

Chapter 4

IoT reference model

ADVANCED TOPICS IN DATA SCIENCE

A solid blue horizontal bar at the bottom of the slide.

Outline

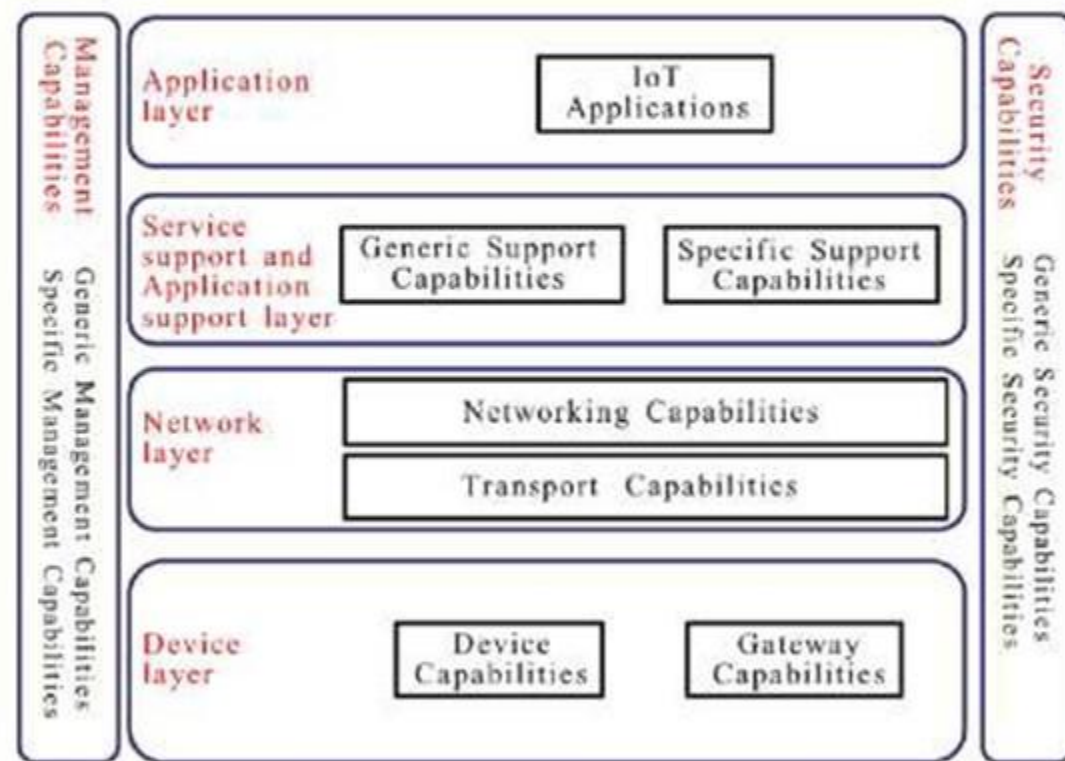
- IoT reference model
- Application Layer
- Service support and application support
- Network Layer
- Device Layer
- Management capabilities
- Security capabilities

IoT Reference Model

- IoT provides new opportunities but also brings new challenges on the interaction between things, levels of functionalities, security, etc.
- This motivates the creation of a Reference Model for the IoT domain in order to promote a common understanding.
- A Reference Architecture should be considered to explain essential building blocks to deal with conflicting requirements regarding functionality, performance, deployment and security.
- Reference model is a division of functionality into elements together with the data flow among those elements.

IoT Reference Model

- Up to now, few standard committees have been researched in IoT reference model.
- Among them, the International Telecommunication Union (ITU) is one of the best organizations that proposed a comprehensive reference model in IoT environment.
- ITU recommended reference model for IoT is composed of **4 layers** as well as **management** and **security** capabilities which are associated with the four layers.



ITU recommended reference model for IoT

IoT Reference Model

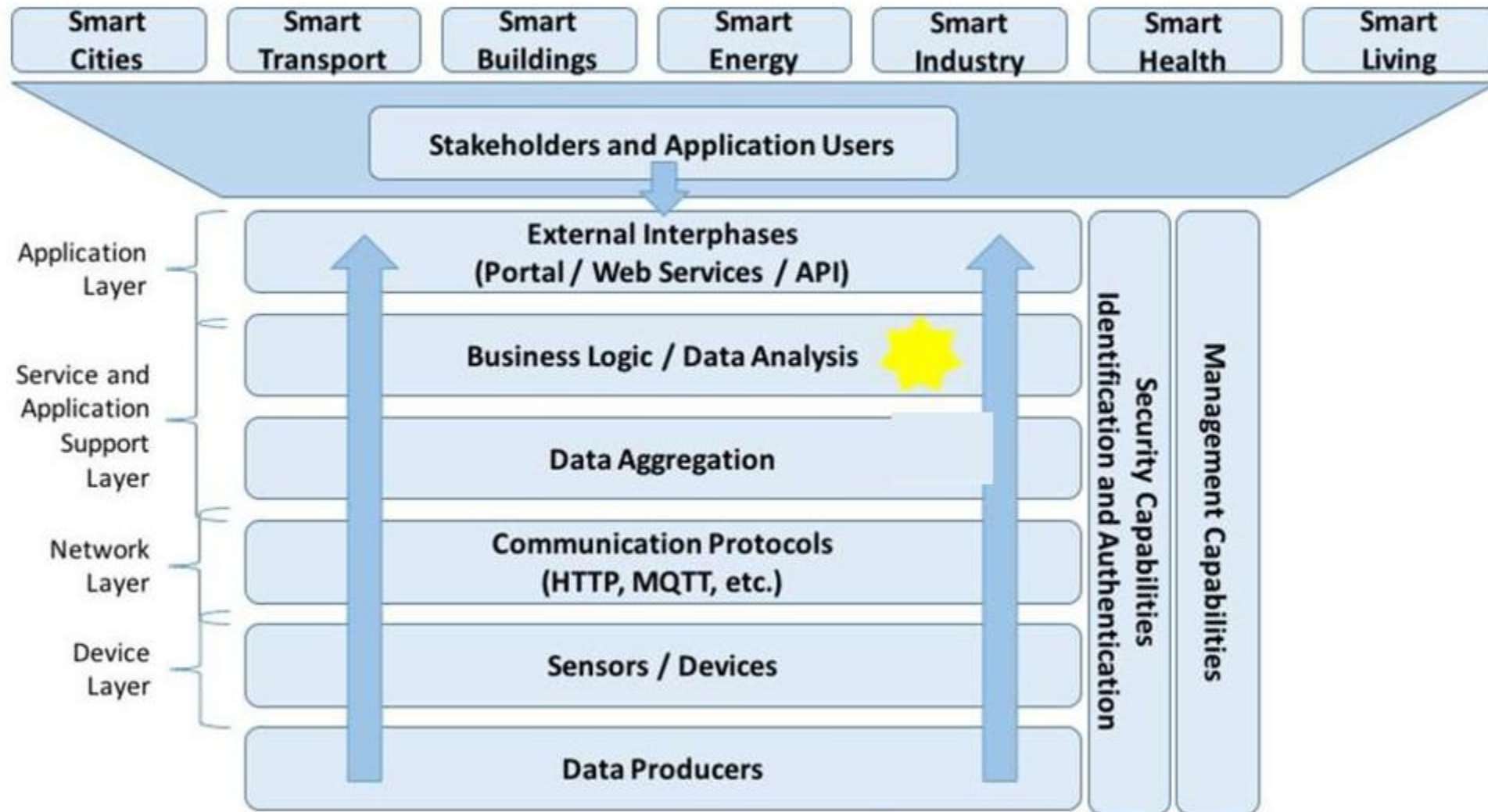


Figure 1. IoT Layered Architecture. Adapted from the ITU-T Reference Model [7]

Application Layer

- This layer contains the IoT applications.
- The IoT Reference Model does not strictly define an application.
- This layer addresses the delivery of the services for the final user.

Service support and application support

The service support and application support layer consists of the following two capability groupings:

- **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, e.g., to build other specific support capabilities.
- **Specific support capabilities:** The specific support capabilities are particular capabilities which cater for the 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.

Network Layer

It consists of the following two types of capabilities:

- **Networking capabilities:** provide relevant control functions of network connectivity, such as access, authentication, authorization ...
- **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.

Device Layer

Device layer capabilities can be logically categorized into two kinds of capabilities:

1. Device capabilities: The device capabilities include but are not limited to:

- **Direct 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 (e.g., commands) from the communication network.
- **Indirect interaction with the communication network:** Devices are able to gather and upload information to the communication network indirectly, i.e., through gateway capabilities. On the other side, devices can indirectly receive information (e.g., commands) 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.

Device Layer

2. Gateway capabilities: The gateway capabilities include but are not limited to:

- **Multiple interfaces support:** At the device layer, the gateway capabilities 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 technology protocols and Bluetooth technology protocols, the other one is when communications involving both the device layer and network layer use different protocols e.g., a ZigBee technology protocol at the device layer and a 3G technology protocol at the network layer.

Management capabilities

The IoT management capabilities can be categorized into generic management capabilities and specific management capabilities.

1. **Essential generic management capabilities** in the IoT include:

- device management, such as remote device activation, diagnostics, 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.

2. Specific management capabilities are closely coupled with application-specific requirements, e.g., smart grid power transmission line monitoring requirements.

Security capabilities

There are two kinds of security capabilities: generic security capabilities and specific 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, user 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.

Questions