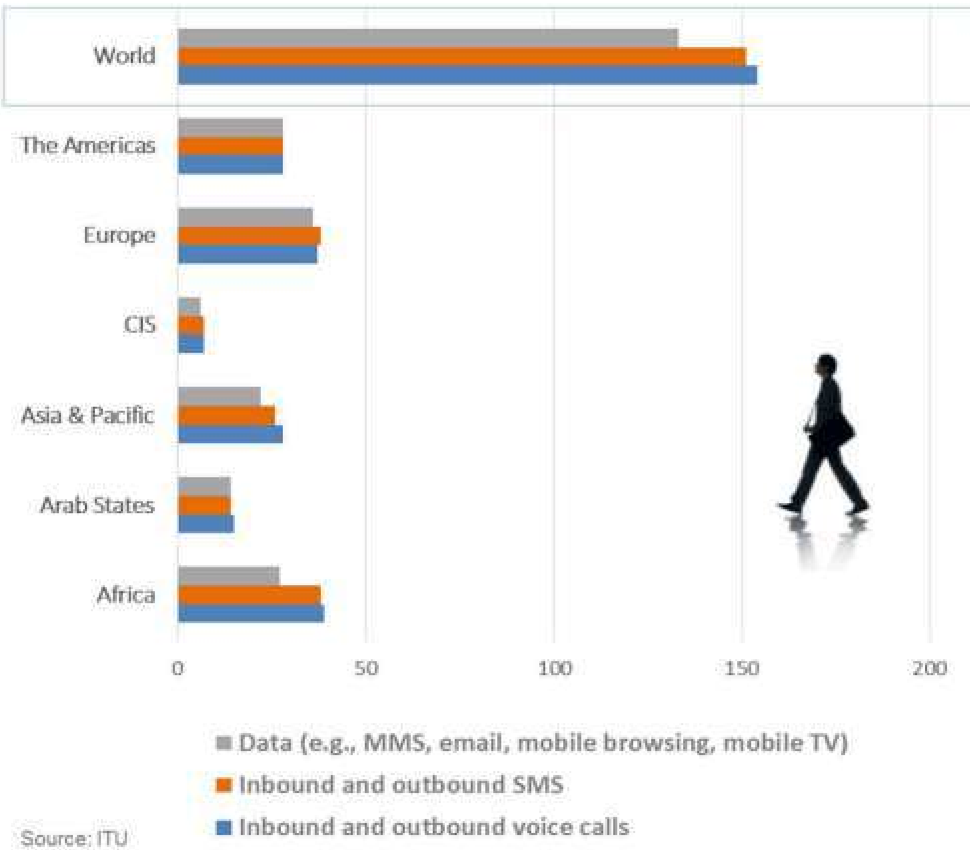
Experiences in regional roaming: Central Africa

- In July 2013: the Telecommunications Regulators of Central Africa (ARTAC) made recommendations, in particular for the establishment of roaming.
- In November 2016: the Telecommunications / ICT Ministers of ECCAS member states, mandate ECCAS to implement roaming with the support of the United Nations Commission for Africa.

ITU activities

- ITU-T SG3 has developed Recommendations on tariffs for mobile roaming services (D97 & D98)
- ITU-T recommendations include, among others:
  - transparency obligation for operators;
  - introduction of consumer protection measures;
  - encouragement of competition on the service;
  - ceiling on invoices and / or tariffs.

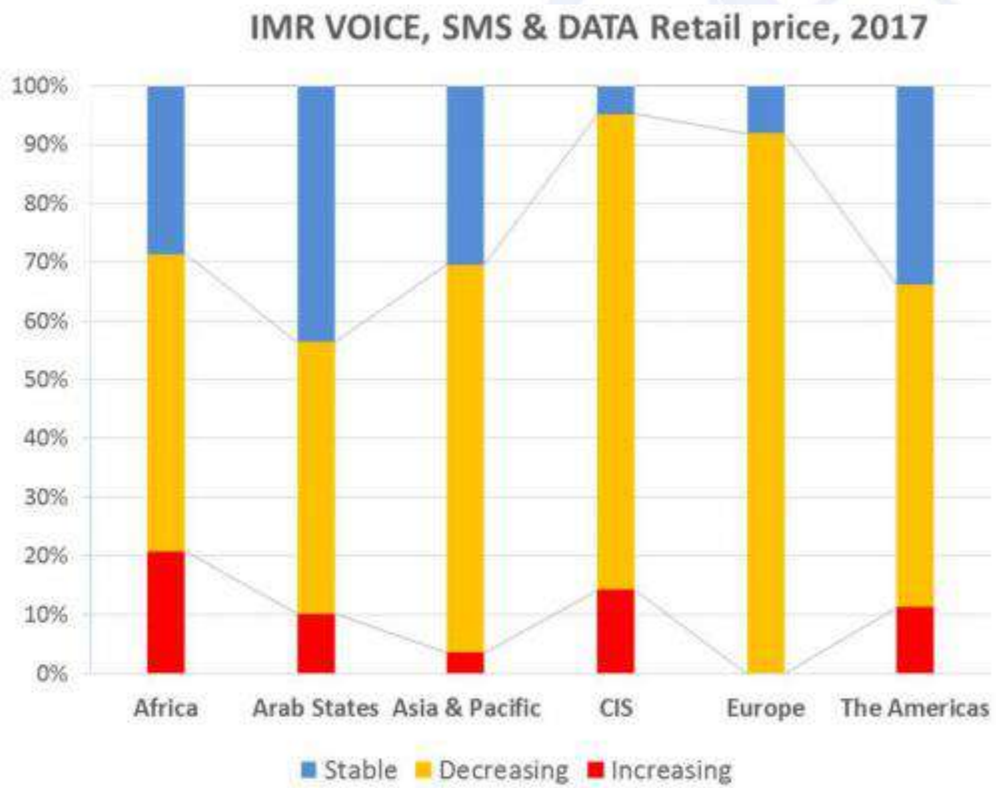
Availability of roaming services



- The availability of roaming services is growing in all regions.
- Despite this global increase, there are still gaps in the availability of data roaming.

Source : ITU ICTEye

The price of roaming services is falling ... but still not enough

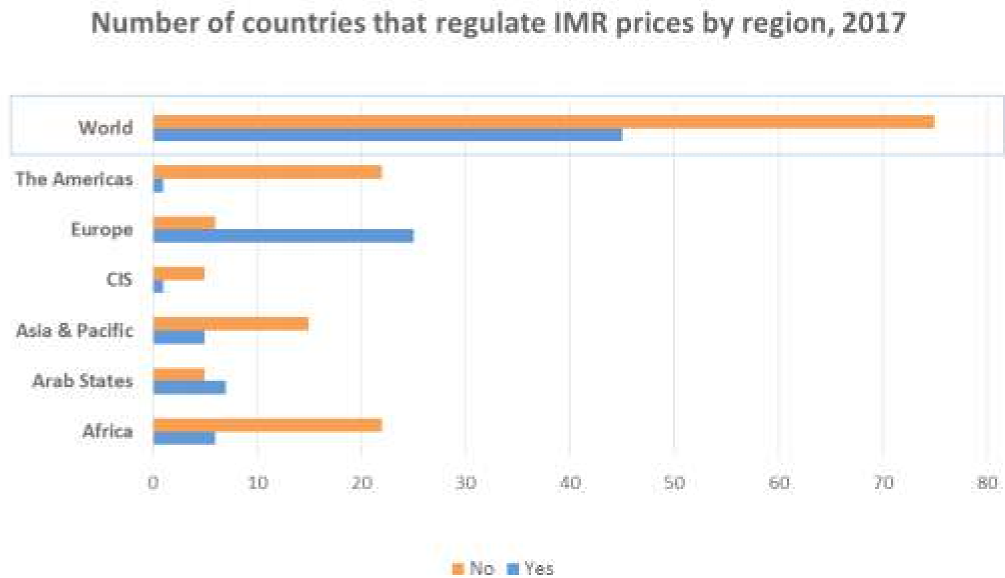


A global comparison of IMR and national prices showed that roaming calls and SMS prices were **three to six times higher** than the corresponding national tariffs[2].

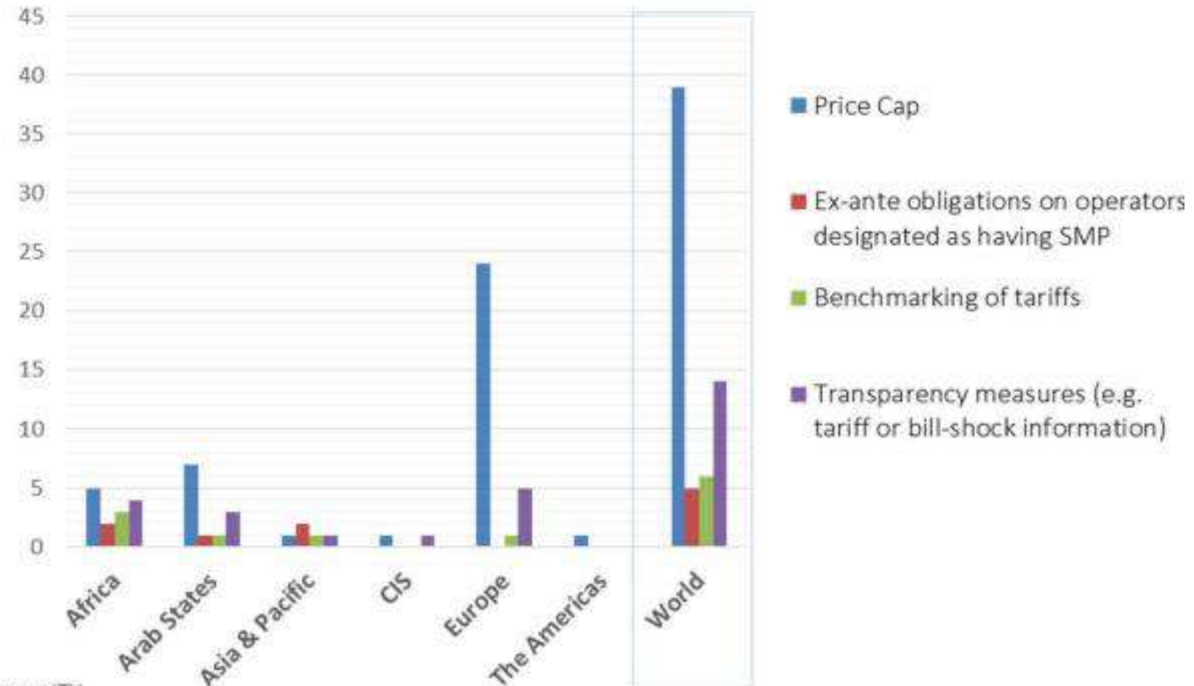
Source : ITU ICTEye

Roaming regulation

- The number of countries applying IMR regulations, targeting retail prices, is very low in all regions except Europe.



Regulatory practices applied by NRAs



ìource: ITU

Permanent Roaming regulation problem

- The current national, regional or international roaming regulations are focusing on the consumer protection of Person-to-Person communication service.
- IoT services based on cellular connectivity use Permanent raoming to connect IoT devices outside their country of production, while the SIM card comes from the country of production.
  - For example, connected cars use SIM cards from their country of production while these cars are used all over the world.
- There is no uniform treatment of permanent roaming in the regulations of different countries.

→ This is problematic because the restrictions on permanent roaming, in a country prevent the use of data internationally and present challenges for the global deployment of devices.

Regulatory situation

Permanent roaming:

- is allocated in some countries such as: Canada, United States, France, Germany, Japan and South Korea
- Prohibited in Brazil, Singapore and UAE.
- The regulations are ambiguous in China and Australia: the use of permanent roaming or not is managed between operators.

Permanent roaming and the future of IoT

Future work of the regulations on the subject of "Pemanent Roaming" could impact the economic model of IoT in case this regulation:

- imposes restrictive pricing policies on mobile operators;
- remains ambiguous on the subject and opens the door to unfair competition between mobile operators;
- Prohibits permanent roaming and forces providers of IoT solutions to migrate to other communications technologies rather than mobile communications.

Conclusion

- The tariffs for roaming services (IMR) at national, regional and international level are always the concern of decision-makers and national regulatory authorities (search for regulatory and commercial solutions).
- Discussions do not focus solely on voice or data roaming, or on principles related to international trade; but also on the evolution of traffic and usage revenues, new economic models as well as new opportunities and innovations related to roaming of IoT and M2M communications.

Conclusion

A new subject of study under Question 8/3 of SG3, the main objective of which would be to study the economic implications of alternative appeal procedures and to develop guidelines or a draft Recommendation ITU- T.

Thank you!

Tableau de conversion du binaire-hexadécimal

Binaire	hexadécimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Les couches MAC définies par l'IEEE

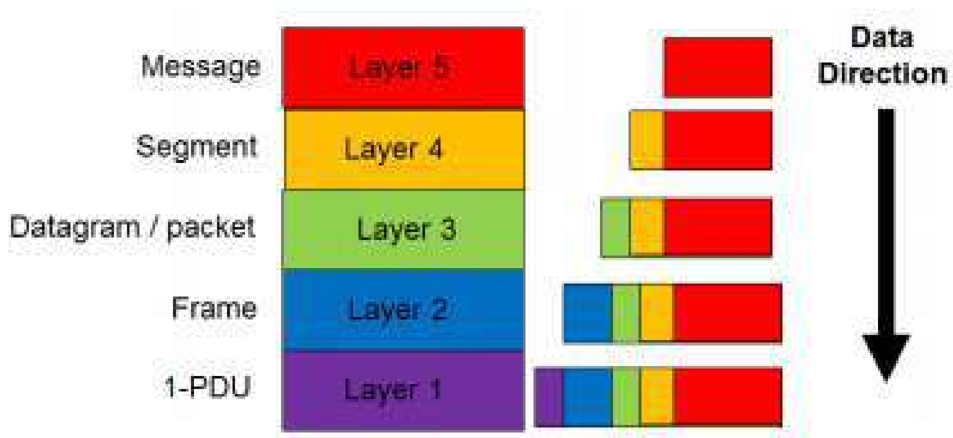
Couche MAC	Utilisation	Bande
802.11	Wi-Fi	802.11, 802.11b, 802.11g, 802.11n : ISM 802.11a : U-NII
802.15.1	Bluetooth	ISM 2,4 GHz
802.15.4	ZigBee, 6LoWPAN	ISM 2,4 GHz dans le monde entier ISM 902–928 MHz aux USA 868,3 MHz dans les pays européens 802.15.4a : 3,1–10,6 GHz
802.16	Réseaux métropolitains sans fil (WMAN, *Wireless Metropolitan Access Network*) Technologie large bande mobile (BWA, *Broadband Wireless Access*), WiMax	802.16 : 10–66 GHz 802.16a : 2–11 GHz 802.16e : 2–11 GHz pour le fixe et 2–6 GHz pour le mobile

Technologies de connectivité

La connectivité WAN (réseau global)		La connectivité LAN (réseau local)	
Les liaisons filaires	Limité aux systèmes fixes pour les bâtiments d'entreprises, infrastructures publiques ou maisons connectées.	Wifi, Wifi Halow (traverse plus facilement les obstacles et consomme moins) et WiGig (débit ultra rapide)	Dédié aux objets alimentés sur secteur en raison de la consommation énergétiques
Les réseaux cellulaires traditionnels	GPRS, EDGE, 3/4G, LPWA (réseau "low power wide area" dédiés IoT)	LiFi (Light Fidelity) ou VLC (Visible Light Communication)	Pour utilisation de lumière entre bleue et rouge diffusée par LED (problèmes de malillumination)
Les réseaux radio basse consommation dédiés	LP-WAN (technologies LoRa, Sigfox et Weightless et Qowisio en développement)	BLE (Bluetooth Low Energy)	Utilisations multiples faible portée faible consommation.
Les réseaux par satellite	Pour les zones non couvertes par les réseaux terrestres (5% du globe)	ANT	Protocole unidirectionnel faible portée pour capteurs dans le domaine du sport.
Les approches hybrides	Combinaisons de plusieurs de ces solutions selon le contexte	Z-Wave	Pour la maison connectée, portée de 50m.
Les approches futuristes	Projet de Web global par ballons / satellites / drones	ZigBee	Pour plusieurs utilisations, portée de 100m.
		EnOcean	Portée de 300m, ultra basse consommation et capteurs autoalimentés. Utilisable pour la domotique (en développement).
		6LoWPAN	Standard permettant de diminuer la consommation d'énergie et rendre compatible le protocole IP avec le domaine IoT.

Encapsulation

- Flux de données dans la pile de protocoles



PRIDA Track 1 (T1)

IoT Lab Experiment

Agenda

- Part 1: Reminder
- Part 2: Business model and use cases
- Part 3 : IoT use cases design
- Part 4 : Firebase tutorial

IoT Architecture (Reminder)

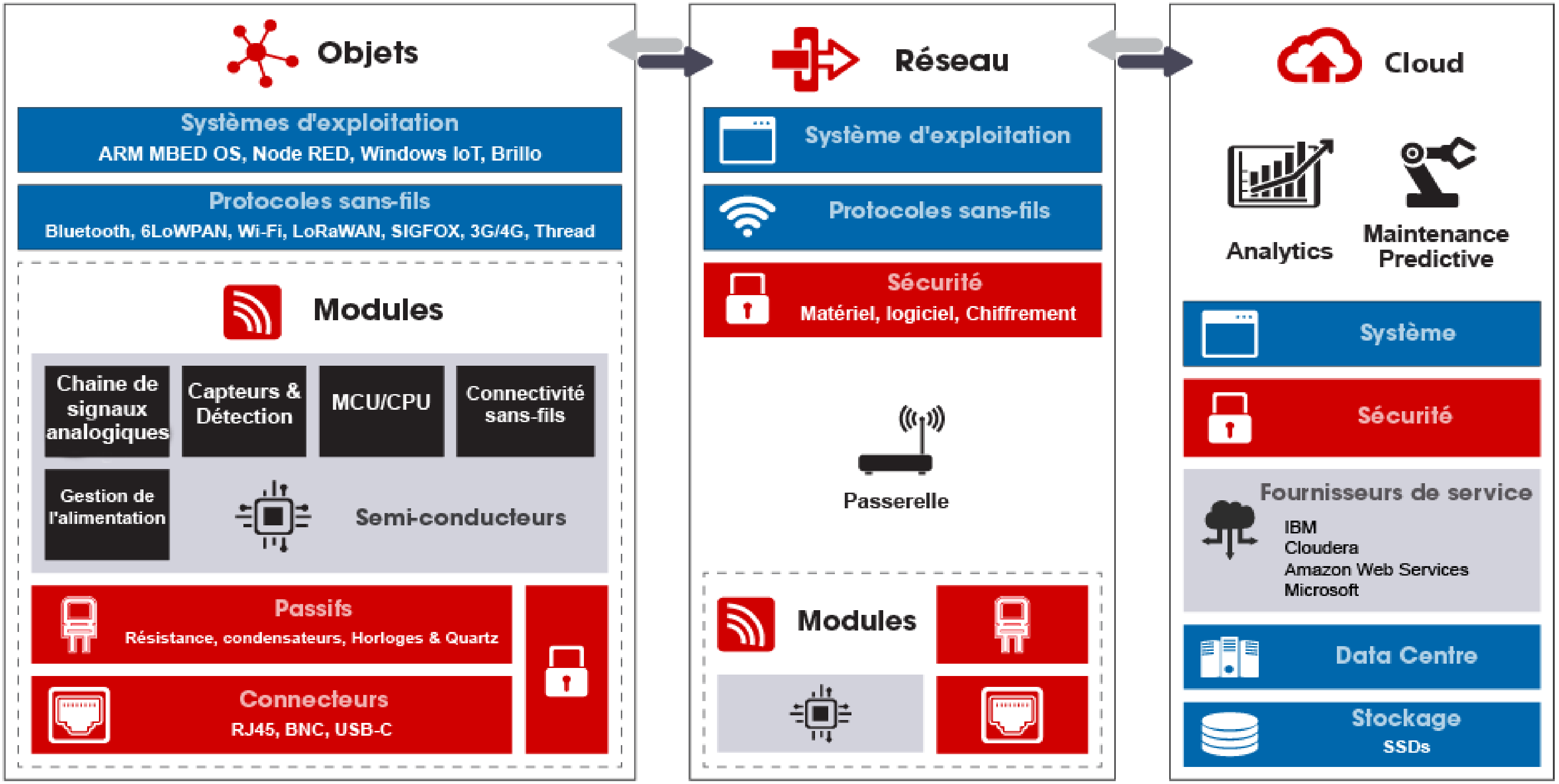
Application layer

Information processing layer

Network layer

Perception layer

Functional architecture (Reminder)



Source : https://fr.rs-online.com/web/generalDisplay.html?id=i/ido-internet-des-objets

IoT components (Reminder)

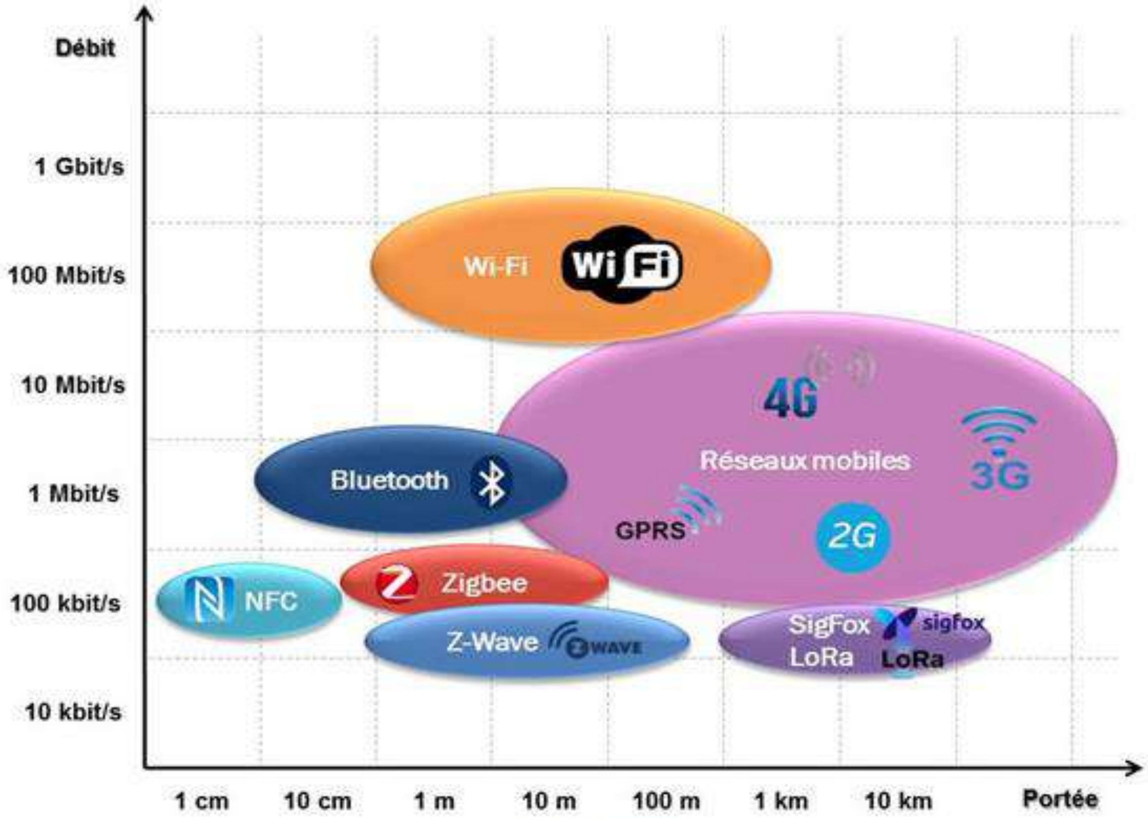
- Sensors/actuators
- Gateways
- Connectivity
- Platforms
- Application/services

Sensors and gateways

Criteria for choosing connectivity technologies

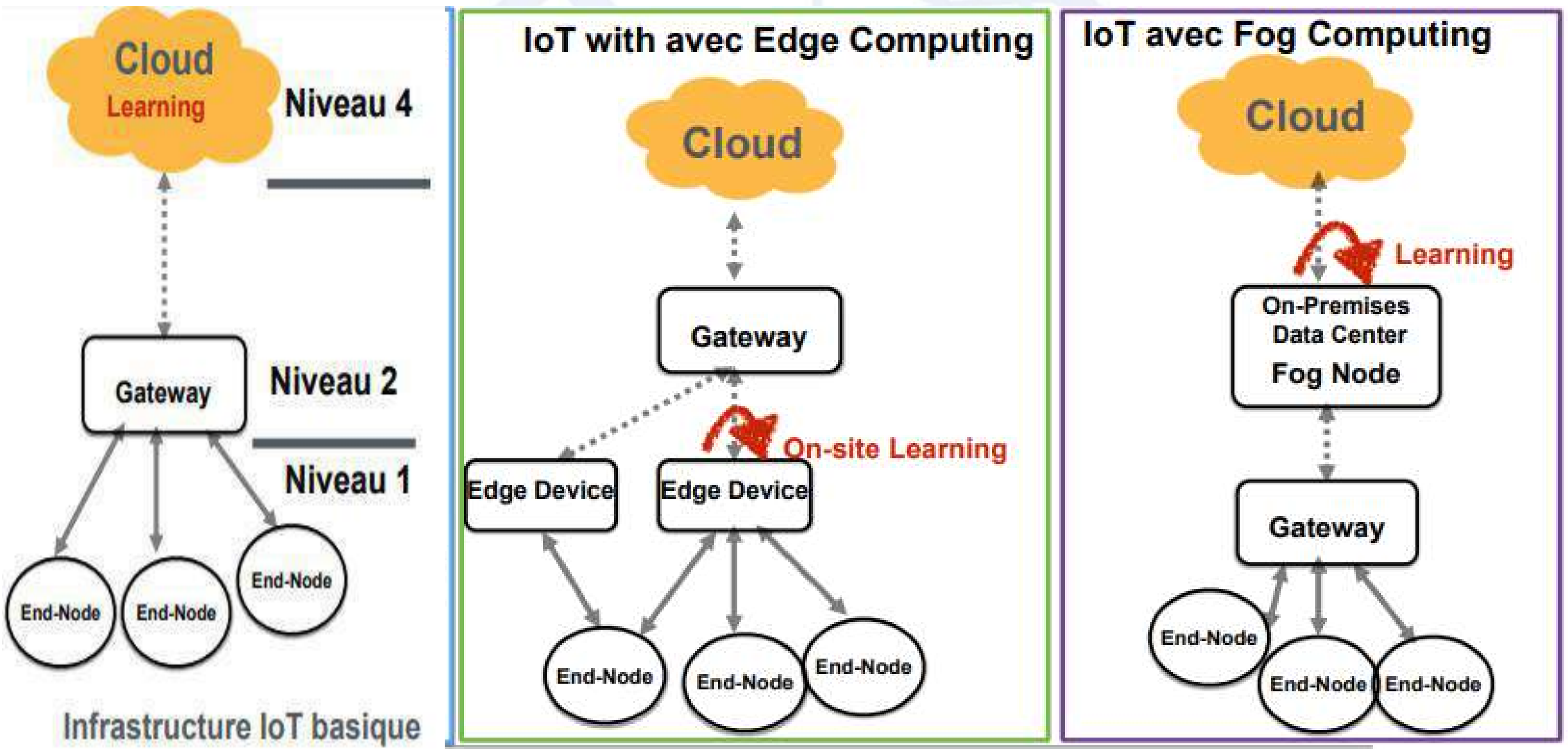
- Network area
- Spectrum (dedicated or shared)
- Batterie life
- Connectivity cost
- Module cost
- Bandwidth

Connectivity technologies



Source : CRE

Cloud Platforms (Reminder)



Edge Computing

Benefits of the Edge Architecture

- Reduce the latency times resulting from sending data to the cloud;
- Reduce use of bandwidth, thus saving money and avoiding bottlenecks;
- Rapid analysis and/or fast action *(intelligence shifting to the edge, including real-time decisions)*
- help strengthen security through encryption at the source before relaying data to the cloud.

Security measures

- Security of the IoT system can be assessed by employing classical security and risk analysis measures.
- Typical security requirements should be employed in the IoT system:
  - Authentification
  - Confidentiality
  - Integrity
  - Availability
  - Public Key infrastructure

Privacy and liability

- Measures for privacy protection:
  - Privacy by design
  - **Choice and notice** states that entities that collect data should give users the option to choose what they reveal and notify users when their personal information is being recorded.
  - **Purpose specification and use limitation** states that entities collecting data must clearly state the purpose to the authority that permits the collection of those data.
  - **Data minimization s**uggests that a company can collect only the data required for a specific purpose and delete that data after the intended use.
  - **Security and accountability s**tates that entities that collect and store data are accountable and must deploy security systems to avoid any unauthorized access, modification, deletion, or use of the data.

IoT value chain

Devices

- Sensors
- Embedded Chips
- MEMS
- Actuators
- Modules
- SIM Card
- System Design
- Firmware& Drivers
- Interoperability

Connectivity

- Network Equipment
- Connectivity
- Network Service Provider
- Protocols
- Device Provisioning & Configuring

Platform/ Enablement

- IoT Platforms
- Cloud
- Analytics
- Middleware
- Integration with third-party applications
- Testing
- API Development
- Billing

Applications

- Applications Development
- UI/UX Design
- Building Vertical Solutions
- Bundling of Services
- API Development & Management

Activities model

- Actors in the IoT ecosystem can have a variety of relationships in actual deployments. The diversity of these relationships is presented by business models

UIT Recommandation 2060

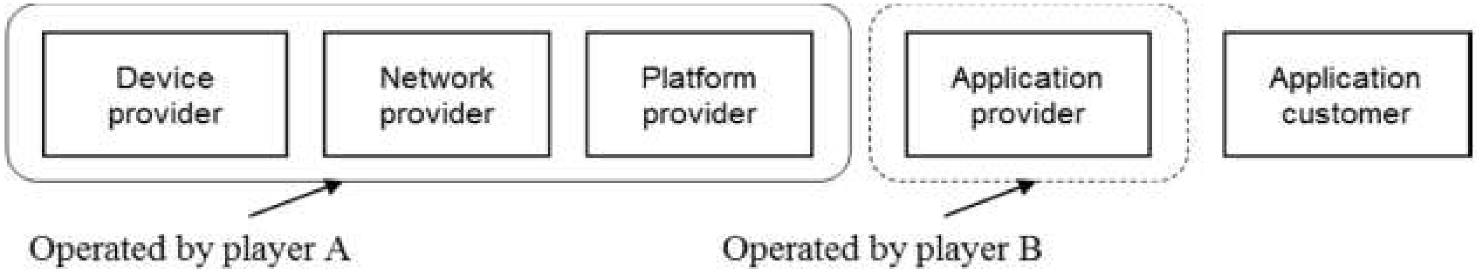
Model 1

Example :

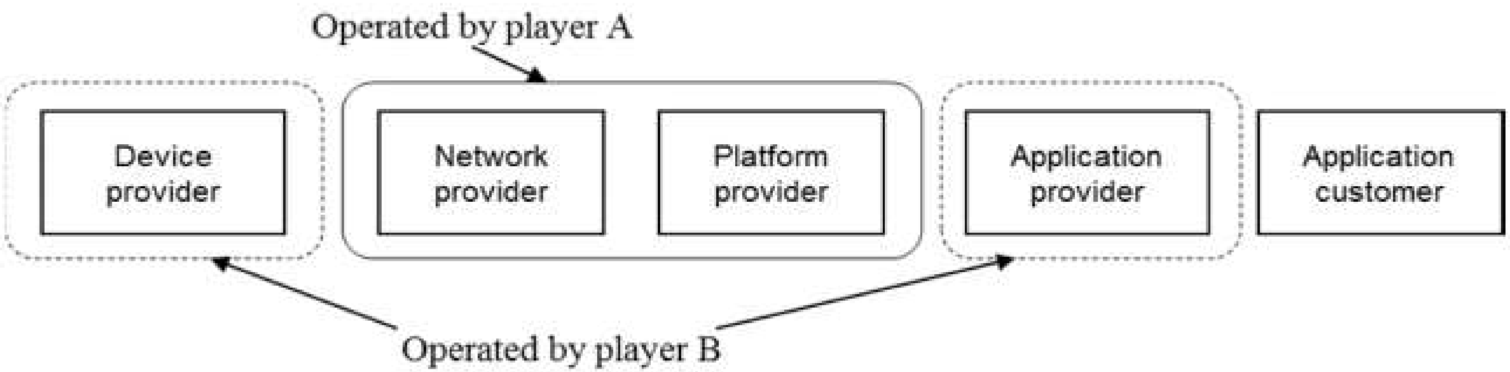
In general, telecom operators and some vertically integrated businesses (such as smart grid and intelligent transport systems (ITS) businesses) act as player A in model.

Activities model

Model 2 :

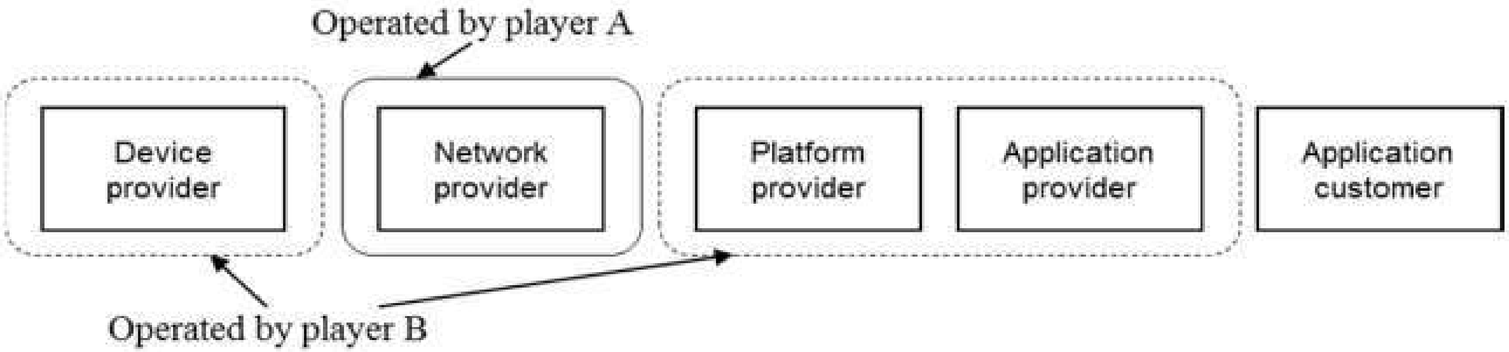


Model 3 :

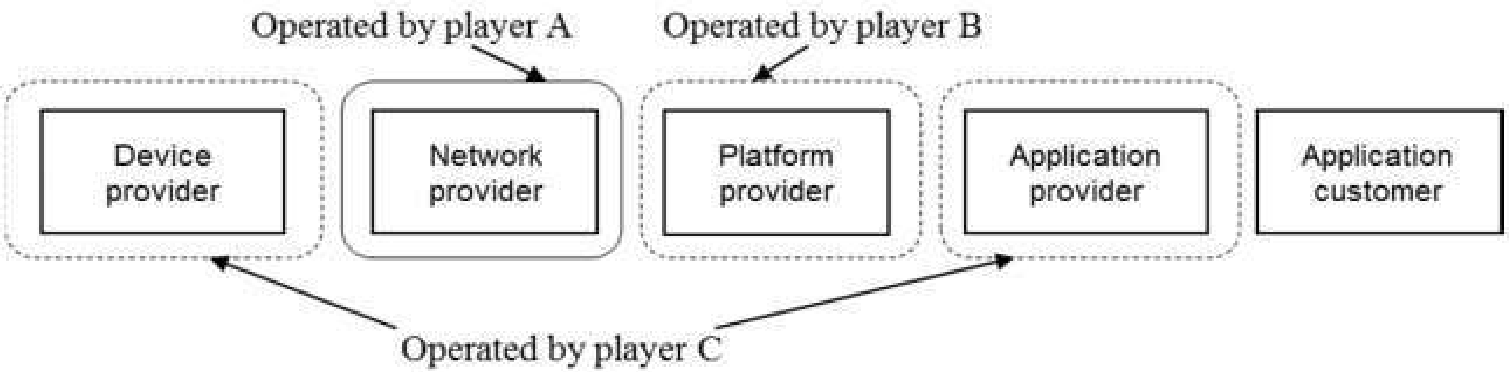


Activities model

Model 4 :



Model 5 :



Part 2: Business Model

Old business models

The basic business models that currently exist :
Retail sales : Equipment or device manufacturer expends its own money or raises financing to build products which are then sold to customers. The equipment or device manufacturer only captures value during that one transaction, the expectation is that there is a positive margin between revenue and expenses and that customers will buy more of the same product or other products.
Product lease/Subscription : Instead of selling the machine/device, the vendor leases the product to the customer.

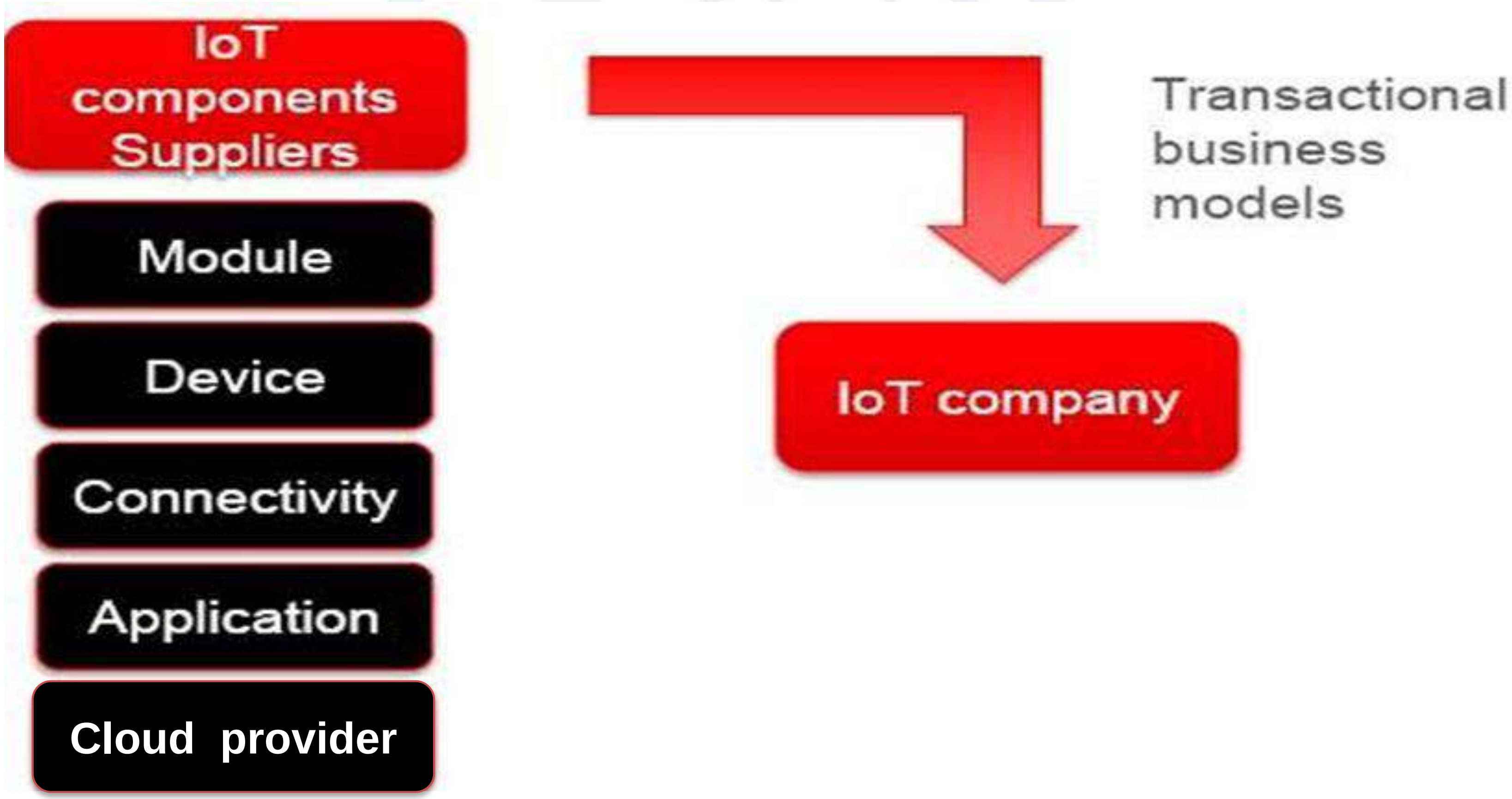
New models

It’s imperative that new businesses and startups should explore new models for value creation and capture. The new business models will stem from the increased interactions afforded by IoT devices.

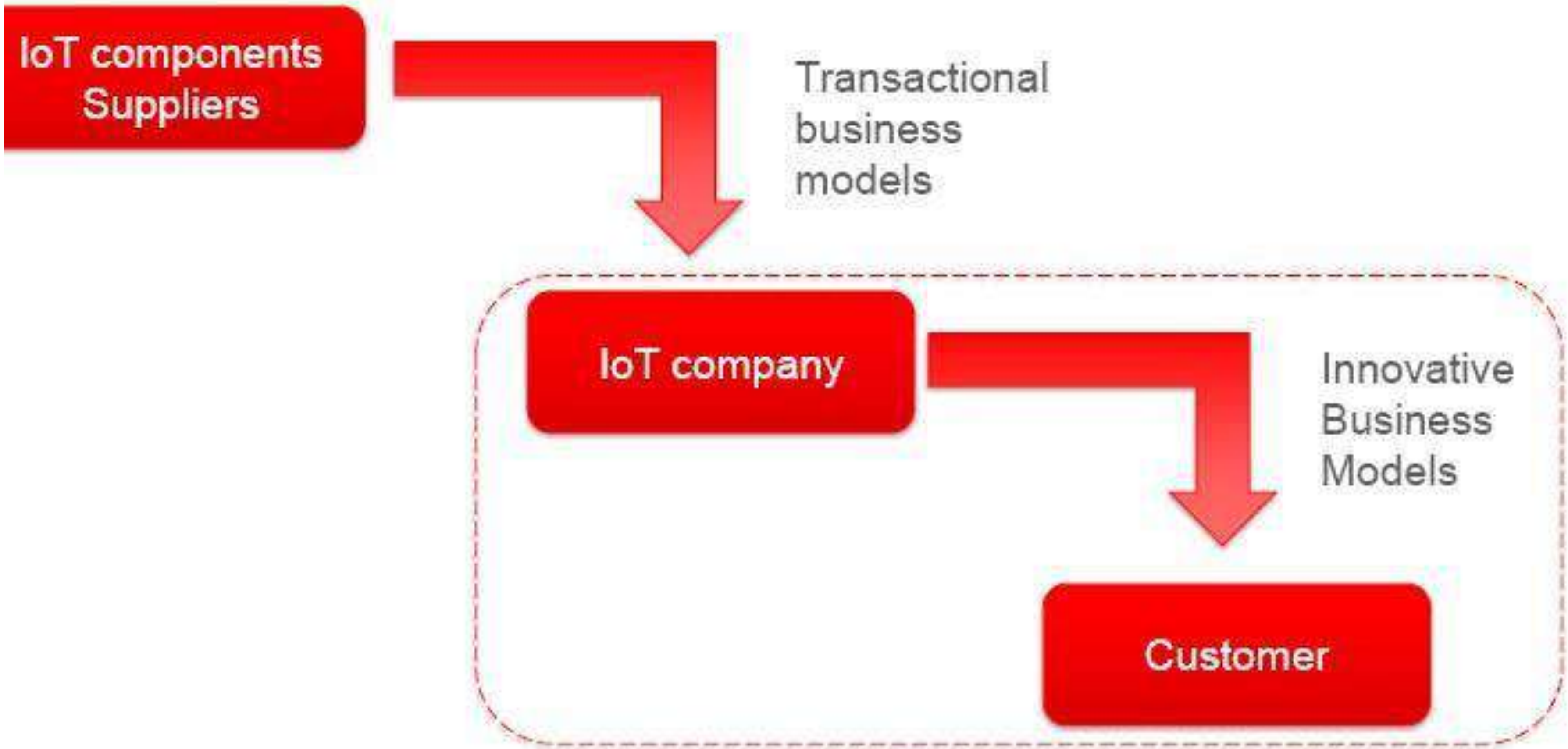
Business Model for IoT

1. IoT can provide significant innovation in business models
2. Business model innovation will have most impact where the IoT company interacts with the customer

Business Model



Business Model



Main Business Models

Business models
Revenue-sharing
Cost-savings sharing
Product-sharing
Product-as-a-Service
Performance-as-a-Product
Transactional

Main Business Models

Business models	Revenue of the IoT company			Device ownership	
	Upfront	Recurring	Usage	User	IoT company
Revenue-sharing		✓			✓
Cost-savings sharing		✓			✓
Product-sharing			✓		✓
Product-as-a-Service		✓			✓
Performance-as-a-Product			✓	✓	
Transactional	✓			✓	

The descriptions above are the most common and variations are possible.
For example, transactional may also include device ownership from the IoT company.

Revenue sharing

Problem	Luggage lost in air transit.
Traditional solution	• The airline would try to find the lost luggage using manual processes, which are costly, time consuming and generate customer dissatisfaction.
IoT solution	• A tracking device is placed inside the luggage and transmits its location using 2G. The user can track his luggage using a smartphone app.
IoT business model	• The airline charges a fee to its customers for using the luggage tracking service, or offers the service for no charge to premium customers. A share of the revenue generated is paid to the IoT company, which maintains the IoT solution.

Revenue sharing

Traditional business model

IoT business model

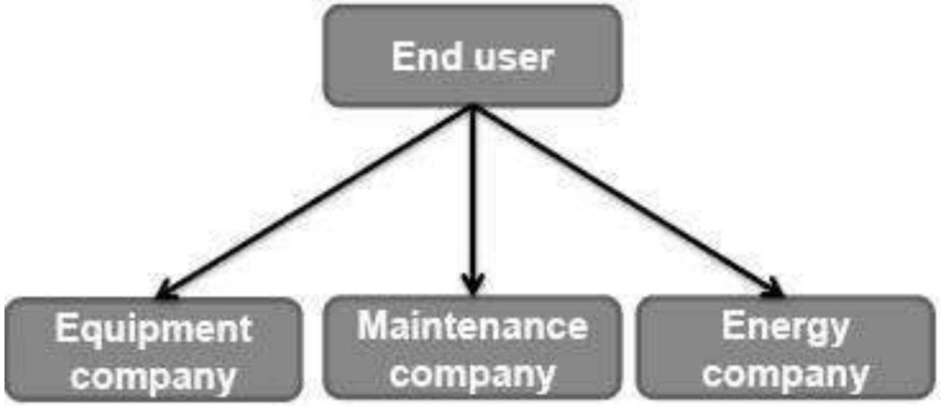
The IoT solution allows the airline to generate fees and differentiate its service

Costs savings sharing

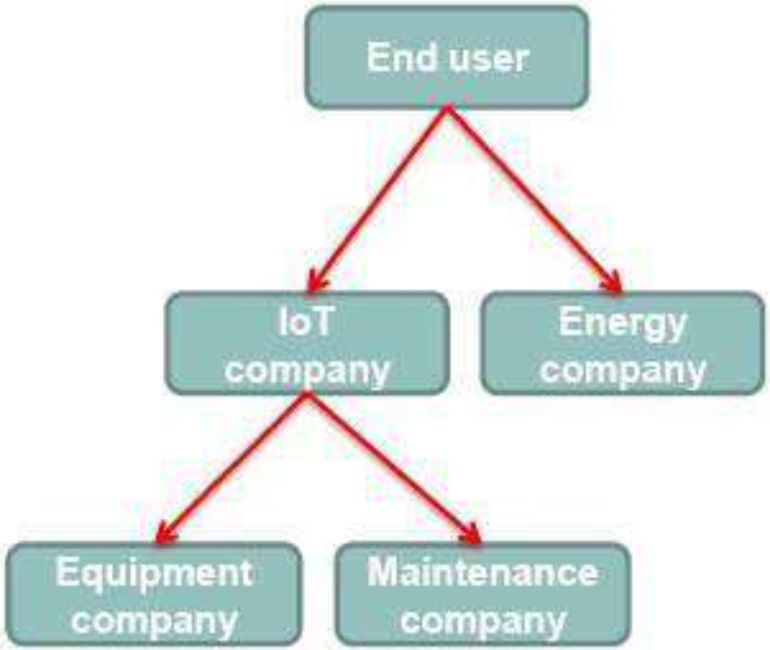
Problem	Home/building energy consumption.
Traditional solution	• The end user pays for the Heating, Ventilating and Air Conditioning (HVAC) system and its maintenance, and also pays the energy company pays for its power consumption.
IoT solution	• The end user installs equipment to monitor and control the HVAC system, so it can automatically adjust to the user's requirements and optimise its energy consumption.
IoT business model	• The IoT company installs the monitoring and control equipment with no up-front fees. • The end user pays for the equipment rental from the energy savings generated by the IoT solution. If the savings amount to $100 and the rental is $40, the end user keeps $60 as overall savings.

Costs savings sharing

Traditional business model



IoT business model

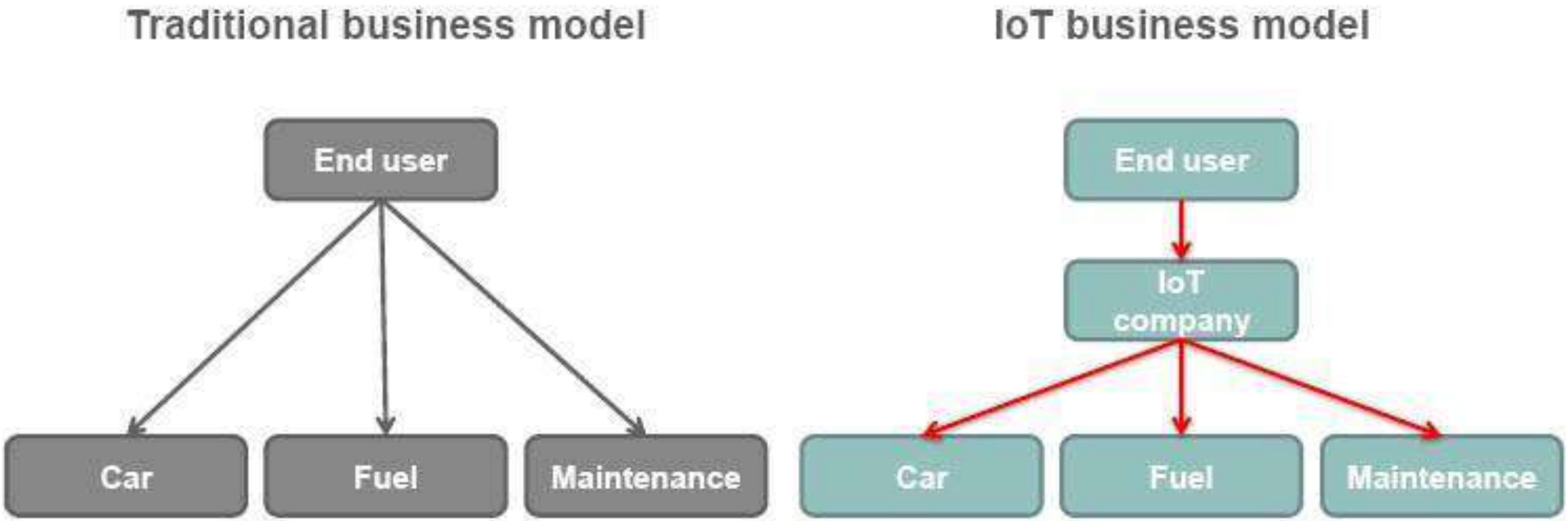


The IoT solution allows end users to save on their energy consumption costs and use part of the savings to pay for the IoT solution

Product - sharing

Problem	Relatively high investment and maintenance costs of a car.
Traditional solution	• The end user buys the car upfront and pays for its ongoing maintenance, fuel and insurance.
IoT solution	• The end user can drive a number of cars made available across a city, without needing to own one. • All car related costs are managed by the IoT company. A smartphone app, allows users to reserve the car, locate and unlock it.
IoT business model	• The IoT company charges end users by the minute for using a car. The fees include the cost of the car, its maintenance, fuel and insurance. • From managing a large fleet of vehicles, the IoT company can achieve economies of scale, which can be translated into competitive prices for the end user.

Product - sharing

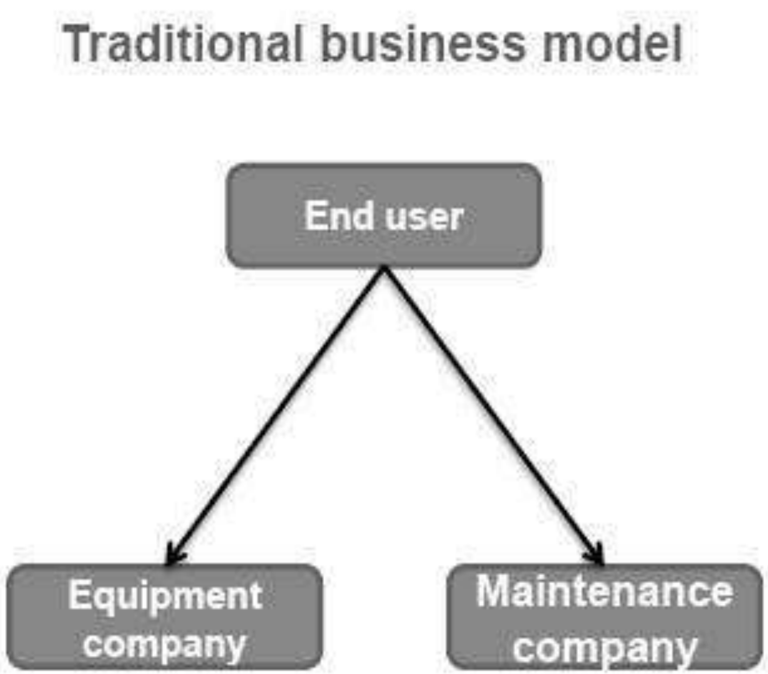


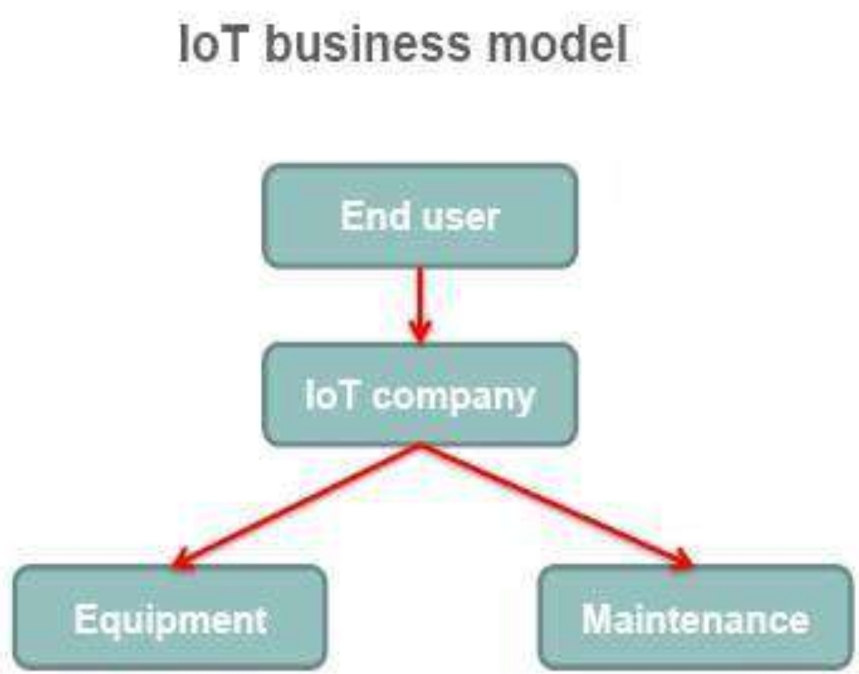
The IoT business model allows the IoT company to transfer savings from economies of scale to the end user

Product-as-a-Service

Problem	High investment and maintenance cost of heavy medical equipment.
Traditional solution	• The user (e.g. hospital) buys the equipment upfront and can face high maintenance costs. Different suppliers may be involved in selling and supporting the equipment.
IoT solution	• The hospital pays for the equipment and maintenance to the IoT company. • The equipment is remotely monitored in terms of usage and performance, allowing the IoT company to perform predictive maintenance. As a result, the end user can benefit from reduced or no disruption from equipment downtime.
IoT business model	• The IoT company charges a recurring fee to the hospital. This fee includes the use of the equipment and its maintenance. • The equipment is owned by the IoT company, who by actively monitoring it, may pre-empt potentially serious issues resulting in expensive maintenance.

Product-as-a-Service



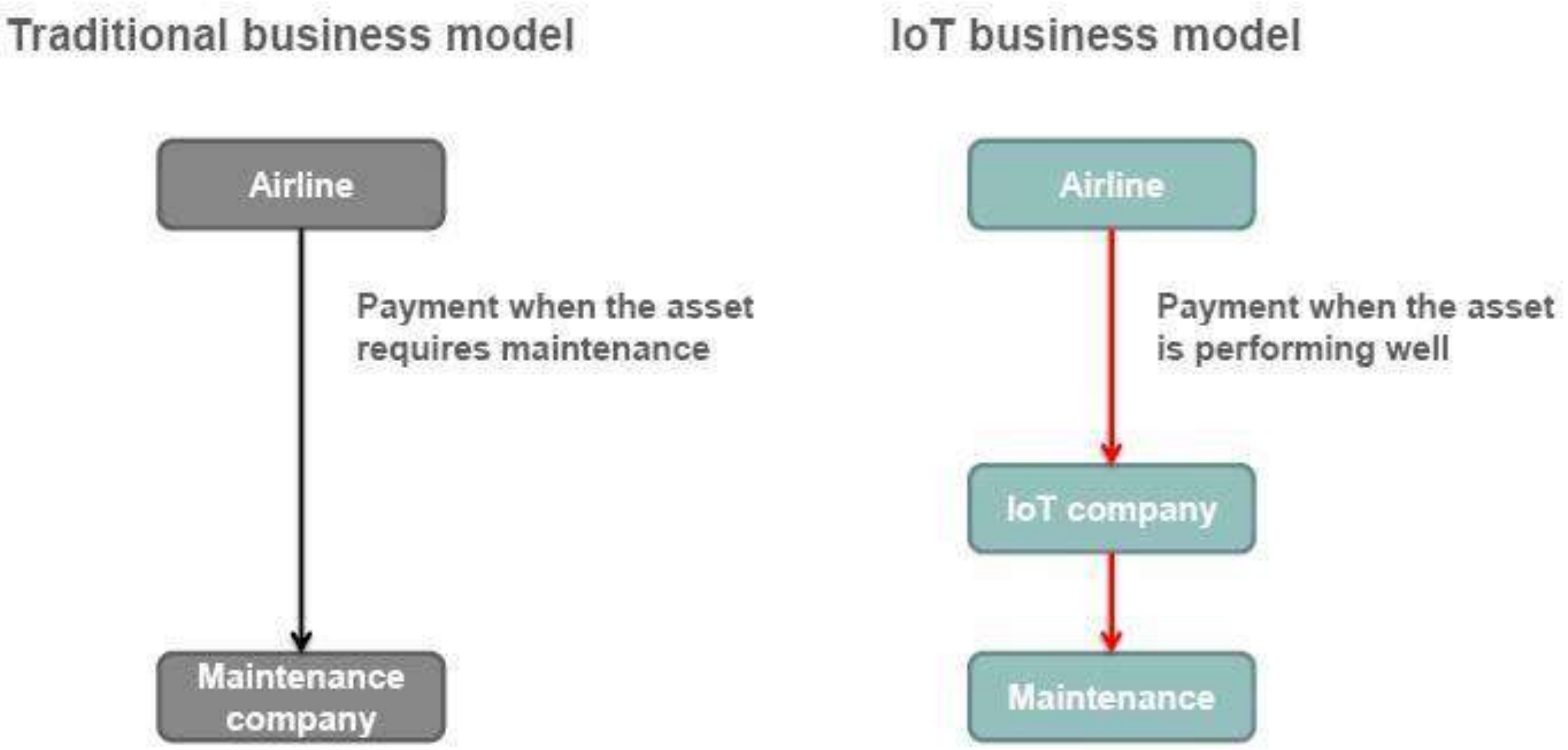


The IoT solution can perform predictive maintenance, allowing the end user to benefit from lower or no disruption and more affordable cost

Performance-as-a-product

Problem	Uncertain aircraft engine maintenance cost.
Traditional solution	• Airlines would buy the engine from manufacturers such as Rolls-Royce and take on the risk of the engine becoming inoperable and possible high maintenance cost.
IoT solution	• The aircraft engines have embedded sensors that send data back to the engine manufacturer (IoT company). • This information is used by the IoT company to identify and fix problems remotely, minimising the risk of engine downtime.
IoT business model	• Rolls-Royce's TotalCare program is sold to airlines as a solution to make the engine's maintenance costs predictable. • Under this program, Rolls-Royce is responsible for the engine's maintenance and only gets paid if the engine is operational. Its revenues equal a fixed fee per flying hour.

Performance-as-a-product



The IoT solution aligns the interests of the airline with the maintenance provider

Case study 1 : Farm water monitoring

Problem: How do I know if my water tanks need to be refilled?

Customers	• Farmers
Needs to address	• Water availability for animals. This is particularly relevant in dry lands (e.g. certain areas of Africa)

Case study 1 : Farm water monitoring

IoT solution & benefits

IoT solution	• A sensor is placed in the water tanks and troughs to monitor the water level sending an alert to the controlling station (or via SMS text or email) If water levels flow or pressures go outside a pre-configured range
Benefits	• The solution increases the efficiency in the water usage, which can be particularly important in developing countries and in dry lands

Case study 1 : Farm water monitoring

Technologies

Feature	Requirement	Comment
Network Area	▪ Wide	Extended fields in remote locations can require significant signal coverage
Spectrum	▪ Shared / Dedicated	Quality of service of transmission is not a crucial factor
Battery life	▪ Long	The sensors may be placed in remote points of the field and need to have long battery life. Solar panels may contribute to extending battery life
Connectivity cost	▪ Low	Associated to the low bandwidth requirement
Module cost	▪ Medium	Price may be an issue in developing countries
Bandwidth	▪ Low	Data needed to monitor water level is limited

Technologies: LPWA 2G

Farm water monitoring

Business models	Revenue of the IoT company	Device ownership
Revenue-sharing	Recurring	IoT company
Cost-savings sharing	Recurring	IoT company
Product-sharing	Usage	IoT company
Product-as-a-Service	Recurring	IoT company
Performance-as-a-Product	Usage	User
Transactional	Upfront	User

Most likely business models

Liability

Liability

- Establishing responsibility needs to be clear in the event of damages resulting from the IoT solution
- If the solution fails and animals die because of lack of water, who is to blame:
  - The local reseller installer?
  - The IoT technology company?
  - The network operator?
  - The farmer?

Case of study 2 : Elderly care monitoring

Problem: How can I monitor an elderly family member?

Customers	• People with elderly family
Needs to address	• Monitoring the activity of the elder • Alert if the activity significantly changes from what is expected

Case of study 2 : Elderly care monitoring

IoT solution & benefits

IoT solution	• Movement sensors are placed around the home, transmitting data on activity (e.g. doors, people) • The sensors are connected to a hub that sends data to an application, using cellular connectivity
Benefits	• The monitoring system can reduce family members' anxiety regarding the well being of their elderly relative • Elderly can continue living in their homes, avoiding being taken to a care home

Case of study 2 : Elderly care monitoring

Technologies

Feature	Requirement	Comment
Network Area	▪ Wide	The hub sending data to an application uses cellular connectivity, so requires wide network area
Spectrum	▪ Dedicated	The connectivity service should be reliable
Battery life	▪ Low	The hub is plugged in to an electrical outlet
Connectivity cost	▪ Medium	Price sensitivity will vary by person/country. We assume the price will need to be moderate
Module cost	▪ Medium	Again, price sensitivity will vary but we assume it will need to be moderate
Bandwidth	▪ Low	The application requires low bandwidth

Technologies: 2G ? ?

Elderly care monitoring

Business models	Revenue of the IoT company	Device ownership
Revenue-sharing	Recurring	IoT company
Cost-savings sharing	Recurring	IoT company
Product-sharing	Usage	IoT company
Product-as-a-Service	Recurring	IoT company
Performance-as-a-Product	Usage	User
Transactional	Upfront	User

Most likely business models

Privacy and data protection

Data collection	• Who collects, shares and uses the individuals' data and why?
Data protection	• How is the security of individuals' data ensured? • How is the privacy of individuals' data ensured?
Data use	• How can individuals exercise choice and control over how their data will be used?

Case study 3 : smart public garbage bin

Problem: How can you improve the efficiency of waste collection in cities?

Customers	• Cities and towns
Needs to address	• Improve the public waste collection service • Save costs on public waste management by making the service more efficient

Case study 3 : smart public garbage bin

IoT solution & benefits

IoT solution

- The smart garbage bin monitors and reports the bins status, alerting when it needs to be emptied
- The solutions help optimise waste collection (i.e., only emptying bins when necessary

Benefits

- Pollution is reduced as bins are never full and traffic on the roads is reduced
- Taxes can be spent more efficiently

Case study 3 : smart public garbage bin

Technologies

Feature	Requirement	Comment
Network Area	▪ Wide	The bins are located community-wide or city-wide
Spectrum	▪ Shared / Dedicated	Quality of service (timeliness) of transmission is not a crucial factor
Battery life	▪ Long	Battery life has to be long, but use of solar panels may help widen the battery life
Connectivity cost	▪ Low	Expected to be low and in line with bandwidth requirements
Module cost	▪ Low	The cost per bin needs to be low so it is feasible to deploy across all bins in a given community/city. Bins are exposed and easily subject to theft.
Bandwidth	▪ Low	The application requires low bandwidth

Technologies: LPWA 2G ?

Smart public garbage bin

Business models	Revenue of the IoT company	Device ownership
Revenue-sharing	Recurring	IoT company
Cost-savings sharing	Recurring	IoT company
Product-sharing	Usage	IoT company
Product-as-a-Service	Recurring	IoT company
Performance-as-a-Product	Usage	User
Transactional	Upfront	User

Most likely business models

Smart public garbage bin

Privacy

Data collection

- Regulators should support and encourage measures by which industry can identify and mitigate risks to privacy, and through which they can demonstrate accountability.
- This objective can be achieved through privacy enhancing technologies and tools that help consumers to manage their privacy and control how their data are used.

- In 2013, the City of London fitted devices in recycling bins to collect data on footfall.
- The data was collected by logging the media access control (MAC) of passing phones and done without the knowledge of those individuals.
- European Union regulation forbids mining personal data using 'cookies', which involves installing a monitoring device on individuals' phones or computers. However, tracking MAC codes leaves no trace on phones.

Case study 4 : Security alarms

Problem: How can I keep my home protected?

Customers	• Property owners
Needs to address	• Alert the police and property owner in case of intrusion • The system needs to be able to work without a local power source or fixed connectivity

Case study 4 : Security alarms

IoT solution & benefits

IoT solution

- Sensors are spread around the property to detect motion and sound
- When a sensor is activated, it sends an alert to property owner and/or control centre, who can warn the police
- The security system can be monitored and armed/disarmed using a smartphone app or web interface

Benefits

- Reductions of crime. The dissuasive effect of the alarm system can help reduce chances of a break in
- Reduction of negative outcome from break-in, due to early dispatch of police and system's ability to operate without fixed line connection and local power source

Case study 4 : Security alarms

Technologies

Feature	Requirement	Comment
Network Area	▪ Wide	The area to be covered is indoors and needs to operate without fixed line
Spectrum	▪ Dedicated ▪ Shared	Ideally, the service would have some quality guarantee, but it could also work in shared spectrum
Battery life	▪ Short	Battery life can be short as the alarm can be connected to a local power source
Connectivity cost	▪ Low	The cost is expected to account for a relatively low amount of the security alarm system's recurring fee
Module cost	▪ Medium	The cost is expected to account for a relatively low amount of the security alarm system's cost
Bandwidth	▪ Low	The application requires low bandwidth

Technologies: 2G ZigBee RF-Mesh

Security alarms

Business models	Revenue of the IoT company	Device ownership
Revenue-sharing	Recurring	IoT company
Cost-savings sharing	Recurring	IoT company
Product-sharing	Usage	IoT company
Product-as-a-Service	Recurring	IoT company
Performance-as-a-Product	Usage	User
Transactional	Upfront	User

Most likely business models

Case study 4 : Security alarms

Operational issues & policy topics

Operational considerations

- Interference
- Alarm fails to trigger
- False alarms
- Reputation

Policy areas

- Traffic management
- Security
- Privacy

THE INTERNET OF THINGS REQUIRES A MINDSET SHIFT

Because you'll create and capture value differently.

		TRADITIONAL PRODUCT MINDSET	INTERNET OF THINGS MINDSET
VALUE CREATION	Customer needs	Solve for existing needs and lifestyle in a reactive manner	Address real-time and emergent needs in a predictive manner
	Offering	Stand alone product that becomes obsolete over time	Product refreshes through over-the-air updates and has synergy value
	Role of data	Single point data is used for future product requirements	Information convergence creates the experience for current products and enables services
VALUE CAPTURE	Path to profit	Sell the next product or device	Enable recurring revenue
	Control points	Potentially includes commodity advantages, IP ownership, & brand	Adds personalization and context; network effects between products
	Capability development	Leverage core competencies, existing resources & processes	Understand how other ecosystem partners make money

SOURCE SMART DESIGN

HBR.ORG

Part 3 : IoT use cases design

PRIDA Track 1 (T1)

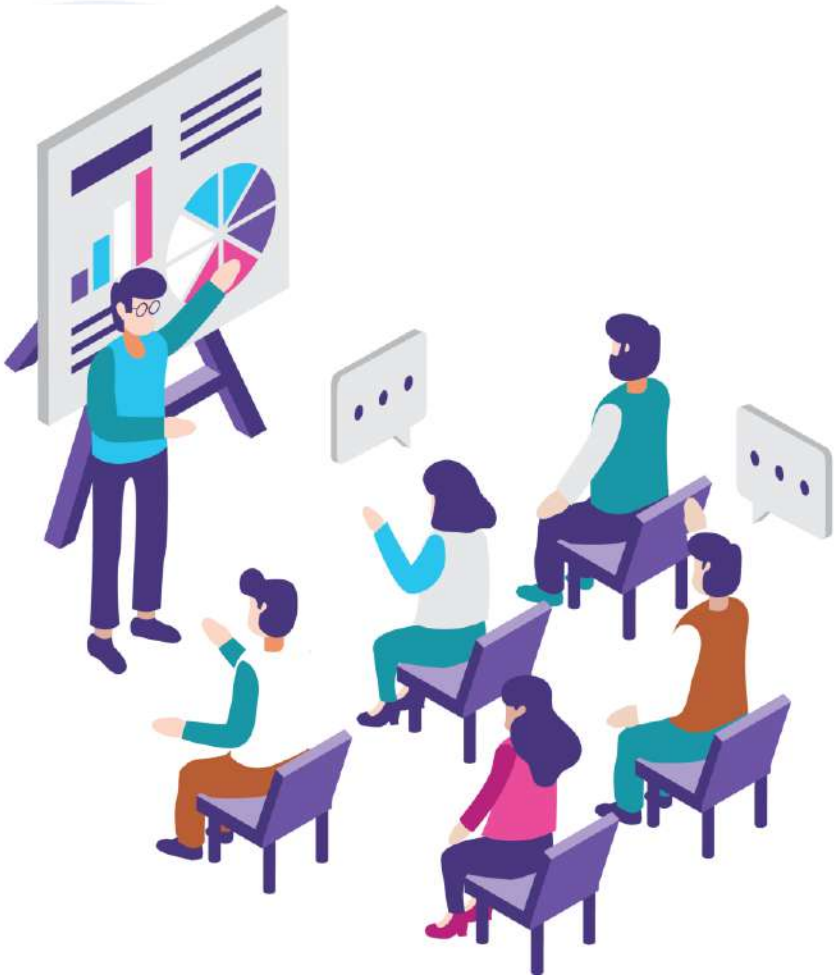
IoT Lab Experiment

Agenda

- Part 1: Reminder
- Part 2: Business model and use cases
- Part 3 : IoT use cases design
- Part 4 : Firebase tutorial

Workshop plan

- Objective of the workshop
- Technical approach
- First part :
  Problems to be solved
- Second part :
  Brainstorming
- Third part :
  Practical demonstration



Goal of the workshop

- The first goal of this practical training is to understand the importance of the IoT as a modern technological tool able to solve complex problems.
- The second objective is to allow participants to initiate a technical sizing and technological choice of an IOT architecture using open source tools
- Finally, in order to be able to master the practical aspect, we will together demonstrate the development of an IOT solution with the objective of solving a current problem.

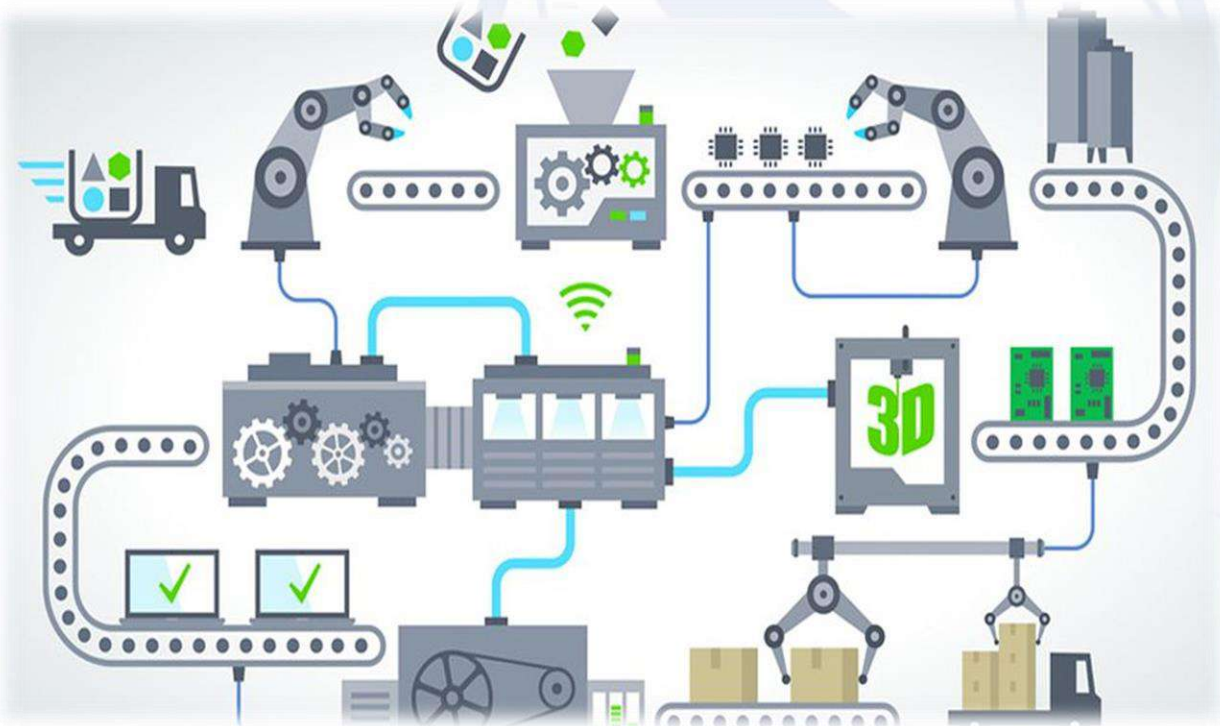
Technical approach

In order to master the practical aspect and understand the principle of IOT, it is important to discover the different areas of application of this technology.
To do this, we will discuss chronic issues in vital sectors and participants will be invited to draw on old theoretical training to define the elements of the solution to be proposed.
Next, we will discuss together around the architectures presented
Finally we will make a practical application in a concrete way.

Part 1: Problematic

Topic 1: Connected industry 4.0

The Fourth Industrial Revolution (or Industry 4.0) is the ongoing automation of traditional manufacturing and industrial practices, using modern smart technology. Large-scale machine-to-machine communication (M2M) and the internet of things (IoT) are integrated for increased automation, improved communication and self-monitoring, and production of smart machines that can analyze and diagnose issues without the need for human intervention



Topic 1: Connected industry 4.0

Nowadays monitoring of production and feedback in real time has become a necessity to ensure competitiveness in the industrial sector. This in order to react quickly and to make the right decisions. To do this, the Internet of Things asserts itself as the convergence of the virtual world, digital design, management with real world products and objects.

Specifications

Subject 1:
The problem is to design a solution allowing manufacturers to monitor the energy consumption of their machines in real time and remotely.

Subject 2:
The problem is to develop a solution for the remote supervision of an industrial production line

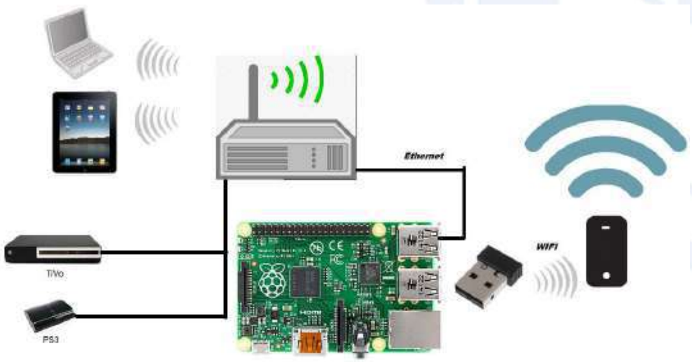
Hardware Tools : Connected industry 4.0

Energy measurement unit

Voltage sensor

Current sensor

Interface card



Gateway to Raspberry Pi Board Base

Gateway to Arduino Board Base

Topic 2: Smart agriculture

The world is changing with the emergence of new needs in various vital sectors, especially agriculture. It's a vital sector for the country. Currently the integration of new technologies has become a necessity to ensure sustainable development. Smart Agriculture is a hi-tech and effective system of doing agriculture and growing food in a sustainable way. It is an application of implementing connected devices and innovative technologies together into agriculture.

Topic 2: Smart agriculture

Smart Agriculture majorly depends on IoT thus eliminating the need of physical work of farmers and growers and thus increasing the productivity in every possible manner. IoT improves the entire Agriculture system by monitoring the field in real-time. With the help of sensors and interconnectivity, the Internet of Things in Agriculture has not only saved the time of the farmers but has also reduced the extravagant use of resources such as Water and Electricity.

Specifications

Subject 1:
The problem is to design a solution that allows farmers to manage their irrigation system remotely.

Subject 2:
The problem is to develop a solution for the remote supervision of an aquaculture station.

Hardware Tools: Smart agriculture

Water pump

Solenoid valve

Temperature sensor

Gateway

Dissolved oxygen sensor

Weather Channel

Soil moisture sensor

Topic 3 : Telemedecine

Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare illustrates the innovative concepts, methodologies and frameworks that will increase the feasibility of the existing telemedicine system.

Thanks those technologies, telemedicine allows remote access from a patient to a doctor or a medical team. It represents another way of treating, with the same quality and safety requirements..

Topic 3 : Telemedecine

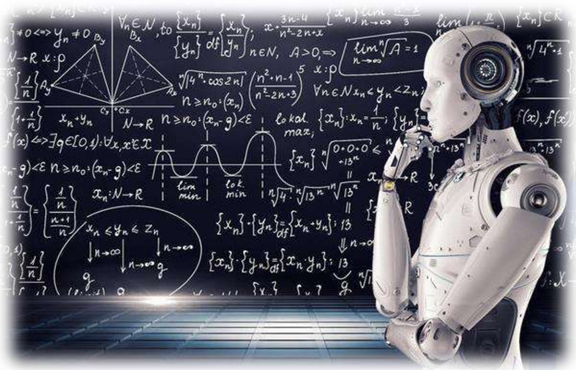
Telemedicine brings together medical practices permitted or facilitated by telecommunications. It is an exercise of medicine through telecommunications and technologies that enable remote health services and the exchange of related medical information.

Specifications

Subject 1:
The problem is to design a solution to detect symptoms and signs reminiscent of covid-19 infection in the population and to monitor daily clinical evolution of symptoms of infection in users

Subject 2:
The problem consists to develop a solution for remote supervision of the vital parameters and the ECG tracing of hospitalized patients.

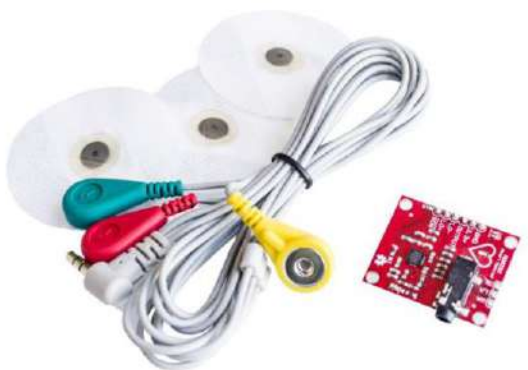
Hardware & Software Tools: Telemedecine



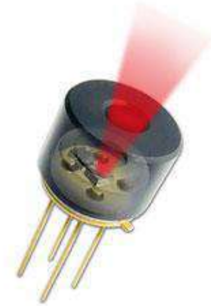
Artificial intelligence

Massive database

Protection of personal data



ECG sensor



Non-contact body temperature sensor

WEB / mobile platform

Topic 4: Smart City

Smart cities use a combination of the internet of things (IoT) devices, software solutions, user interfaces (UI) and communication networks. However, they rely first and foremost on the IoT. The IoT is a network of connected devices -- such as vehicles, sensors or home appliances -- that can communicate and exchange data. Data collected and delivered by the IoT sensors and devices is stored in the cloud or on servers. The connection of these devices and use of data analytics (DA) facilitates the convergence of the physical and digital city elements, thus improving both public and private sector efficiency, enabling economic benefits and improving citizen's lives.

Topic 4: Smart City

A smart city is a municipality that uses information and communication technologies (ICT) to increase operational efficiency, share information with the public and improve both the quality of government services and citizen welfare. While the exact definition varies, the overarching mission of a smart city is to optimize city functions and drive economic growth while improving quality of life for its citizens using smart technology and data analysis

Specifications

Subject 1:
The problem is to design a solution allowing municipalities to monitor in real time the percentage of filling of buried bins.

Subject 2:
The problem is to develop a WEB and mobile platform allowing citizens to recover their sorted household waste.

Tools : Smart City

Ultrasonic sensor

GSM module

GPS module

Lithium battery

LoRa Node

LoRa Gateway

Firebase

NoSql Database

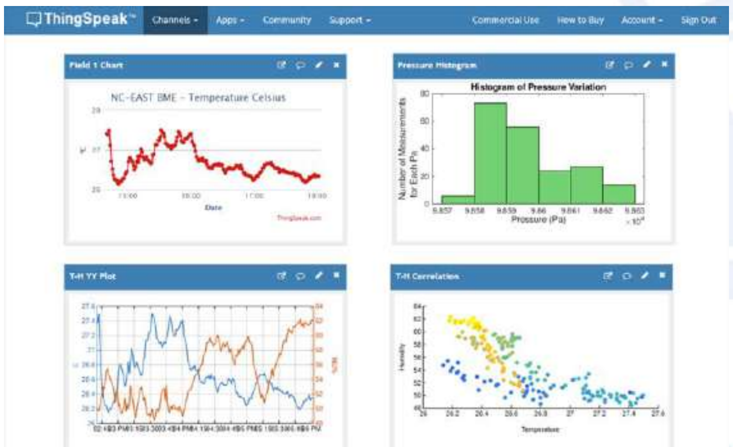
The expectations of the brainstorming exercise

- Choice of the problem to be solved
- Choice of the architecture of the IoT solution

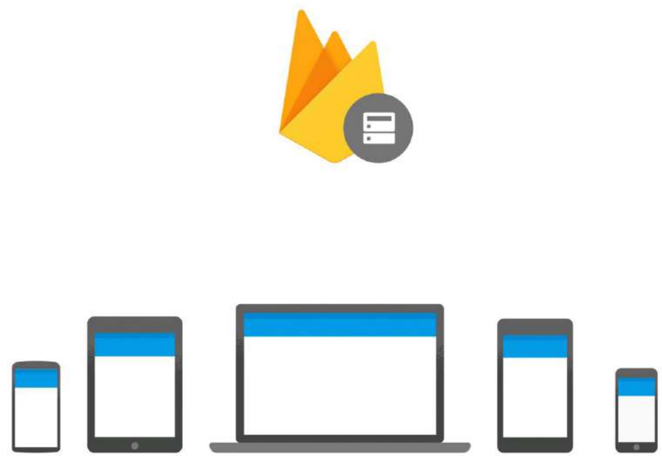
- Functional requirements (security, availability, etc.)
- Components of the solution :

- Sensors
- Gateways
- Connectivity technologies (coverage, battery life, bandwidth, battery life, connectivity cost, module cost, spectrum)
- Type of development platform (middleware, cloud, etc.)
- IoT application (business services to offer, etc.)

Software Tools



Digital platform



NoSql database

Development software

Part 3:
Firebase Platform

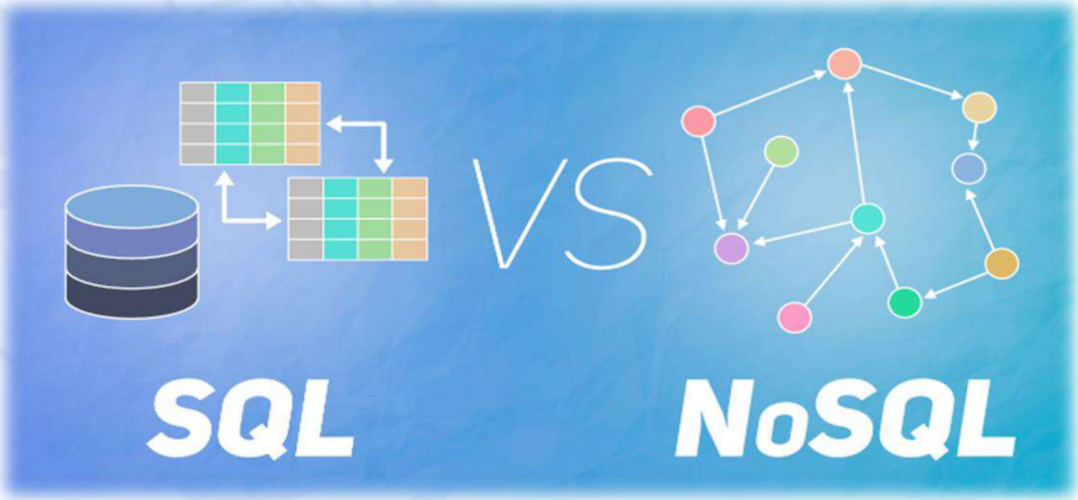
Firebase is a set of hosting services for any type of application. It offers to host in NoSQL and in real time databases, content, social authentication, and notifications, or even services, such as for example a real time communication server.

Why Firebase for IoT?

The main challenges of the IoT are:
a) Provide low latency content (Firebase Realtime Database)
b) Secure communication between devices and the backend (Firebase Authentication).

Software Tools

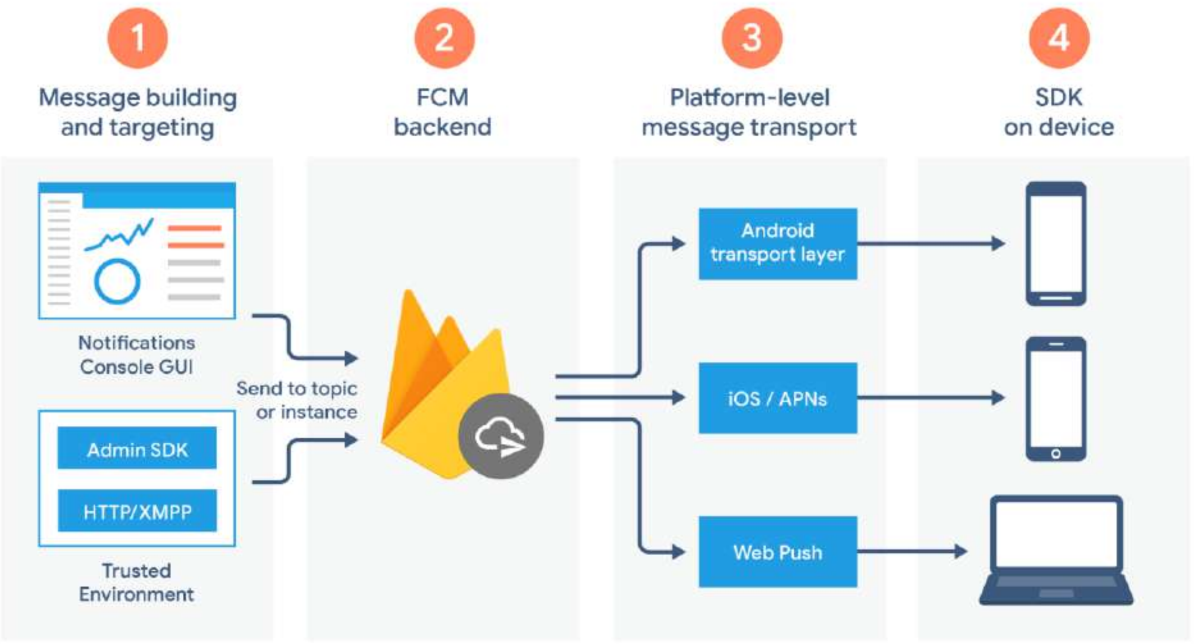
SQL databases have a predefined schema while NoSQL databases have a dynamic schema for unstructured data. SQL databases are scalable vertically, while NoSQL databases are scalable horizontally. SQL databases are scaled by increasing the power of the hardware. NoSQL databases are scaled by increasing the number of database servers in the resource pool to reduce the load.



This means that SQL databases represent data in the form of tables consisting of n number of rows of data, while NoSQL databases are the collection of key-value pairs, documents, graphical databases, etc. that do not have standard schema definitions.

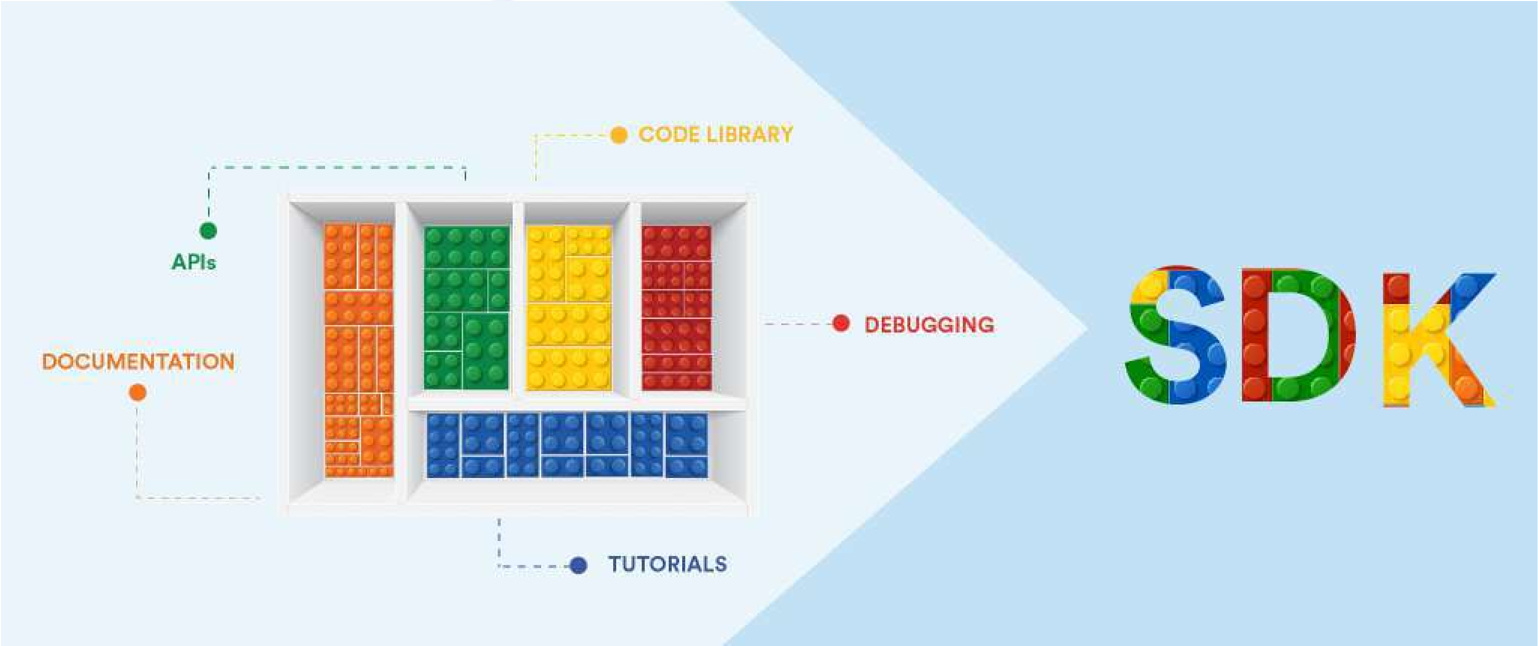
Software Tools

Firebase takes care of a lot of the services that developers themselves would normally have to create, such as authentication, databases, notifications, server hosting etc.



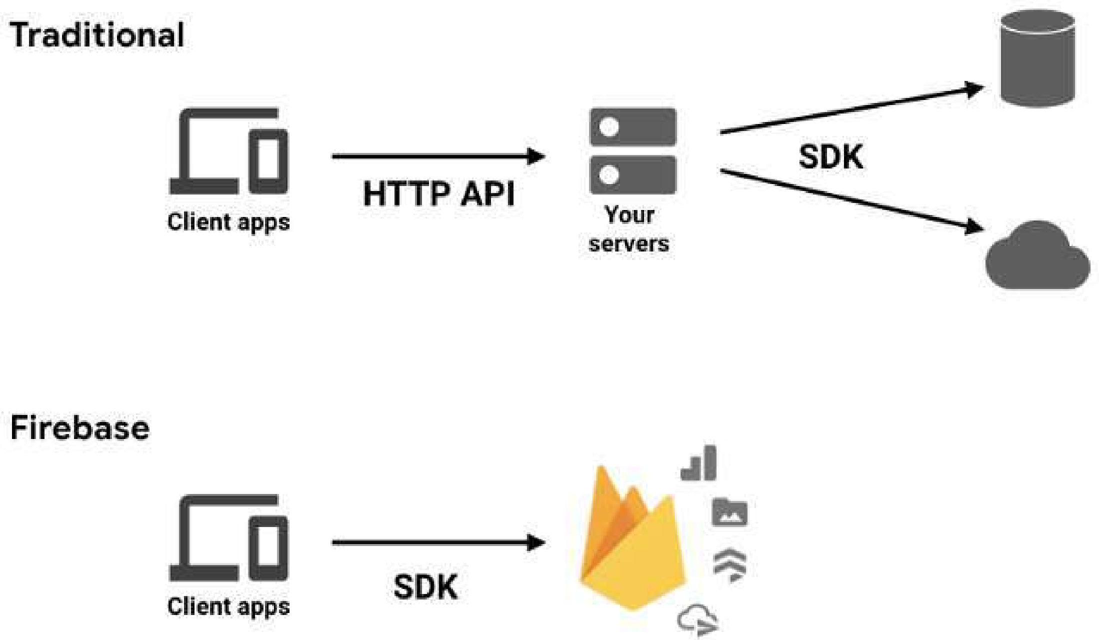
The services offered by Firebase are hosted in the cloud and they are scalable with little to no effort on the part of the developer. These services have backend components which are fully managed and maintained by Google.
Firebase offers client SDKs that interact with these components directly without the need to place middleware between the application and the services

Software Tools



SDK (Software Development Kit) refers to a set of tools used by developers for the development of software for a specific platform (Android, iOS, etc.).
An SDK can have one or more targets such as an operating system, a web application, a web server, video game, etc.
To develop an Android application, you need the Firebase Android Client SDK.
To develop a web application, you need the Firebase web client SDK, etc.

The Firebase SDK which allows direct interaction between a client and Firebase services imports a new concept of development that differs from the traditional method where a backend part and a frontend part must be developed, while in the case of Firebase we bypass the backend part and therefore the execution logic is placed at the customer (frontend). See following figure. Administrator access is provided through the "Firebase console" area.

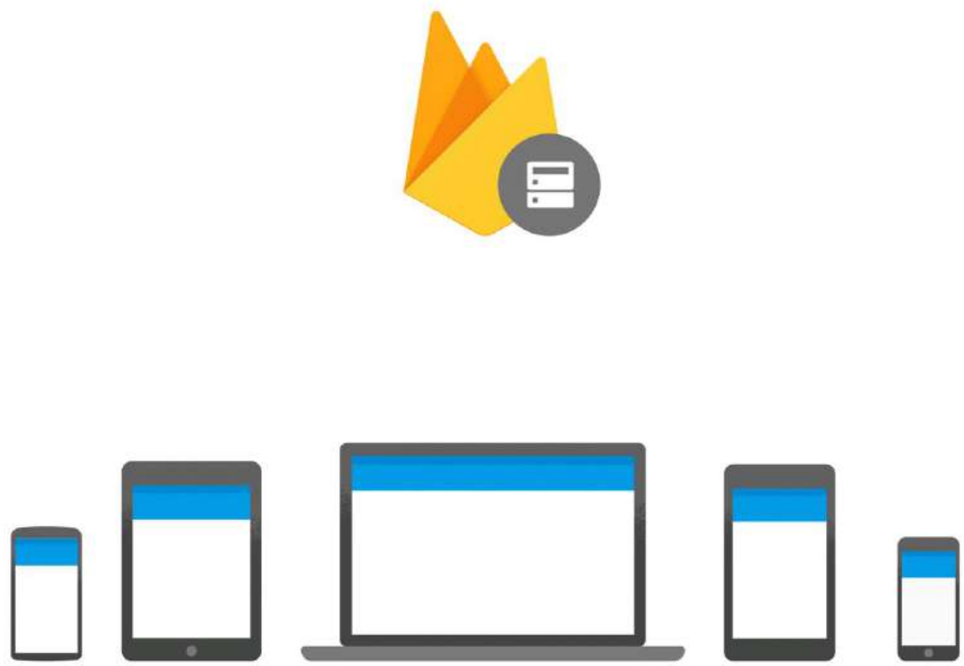


Comparison between classic development and development with Firebase

Firebase services

Firebase Realtime Database and Cloud Firestore.
These are the two databases offered by Firebase, they are described as real-time databases, hosted in the Cloud and NoSQL)

Cross platform clients share the same resource in the database. If there is a change, all clients receive automatically instant update.



Firebase store data in JSON format and it uses the NoSQL type for its databases, which depletes us from the constraint of relational database tables (SQL for example), thus allowing to create and size in a way more free and easier a database.

Software Tools

KEY DIFFERENCES BETWEEN REALTIME DATABASE AND CLOUD FIRESTORE

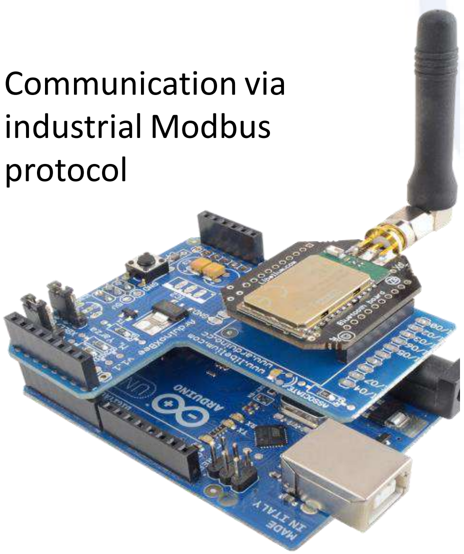
CLOUD FIRESTORE	REALTIME DATABASE
ALLOWS MULTIPLE FIELD COMPARISONS	ALLOWS FOR SINGLE SORTING PARAMETER
EVERY ONE-TIME FETCH QUERY IS ORGANIC	ALLOWS ONE TO UPLOAD TOTALLY NEW DATASETS
ACCEPTS UPTO 1,000,000 CONCURRENT CLIENT CONNECTIONS	THE UPPER LIMIT IS 100,000 CONCURRENT CONNECTIONS
OFFERS REGIONAL INSTANCES IN LOCATION AROUND THE WORLD	ONLY HOSTED IN NORTH AMERICA

Cloud Storage provides massively scalable file storage, it allows customers (a customer can be an IoT device too!) To publish and download files (images, text, etc.) Cloud Functions using Firebase's Cloud Functions service, one can deploy code running on Google's server infrastructures that automatically responds to events from other Firebase services.

Second part : Brainstorming

Elements of the solution: Connected Industry 4.0

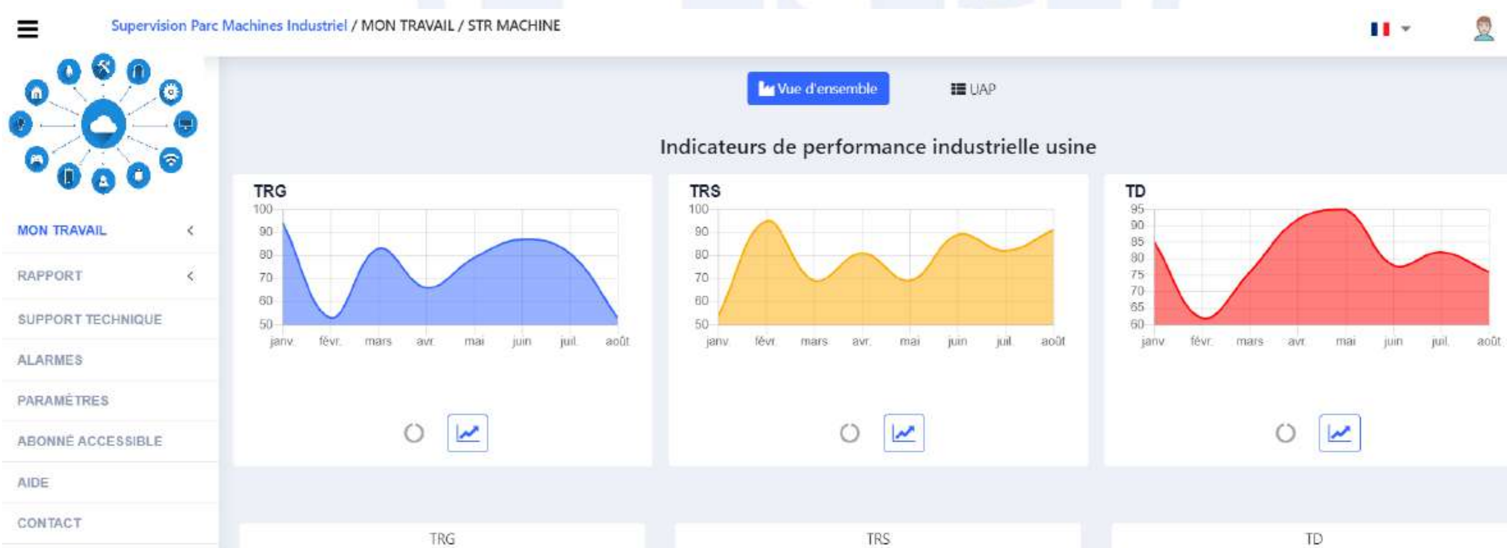
Communication via industrial Modbus protocol



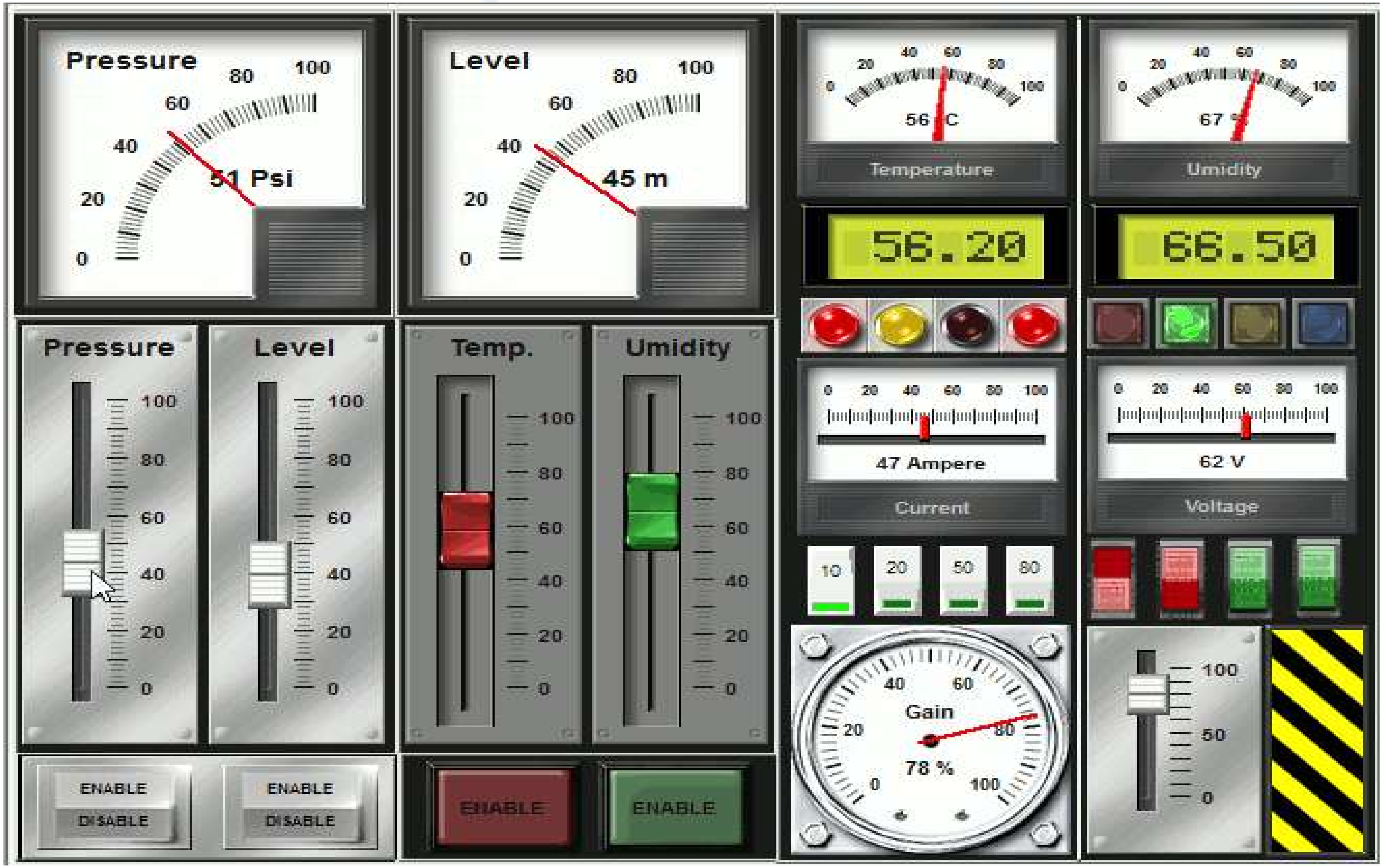
Connectivity technology: Wi-Fi, 4G

Elements of the solution: Connected Industry 4.0

Real-time communication between the database and the platform



Elements of the solution: Connected Industry 4.0



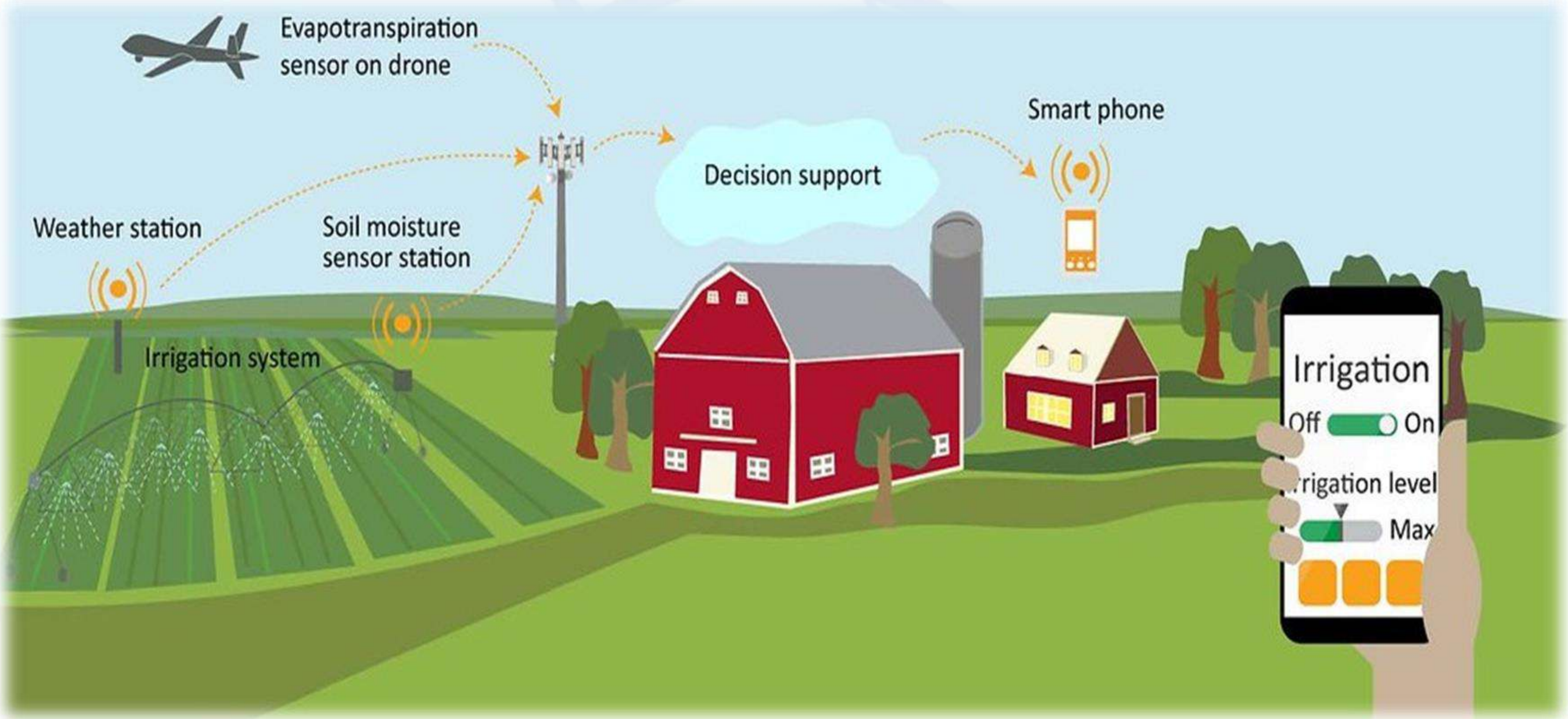
Dashboard accessible on the platform

SMART Irrigation application demonstration

The solution mainly contains a remote control kit for irrigation valves and motor pumps via a mobile application. This tool allows the farmer to save travel on site and it allows him to define precise irrigation times. The second component of the project is to sample different soil levels to inform the farmer about the percentage of soil moisture. This is to know the amount of irrigation water needed.

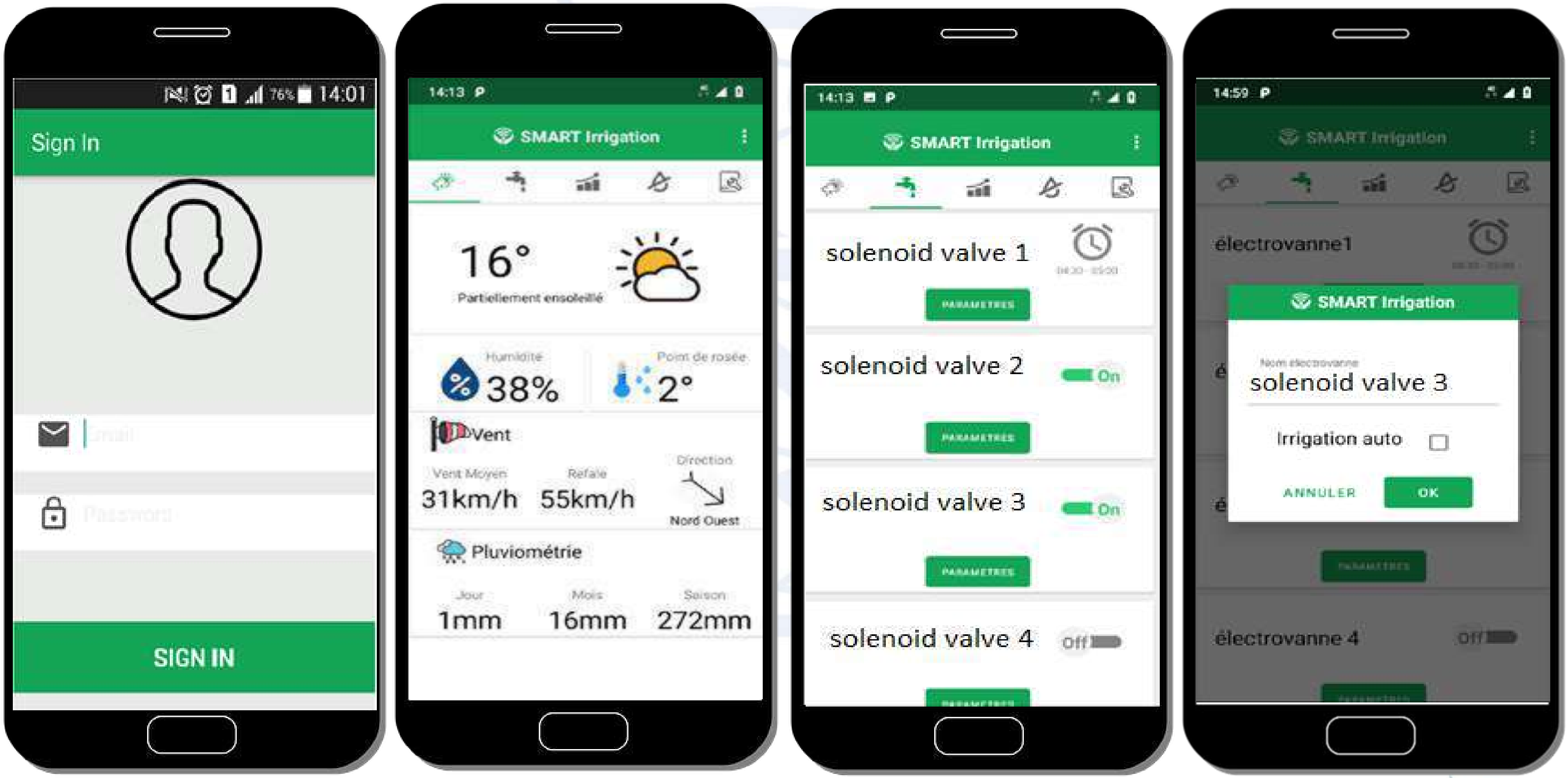
Connectivity technology: 2G, LoRa

Elements of the solution: Smart agriculture

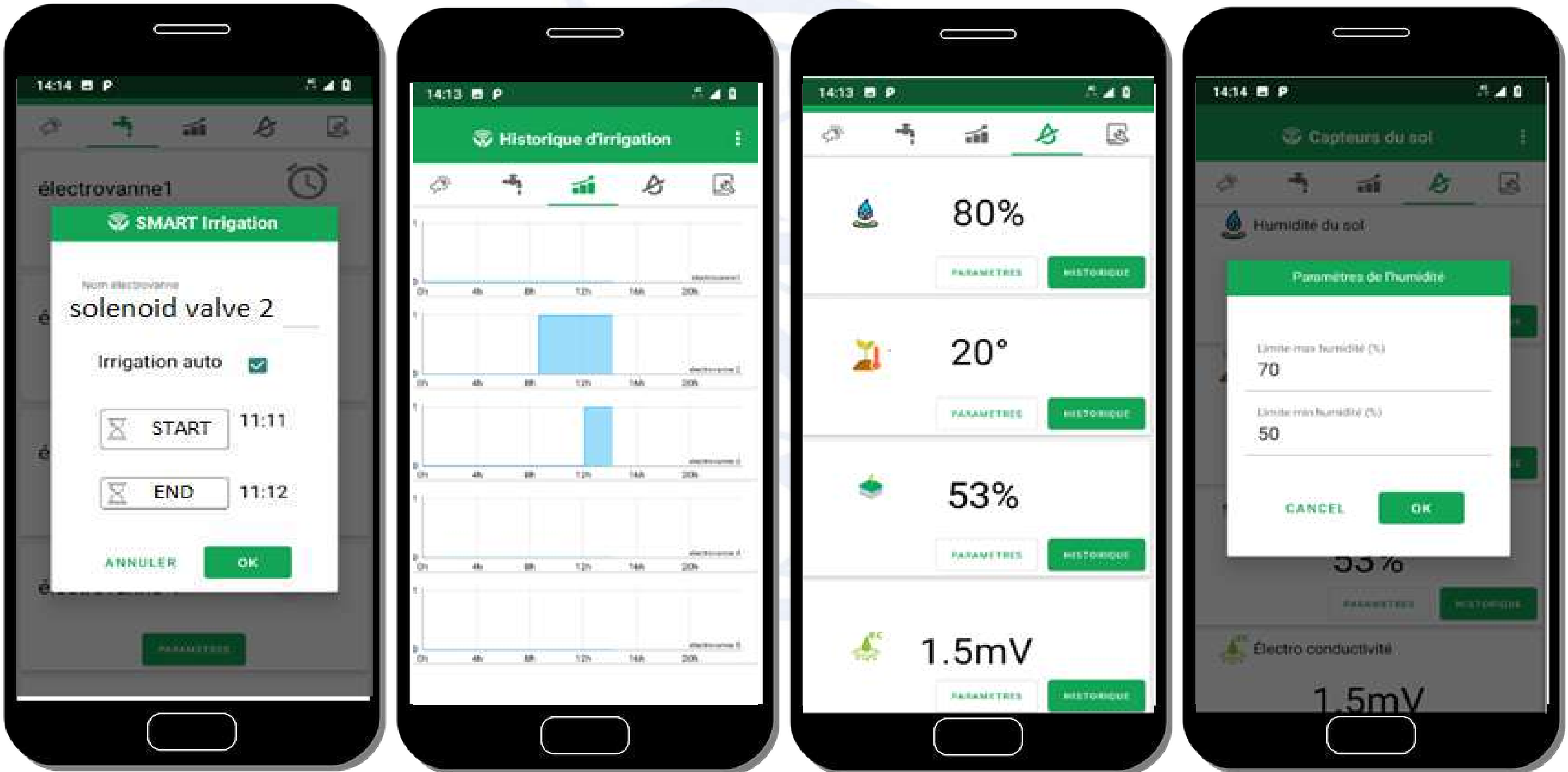


Farmers have large portions of land which they use for farming and irrigation. It is difficult for them to track and take care of each portion of it. Thanks to IOT and decision-making tools, it has become possible and easy to manage automatically with remote control.

Elements of the solution: Smart agriculture



Elements of the solution: Smart agriculture



Elements of the solution: Telemedicine

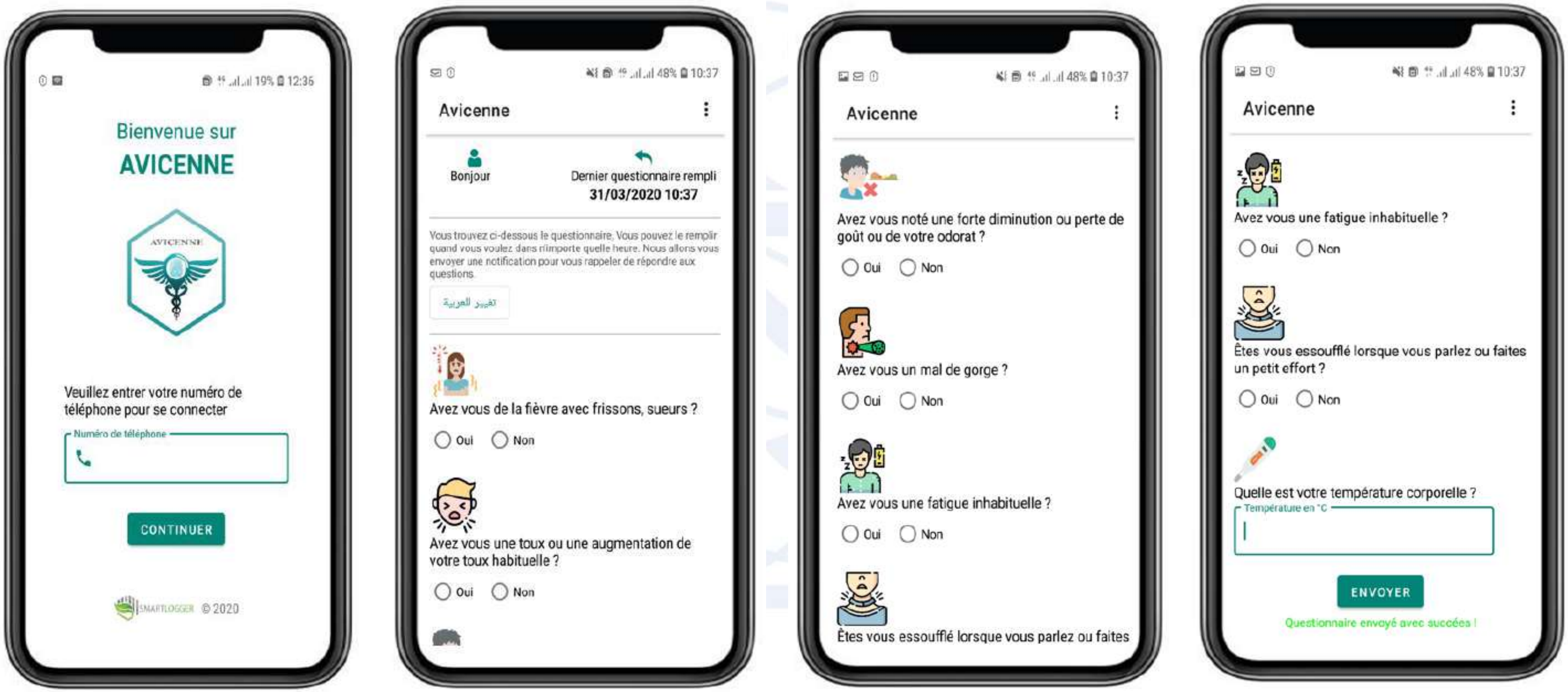
Goals :

- ✓ Screen the population for symptoms and signs suggestive of covid-19 infection,
- ✓ Daily monitor the clinical course of symptoms of infection in users,

- ✓ Allow medical staff to detect suspected patients carrying covid-19,
- ✓ Allow medical staff to indicate the practice of the diagnostic test for covid-19,
- ✓ Allow medical staff to select patients at risk of developing severe forms,
- ✓ Allow the medical staff to indicate the hospitalization of patients,
- ✓ Allow medical staff to verify compliance with the containment of suspected patients by geolocation,
- ✓ Allow the Ministry of Health to generate statistics on the evolution of the epidemic,

- ✓ Save and archive all data and information collected from users,
- ✓ WEB platform accessible by several users with secure access control,
- ✓ Separate personal information from that for anonymous use,
- ✓ Size the server to be able to manage a number of simultaneous users> 10 million

Elements of the solution: Telemedicine

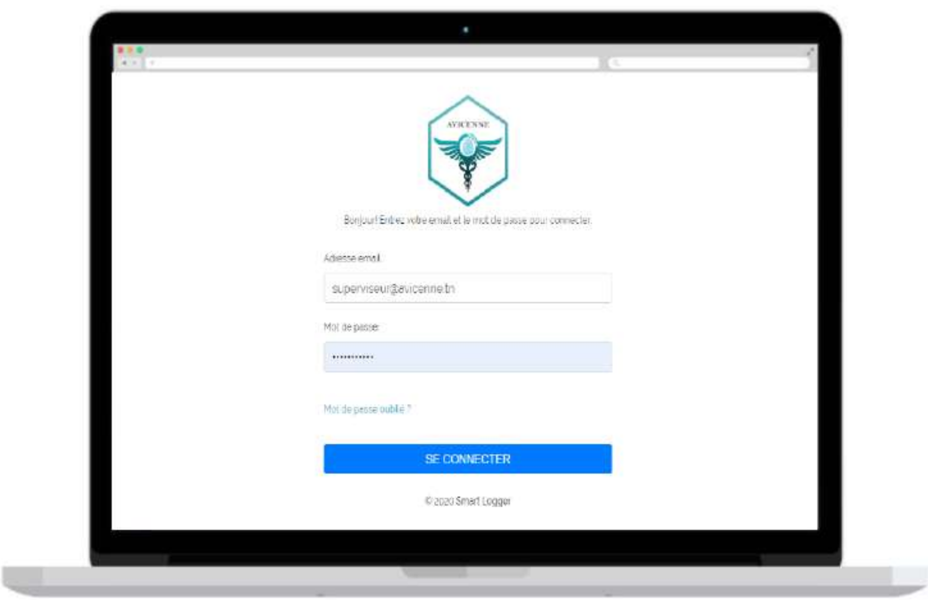


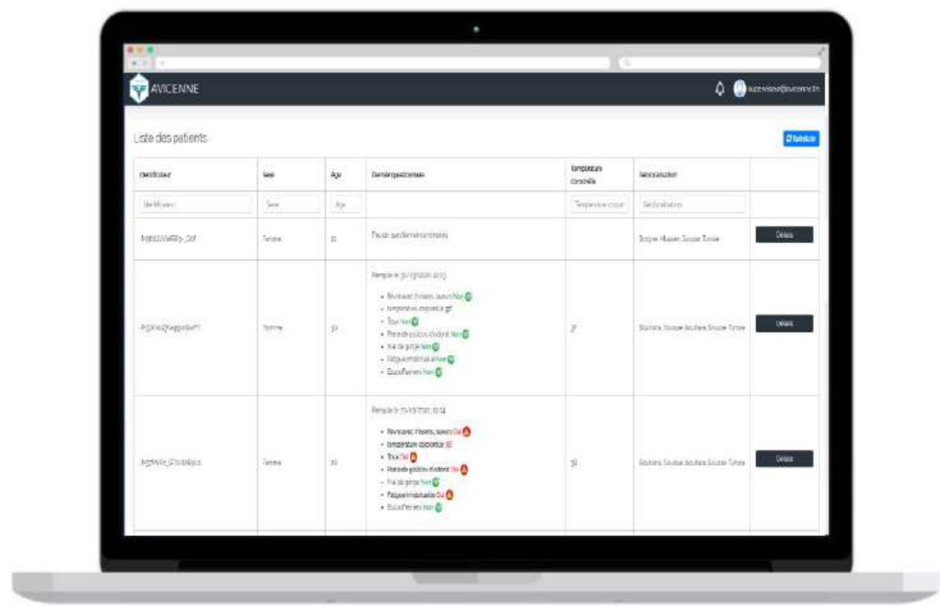
Connectivity technology : Wi-Fi, 4G

Elements of the solution: Telemedicine

The dashboard for the medical administrator containing a ranking of the users of the mobile application indicates their ages, last answer to the questionnaire, last body temperature sample.

Medical staff can sort users by age category, body temperature value, and geographic area.

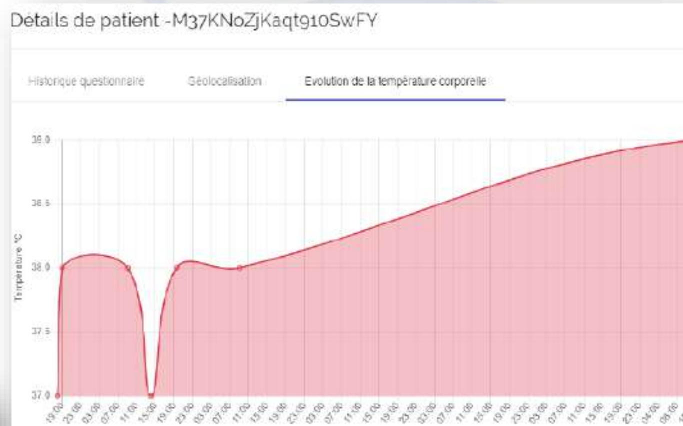




WEB administrator platform

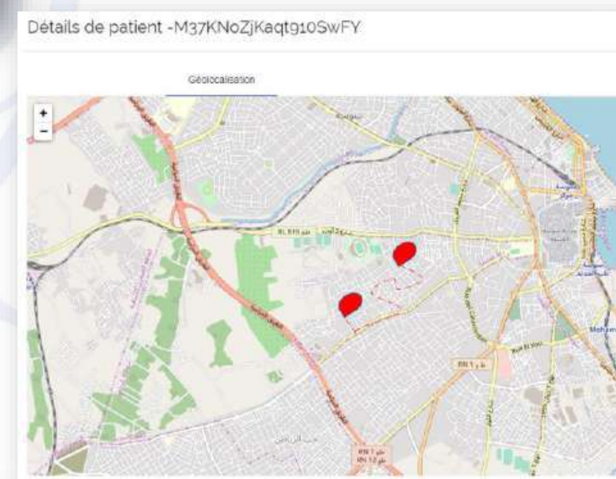
Elements of the solution: Telemedicine

In the event of an emergency detected, the medical staff can view the history of the patient's responses with more details on the progress of his health.

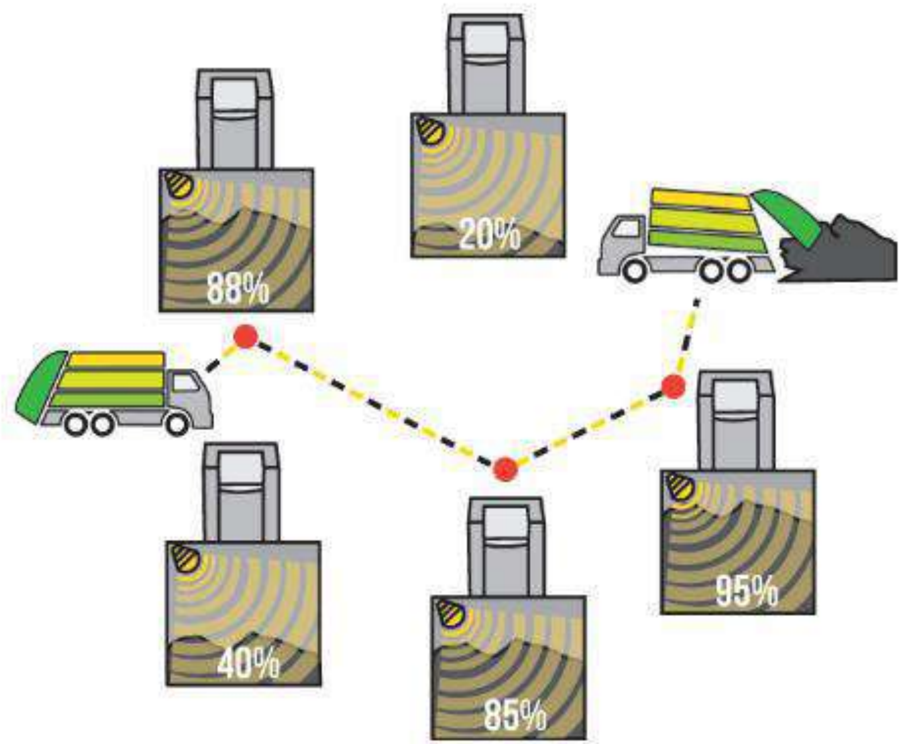


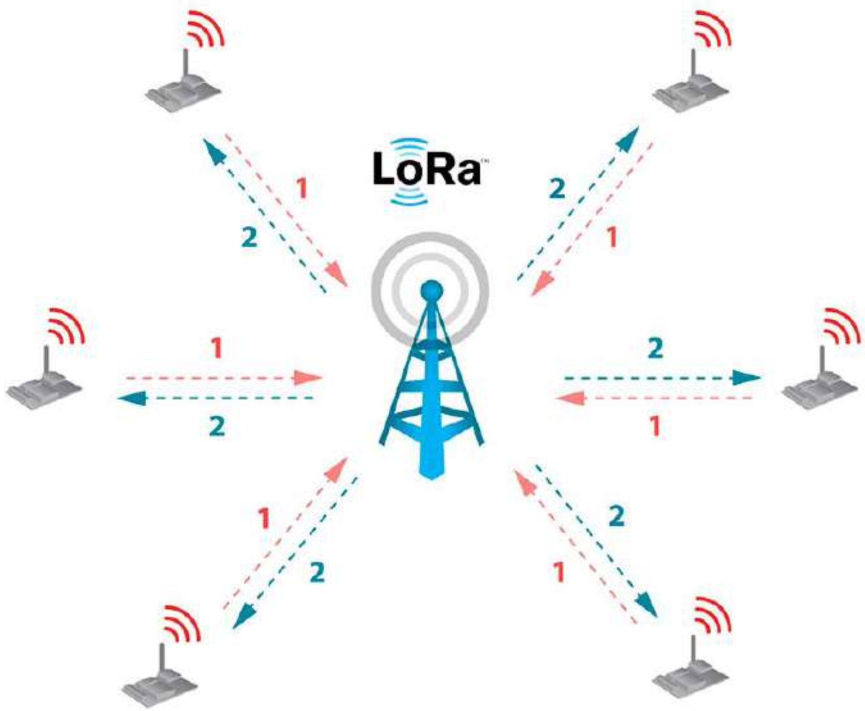
The dashboard for the security administrator containing the approximate address and a geographical distribution statement for patients with covid-19 must be placed in quarantine.

Similarly, if necessary, the medical staff can view a detailed reading of the evolution of the patient's body temperature throughout his use of the AVICENNE application



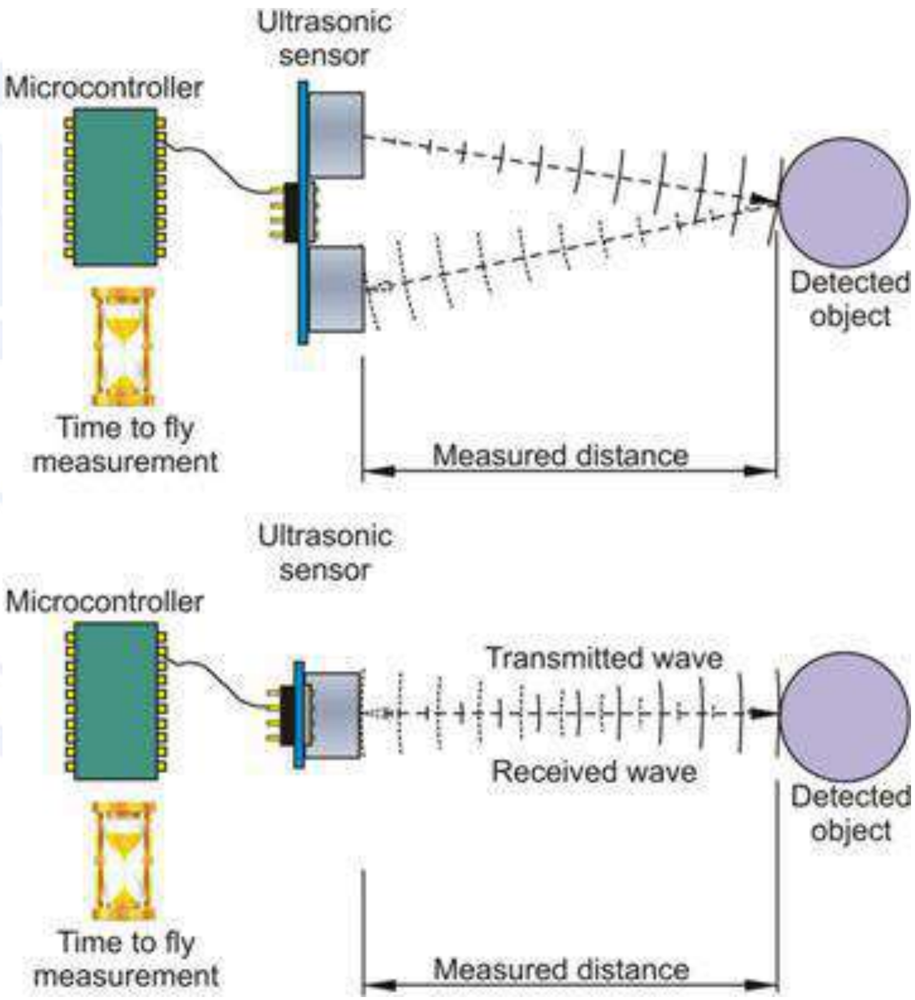
Elements of the solution: Smart City

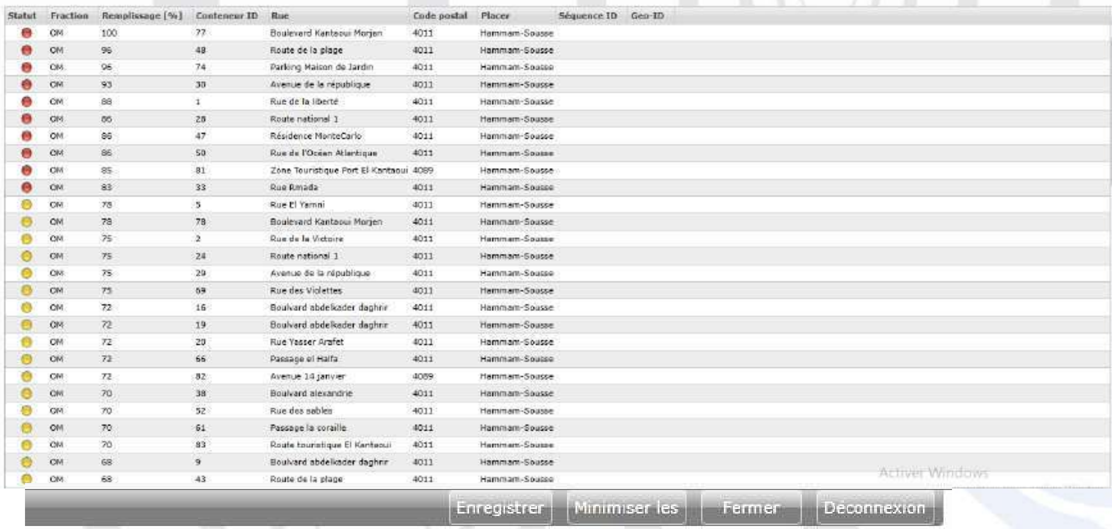




Connectivity technology: LoRa, 2G

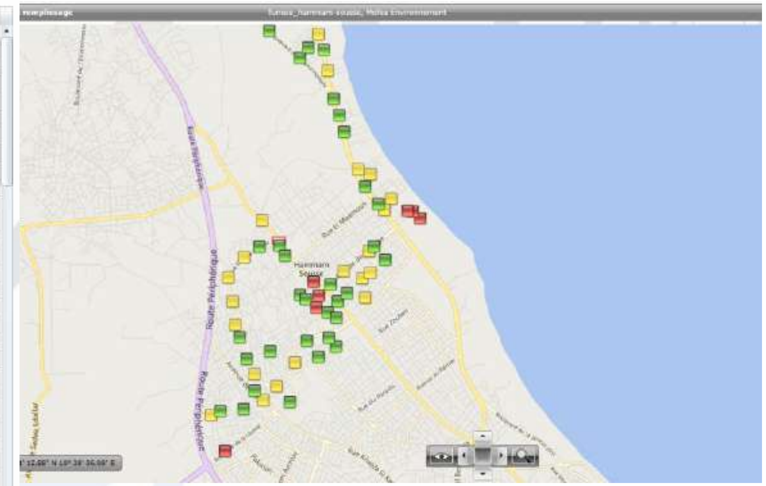
Elements of the solution: : Smart City

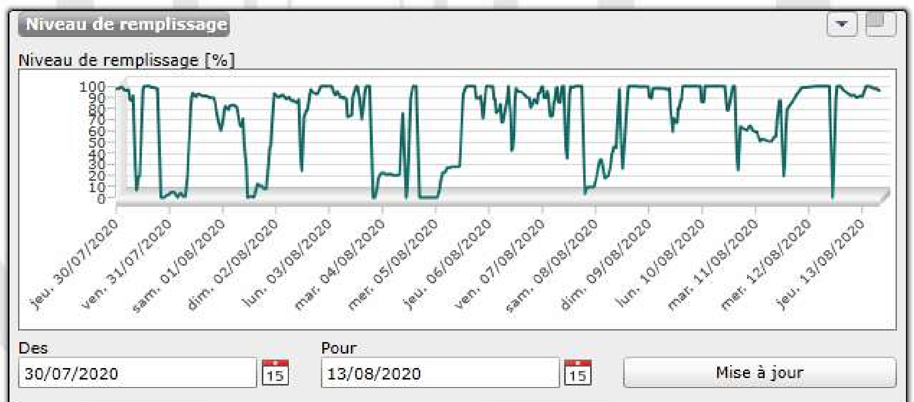


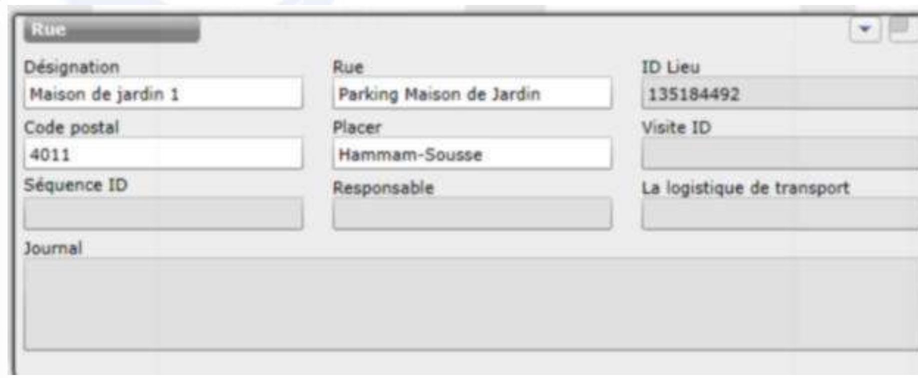


Statut	Fraction	Remplissage [%]	Conteneur ID	Rue	Code postal	Placer	Séquence ID	Geo-ID
	OM	100	77	Boulevard Kantaoui Morjen	4011	Hammam-Sousse		
	OM	96	48	Route de la plage	4011	Hammam-Sousse		
	OM	96	74	Parking Maison de Jardin	4011	Hammam-Sousse		
	OM	93	30	Avenue de la république	4011	Hammam-Sousse		
	OM	88	1	Rue de la liberté	4011	Hammam-Sousse		
	OM	86	28	Route national 1	4011	Hammam-Sousse		
	OM	86	47	Résidence MonteCarlo	4011	Hammam-Sousse		
	OM	86	50	Rue de l'Océan Atlantique	4011	Hammam-Sousse		
	OM	85	81	Zone Touristique Port El Kantaoui	4089	Hammam-Sousse		
	OM	83	33	Rue Rmada	4011	Hammam-Sousse		
	OM	78	5	Rue El Yamni	4011	Hammam-Sousse		
	OM	78	78	Boulevard Kantaoui Morjen	4011	Hammam-Sousse		
	OM	75	2	Rue de la Victoire	4011	Hammam-Sousse		
	OM	75	24	Route national 1	4011	Hammam-Sousse		
	OM	75	29	Avenue de la république	4011	Hammam-Sousse		
	OM	75	69	Rue des Violettes	4011	Hammam-Sousse		
	OM	72	16	Boulvard abdelkader daghrir	4011	Hammam-Sousse		
	OM	72	19	Boulvard abdelkader daghrir	4011	Hammam-Sousse		
	OM	72	20	Rue Yasser Arafet	4011	Hammam-Sousse		
	OM	72	66	Passage el Halfa	4011	Hammam-Sousse		
	OM	72	82	Avenue 14 janvier	4089	Hammam-Sousse		
	OM	70	38	Boulvard alexandrie	4011	Hammam-Sousse		
	OM	70	52	Rue des sables	4011	Hammam-Sousse		
	OM	70	61	Passage la coraille	4011	Hammam-Sousse		
	OM	70	83	Route touristique El Kantaoui	4011	Hammam-Sousse		
	OM	68	9	Boulvard abdelkader daghrir	4011	Hammam-Sousse		
	OM	68	43	Route de la plage	4011	Hammam-Sousse		

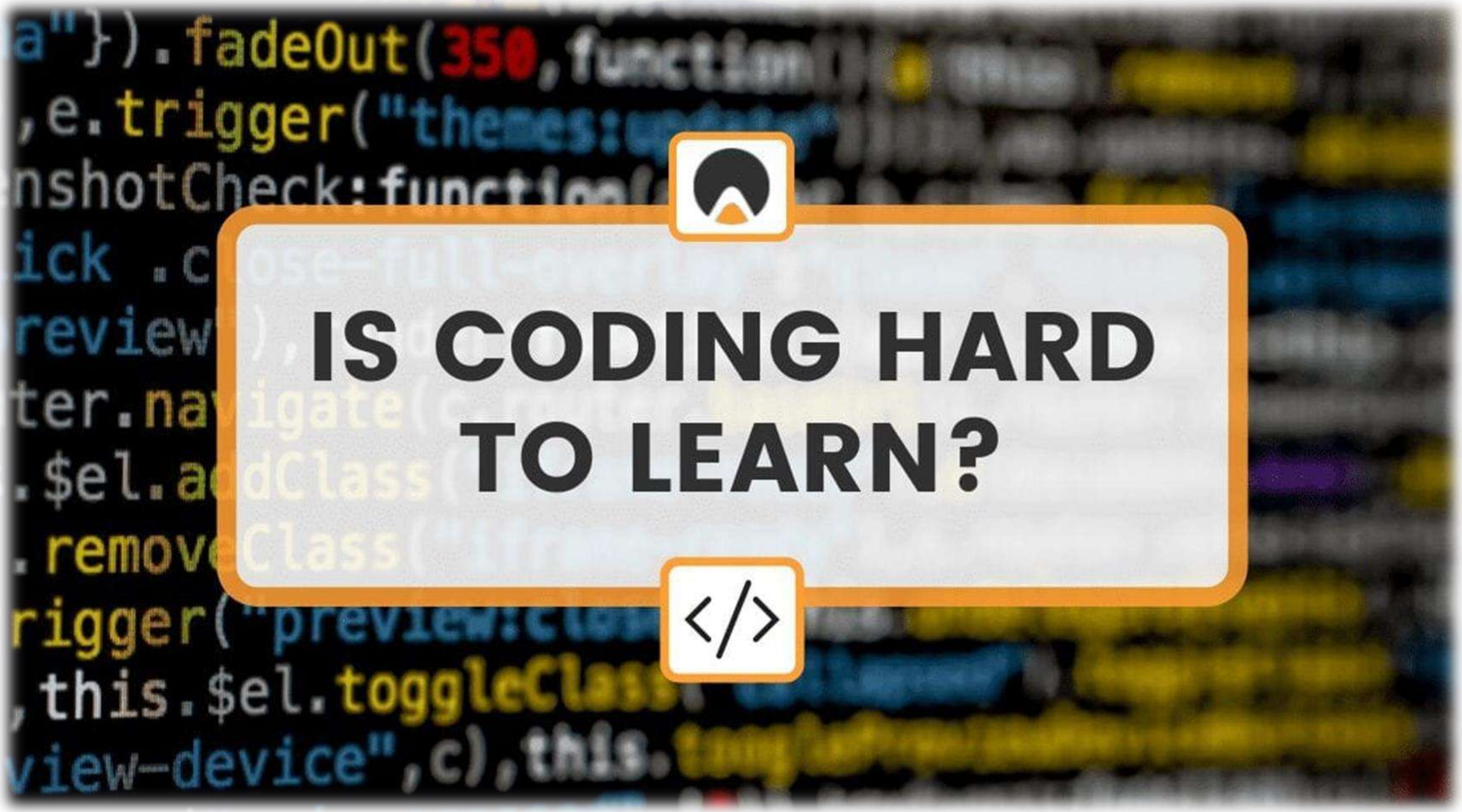
Enregistrer Minimiser les Fermer Déconnexion







Third part : Demonstration

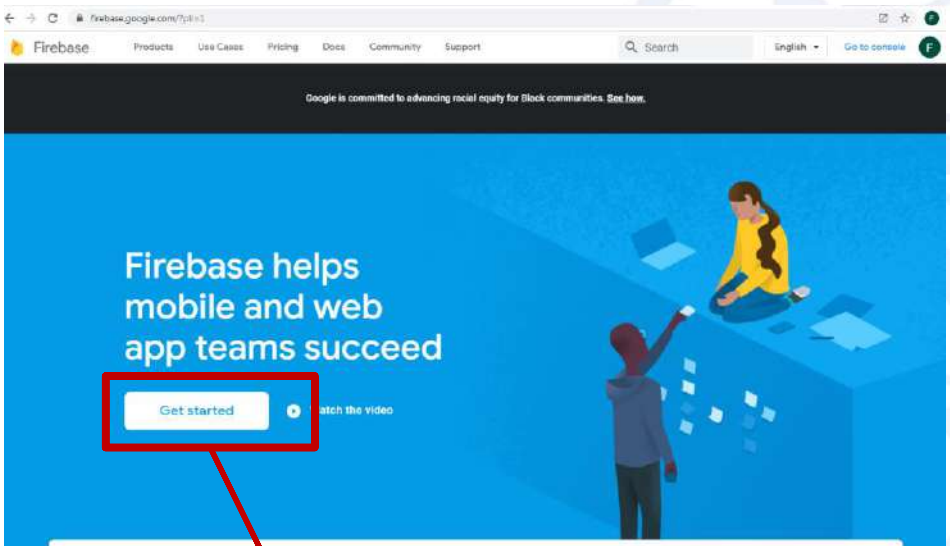


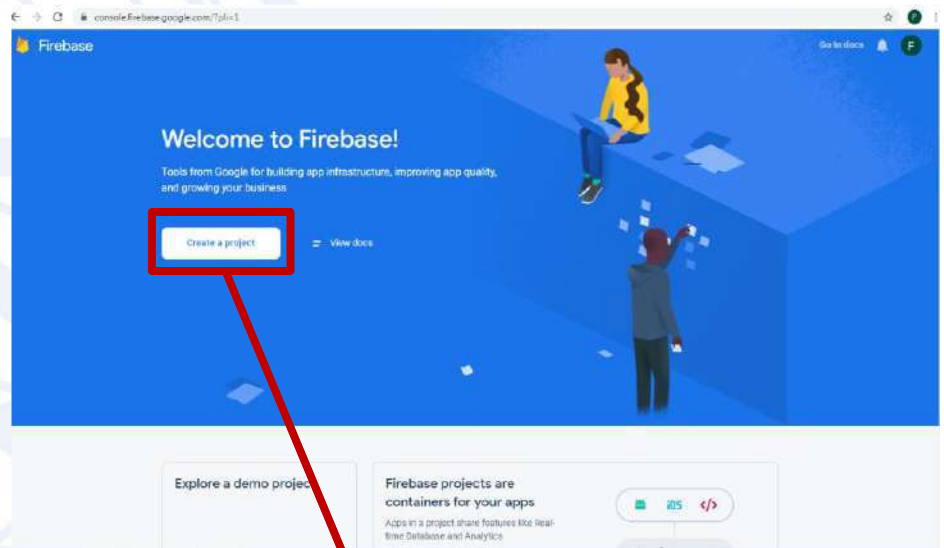
Android Application using Firebase

To develop an application on Android, we need a development environment software (IDE), we will use the official Google IDE "Android Studio" downloadable from this link: https://developer.android.com/studio

You must first have a Google account to use Firebase services, you just need to create a new account for free.
Then visit the Firebase website: https://firebase.google.com/

Procedure for creating an Android Application with Firebase

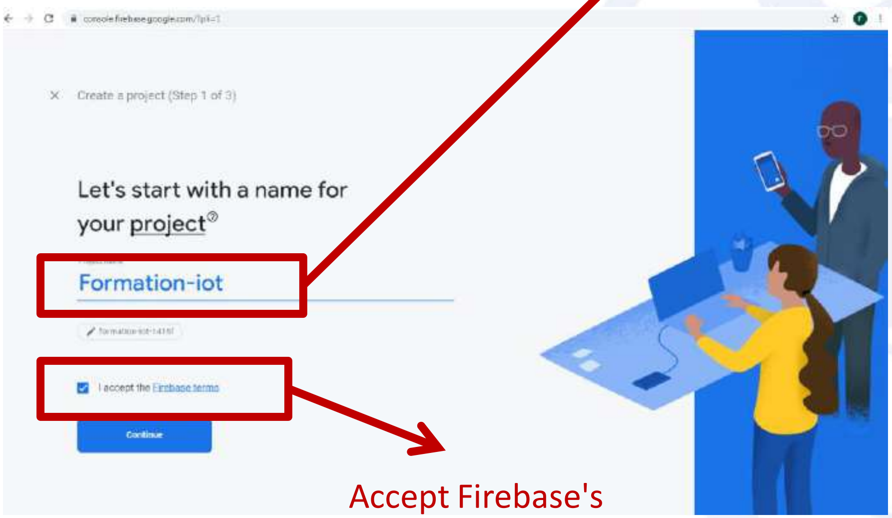


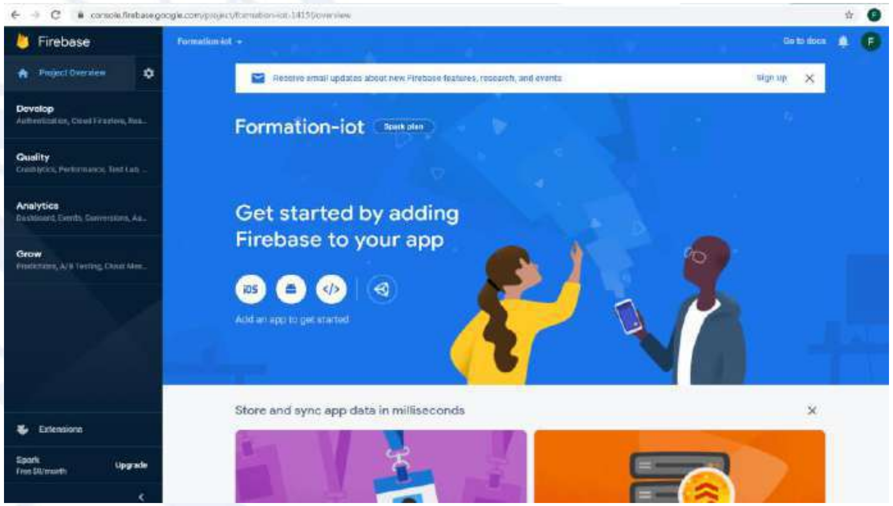


Click on Get started

Click on Create project

Enter a name for
your project

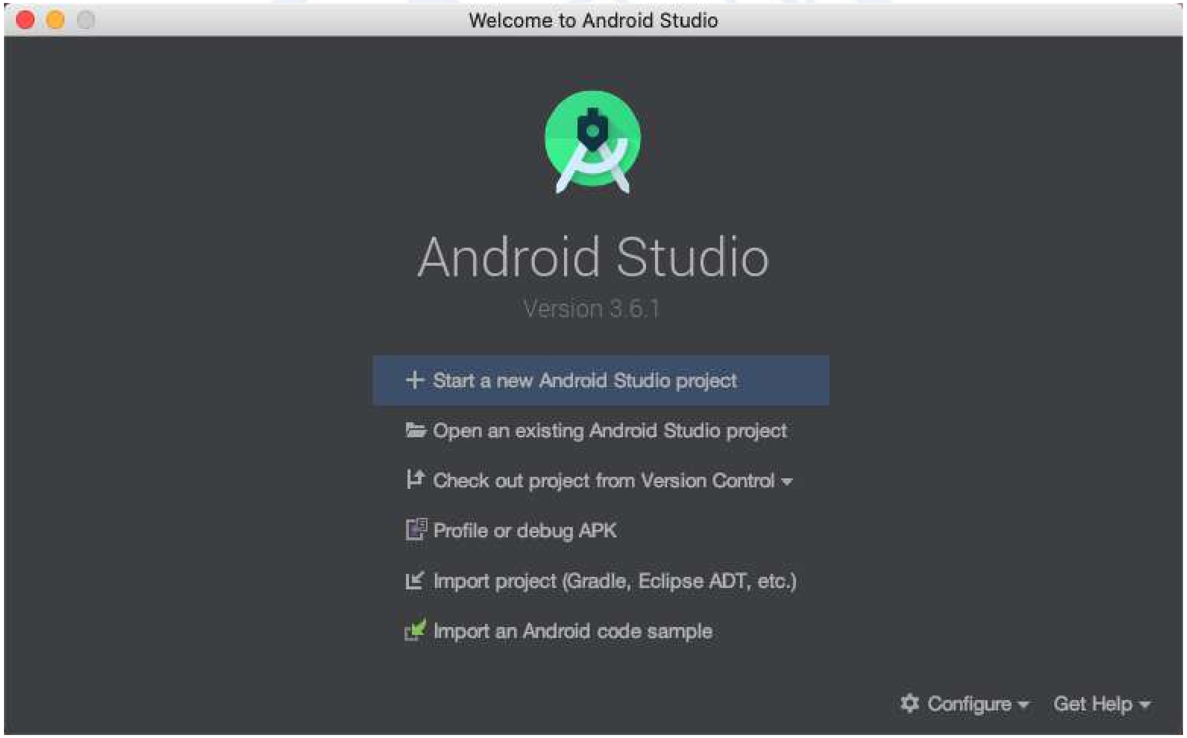




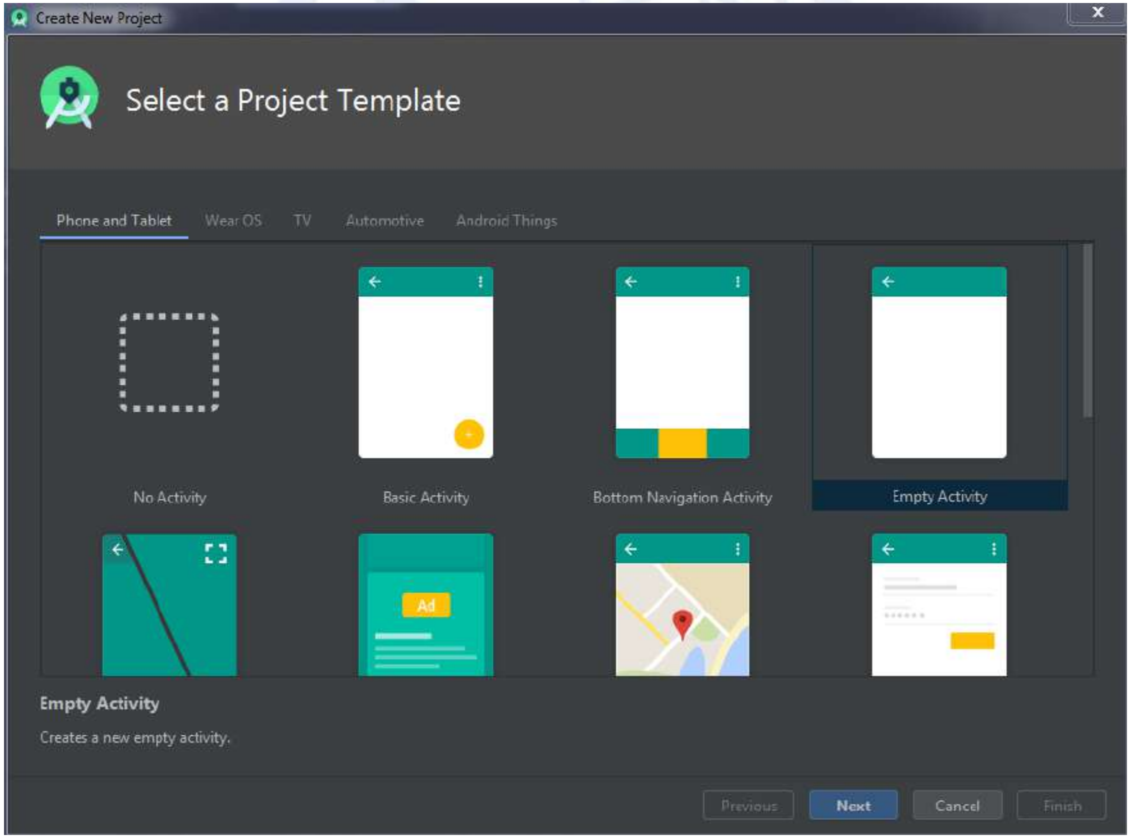
Accept Firebase's
terms of service

You are now on the “Firebase console”

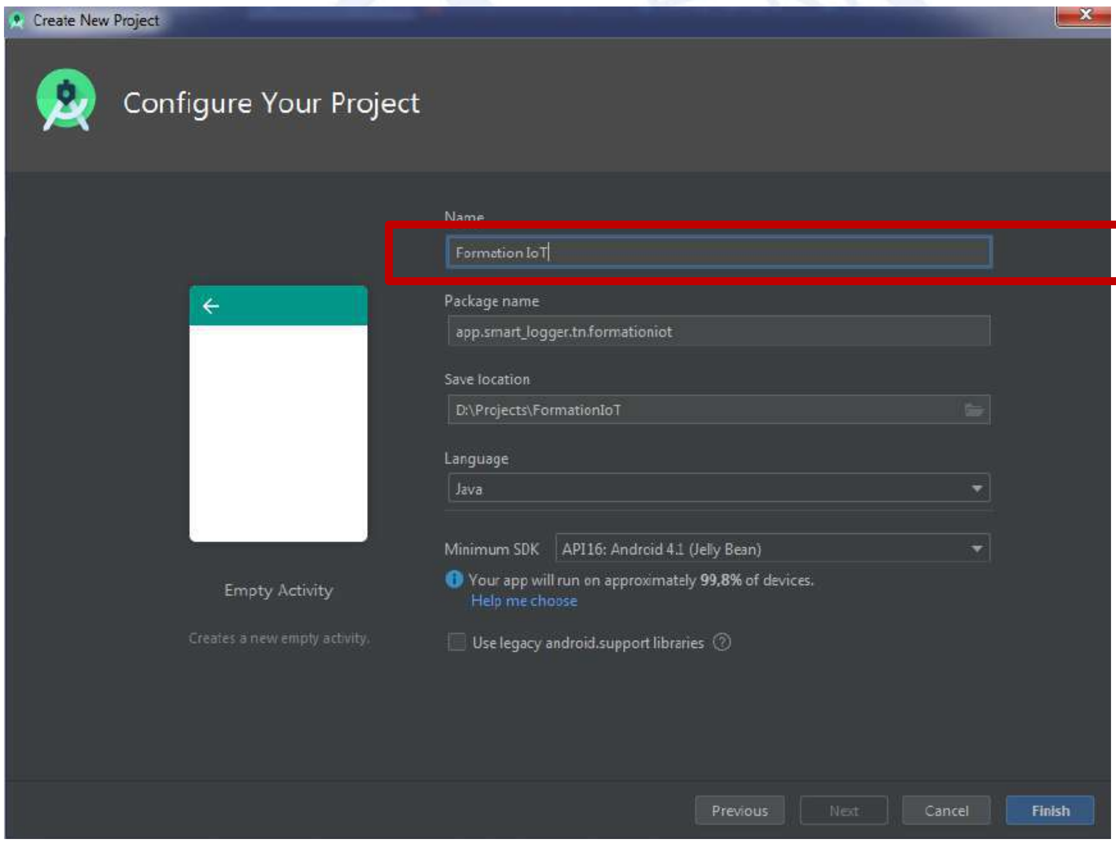
Open Android Studio and click on Start a new Android Studio Project



We are asked to choose a Template for our project, we will choose "Empty Activity"



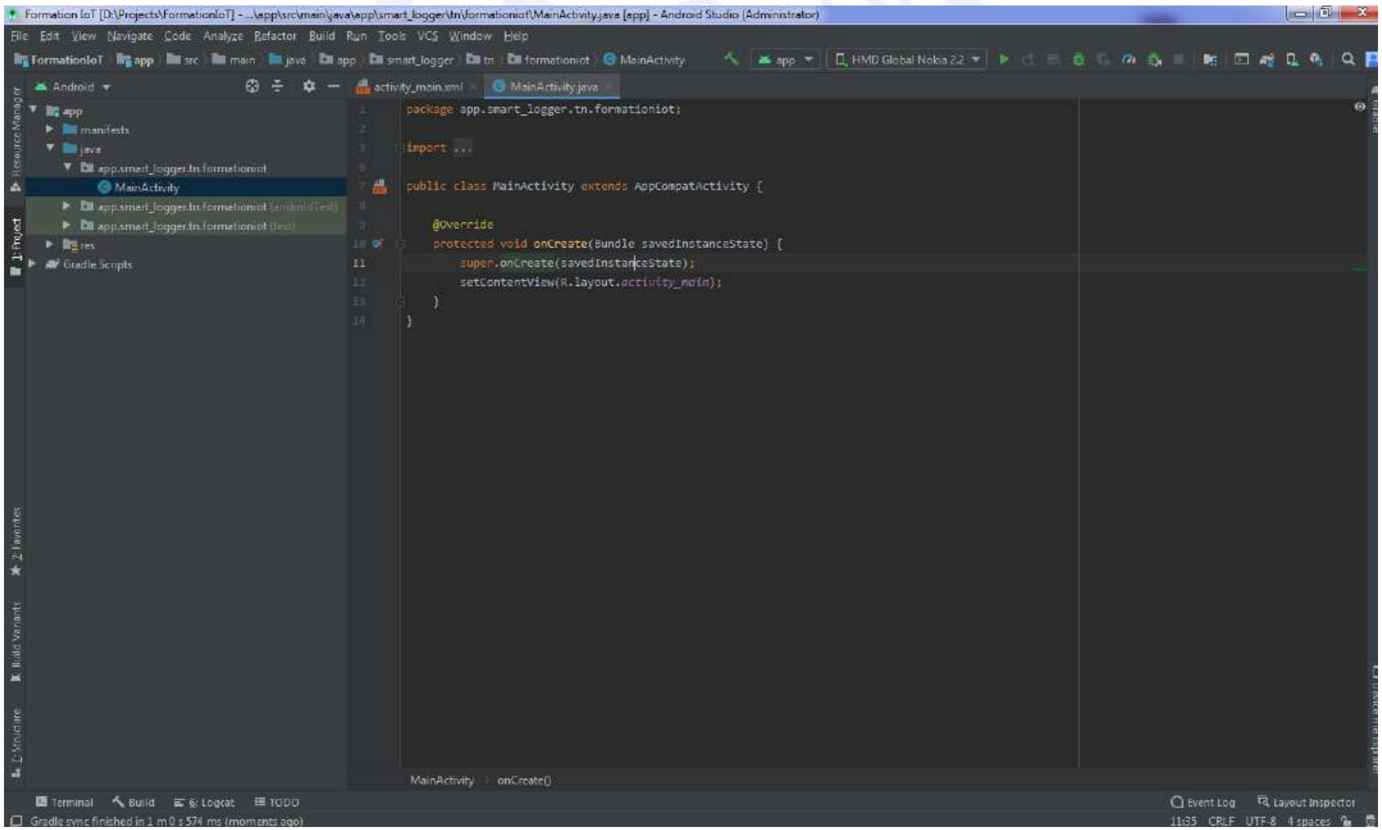
Assign a name to your project and leave all the other fields intact and click on "Finish»



Name of the project

Software Tools

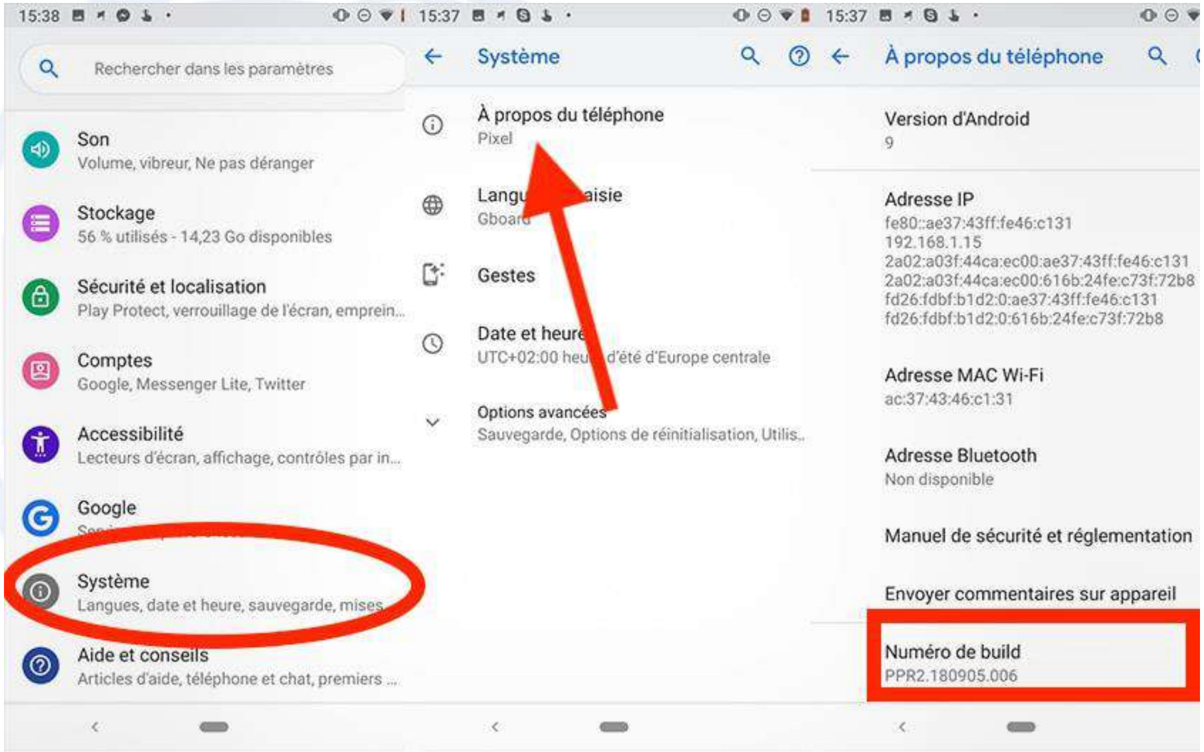
Your project is created! The interface should be like this:



Software Tools

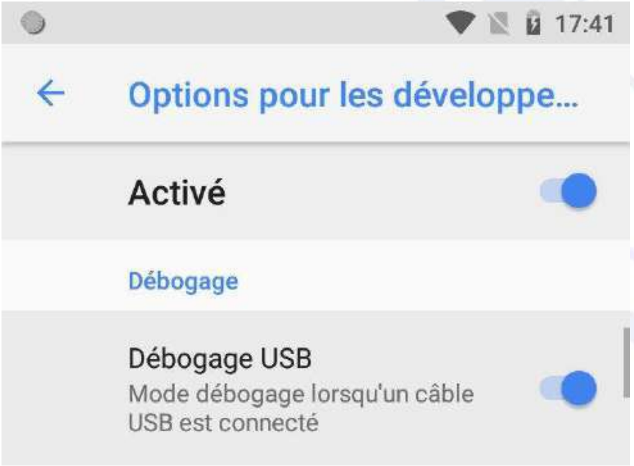
We are now going to run our first application on an Android Smartphone, but first we must configure our Smartphone in developer mode.

<u>Remarque</u>: You can also use the virtual smartphone from Android Studio, but it is better to test on a real device.



Go to your Smartphone settings, then System> About phone> Build number

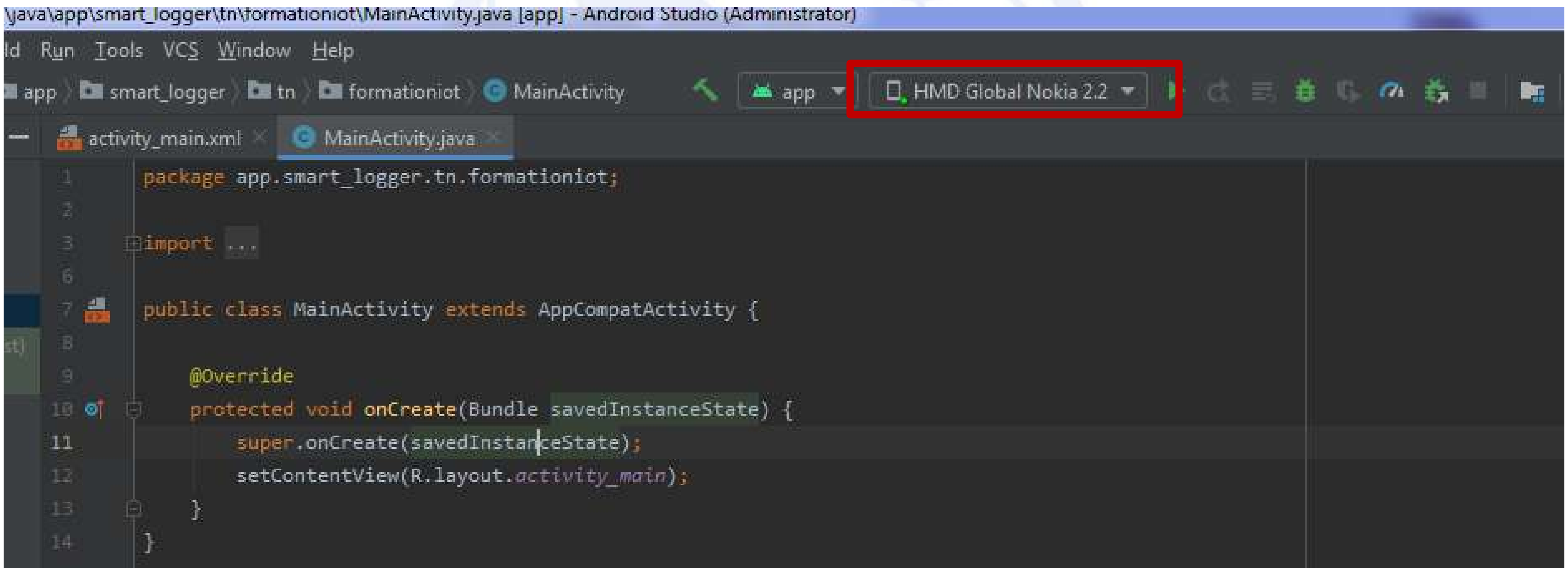
- Successively press the build number several times until the system tells you that developer mode is enabled.
- Go back to system> Developer options, make sure Developer options and USB debugging are enabled.



Connect your Smartphone to your PC using a USB cable, if a dialogue has appeared on your phone, click on "Always allow" then "OK".

Software Tools

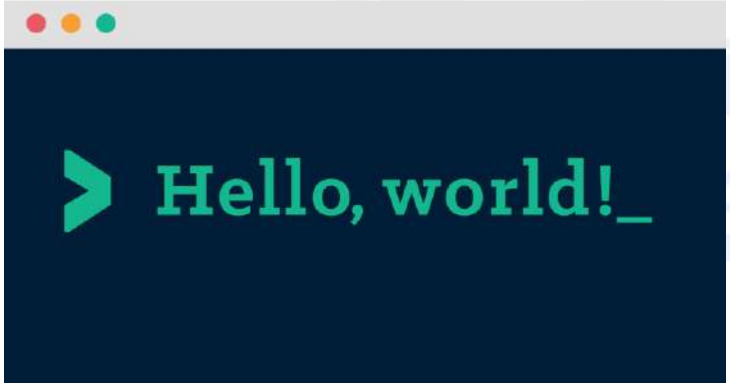
The name of your Smartphone should now appear on Android Studio.
Click on "Run", the green icon next to the name.

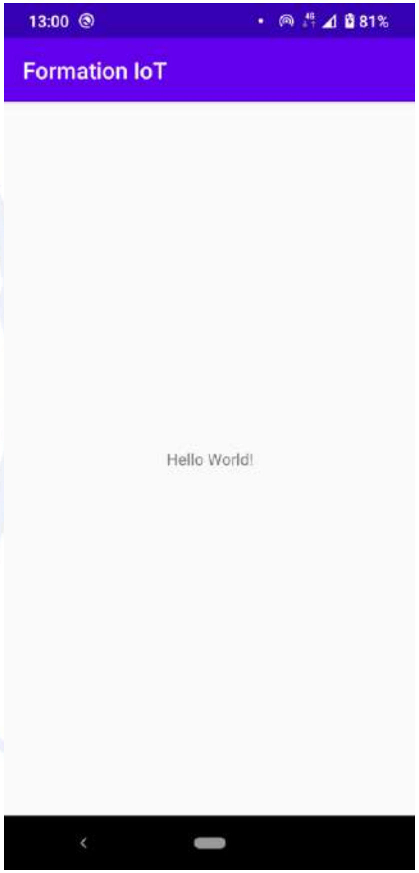


Here is your first hello world app!

Suppose we want to control a door remotely through our application, to achieve this goal we will add a switch to the interface.

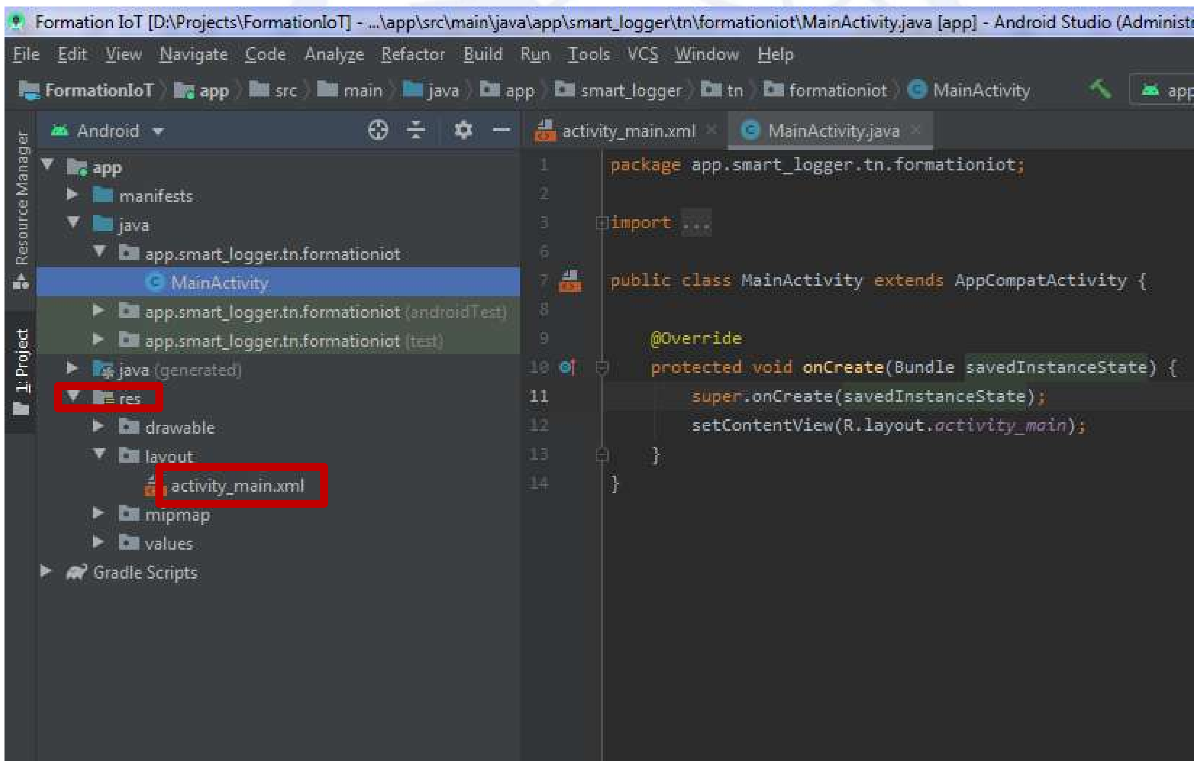
If you activate the switch, the door concerned opens, however if you deactivate it the door closes.





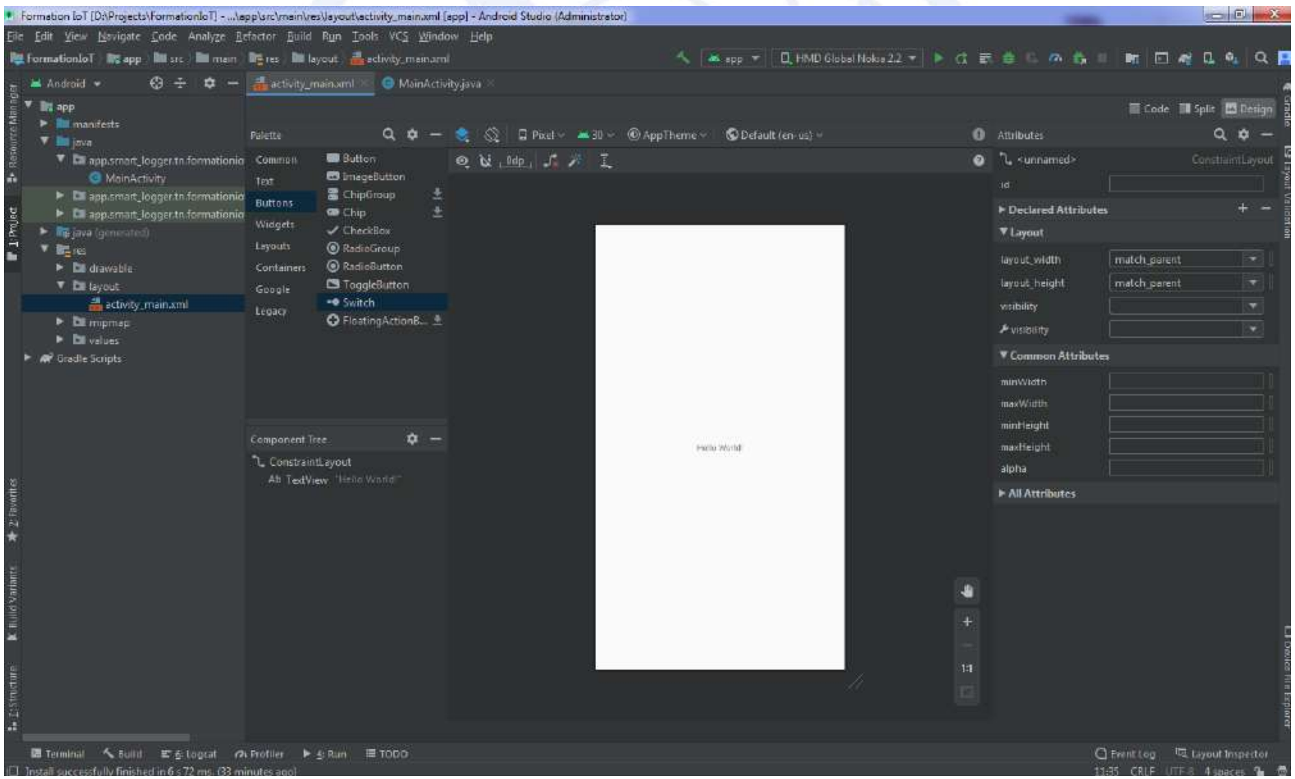
Software Tools

To add a switch in the graphical interface of our application, click on the res folder in the project tree on the left, then layout and then activity_main.xml



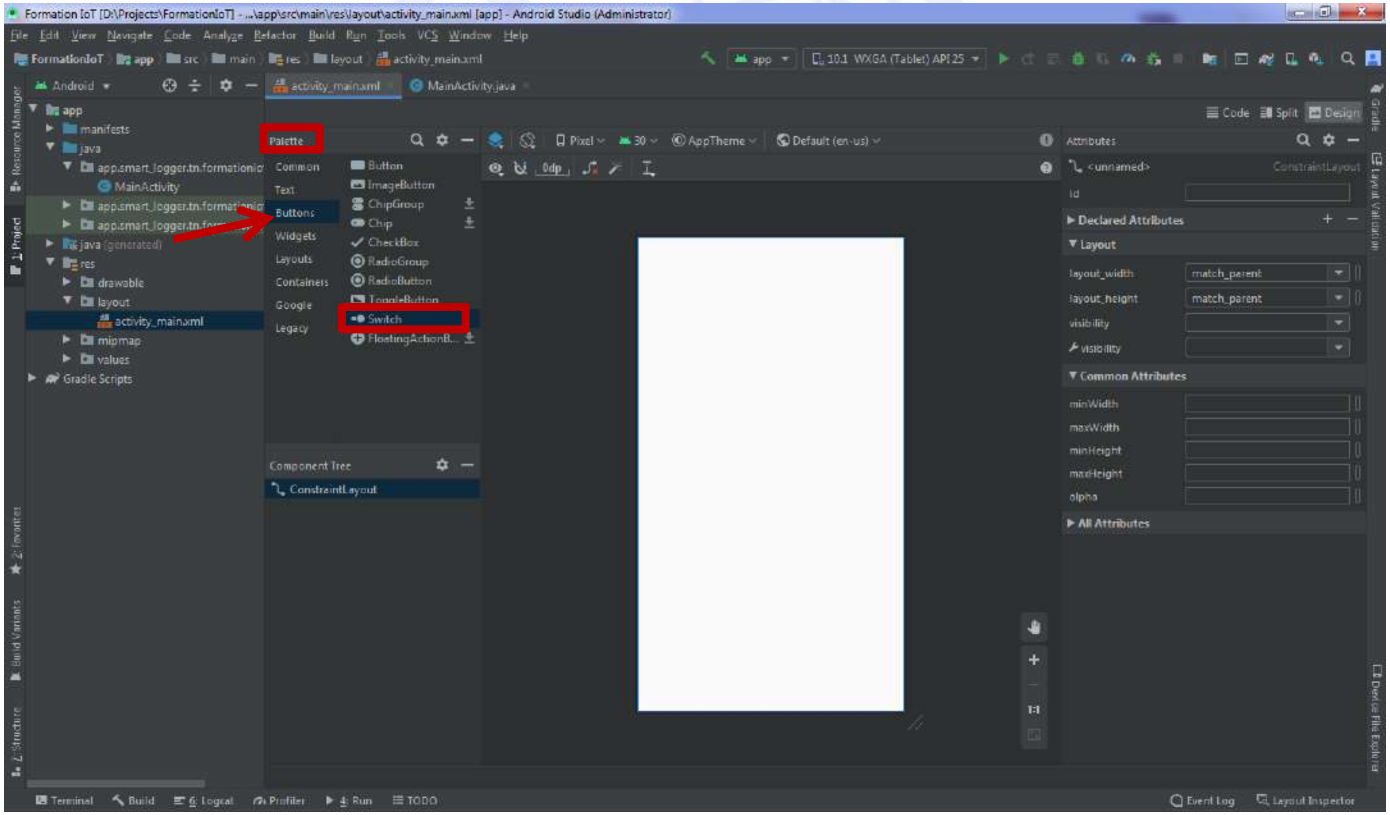
Software Tools

The interface above has appeared, we notice that this is the same content that we saw on our application earlier.

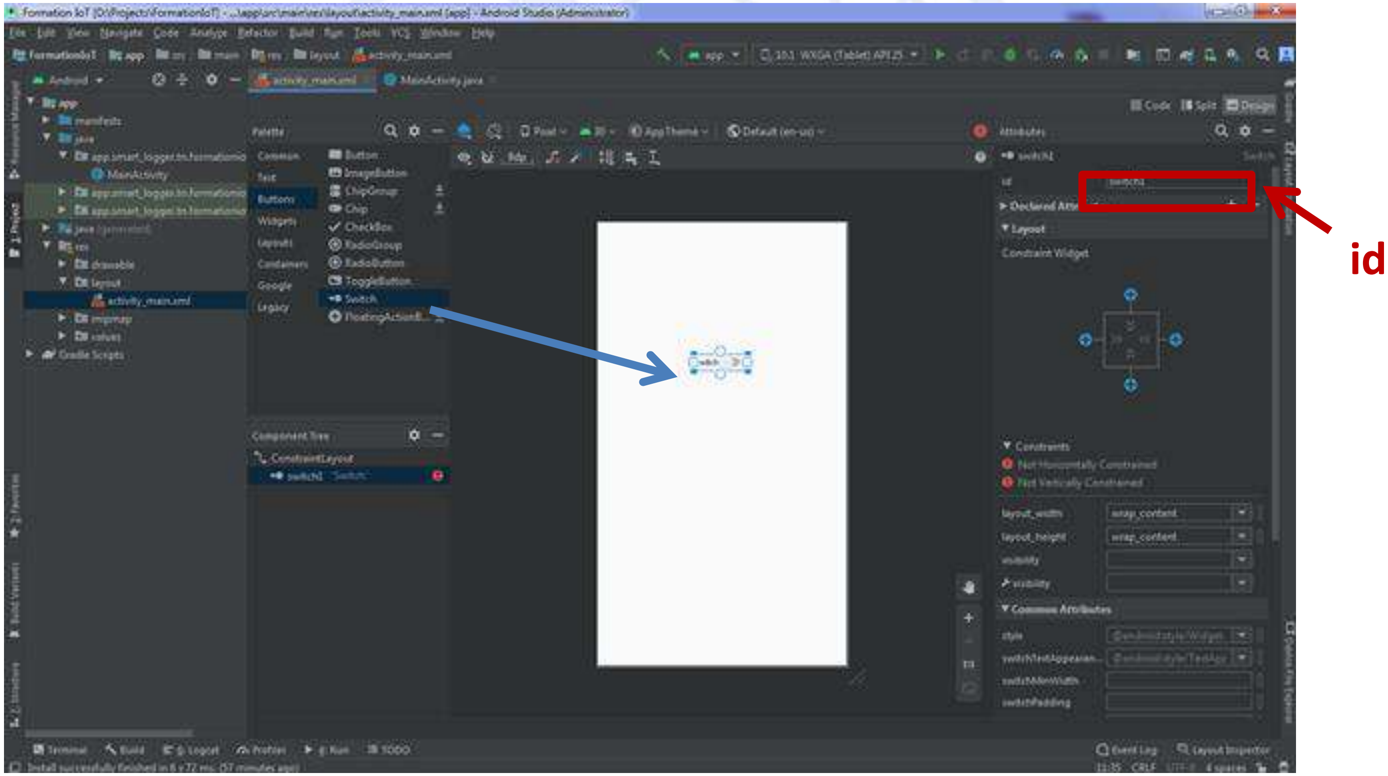


Software Tools

To add a switch click on Palette> Buttons> Switch



Simply, slide the switch to the application interface, the switch is now added to the interface, Please note the id of our switch.



Software Tools

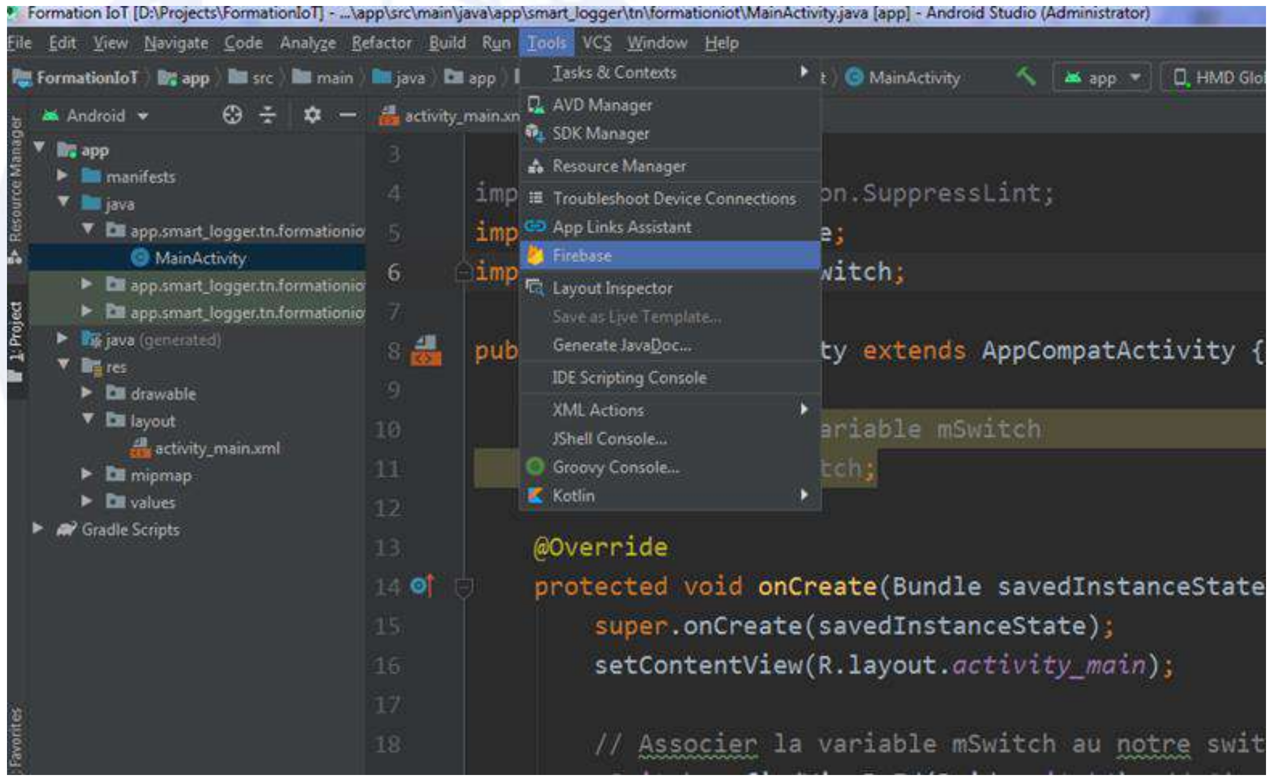
So that our application knows the events coming from switch, we must create a switch instance in the MainActivity.java file. the file should look like the following image

```java
package app.smart_logger.tn.formationiot;
import androidx.appcompat.app.AppCompatActivity;

import android.os.Bundle;
import android.widget.Switch;

public class MainActivity extends AppCompatActivity {

    // Instancier une variable mSwitch
    private Switch mSwitch;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        // Associer la variable mSwitch au notre switch de l'interface graphique
        mSwitch = findViewById(R.id.switch1); // C'est l'id de notre switch vue précédemment!
    }
}
```

Software Tools

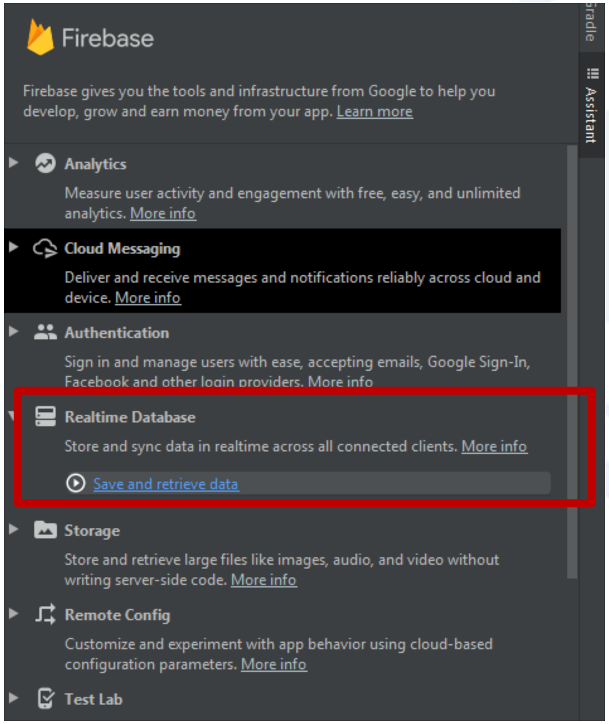
Click Tools> Firebase

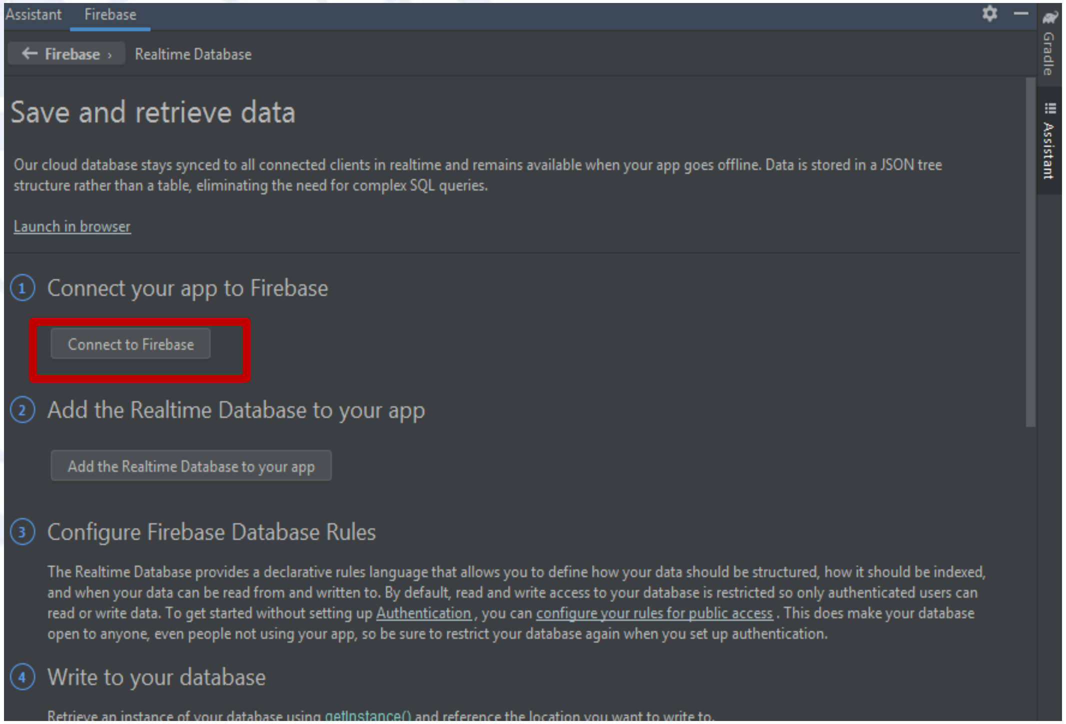
Now, we must associate our Android project with the Firebase project created previously. Android Studio provides a tool that makes it easy to combine different Firebase services. We will take the following steps to use the Firebase Realtime Database service in our Android project



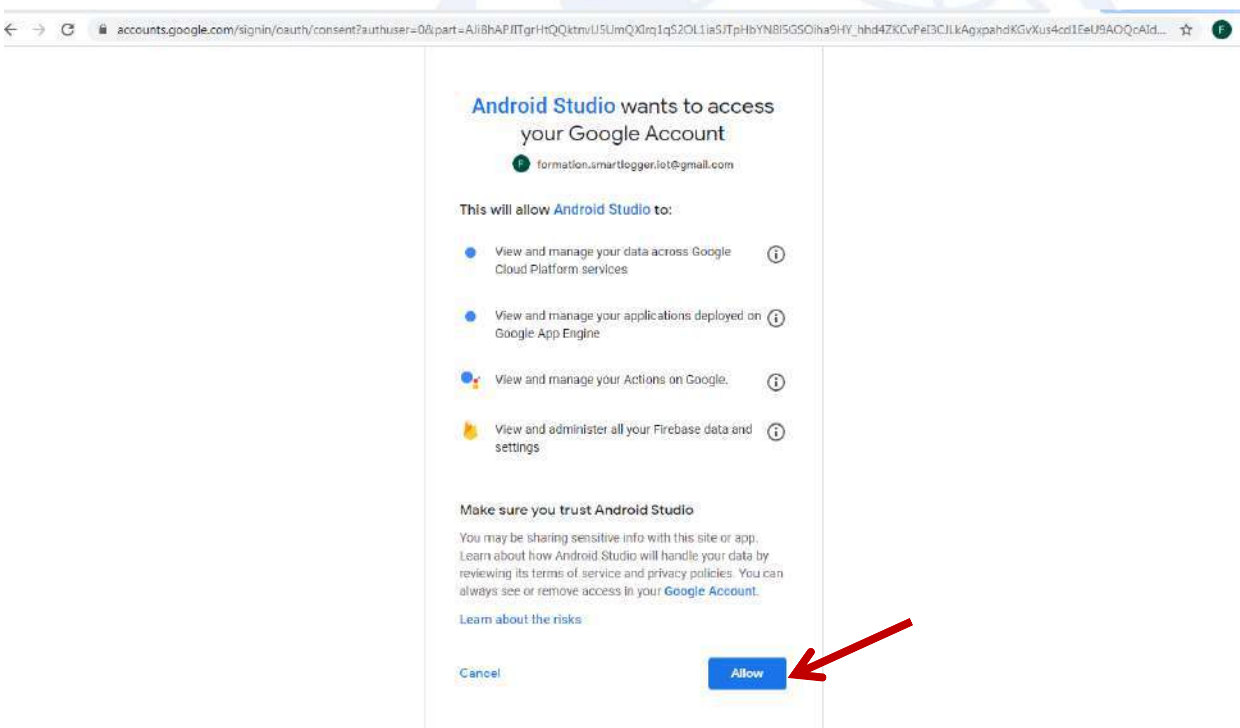
Choose Realtime Database> Save and retrieve data

Then click on "Connect to Firebase"

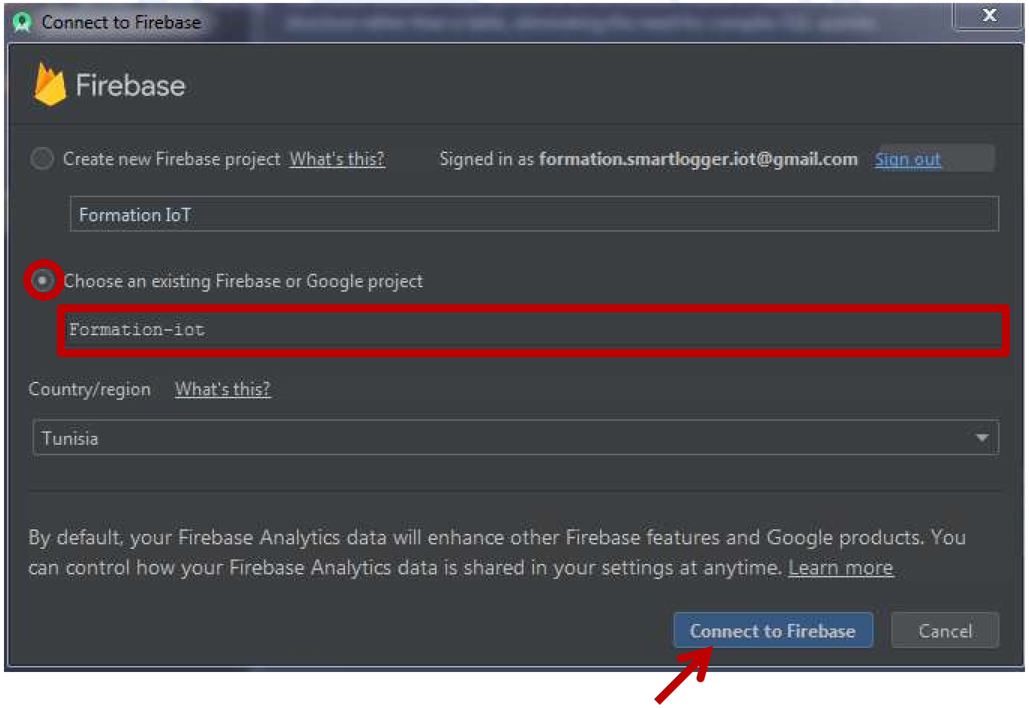




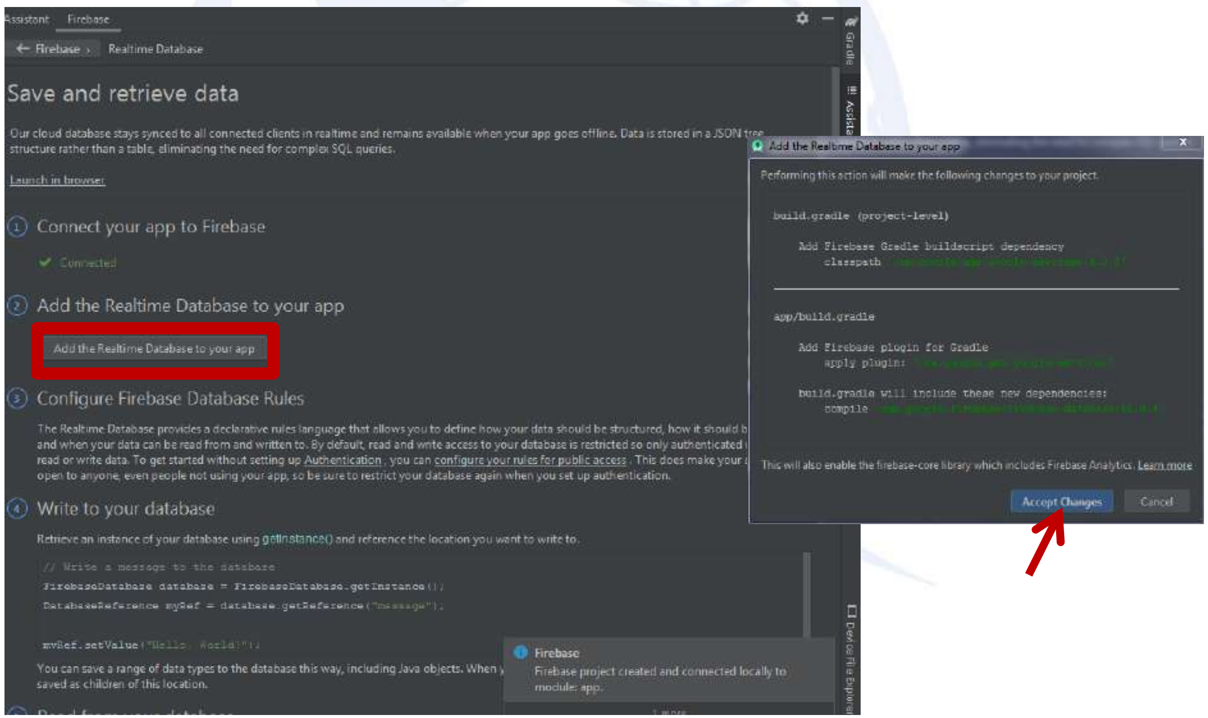
Your browser will launch this, connect to the Google account you used when creating the Firebase project, then click on allow.



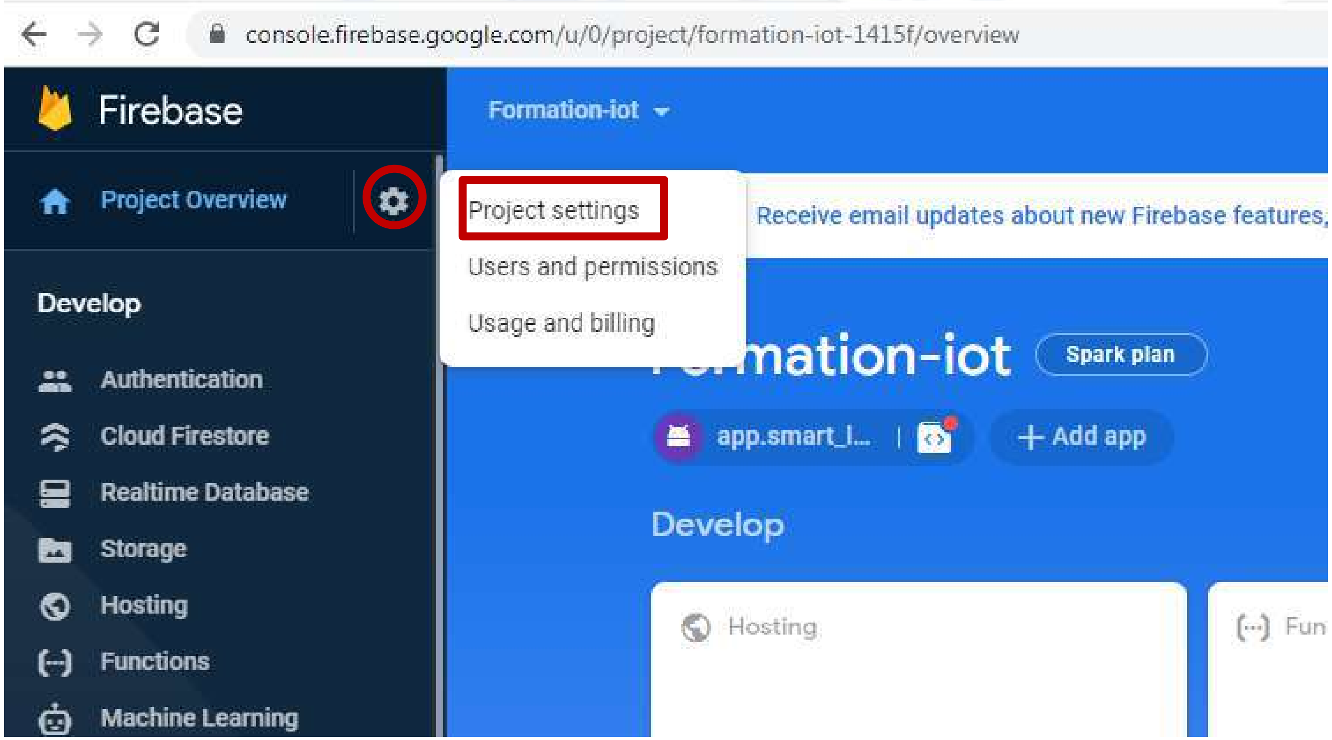
Let's go back to Android Studio, and select Choose an existing Firebase on Google project, choose the project and click on Connect to Firebase.



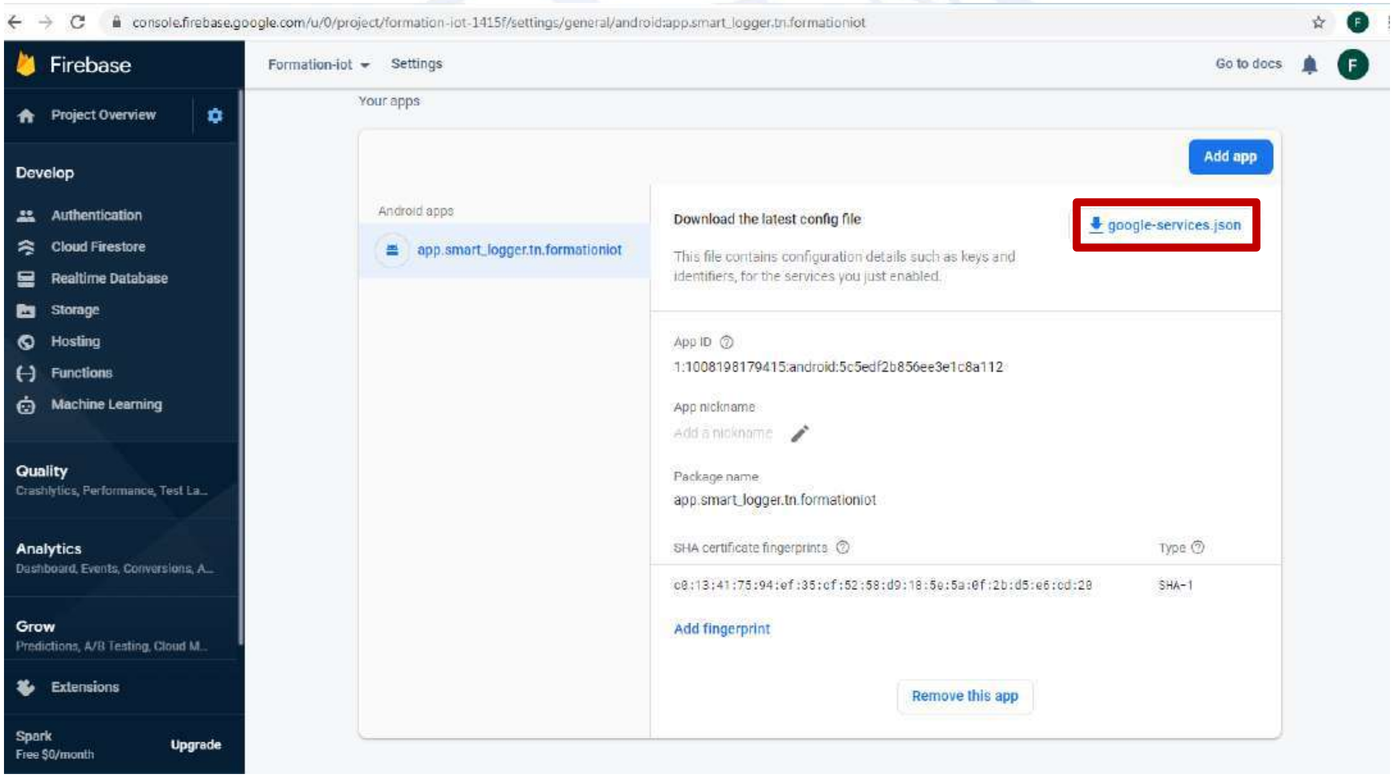
Click on Add the Realtime Database to your app and confirm the changes in the dialog that appears.



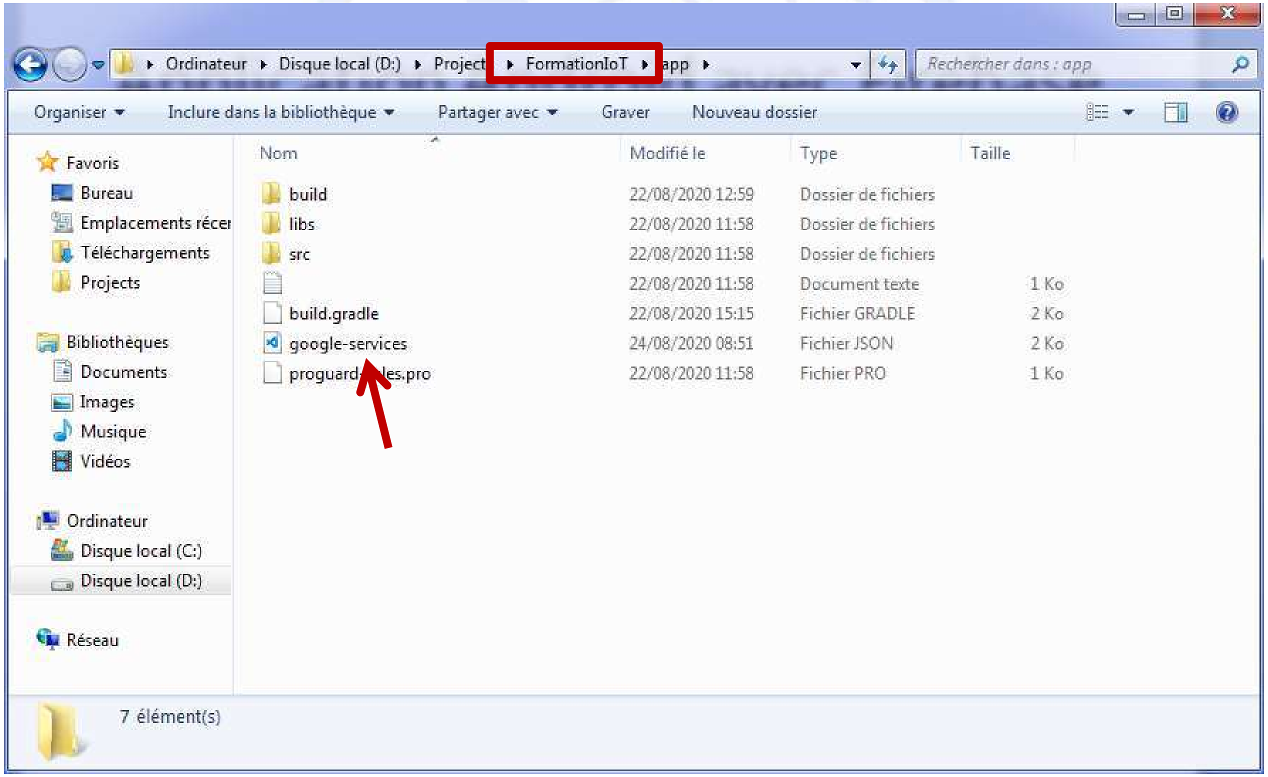
Now back to Firebase console, click on "Project settings".



Click on "google.services.json" to download the Firebase json configuration file.



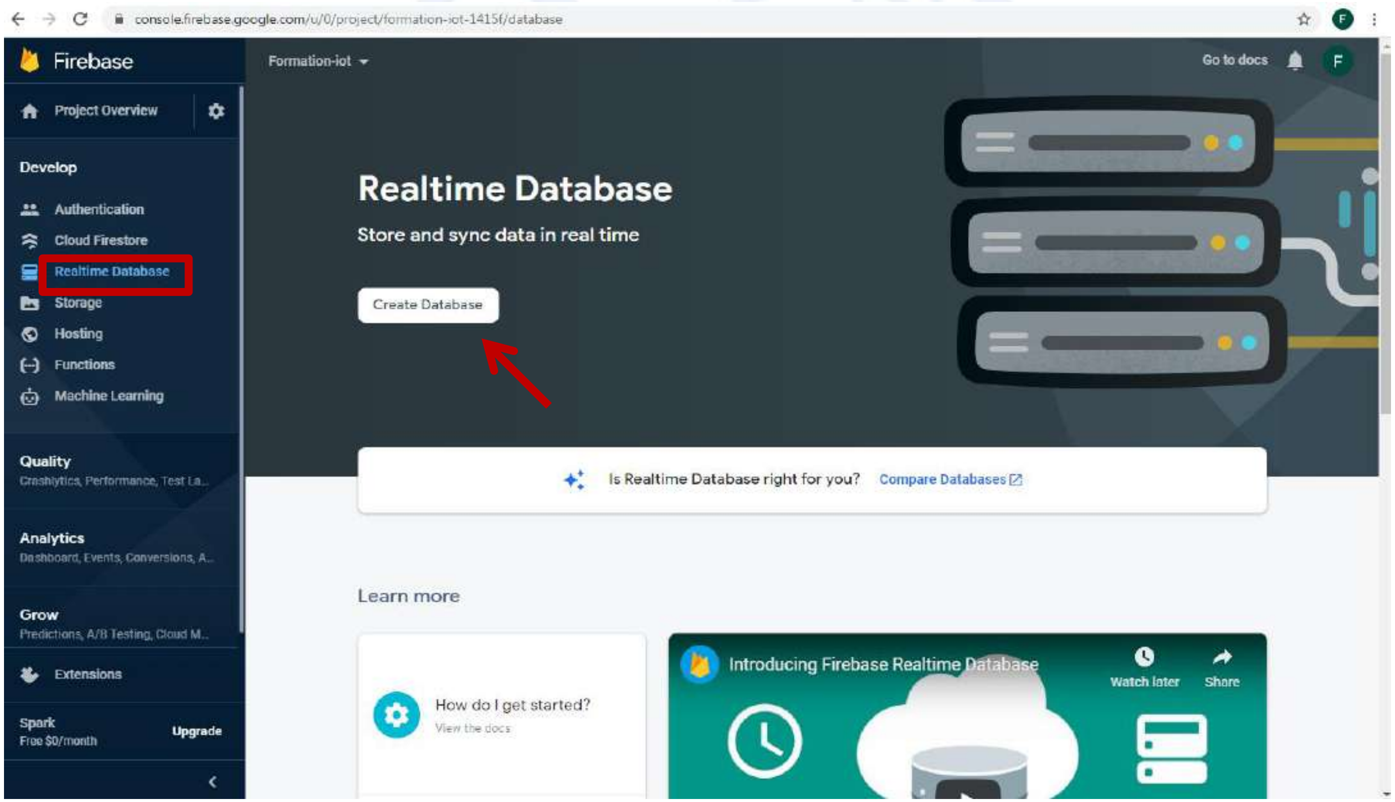
Copy the google.services.json file to the "app" folder of your Android project.



The project is now associated with Firebase Realtime Database. You can run the app on your phone to check if there are any issues.

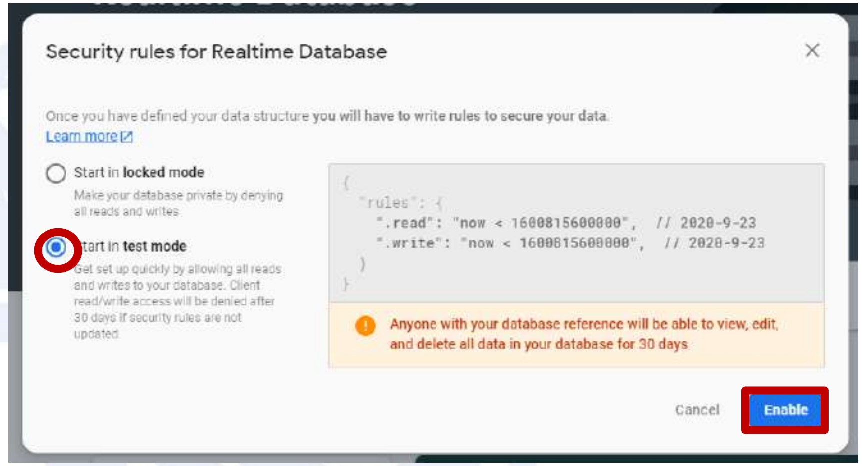
- Let's add a variable in the database to store the gate variable.
- The door has 2 states, either open or closed so we associate it with a Boolean variable:
- true → open door
- false → closed door

In the Firebase console, choose Realtime Database and click on Create Database.

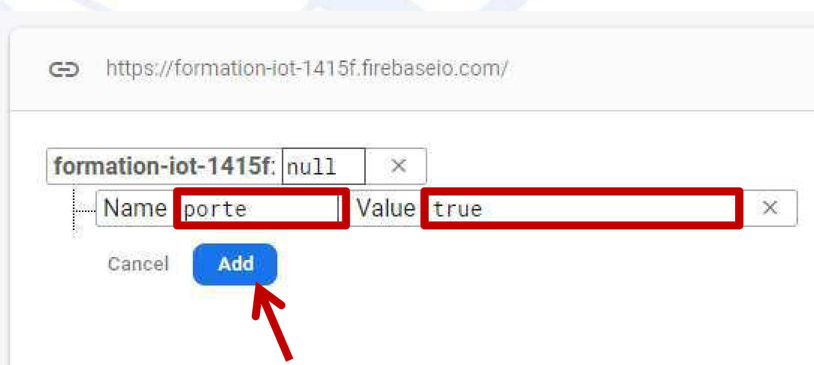


Software Tools

Choose the "test mode" option and click on Enable



To create a door variable in the database, click on “+”, then provide the name of the variable (in our case door), assign a Boolean value (true for example) and validate.



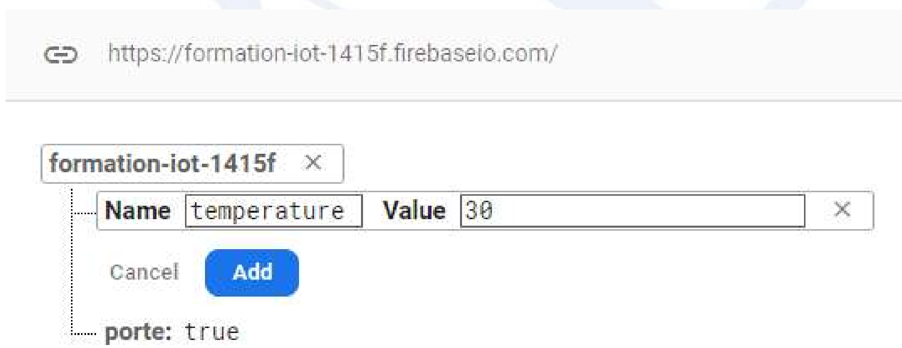
Initialize the switch state according to the value of the gate variable stored in Firebase.
Just at the end of Create method in the MainActivity.java file add the following lines:

```
// Initialiser le switch selon la variable porte stockée dans la base des données
FirebaseDatabase.getInstance().getReference( path: "porte")
        .addValueEventListener(new ValueEventListener() {
            @Override
            public void onDataChange(@NonNull DataSnapshot dataSnapshot) {

                mSwitch.setChecked((boolean) dataSnapshot.getValue());
            }

            @Override
            public void onCancelled(@NonNull DatabaseError databaseError) {

            }
        });
```

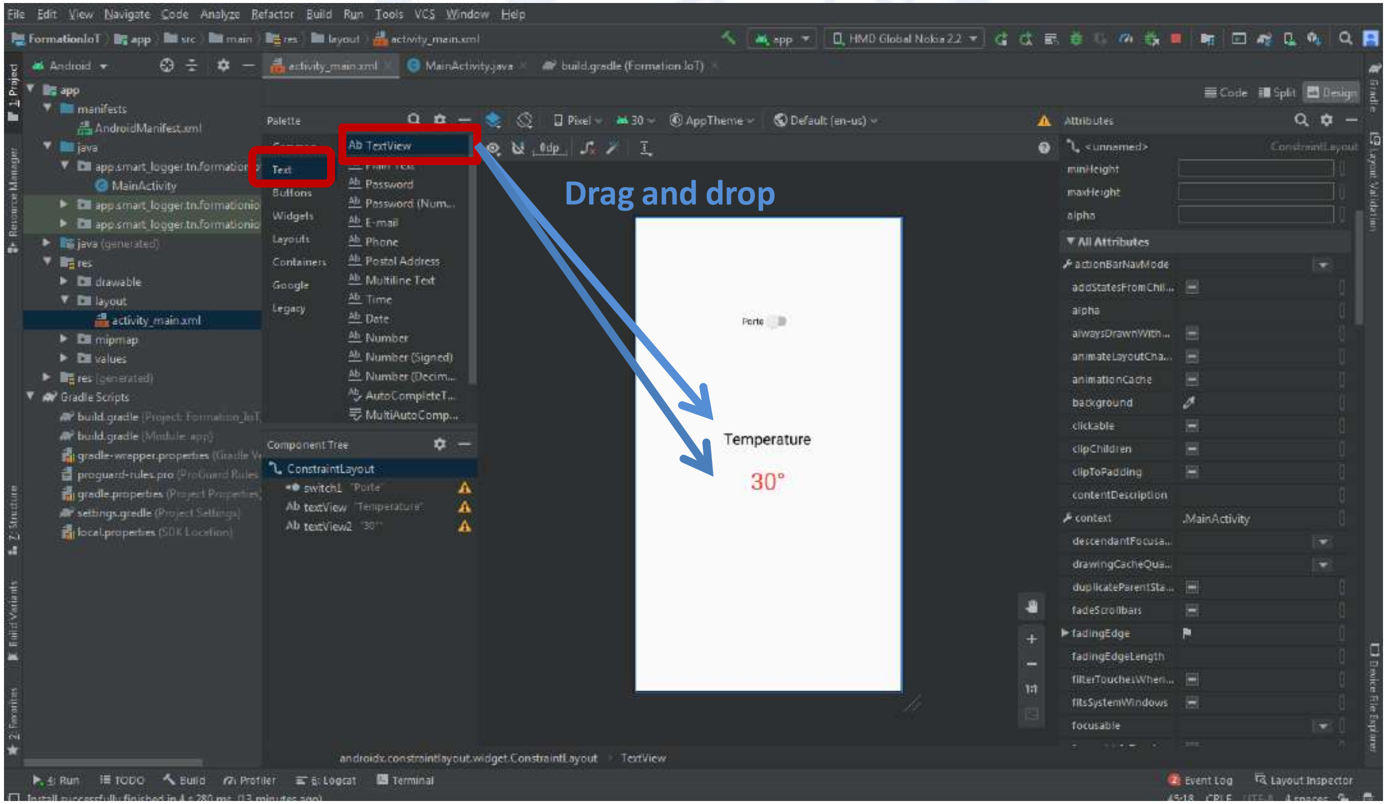
Now read the switch on and off event and save it to the database. Add these lines after the code from the previous step:

```
// Ecout sur les évenements du switch pour changer la variable porte
// dans la base des données en cas de changement d'état.
mSwitch.setOnCheckedChangeListener(new CompoundButton.OnCheckedChangeListener() {
    @Override
    public void onCheckedChanged(CompoundButton compoundButton, boolean b) {
        FirebaseDatabase.getInstance().getReference( path: "porte").setValue(b);
    }
});
```

Run your app. Note that any change made on the switch is immediately memorized in the database. Then, let's add another variable named temperature to our database and assign any numeric variable.



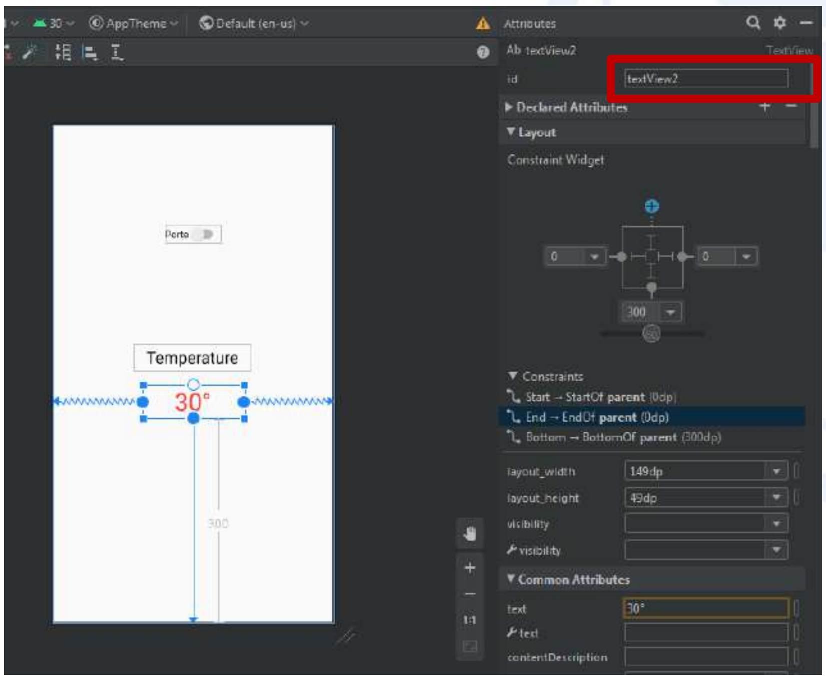
Add two “TextView” in the activity_main.xml file: the Temperature label and its value.

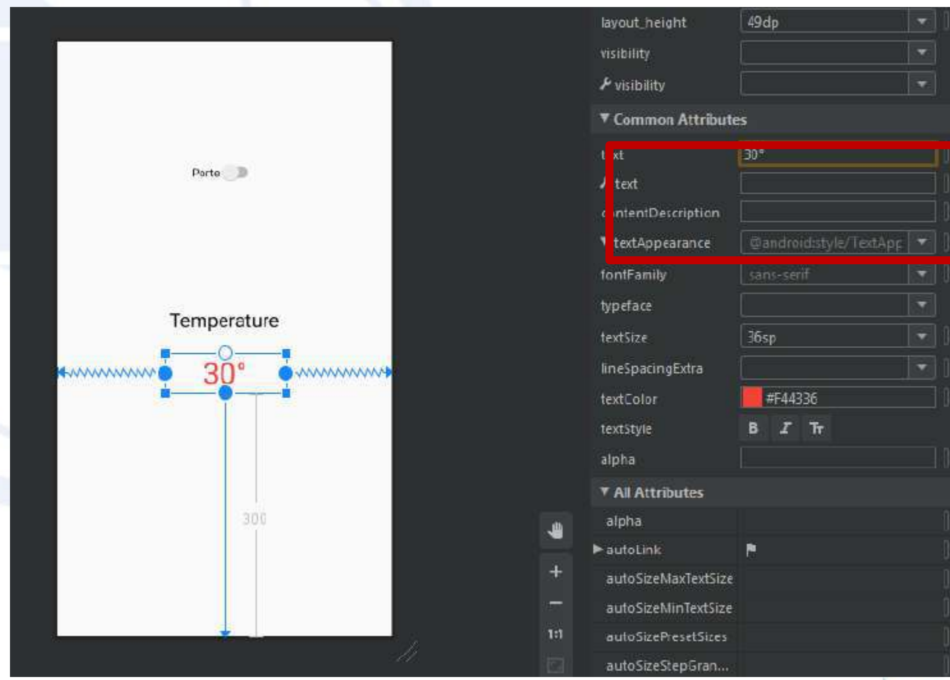


Software Tools

Write down the id of the temperature value.

Change the text size and color as per your choice.





Instantiate the temperature variable after the mSwitch variable

```java
public class MainActivity extends AppCompatActivity {

    // Instancier une variable mSwitch
    private Switch mSwitch;

    // Instancier une variable temperature
    private TextView temperature;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
```

Connect the temperature variable with the TextView in the layout (Graphical interface)

```java
setContentView(R.layout.activity_main);

// Associer la variable mSwitch au switch de l'interface graphique
mSwitch = findViewById(R.id.switch1); // C'est l'id de notre switch vue précédemment!

// Associer la variable temperature au TextView de l'interface graphique
temperature = findViewById(R.id.textView2); // C'est l'id de notre TextView
```

Display the temperature value recorded in Firebase in real time by adding these lines at the end of the onCreate method.

```
// Lire la valeur de la temperature stockée dans la base des données
// et l'afficher dans le TextView
FirebaseDatabase.getInstance().getReference( path: "temperature")
        .addValueEventListener(new ValueEventListener() {
            @Override
            public void onDataChange(@NonNull DataSnapshot dataSnapshot) {
                temperature.setText(dataSnapshot.getValue() + "°");
            }

            @Override
            public void onCancelled(@NonNull DatabaseError databaseError) {

            }
        });
```

Now if you change the temperature in Firebase Realtime Database it will be changed immediately on the application interface!

Thank you!

ITU