TeamSoc21
The ICT Engineer of the 21st Century

Co-funded by the
Erasmus+ Programme
of the European Union

The challenges of the Internet of Things

FILIP TSVETANOV

ftsvetanov@gmail.com

University of Telecommunications and Post
Faculty of Telecommunications
Bulgaria

MAY 2019 VALENSIA

Lecture outline

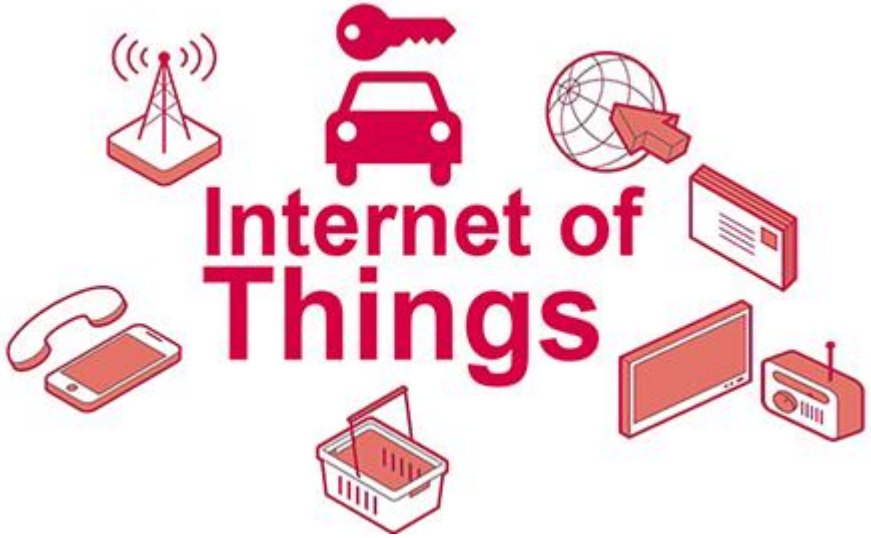
TeamSoc21
The ICT Engineer of the 21st Century

- Introduction
- Architecture
- Communication technologies
- Protocols for smart metering
- Hardware for IoT device
- IoT platforms for Smart metering data.
- Security
- Key takeaways

Introduction

Introduction to Internet of Things

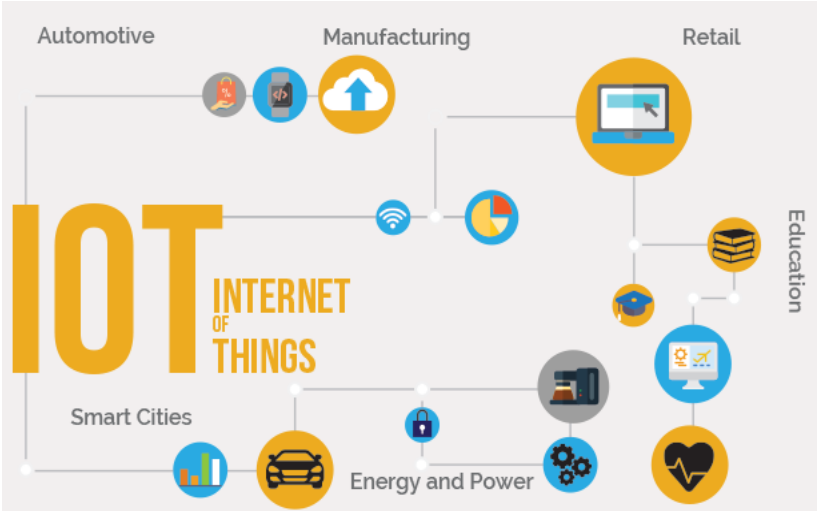
- The Internet of Things (IoT) is a technology in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
- IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems and the Internet.



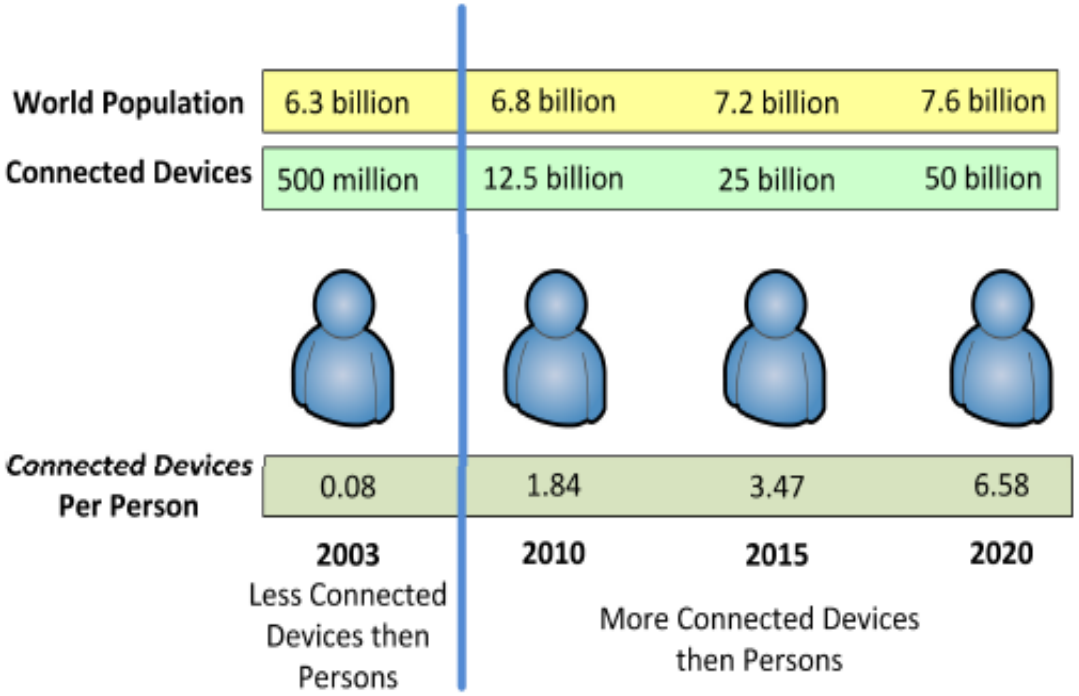
Introduction to Internet of Things

TeamSoc21
The ICT Engineer of the 21st Century

- A thing, in the Internet of Things, can be a person with a heart monitor implant, an animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an **IP address** and provided with the ability to transfer data over a network.
- So far, the Internet of Things has been most closely associated with machine-to-machine (M2M) communication in manufacturing and power, oil and gas utilities. Products built with M2M communication capabilities are often referred to be called smart.



Introduction to Internet of Things



Architecture of IoT

Reference architecture of IoT

TeamSoc21
The ICT Engineer of the 21st Century

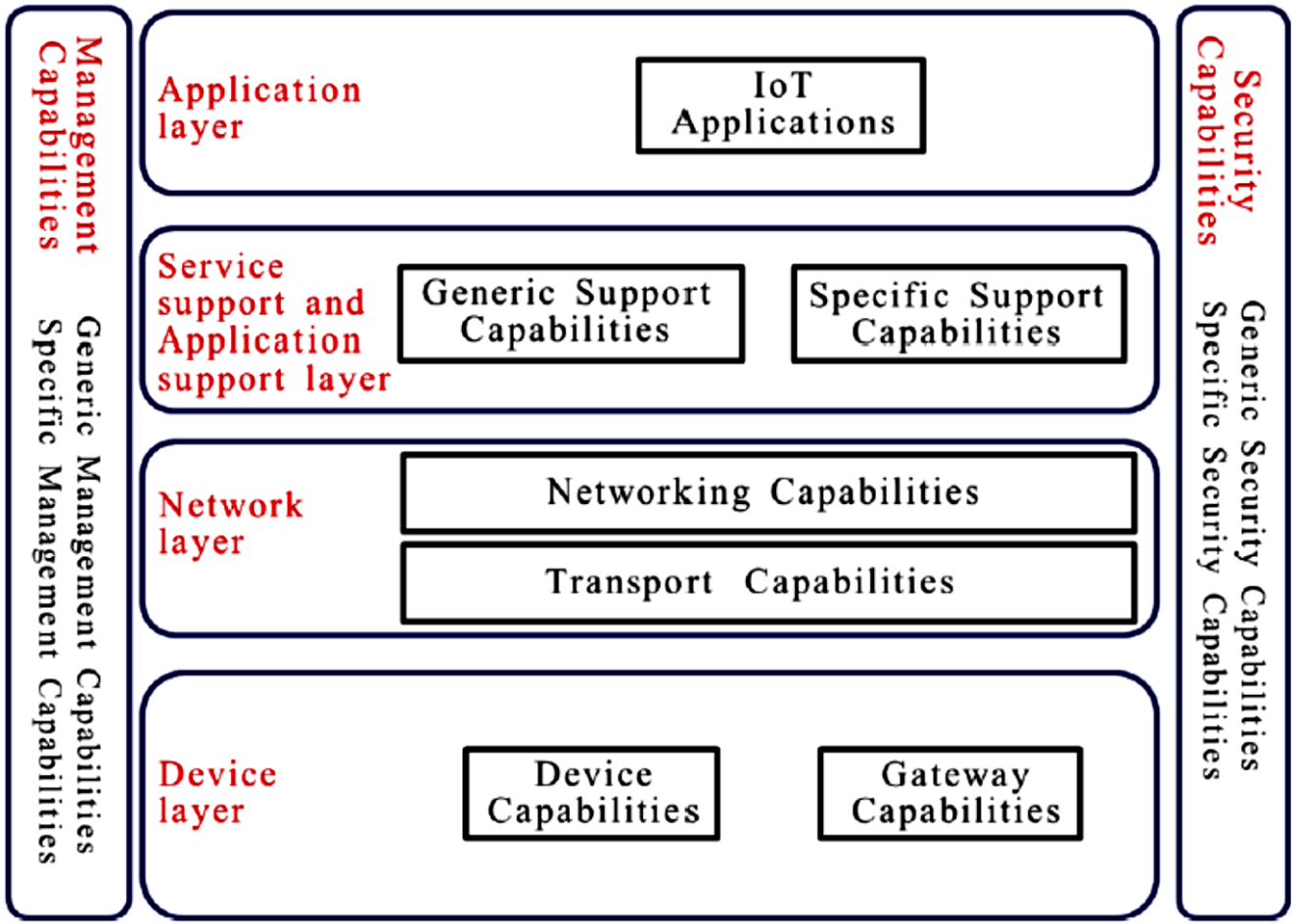
Why?

- ❑The Internet of things devices are interconnected;
- ❑There are currently billions of such devices, so rules are needed to include them.
- ❑Devices interact 24 hours a day and seven days a week, so data needs to be accessed and allow recovery in the event of an accident.
- ❑Devices are used daily, so it is important to keep automatic updates and remote control.

- The Reference Architecture of the Internet of Things network should ensure integration between systems and devices as well as security of transmitted and processed data.

Reference architecture of IoT

- The International Union of Electrotechnics offers standardization of the Internet of Things - IoT-GSI (Global Standards Initiative on Internet of Things).
- Recommendation Y.2060 [8] proposes a reference model for the Internet of Things, which includes four basic horizontal layers and two vertical layers.

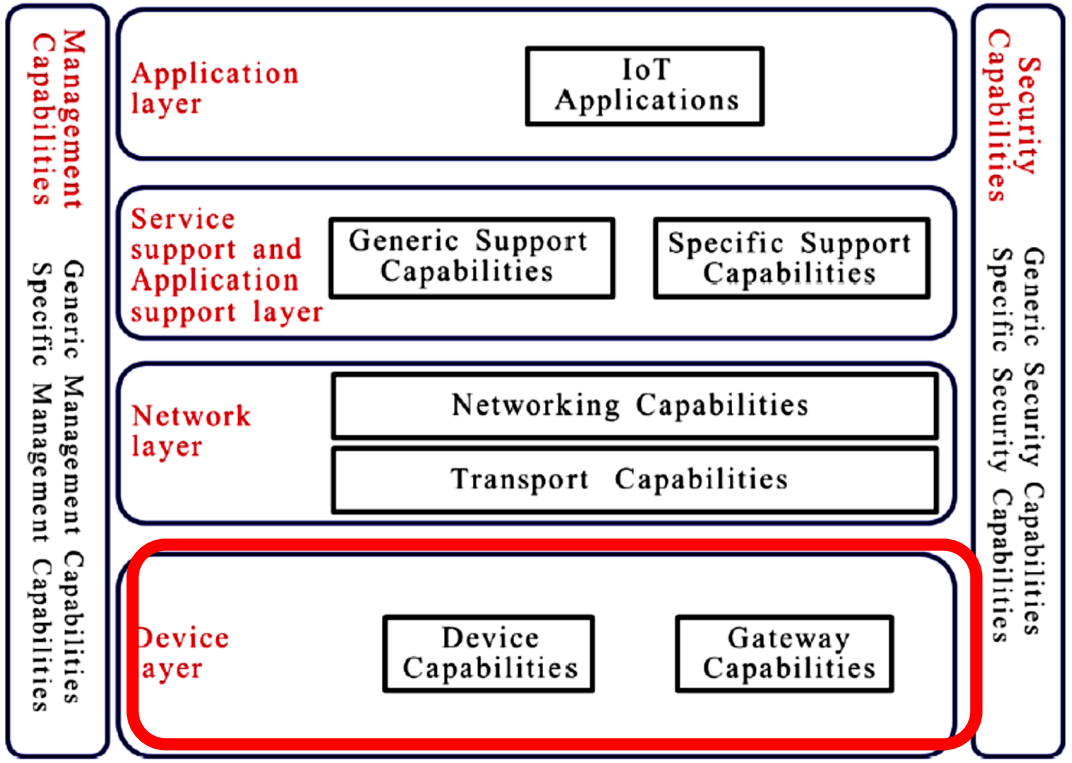


Reference architecture of IoT

TeamSoc21
The ICT Engineer of the 21st Century

Device layer

- **IoT Device capabilities** include but are not limited to:
- **Direct and Indirect interaction with the communication network**: Devices are able to gather and upload information directly (i.e., without using gateway capabilities) to the communication network and can directly receive information from the communication network.
- **Ad-hoc networking**: Devices may be able to construct networks in an ad-hoc manner in some scenarios which need increased scalability and quick deployment.
- **Sleeping and waking-up**: Device capabilities may support "sleeping" and "waking-up„ mechanisms to save energy.

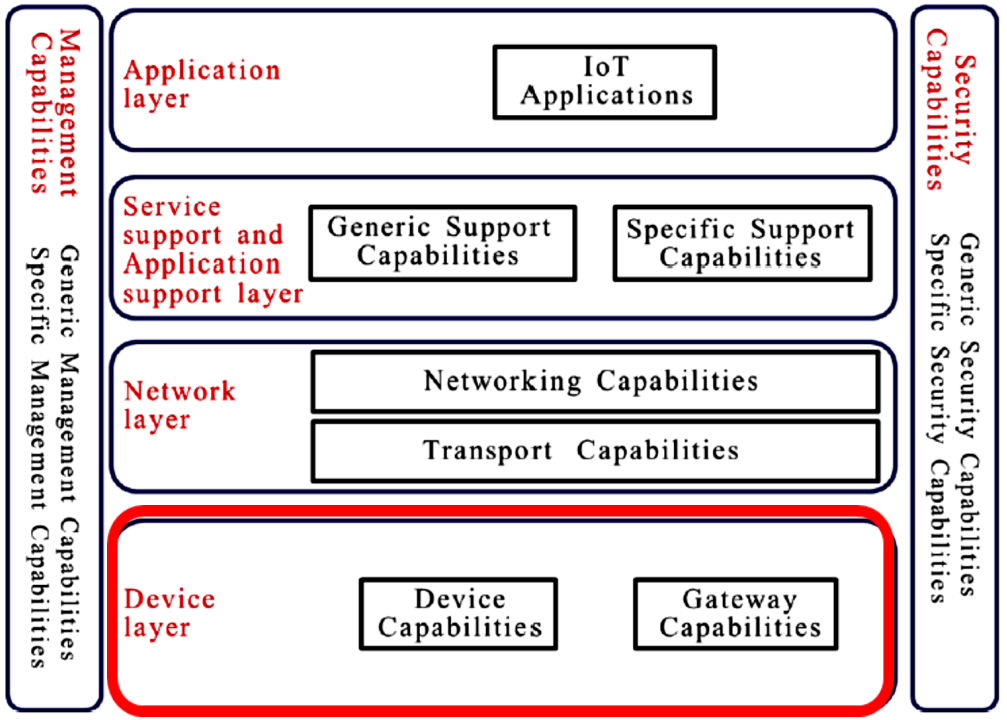


Reference architecture of IoT

TeamSoc21
The ICT Engineer of the 21st Century

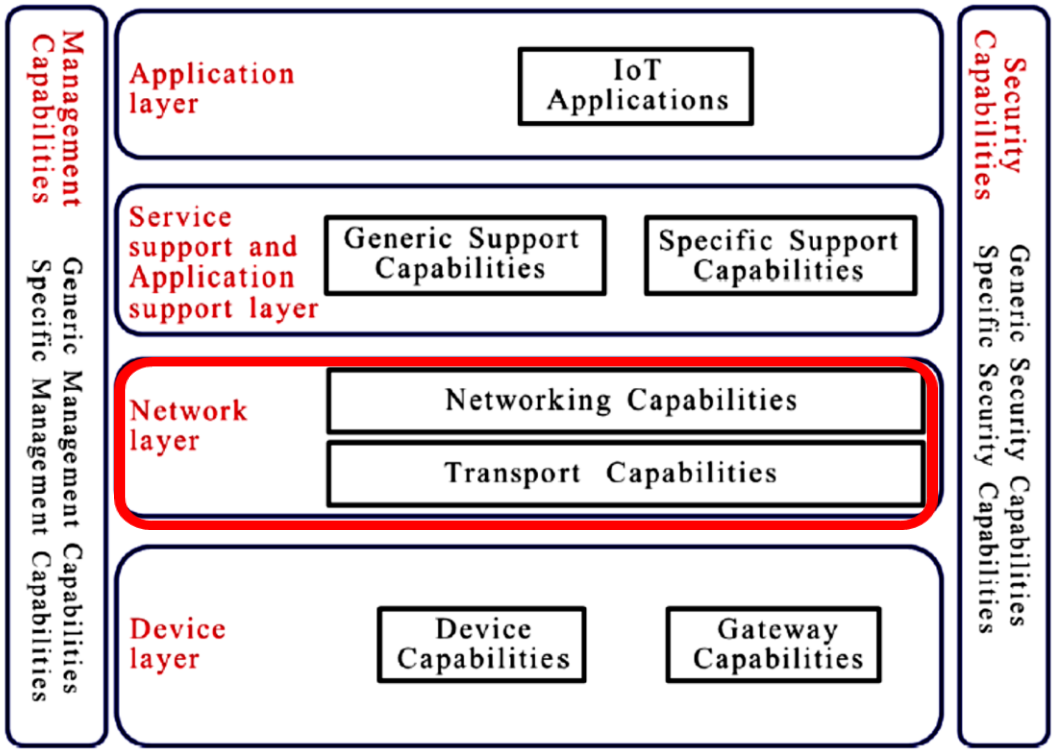
Device layer

- **Gateway capabilities**: The gateway capabilities include but are not limited to:
- **Multiple interfaces support**: support devices connected through different kinds of wired or wireless technologies, such as a controller area network (CAN) bus, ZigBee, Bluetooth or Wi-Fi. At the network layer, the gateway capabilities may communicate through various technologies, such as the public switched telephone network (PSTN), second generation or third generation (2G or 3G) networks, long-term evolution networks (LTE), Ethernet or digital subscriber lines (DSL).
- **Protocol conversion:** There are two situations where gateway capabilities are needed. One situation is when communications at the device layer use different device layer protocols, e.g., ZigBee protocols and Bluetooth protocols, the other one is when communications involving both the device layer and network layer use different protocols, a ZigBee technology protocol at the device layer and a 3G technology protocol at the network layer.



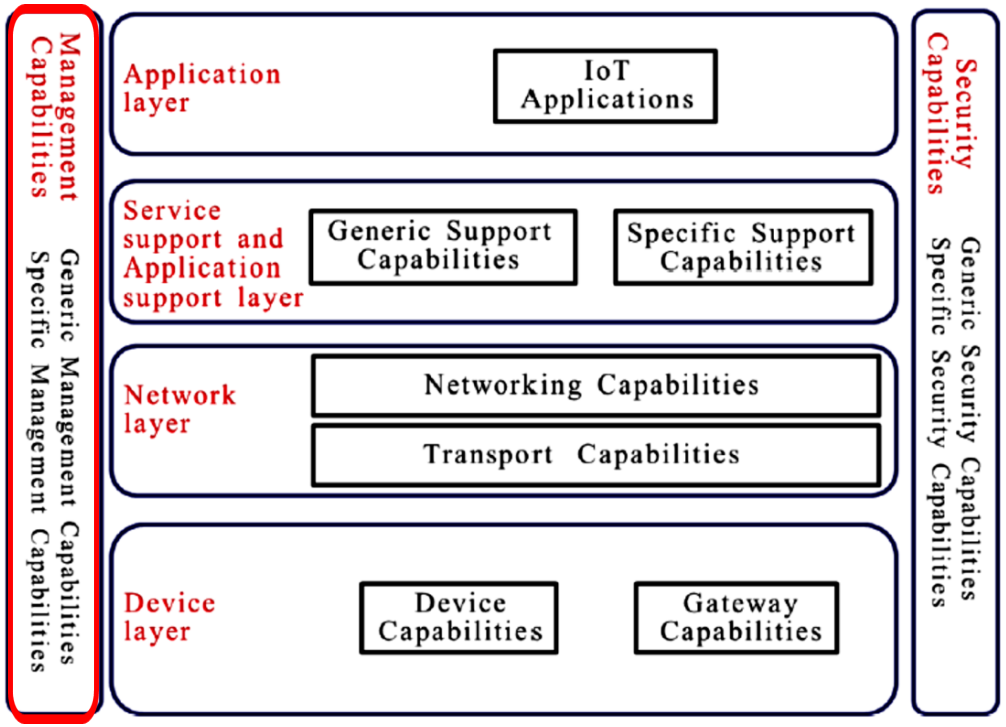
Reference architecture of IoT

- **Network layer**
- This consists of the following two types of capabilities:
- – **Networking capabilities:** provide relevant control functions of network connectivity, such as access and transport resource control functions, mobility management or authentication, authorization and accounting (AAA).
- – **Transport capabilities**: focus on providing connectivity for the transport of IoT service and application specific data information, as well as the transport of IoT-related control and management information.



Reference architecture of IoT

- **Management capabilities**
- The IoT management capabilities can be categorized into **generic management capabilities and specific management capabilities.**
- **Essential generic management** capabilities in the IoT include:
- – device management, such as remote device activation and de-activation, diagnostics, firmware and/or software updating, device working status management;
- – local network topology management;
- – traffic and congestion management, such as the detection of network overflow conditions and the implementation of resource reservation for time-critical and/or life-critical data flows.
- **Specific management capabilities** are closely coupled with application-specific requirements, e.g.,
- smart grid power transmission line monitoring requirements.



Reference architecture of IoT

- **Security capabilities**

There are two kinds of security capabilities:

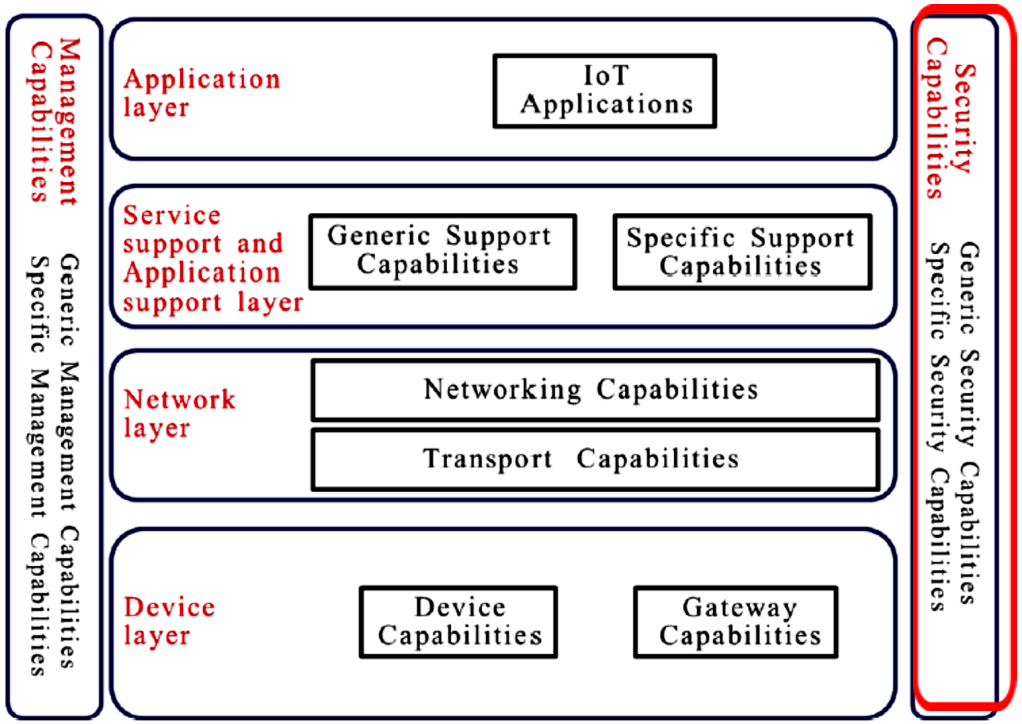
- **Generic security capabilities** are independent of applications. They include:

➢ at the application layer: authorization, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus;

➢ at the network layer: authorization, authentication, use data and signaling data confidentiality, and signaling integrity protection;

➢ at the device layer: authentication, authorization, device integrity validation, access control, data confidentiality and integrity protection.

- **Specific security capabilities** are closely coupled with application-specific requirements, e.g., mobile payment, security requirements.



Reference architecture of IoT

TeamSoc21
The ICT Engineer of the 21st Century

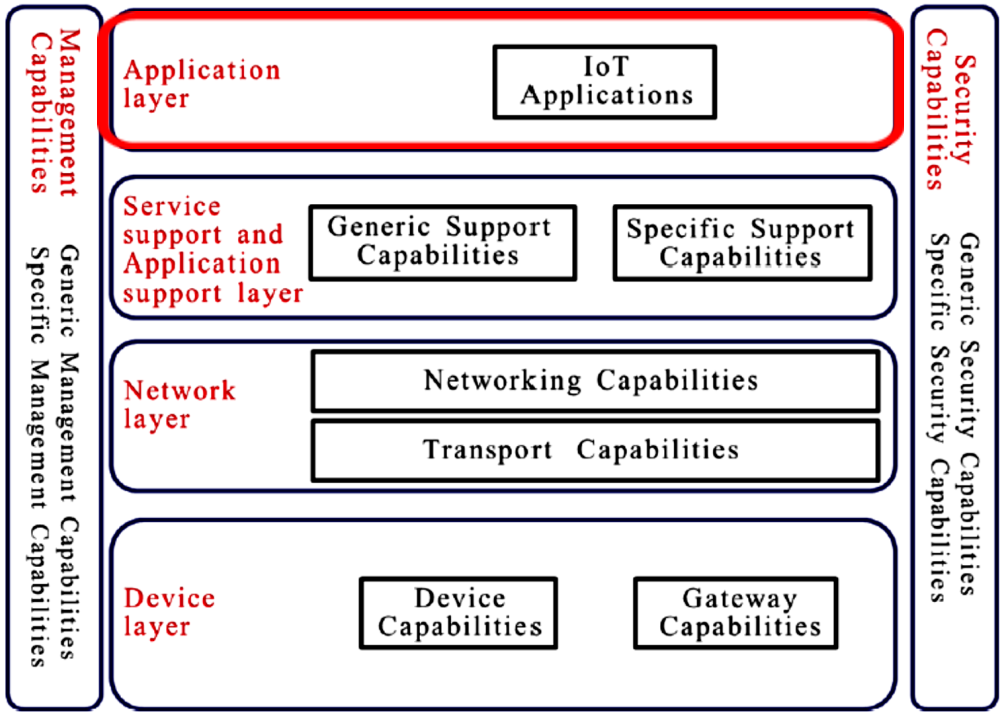
- **Application layer**

The application layer contains IoT applications.

- **Service support and application support layer** consists:

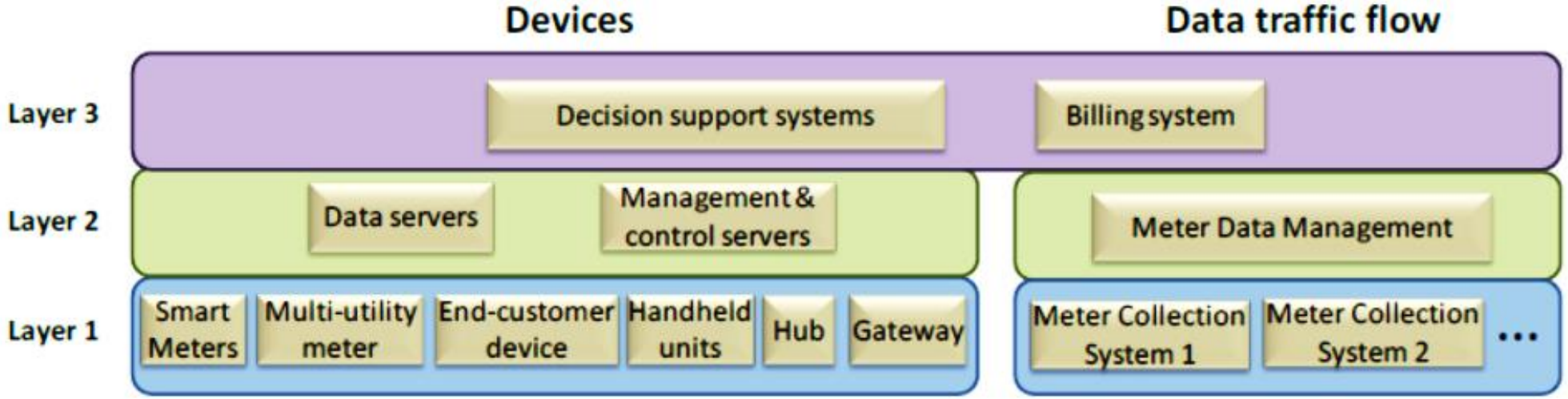
➢**Generic support capabilities**: The generic support capabilities are common capabilities which can be used by different IoT applications, such as data processing or data storage. These capabilities may be also invoked by specific support capabilities, to build other specific support capabilities.

➢**Specific support capabilities**: The specific support capabilities are particular capabilities which provide requirements of diversified applications. In fact, they may consist of various detailed capability groupings, in order to provide different support functions to different IoT applications.



Architecture for smart metering

A layered architecture allows us to classify all components and interfaces into different categories according to their features and purposes.
The proposed architecture uses three layers [10].
Layer 1 - Smart meters, network devices and communication protocols to allow smart metering through Internet.
Layer 2 - Devices in charge of receiving data at the utility side form.
Layer 3 - Includes artificial intelligent systems in big data in order to provide information to the decision systems and the billing systems.



Source [10].

Architecture for smart metering -protocols

For smart metering electrical power have proposed new communication protocols which do not use the power line to transmit the information, so they can be also used in water and gas metering. The protocols are classified into several categories:

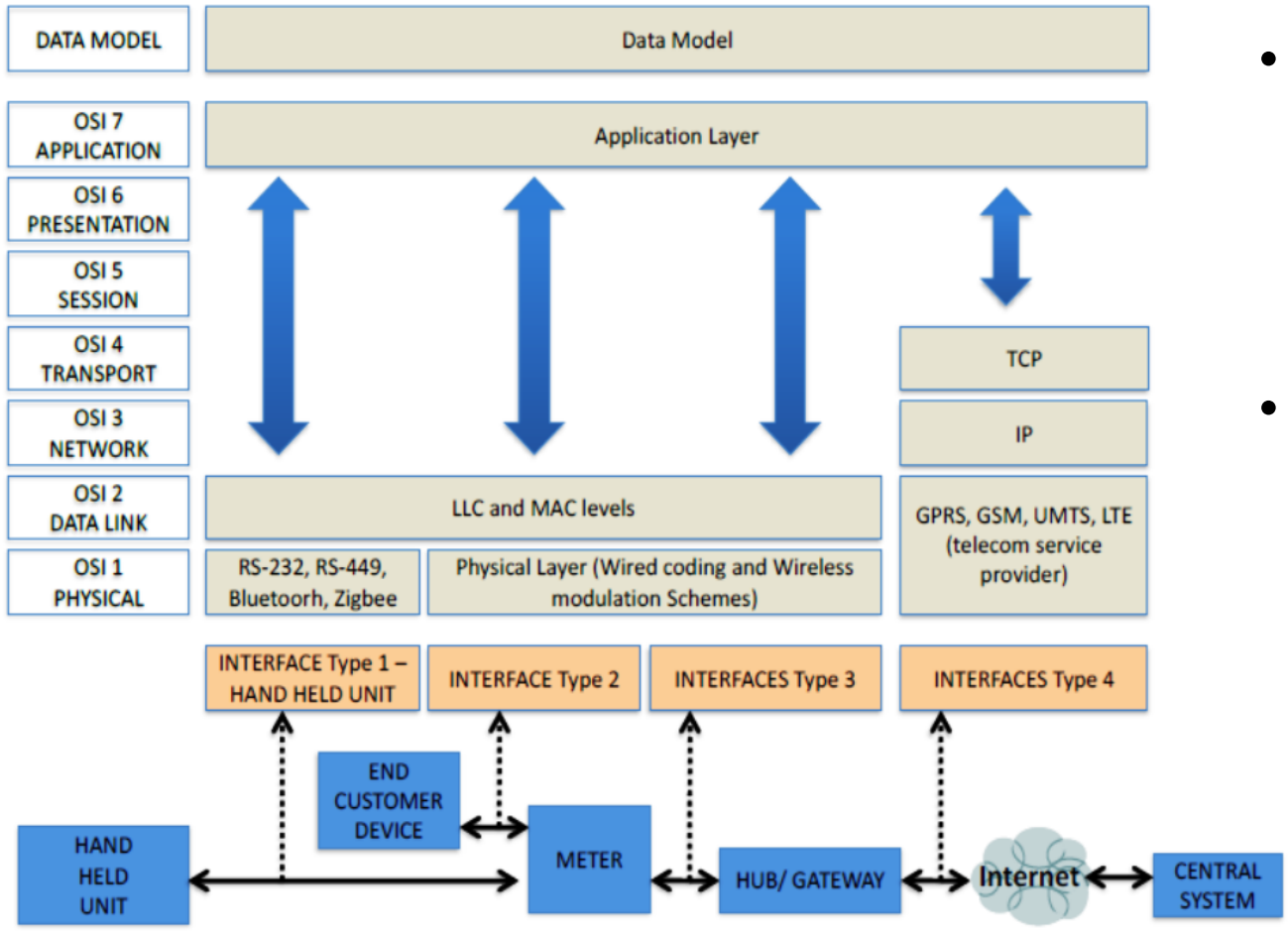
- **First category** includes the **standardized and open meter access protocols.** The main ones are EN 13757 (M-bus), which can alternatively be used with DLMS/COSEM, ANSI C12.18, ANSI C12.21, CzBus, Wavenis, EverBlu, Serial Coded Tele-Metering (SCTM) protocol (IEC 60870-5-102), KNX, LonTalk, LonWorks, IEC 62056, IEC 62056-21 (also known as IEC 1107).

Architecture for smart metering -protocols

- The **second category** includes **general purpose standardized communication protocols.** There are network topologies where data are sent wirelessly to a nearby hub or gateway directly or to a set of sub-trees with a root node. In other cases there is a wireless ad-hoc network or a wireless mesh network with a gateway. They are **IEEE 802.15.1 or 802.11 (Bluetooth), IEEE 802.15.4 [11], 6LoWPAN, and IEEE 802.11 (WiFi).**

- The **third category** includes some well **stablished proprietary systems.** E.g. Plextek, which is based on a proprietary Ultra Narrow Band technology, includes a proprietary digital signal processing techniques and an additional frequency hopping. It is a short-range low-cost radio solution, which operates in the **868 MHz or 915 MHz** ISM frequency bands. It uses a point-to-multipoint architecture allowing handling a large numbers of devices (typically 5,000 - 10,000) per hub, and has modest data rate requirements. Hubs have a 2 – 20 km cell radius.

Architecture for smart metering



Four different types of interfaces to connect devices from different communication transmission environments [10].

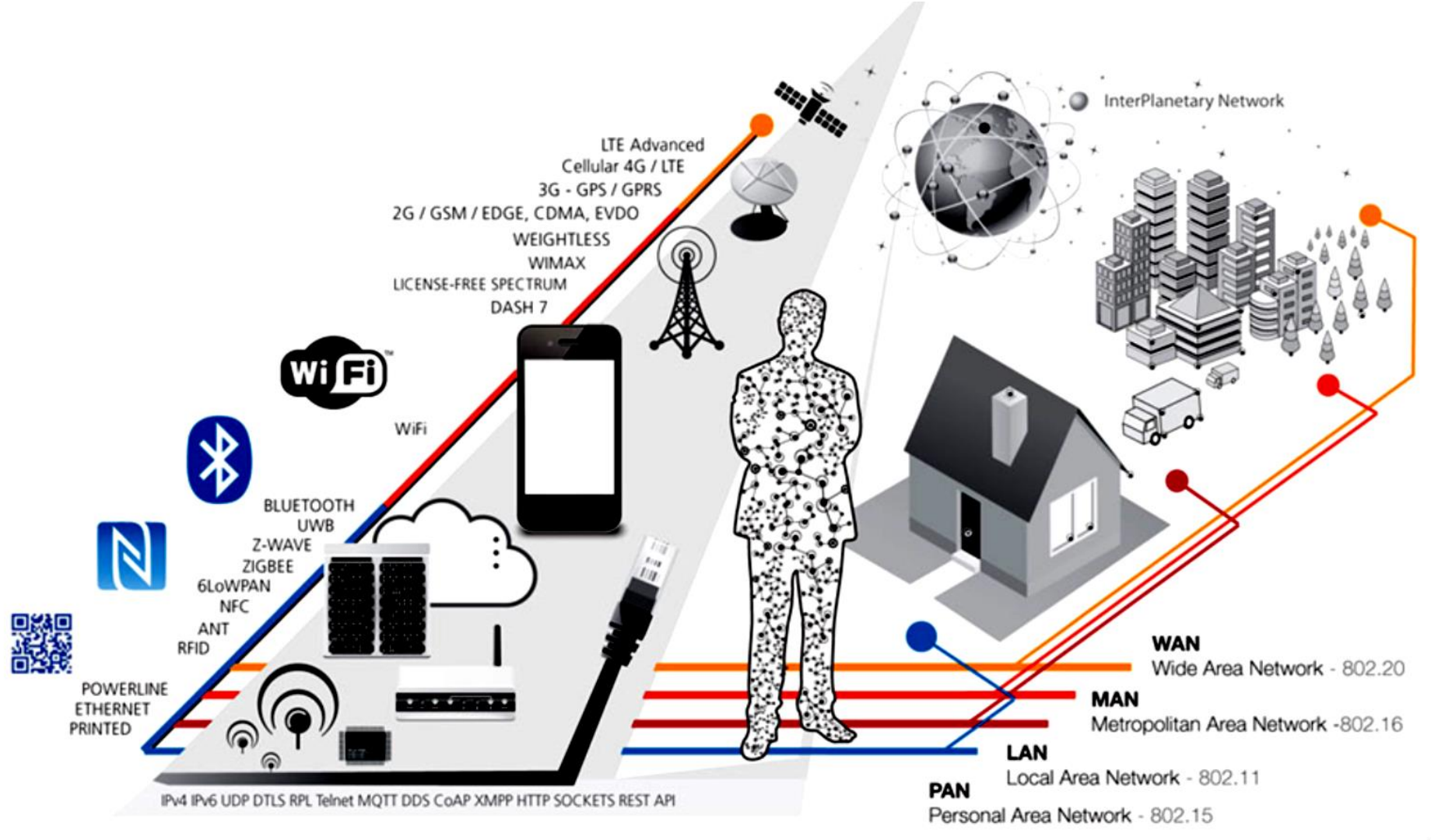
- Used **wired technologies** include Public Switched Telephone Network (PSTN), the Asymmetric Digital Subscriber Line (ADSL) and the Fiber to the Building or Fiber to the Home (FTTx).
- The **wireless technology** have wide range of solutions: Terrestrial Trunked Radio (TETRA), ERMES and ReFLEX, 2G (Global System for Mobile communications, GSM, General Packet Radio Service, GPRS, and Enhanced GPRS, EGPRS), 3G (Universal Mobile Telecommunications System, UMTS, High Speed Downlink Packet Access, HSPA and HSPA+), IEEE 802.16, Long Term Evolution (LTE), and Mobile satellite communication.

Communication technologies

Comunication technologies for IoT

- Communication Protocols form the backbone of IoT systems and enable network connectivity and coupling to applications.
- Communication protocols allow devices to exchange data over the network.
- The protocols define the data exchange formats, data encoding, addressing schemes for devices and routing of packets from source to destination.
- Other functions of the protocols include sequence control, flow control, and retransmission of lost packets.

Communication technologies for IoT



Source: https://sites.google.com/site/iotsamos/iot-in-general/iot-connectivity-technolo

Comunication technologies for IoT

TeamSoc21
The ICT Engineer of the 21st Century

The most popular communication protocols are:

	Owner	Frequency (MHz)	Range	Power requirement	Security	Compatibility
Zigbee	Zigbee Alliance	868 - 868.6 (Europe) 902 - 928 (US)	10–100 meters line-of-sight	Low-Power, Potential Batteryless	Low, basic encryption	Compatible across Zigbee devices. DotDot OS.
Lo-RaWan	LoRa Alliance	169, 433, 868 (Europe) 915 (US)	Up to 6.2 miles or 10 km.	Low-Power	Basic 64-128 bit encryption	Depends on OEM
LTE-M	GSMA - Cellular Carriers	LTE Bands: 450-2350 (uplink)	Global	Band dependant	NSA AES-256	Application dependant
IEEE 802.11af (White-Fi)	Open - IEEE Certified	470 - 710 (Digital Dividend)	Short, up to 100m	Low	WPA	Application dependant
IEEE 802.11ah (HaLow)	Open - IEEE Certified	850 (Europe) 900 (US) 700 (China)	Up to 13 miles or 20 km.	Medium	WPA	Application dependant

Communication technologies for IoT

- **Wi-Fi** is a technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections.
- The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards"
- 802.11a/b/g/n/af, WiFi Direct, WPS
- Frequency: 2.4 GHz, 3.6 GHz and 4.9/5.0 GHz bands.
- Range: Common range is up to 100m but can be extended.
- Applications: Routers, Tablets, etc.

Comunication technologies for IoT

TeamSoc21
The ICT Engineer of the 21st Century

- **White-Fi and HaLow**: low-cost, unlicensed spectrum, extended range.
- IEEE 802.11af (White-Fi) and IEEE 802.11ah (HaLow) are the most sought-after solutions for connectivity. Both use previously unlicensed spectrum and do not interfere with traditional Wi-Fi signals in the 2.4-GHz and 5-GHz bands nor with 2G and 3G cellular networks. Some of the spectrum is shared with some LTE channels used in the United States.
- HaLow extends Wi-Fi into the 900-MHz band, enabling the low power connectivity necessary for applications, including sensors and wearables. HaLow is the preferred Wi-Fi standard for IoT.
- The biggest problem for HaLow is that unlicensed spectrum is not harmonized across the globe: HaLow operates at 900 MHz in the U.S., 850 MHz in Europe and 700 MHz in China and does not even have operating spectrum in many countries.
- The technology is not suitable for high-speed or high-volume data transmission. HaLow provides for data rates as low as 150 Kbps.
- HaLow have power-saving features, such as Target Wake Time (TWT) and Traffic Indication Map (TIM), enabling the IoT devices to communicate at selected intervals, thus saving battery power.

Comunication technologies for IoT

- In 2017 IEEE introduced another Wi-Fi standard for IoT: **802.11ax**. It's advantage over HaLow is the use of the 2.4-GHz and 5-GHz frequency bands, common on most Wi-Fi access points.
- 802.11ax is better-suited to local-range IoT than HaLow. The expectations for 802.11ax are high due to it's network access enhancements, which will naturally provide secondary benefits of IoT enablement.
- Security is the biggest issue. Wi-Fi lacks the protection of the secure element and hardware encryption provided by SIM's on cellular networks. To deploy hundreds or thousands of wireless sensors in a wide area, however, White-Fi and HaLow can provide low-cost connectivity and good performance.

Comunication technologies for IoT

TeamSoc21
The ICT Engineer of the 21st Century

- **Zigbee:** proprietary, short-range, inexpensive and basically secure have over 2200 products certified.
- ZigBee provides most of the basic features (connectivity, range, security) it allows interoperability with any ZigBee-certified device.
- ZigBee is a low-power, low-data-rate, close-proximity ad-hoc wireless network, supporting mesh network topology. It is especially suited for home and office applications, where devices are located in a small area. It only works in distances from 10 to 100 meters line-of-sight. It uses the IEEE 802.15.4 WPAN specification, providing data rates of 250 kbps, 40 kbps and 20 kbps.
- The low data rates and proximity allow devices using smaller batteries to last for years.
- ZigBee launched it's anticipated **IoT basic language, Dotdot**, which makes it possible for smart objects to work together on any network. Dotdot is not limited to ZigBee; it can work together on Zigbee, IP and other networks. Recently, the ZigBee Alliance also announced Dotdot over Thread, an IPv6 protocol to connect home devices.

Comunication technologies for IoT

TeamSoc21
The ICT Engineer of the 21st Century

- **LoRa:** proprietary, long-range, inexpensive and secure
- LoRa focuses on wide-area networks and is especially suited for long-range communications, LoRa uses unlicensed radio frequency bands like 169 MHz, 433 MHz, 868 MHz (Europe) and 915 MHz (North America). The low bands allow for data rates from 0.3 kbps to 50 kbps.
- LoRa is the preferred choice for deploying **a large number of non-critical sensors and control devices in large areas**. It's use of unlicensed radio makes it the perfect choice for city-wide environmental sensors, streetlamp control and monitoring, basic control units for agricultural farms and monitoring of small objects.
- The protocol can use 64-bit and 128-bit keys for network, application and device encryption.
- It's main drawback is the lack of hardware security. M2M devices have been using cellular carrier's Subscriber Identity Modules (SIM) chips that can be used to store and certify encryption keys. **LoRaWan uses software-based encryption.**

Comunication technologies for IoT

TeamSoc21
The ICT Engineer of the 21st Century

- **LTE-M**: 4G cellular networks
- LTE-M is the potential for worldwide connectivity, and it is the only system suitable for tracking moving objects over long distances. The technology provides improved both indoor and outdoor coverage, supports massive numbers of low throughput devices, low delay sensitivity, ultra-low device cost, low device power consumption and optimized network architecture."
- LTE-M can be used to monitor, control and receive information from IoT devices loaded into most forms of transportation, such as trucks, trains, boats, etc. When an LTE network is not available, the system can fall back to WCDMA (3G) or GPRS/EDGE (2G) to maintain connectivity.
- The biggest advantage of LTE-M, however, is **security**. Cellular-connected devices need to be fitted with a SIM chip. SIM's are secure modules that can provide NSA Suite B AES-256 encryption and Identity Certification.
- Another advantage is the ability to remain connected even during a power failure. As it is connected to cellular networks, it doesn't require an Access Point (AP) and, as long as the IoT device battery is functioning, it can remain connected.
- That's why cellular-based IoT connectivity is widely used **for critical applications such as power grids, home and office security, fleet managemen**t, etc.

Communication technologies for IoT

TeamSoc21
The ICT Engineer of the 21st Century

- 6LoWPAN
- 6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks.
- The 6LoWPAN is especially **designed for home or building automation** the IPv6 provides a basic transport mechanism to produce complex control systems and to communicate with devices in a cost-effective manner via a low-power wireless network. The most common cases for it's use are:

✓**Smart home**

✓**Smart Agriculture;**

✓**Industrial IoT.**

Comunication technologies for IoT

TeamSoc21
The ICT Engineer of the 21st Century

- **What is the best option for you?**
- It depends. If you're looking for a low-cost solution to connect non-critical devices in close proximity, then Zigbee or White-Fi are the probably the best options. Zigbee's DotDot software will help you develop a solution compatible with other Zigbee devices, but you'll have to join the Zigbee Alliance to use it.
- For long-range applications, Lo-RaWan or LTE-M are the best options.
- LTE-M is the most robust and secure, as well as being backed by cellular networks, but it's probably the most expensive. It is the only standard that guarantees truly worldwide connectivity and can be used for cargo and fleet management.
- LoRa is a good solution for local medium-range networks that don't require positioning services or NSA-grade security.

Hardware for IoT devices, Gateway

Hardware for IoT devices

- IoT hardware includes a wide range of **devices such as devices for sensors, routing, bridges**, etc.
- The IoT devices manage key tasks and functions such as system **activation, security, action specifications, communication, and detection of support-specific** task and actions.
- Most of the time it been use IoT Hardware Prototyping Kits for IoT applications. Many are open source platforms, initially created for education purposes, and most are pretty affordable (in the $3-$60 range). Examples include Arduino Uno, Raspberry Pi, BeagleBone Black, mbed LPC1768 etc.

Hardware for IoT devices

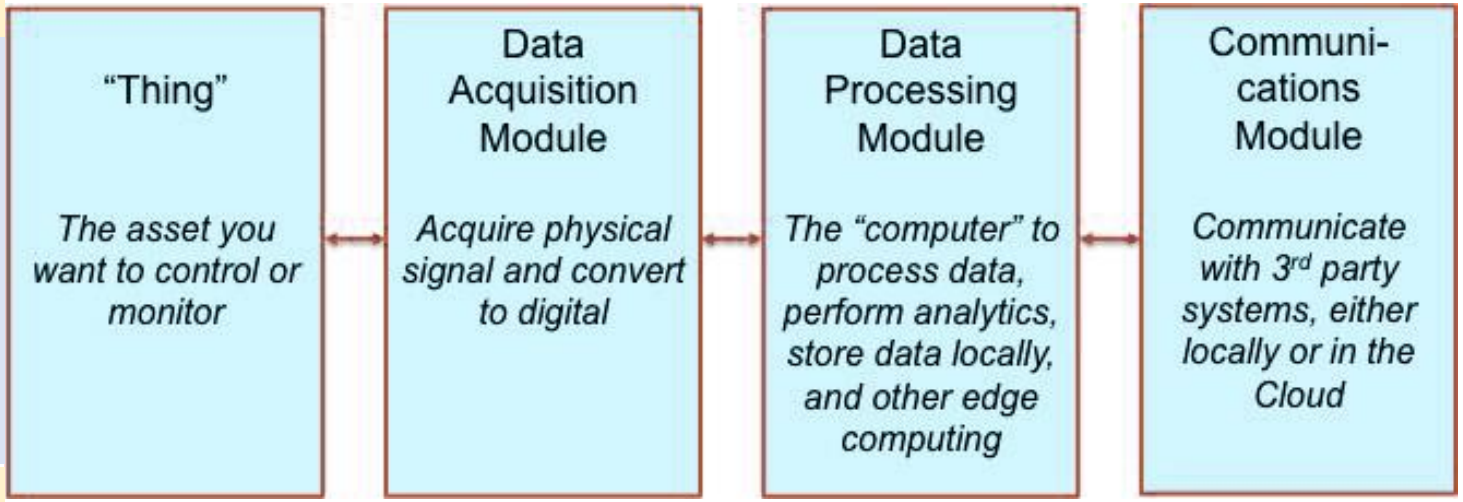
TeamSoc21
The ICT Engineer of the 21st Century

Building Blocks of IoT Hardware

"Thing" gets fully integrated into a smart device. These products control and monitor themselves.

Data Acquisition Module
The data acquisition module contains all the sensors that help in acquiring real-world signals such as temperature, pressure, density, motion, light, vibration, etc. This module also includes the necessary hardware to convert the incoming sensor signal into digital information.

Data Processing Module
This module is the actual "computer" and the main unit that processes the data performs operations such as local analytics, stores data locally, and performs some other computing operations.



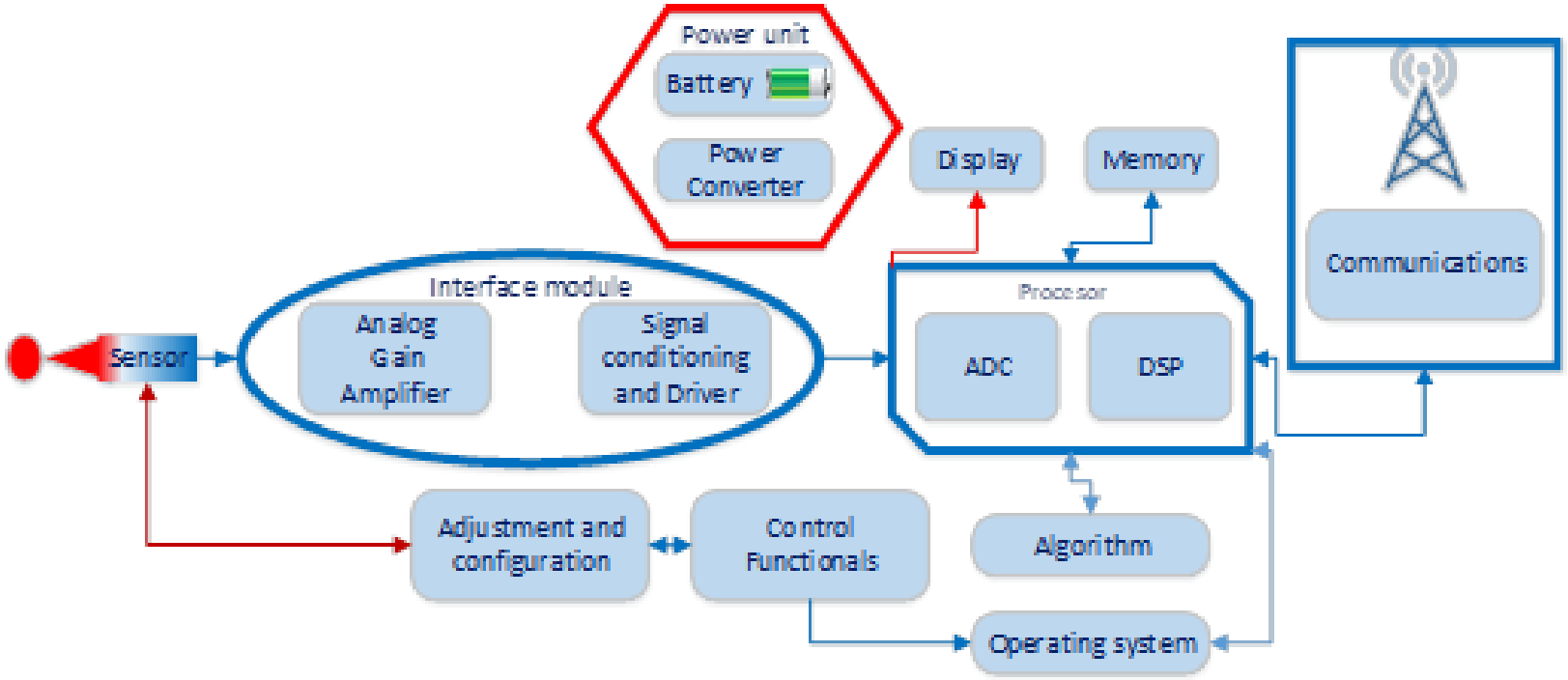
Communication Module
This is the part that enables communications with your Cloud Platform, and with 3rd party systems either locally or in the Cloud.

Hardware for IoT devices

- **IoT Sensors**

These devices consist of a variety of modules such as:

- sensing modules;
- energy modules;
- Power management modules;
- RF modules;
- Interfaces module;
- Processor and memory



IoT Hardware – IoT Sensors

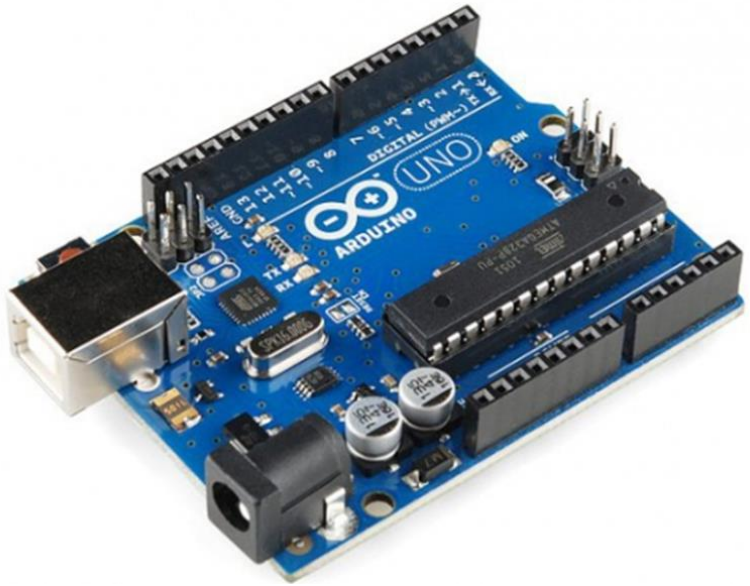
Hardware for IoT devices

TeamSoc21
The ICT Engineer of the 21st Century

The devices involved in the construction of networks Internet of Things can be divided into three classes:

- **First class**, these are the smallest devices that have built-in 8-bit System-On-Chip (SOC) controllers. An example of such an open source device is the Arduino hardware platform (the Arduino Uno platform or other 8-bit Arduino boards);

IoT Hardware components can vary from low-power boards; single-board processors like the Arduino Uno which are basically smaller boards that are plugged into mainboards to improve and increase its functionality by bringing out specific functions or features (such as GPS, light and heat sensors, or interactive displays). A programmer specifies a board's input and output, then creates a circuit design to illustrate the interaction of these inputs and outputs.



Hardware for IoT devices

- In the **second class**, more complex devices are built, which are based on Atheros and ARM chips, which have a very limited 32-bit architecture. They often include small home routers and derivatives of these devices. Typically, they run a cut-down or embedded Linux platform, such as OpenWRT, or embedded operating systems. In some cases, they can not use OS, such as Arduino Zero or Arduino Yun.

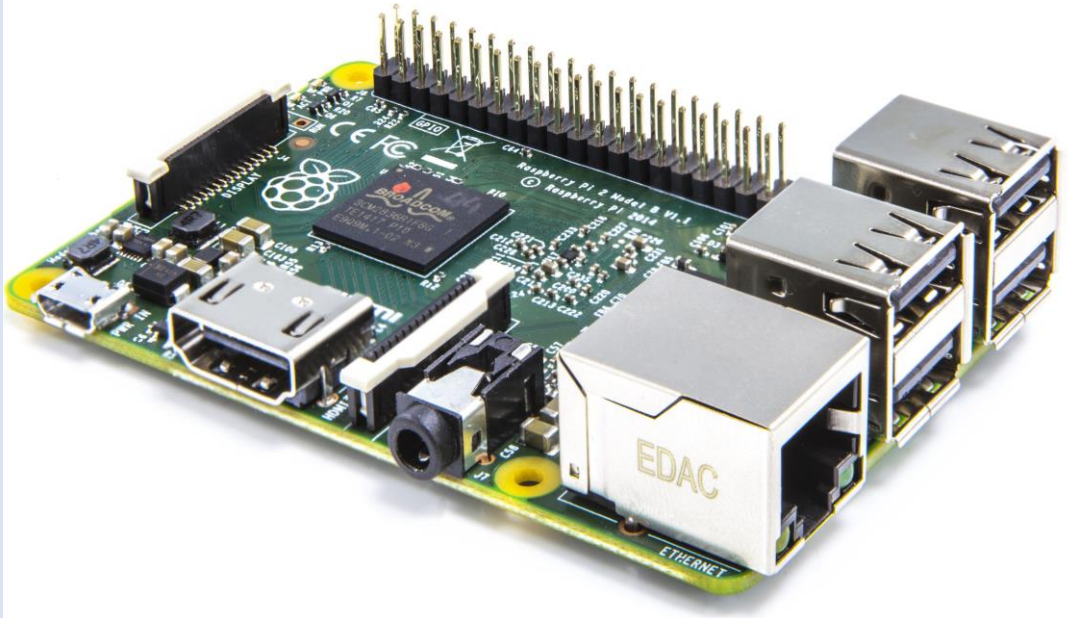
Source: https://hothardware.com/news/microsoft-licenses-arm-chip-technology-could-lead-to-new-microprocessors

Source: http://ereadertech.com/tag/atheros/

Hardware for IoT devices

TeamSoc21
The ICT Engineer of the 21st Century

Third-class devices have the greatest capabilities. These devices are built on full 32-bit or 64-bit computing platforms. These systems, such as Raspberry Pi or BeagleBone, can run on a Linux OS or other appropriate operating system such as Android. In many cases they are either mobile phones or smartphones. These devices can act as gateways or bridges for smaller devices, for example, if they connect via Bluetooth Low Energy with a cell phone or Raspberry Pi.



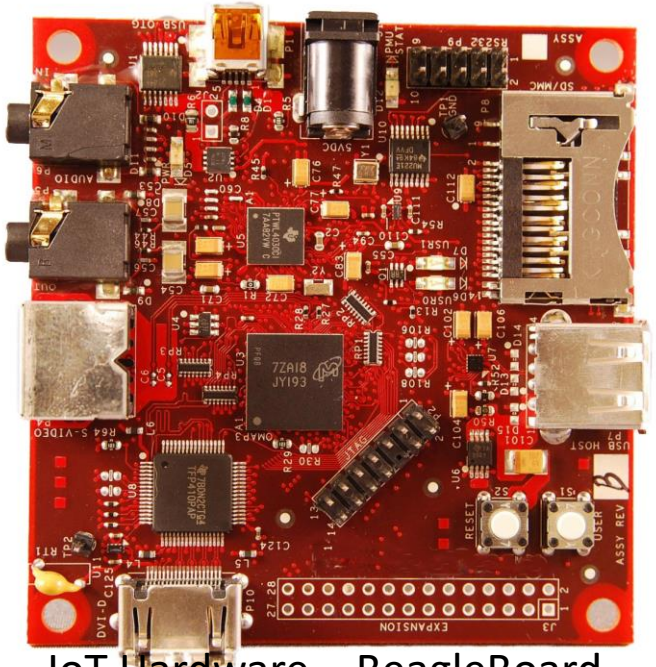
IoT Hardware – Raspberry Pi 2

- Raspberry Pi 2 is a very affordable and tiny computer that can incorporate an entire web server. Often called “RasPi,” it has enough processing power and memory to run Windows 10 on it as well as IoT Core. RasPi exhibits great processing capabilities, especially when using the Python programming language.

Hardware for IoT devices

TeamSoc21
The ICT Engineer of the 21st Century

- **BeagleBoard** is a single-board computer with a Linux-based OS that uses an ARM processor, capable of more powerful processing than RasPi.
- **Intel Galileo -** Intel Galileo combines Intel technology with support for Arduino ready-made hardware expansion cards (called "shields") and the Arduino software development environment and libraries. At a clock speed of 400 MHz, together with 256 Mb of DDR3 RAM and 8 Mb flash memory, the Galileo is much more powerful than competing Arduino boards.

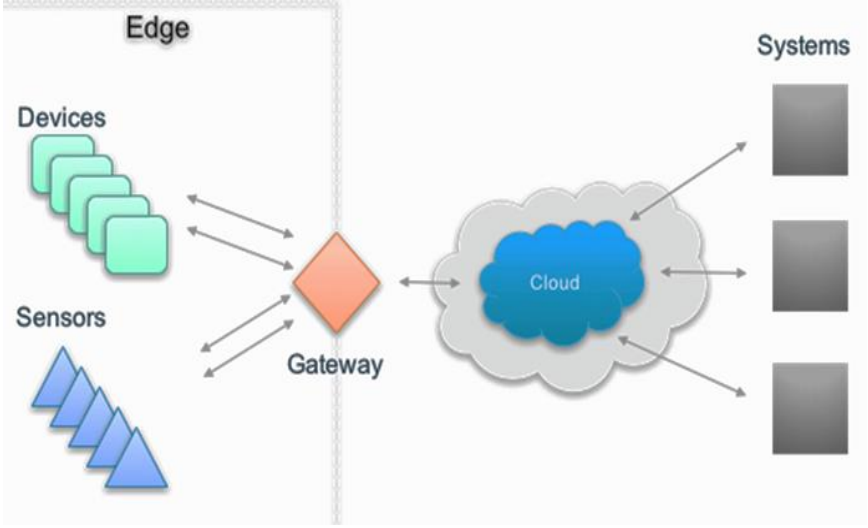


IoT Hardware – BeagleBoard

Intel Galileo 2

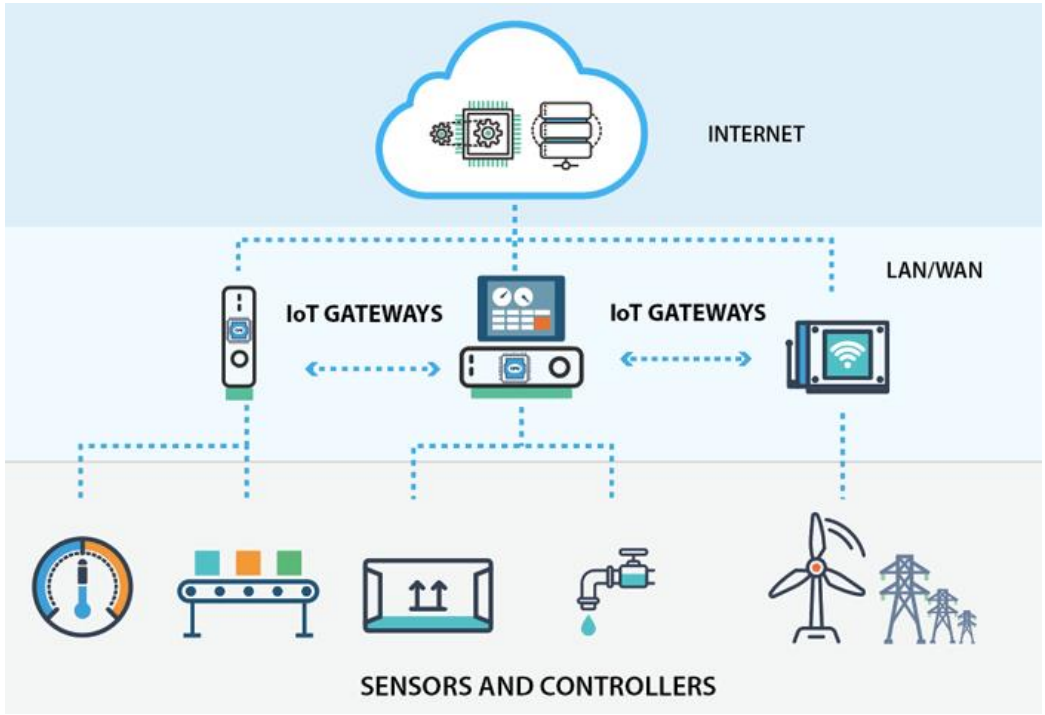
Gateway for IoT

- IoT Gateways perform serving as a communication bridge between the various Internet of Things tools and devices on one hand, and the cloud network on the other.
- The main function of a gateway is to establishing and maintaining a strong, reliable connection between the devices and the cloud – ensuring superior control over the active IoT tools, and ensuring data storage and information processing capabilities.
- IoT Gateways includes a wide range of solutions designed to deliver secure wired and wireless connectivity for all most any device.



Gateway for IoT

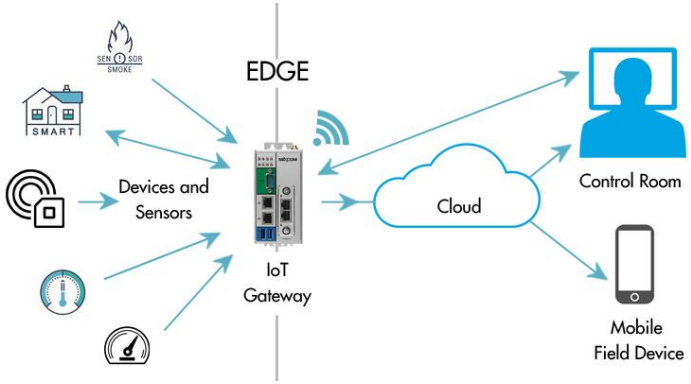
- An **IoT gateway** is a **physical device or software program** that serves as the connection point between the cloud and controllers, sensors and intelligent devices.
- IoT gateways perform several critical functions such as device connectivity, protocol translation, data filtering and processing, security, updating, management, analytics and more. The important advantage of the IoT gateway is to provide **additional security for the IoT network and the data transports**. Gateways manage information moving in both directions, it can protect data moving to the cloud from leaks and IoT devices from being compromised by malicious outside attacks with features such as **tamper detection, encryption, hardware random number generators and crypto engines**.

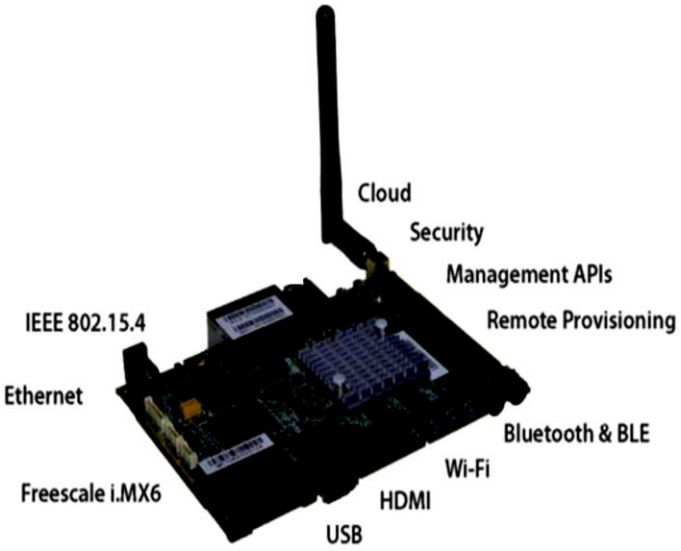


Requirements in gateways

IoT gateways sit at the intersection of edge systems -- connected devices, controllers and sensors and the cloud.

- should support **multiple connectivity protocols**;
- **Storage and analysis** - onboard application development platforms and storage to drive intelligence and decision-making closer to the edge device;
- should allow **data computing** and the edge level;
- **trusted connectivity** ensuring the integrity of the network and system in both directions;
- ability to **manage entire device infrastructure, firmware updates to device diagnostic**;
- **should secure** the entire communication channel - encryption, certification, role authorization and authentication;





https://www.eejournal.com/article/20160111-gateways/

Requirements in gateways

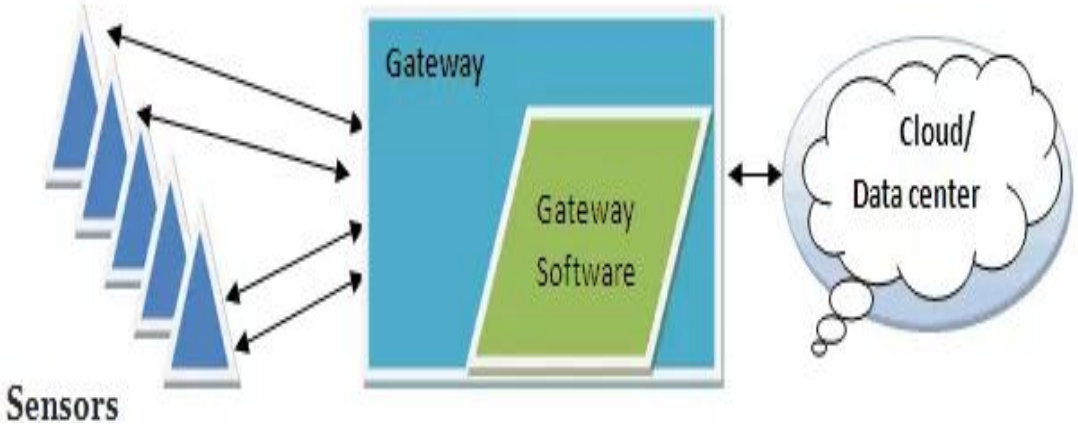
- Data caching, buffering and streaming;
- Data pre-processing, filtering and optimization;
- Some data aggregation;
- Device to Device communications/M2M;
- Networking features and hosting live data;
- Data visualization and basic data analytics via IoT Gateway applications;
- Short term data historian features.

IoT Gateway software

IoT Gateway Software is a platform-independent, edge-computing middleware, that can be deployed on different gateway devices. It runs on common operating systems such as Linux, Windows, mac OS, Android, and VxWorks.

The gateway software is responsible for:

- ✓ collecting messages from the sensors;
- ✓ storing data appropriately until they can be pre-processed;
- ✓ pre-processing that data;
- ✓ sending the results to the data center;
- ✓ decides if the data at a given stage of processing should be temporary, persistent, or kept in-memory;
- ✓ Plug and play-browser-based configuration.



https://iotdunia.com/iot-gateway-architecture/

IoT Gateway manufactures

TeamSoc21
The ICT Engineer of the 21st Century

Software / Edge Analytics

kura · AGILE · ubiworx · FOGHORN · BITSTEW SYSTEMS · ProSyst Bosch Group · BOSCH · PerStream · CISCO · WIND · intel

Hardware Vendors

ADVANTECH · kontron · DELL · ADLINK · NXP · AAEON an ASUS company · OPTION · libelium · MultiTech Systems · CISCO · EUROTECH Imagine. Build. Succeed. · NEXCOM · Hewlett Packard Enterprise · HUAWEI · LANTRONIX CONNECT SMART DO MORE

End-to-End Providers

EUROTECH Imagine. Build. Succeed. · SIERRA WIRELESS · samsara · B-Scada · ADVANTECH B+B SmartWorx

Embedded IoT Gateways

External IoT Gateways

IoT Software languages

TeamSoc21
The ICT Engineer of the 21st Century

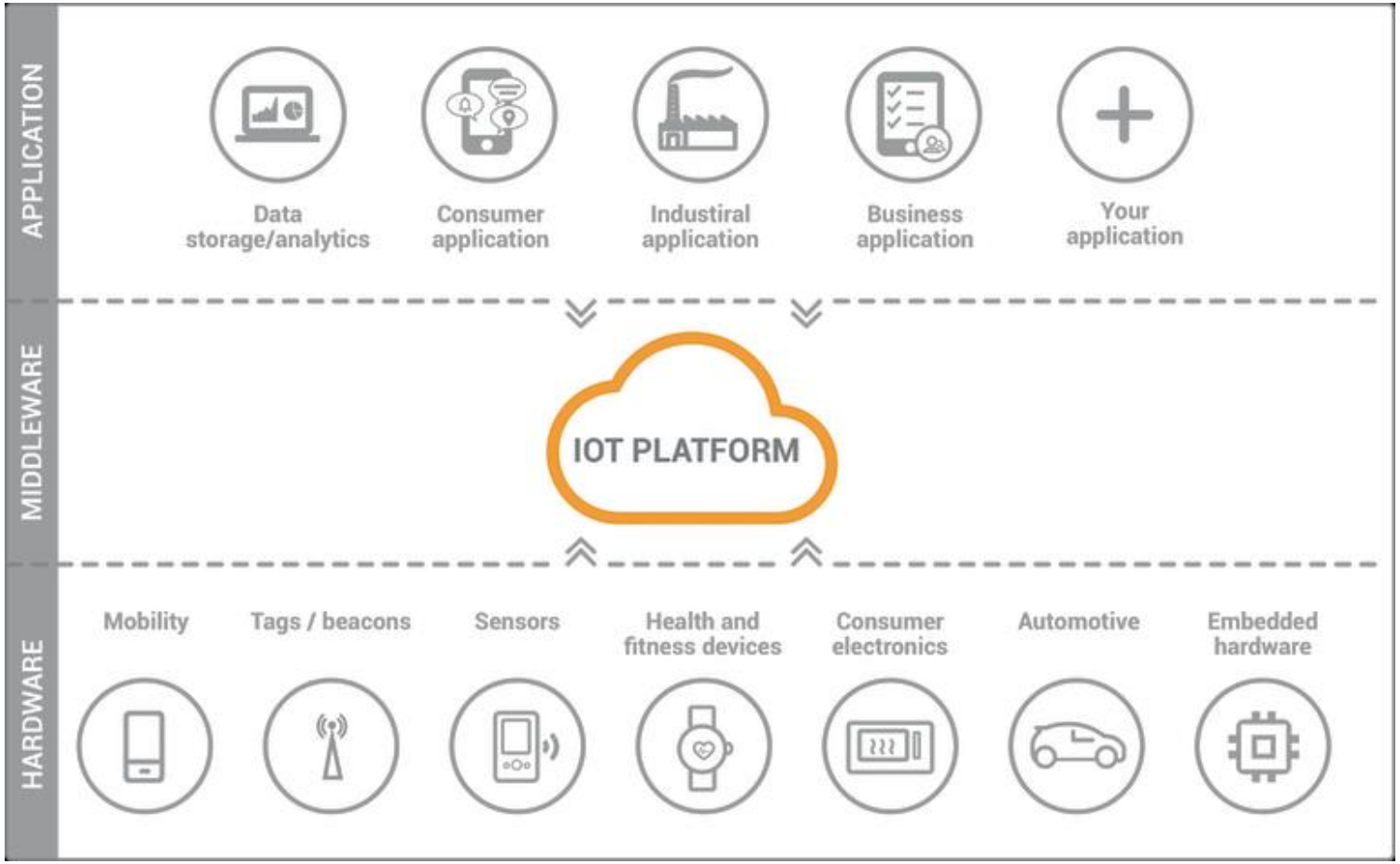
When selecting a programming language, account is taken of the features of the systems involved in the Internet of things such as memory, processing power, data rate, communication protocols, and support for different programming languages. IoT Software languages:

- **C & C++:** C++ is the object-oriented version of C, which is a language popular for both the Linux OS and Arduino embedded IoT software systems.
- **Java:** While C and C++ are hardware specific, the code in JAVA is more portable. It is more like a write once and read anywhere language, where you install libraries, invests time in writing codes once and you are good to go.
- **Python**: It's use for the embedded control in IoT, specially the Raspberry Pi processor and for serving data-heavy applications.

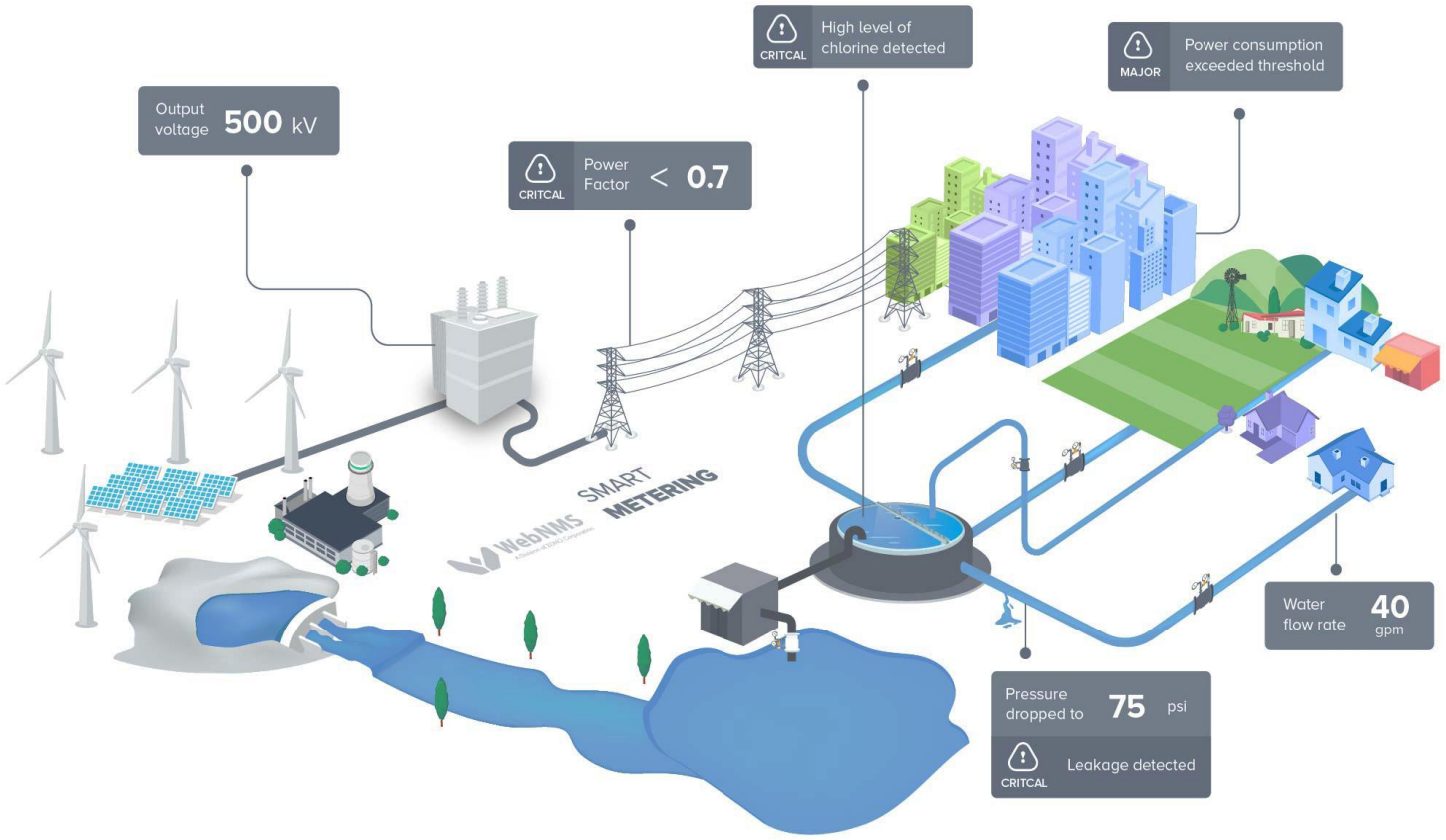
IoT platforms for Smart metering data

IoT platforms

- IoT platforms originated in the form of IoT middleware, which purpose was to function as a mediator between the hardware and application layers.
- It's primary tasks included data collection from the devices over different protocols and network topologies, remote device configuration and control, device management, and firmware updates.



IoT and smart meters



https://www.webnms.com/iot/smart-metering.html

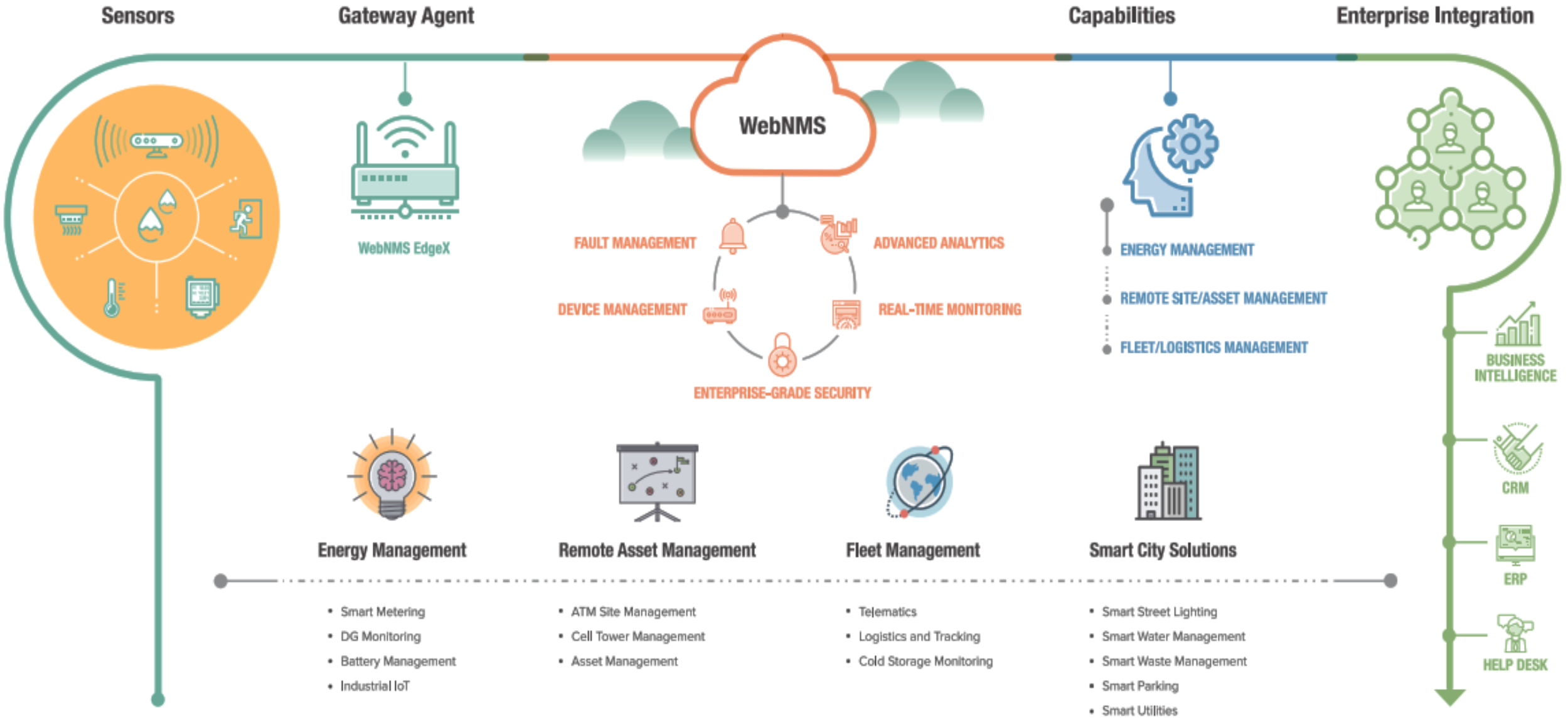
Tele-measurement (or Smart Metering) is one of the most popular domains in the Internet of Things.

Remote reading of energy consumption (water, gas, electricity), the remote measurement of any parameter available on a machine, in a room, an indoor or outdoor environment.

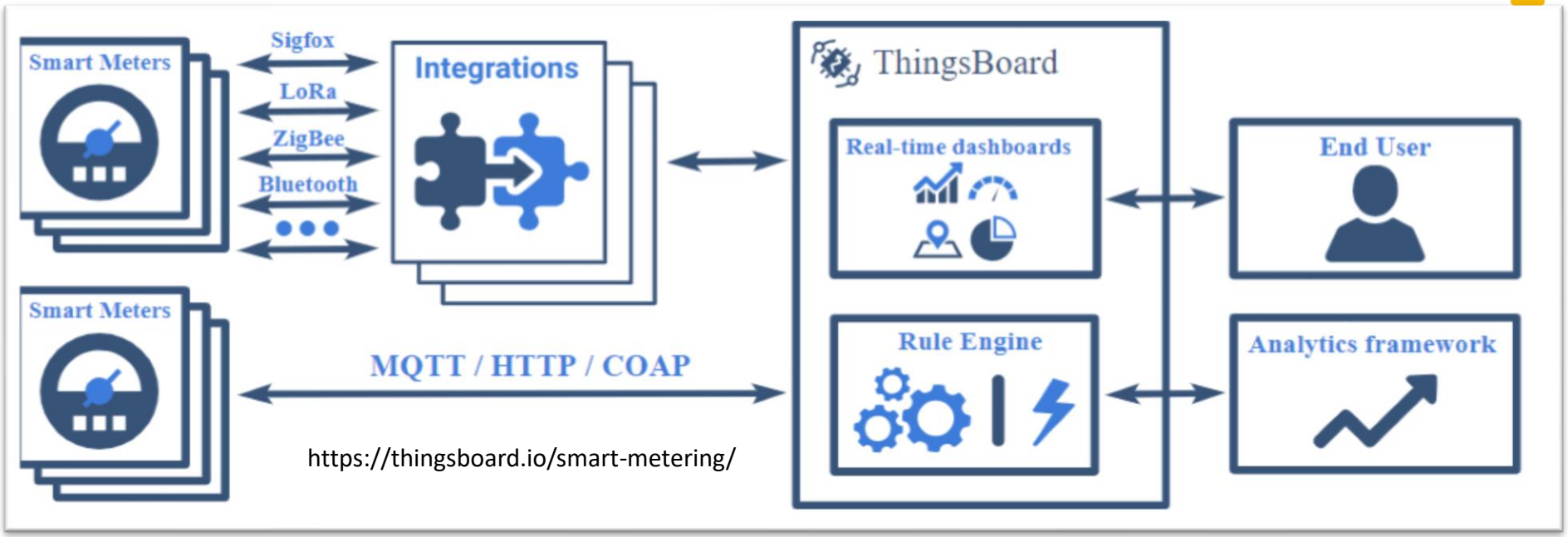
IoT platforms for smart metering, offer a broader range **of remote monitoring** and alerting capabilities as well as provide powerful **data analytics tools** to help companies and individual users **optimize their energy, water, gas, or fuel consumption**.

WebNMS IoT Platform

TeamSoc21
The ICT Engineer of the 21st Century



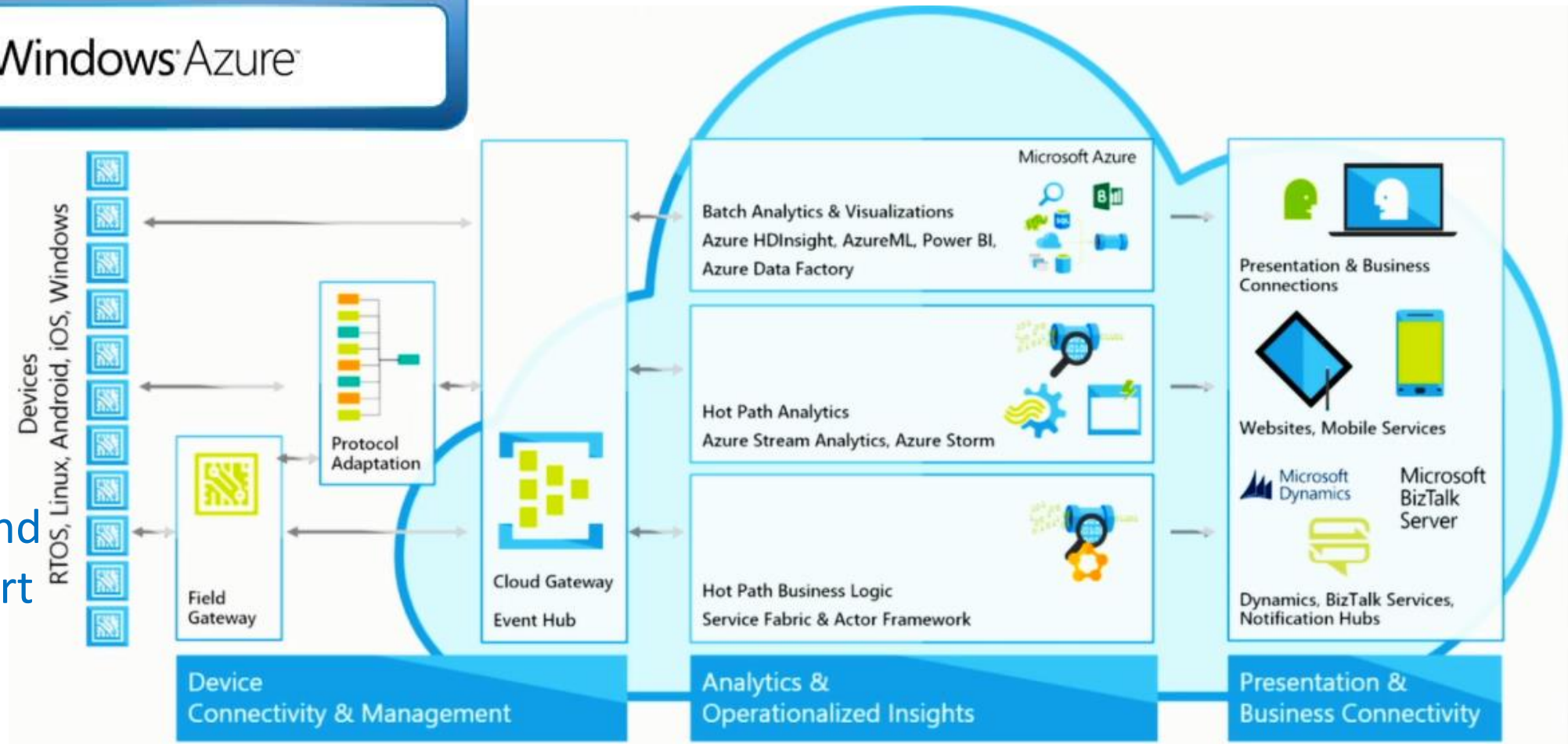
Smart metering -ThingsBoard platform



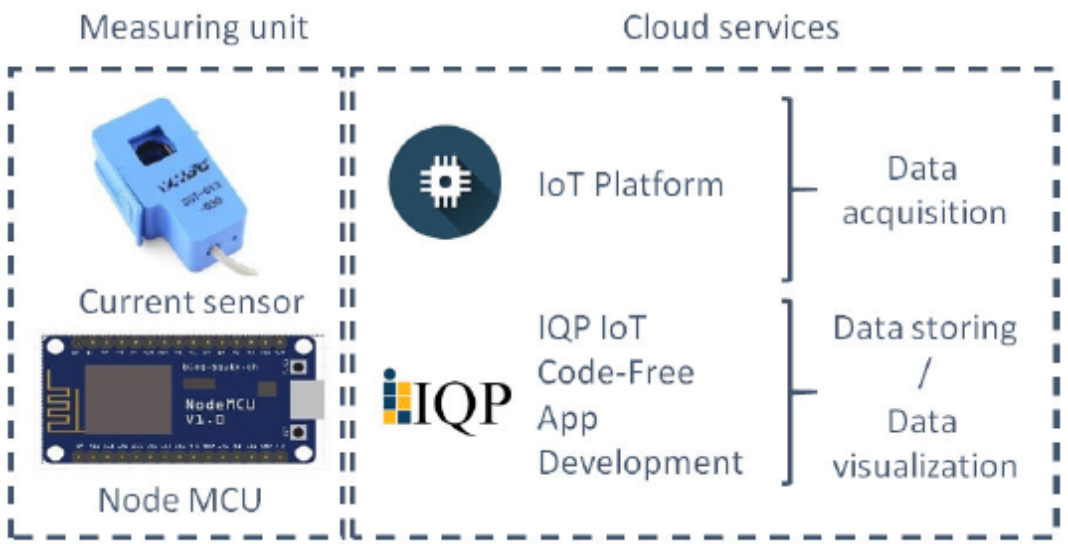
- The diagram identifies data flow and integration points for typical smart metering solution that uses ThingsBoard platform to collect and analyze monitoring data from smart meters.
- There are plenty of connectivity options for smart meters: both via direct connection to the cloud and via Platform Integrations.
- The ThingsBoard platform supports industry standard encryption algorithms (SSL) and device credentials types (X.509 certificates and access tokens). The collected data is stored in Cassandra - a popular NoSQL database, which is widely recognized for it's fault-tolerance and reliability.
- ThingsBoard Rule Engine enables forwarding incoming data to various analytics systems, such as Apache Spark or Hadoop using Kafka or other Message buses.

MS Azure platform

Used services and process of smart metering



IBM Bluemix



Name	Features	Pricing / month
IoT Platform	500 devices, 200 MB /month	0.00 $
IQP IoT Code-Free App Development	3 devices 10 app users	0.00 $

Sourse [11].

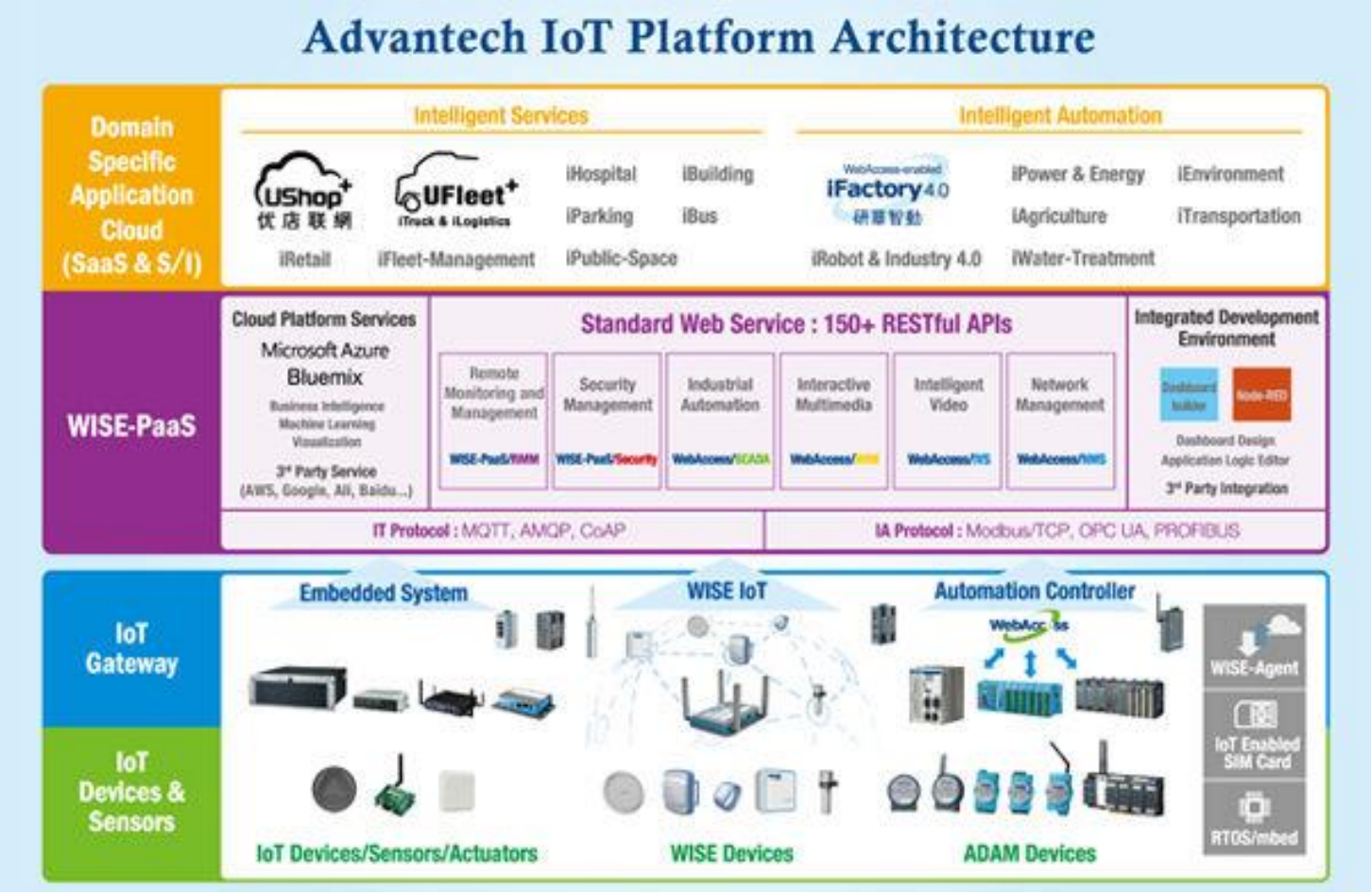
IoT Platform for IBM Cloud is versatile toolkit includes gateway devices, device management, and powerful application access.

By using **Watson IoT Platform**, users can collect connected device data and perform analytics on real-time data from their IoT projects.

Data visualization is done service IQP IoT Code-Free App Development. IQP is a unique development tool that anyone, even non-programmers, can use to quickly create code-free applications for the Internet of Things and Industrial IoT.

IQP offers a complete development solution, from connectivity with sensors and control devices to app customization and design templates. The **code-free applications are fully optimized to be viewed on all mobile phones, tablets, and PCs.**

WISE-PaaS platform

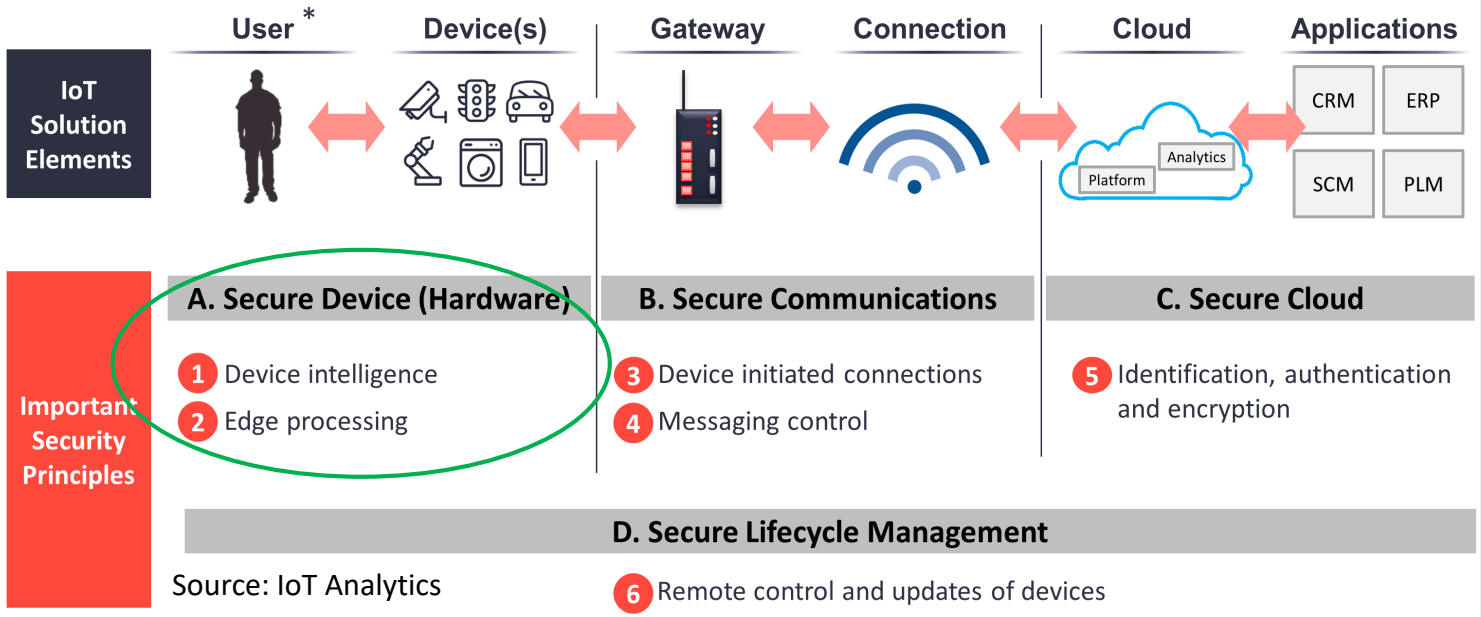


Advantech and Microsoft jointly built WISE-PaaS platform, a software platform services for IoT related companies.

This platform combines Advantech's software solutions of IoT and Microsoft's Azure cloud services, proposed SRP (Solution Ready Package) application service solutions for different industries. It can lower the difficulty of entering the IoT industry, and to help system integrators to quickly construct IoT services.

Security of IoT

Security of IoT



The *IoT Analytics* define six important principles of IoT security across the stack:

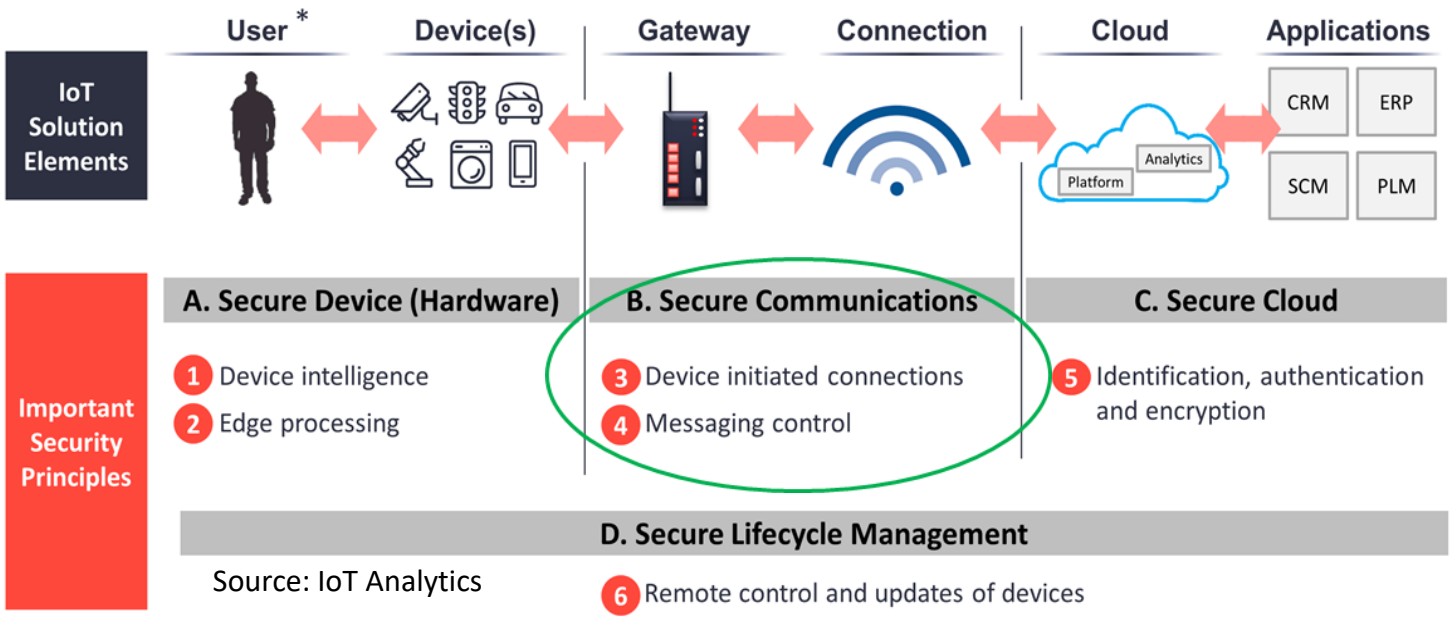
- **Security devices;**
- **Security communications;**
- **Security cloud;**
- **Security Lifecycle Management.**

Secure Device Layer

Devise intelligence -The device layer refers to the hardware level of the IoT solution i.e., the physical "thing" or product. ODMs and OEMs (who design and produce devices) are increasingly integrating more security features in both their hardware and software to enhance the level of security on the device layer.

Edge processing- Edge processing allows smart devices can process data locally before it is sent to the cloud, eliminating the need to forward huge volumes of video to the cloud, and sensitive information need not be sent to the cloud. The processed data, packaged into discrete messages, sent securely to the wanted destination.

Security of IoT



Source: IoT Analytics

Device-initiated connection to the cloud. It must not allow incoming connections. A connection to the cloud can also facilitate a bi-directional channel, thereby allowing the IoT device to be remotely controlled.

Messaging control - Communications to the IoT device with message-based protocols give possibilities for double encryption, queuing, filtering and even sharing with third parties. To increase security required correct messages labelling, control message flow to the desired destination, each message can be handled according to the appropriate security policy.

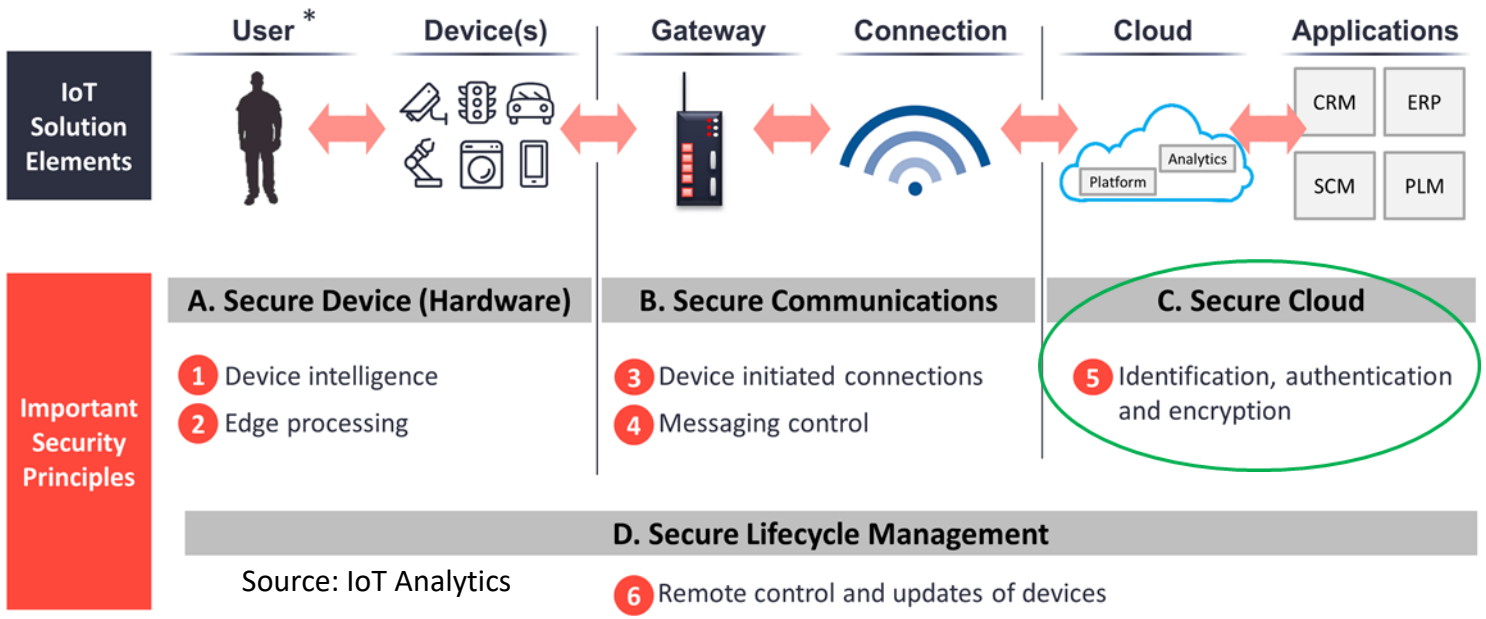
Secure Communications Layer

refers to the connectivity networks of the IoT solution i.e., mediums over which the data is securely transmitted/received. Whether sensitive data is in transit over the ***physical layer*** (e.g., WiFi, 802.15.4 or Ethernet), ***networking layer*** (e.g, IPv6, Modbus), or ***application layer*** (e.g., MQTT, CoAP or web-sockets) unsecure communication channels can be susceptible to intrusions such as man-in-the-middle attacks.

Important IoT security architecture features:

- Data-centric security solutions;
- Firewalls and intrusion prevention systems (IPS) and (IDS).

Security of IoT



Source: IoT Analytics

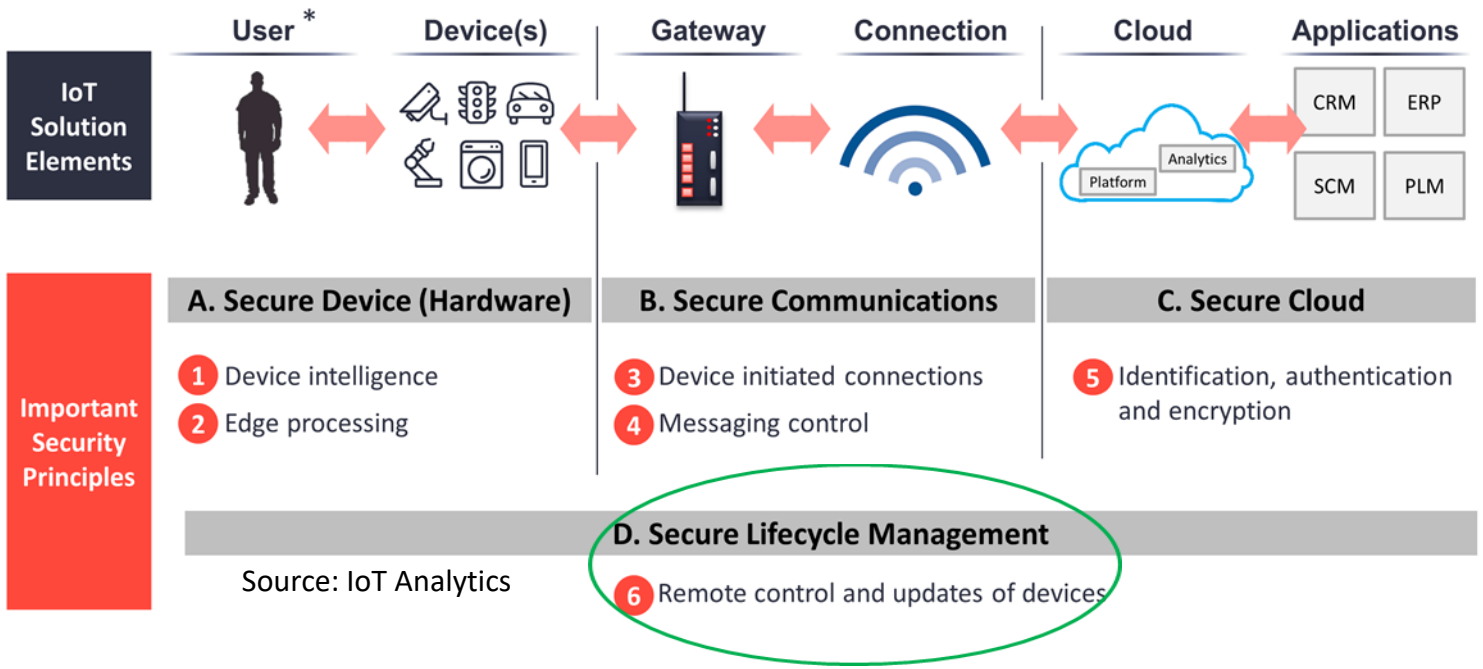
Identification, authentication and encryption for machines.
Passwords are the accepted authentication method for humans to use. Machines, used **digital certificates when accessing cloud services**. Digital certificates use an asymmetric, encryption based, authentication system designed to not only authenticate a transaction but also encrypt the channel from device to cloud before the authentication takes place.
A digital certificate can also provide cryptographic identification that is very difficult to achieve with user-id/password.

Secure Cloud Layer refers to the software of the IoT solution, where data from devices is received, analyzed and interpreted for performing actions.

Important IoT cyber security features:

- ✓ **Sensitive information stored in the cloud must be encrypted to avoid easily exposed data to attacks;**
- ✓ **Verify the integrity of other cloud platforms or third party applications;**
- ✓ **Digital certificates can play a key role for identification and authentication.**

Security of IoT



Remote control and updated of devices - Remote control of a device is essential in allowing remote diagnostics, setting a new configuration, updating buggy software, retrieving files, resetting a machine learning algorithm with a new of set of learning data, adding new functionality to a product and more. The key to security updates and remote control is to ensure that a device does not allow incoming connections, has a bi-directional connection, is correctly secured, uses a message switch as the communications channel and is correctly implemented.

Secure Lifecycle Management

Important IoT cyber security features:

- **Activity monitoring play's** an important role to track, log and detect suspicious activity.
- IoT devices and applications need **regular security patches** in order to stay up-to-date, strengthen resistance against attack and fix possible vulnerabilities.
- Secure **remote control** is essential especially when maintaining billions of IoT devices.

Challenges in securing IoT

- **Bandwidth and Power Consumption**

Generally IoT devices are designed to be lightweight, less powerful, less memory and small in size and they are not equipped with a large battery. IoT contains many interconnected devices and sensors to execute the programmed functionality with substantial security directions which may consume high bandwidth and drain out the devices. IoT systems should be well prepared with a concrete mechanism when there is any such unavailability of internet bandwidth. The minimization of bandwidth and power consumption remains a major challenges in the IoT.

Challenges in securing IoT

- **Complexity**
- The Internet of Things consists of a network of internet-connected physical devices that have their own hardware/software layers and different system architectures for different purposes. All of these interconnected devices that are equipped with different sensors, actuators, protocols and standards accumulate together to execute the programmed function. Hence, it becomes more complex and hard to deal with this heterogeneous architecture in IoT systems.

Challenges in securing IoT

TeamSoc21
The ICT Engineer of the 21st Century

- **Sensing**

Monitoring of these several smart devices continuously and getting back them to the network again for connectivity after it had suffered from device failure or connectivity problems are also challenges for the Internet of Things.

- **Lightweight Computing**

Since IoT devices normally have less memory capacity, traditional cryptographic-algorithms cannot be applied to the IoT system. Advanced cryptographic algorithms have high computing, storing and processing requirements which cannot be supported by IoT devices as they are resource constrained. Therefore, to find a way to implement required security mechanisms with low cost and minimum overhead is necessary for Internet of Things.

Key takeaways

Key takeaways – Technical aspect

There are some specific challenges in implementing IoT based solutions that will help students to analyze and solve the case for integrating smart measurement data into a specific platform such as:

- architectural model for building IoT solutions;
- hardware features of the components to build a solution based on the IoT;
- communication technologies and protocols;
- security for data transmission in the IoT;
- examples of smart metering platforms.

Key takeaways – Business aspect

The potential customers of Smart Solutions based on Internet of Things are:

- companies investing in automation of technological processes, data processing, increasing labor productivity;

The implementation of this new technology will result in:

- increasing the number of high-tech staff of companies;
- increasing the number of service users;
- increasing labor productivity;
- reducing direct costs for consumers.

Key takeaways – Societal aspect

There are some aspects where the entrepreneurial event presents the challenges of using the Internet of Things, which enables:

- the right assessment and selection of hardware, software, communication technologies and the security of the chosen solutions for the Internet of Things;
- the need to prepare specialists for implementation and exploitation in the practice of these technologies;
- reducing the number of low-skilled workers.

References

[1]. Q. Sun et al., “A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks,” in IEEE Internet of Things Journal, vol. 3, no. 4, pp. 464-479, 2016.

[2], J. Lloret, J. Tomas, A. Canovas and L. Parra, “An Integrated IoT Architecture for Smart Metering,” in IEEE Communications Magazine, vol. 54, no. 12, pp. 50-57, 2016.

[3]. Z. Fan et al., “Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities,” in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 21-38, 2013.

[4]. W. R. Kintzel, M. M. Mattos, A. R. Borges, “Hardware Design of a Smart Meter Communication Interface for Smart Grids”, in Conference on Complex, Intelligent, and Software Intensive Systems, book series Advances in Intelligent Systems and Computing, vol. 611, pp. 371-383, 2017.

[5]. A. Berouine, F. Lachhab, Y. N. Malek, M. Bakhouya and R. Ouladsine, “A smart metering platform using big data and IoT technologies” 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, pp. 1-6, 2017

[6]. Ericsson: “Making the metering smart – A transformation towards smart cities”, presentation, URL: https://www.ericsson.hr/documents/20181/21930/Making_the_metering_smart.pdf/d6fd16e2-4dfa-4da0-b7d2-6b3ef223334f?t=1496751016953

[7]. G. Carrozzo, “Platform Federations: Collaboration by symbIoTe-enabled IoT platforms”, symbIoTe Technical blog, 2017, URL: https://www.symbiote-h2020.eu/blog/2017/12/20/platform-federations-collaboration-by-symbiote-enabled-iot-platforms/

[8]. ITU-T: Recommendations: Y Series: Y.2060/ International Telecommunication Union-Telecommunications /Overview of the Internet of things. 2012.

[9] https://data-flair.training/blogs/iot-hardware/

[10]. J. Lloret, J. Tomas, A. Canovas and L. Parra, “An Integrated IoT Architecture for Smart Metering,” in IEEE Communications Magazine, vol. 54, no. 12, pp. 50-57, 2016.

[11]. E.Kajáti, M. Miškuf, I.Ulbricht, I. Zolotová,Comparison of Cloud IoT Platforms for Smart Metering Solution Based on NodeMCU Department of cybernetics and artificial intelligence, WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS, Volume 15, 2018

.

Thank you very match!