1

Internet of Things (IoT)

1.1. Definition

The Internet of Things (IoT) refers to a network of interconnected physical objects capable of collecting, transmitting and exchanging data via the Internet. In general, these objects incorporate sensors, actuators, microcontrollers or embedded systems, enabling them to interact with their environment and automate various tasks (Domingue et al. 2011; Gubbi et al. 2013; Chebudie et al. 2014; Sethi and Sarangi 2017).

The IoT stands out for its ability to connect elements from the physical world to the digital world. This includes a wide range of applications, from smart home devices to complex industrial systems. The main goal of the IoT is to create more efficient, intelligent and responsive systems, contributing to better resource management, process optimization and an improved quality of life (Gubbi et al. 2013; Porkodi and Bhuvaneswari 2014; Al-Fuqaha et al. 2015).

Despite having been the subject of numerous studies, the definition of this technology is still difficult to grasp and is a concept with varied and sometimes ambiguous forms, reflecting multiple perspectives. It is therefore imperative to examine the work of researchers in this field. For some authors, it is a network of physical objects equipped with sensors and microchips, capable of collecting and transmitting data via the Internet without human intervention (Atzori et al. 2010; Dorsemaine et al. 2015; Oxford Dictionaries 2018).

Other researchers describe it as an evolving global infrastructure, where physical and virtual objects interact via intelligent interfaces and standardized protocols (Vermesan et al. 2009, 2013, 2014).

For a color version of all the figures in this chapter, see www.iste.co.uk/saadaoui/innovation.zip

According to Mouha (2021), the IoT is an ecosystem integrating objects, communication, applications and data analysis, enabling interaction with the internal or external environment.

It is also described as a decentralized system of devices endowed with detection, processing and communication capabilities (Gerd et al. 2010).

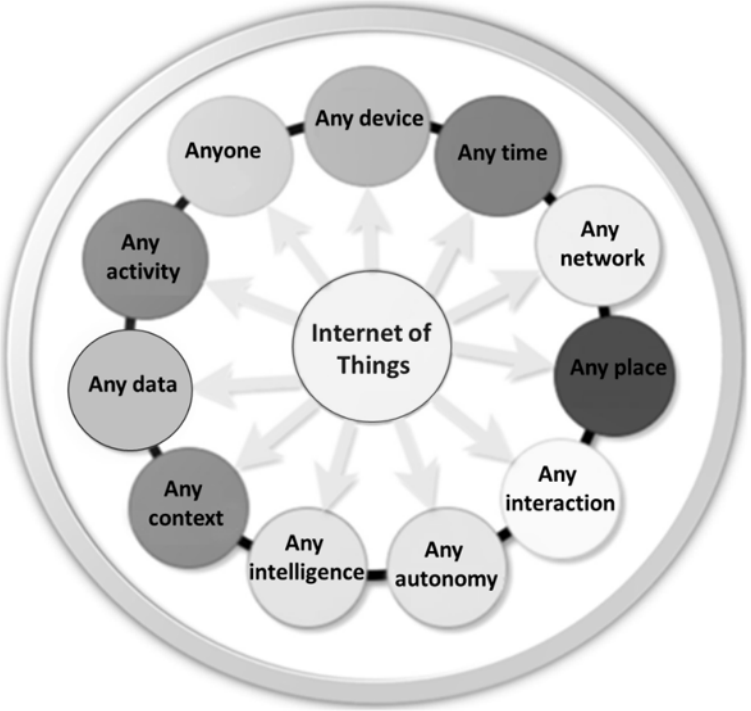

Figure 1.1. *The dimension of the IoT*

The IoT transforms everyday objects into intelligent entities, capable of communicating with each other and with humans, creating a distributed and interactive network (Singh and Singh 2015).

In brief, the IoT connects heterogeneous objects, captures information in real time and transmits it via the Internet, relying on technologies such as Radio Frequency Identification (RFID) and embedded sensors (Vermesan et al. 2014).

The IoT thus connects people, devices and machines, facilitating dynamic interaction, detection of environmental changes and autonomous or collaborative decision-making (Fantana et al. 2013).

As technologies continue to evolve, the IoT will continue to play a key role in building a better connected and intelligent future. Figure 1.1 shows the multiple ways in which the IoT allows people and objects to be connected anywhere, anytime, supported by various networks, services and intelligences while integrating contexts, activities, data, interactions and certain degrees of autonomy (Vermesan et al. 2013).

1.2. Foundations of the IoT

In the era of digital transformation, the IoT is emerging as a major innovation, redefining the way we interact with our environment. Ranging from smart homes and automated factories to connected healthcare and optimized transportation, this technology transcends sectors and is deeply integrated into our daily lives. Its potential is based on essential pillars: connectivity, intelligence, interoperability and automation, paving the way for unprecedented optimization of processes and resources (Da Xu et al. 2014).

1.2.1. *Ubiquitous connectivity*

The IoT relies on robust network infrastructures, making it possible for objects to exchange data in real time. Thanks to technologies such as Wi-Fi, 5G and Bluetooth, interconnected devices can optimize various environments.

A smart thermostat, for example, can adjust home temperature based on weather forecasts, while connected traffic lights streamline traffic flow by adapting to vehicle road traffic.

1.2.2. *Embedded intelligence and data analysis*

One of the most powerful aspects of the IoT lies in its ability to leverage artificial intelligence (AI) to analyze massive volumes of data. Surveillance systems can detect suspicious activity and alert the authorities, while agricultural sensors can assess soil moisture and weather to optimize irrigation. Embedded intelligence transforms the IoT into an important driver for automation and better decision-making.

1.2.3. *System interoperability and collaboration*

The effectiveness of the IoT depends on the ability of devices to communicate with one another, regardless of their manufacturer. In a smart home, equipment from different brands (lighting, security, appliances) must work seamlessly together.

Similarly, in the automotive industry, cooperation between manufacturers and technology companies enables the smooth integration of advanced features such as driver assistance and predictive maintenance.

1.2.4. *Process automation and optimization*

One of the major advantages of the IoT is its ability to perform actions without human intervention. A connected factory can adjust its production to match market needs, while a smart urban lighting system can adapt its intensity based on pedestrian traffic. Not only does automation reduce costs, it also improves energy efficiency and infrastructure sustainability.

1.3. IoT architecture

Over time, the architecture of the IoT has evolved to meet the growing challenges of connectivity, data management and security. IoT architecture is generally organized into layers, each with distinct functions.

Different approaches have been proposed, ranging from three to six layers, each offering improvements in terms of performance and security. The adoption of one approach over the other depends on the complexity of the IoT system, as well as security and data processing requirements (Al-Fuqaha et al. 2015; Husnoo et al. 2021).

1.3.1. *Three-layer IoT architecture (classic or traditional model)*

This first architecture was proposed in the early days of the IoT (see Figure 1.2), mainly for simple systems such as domotics (home automation) or first-generation connected sensors.

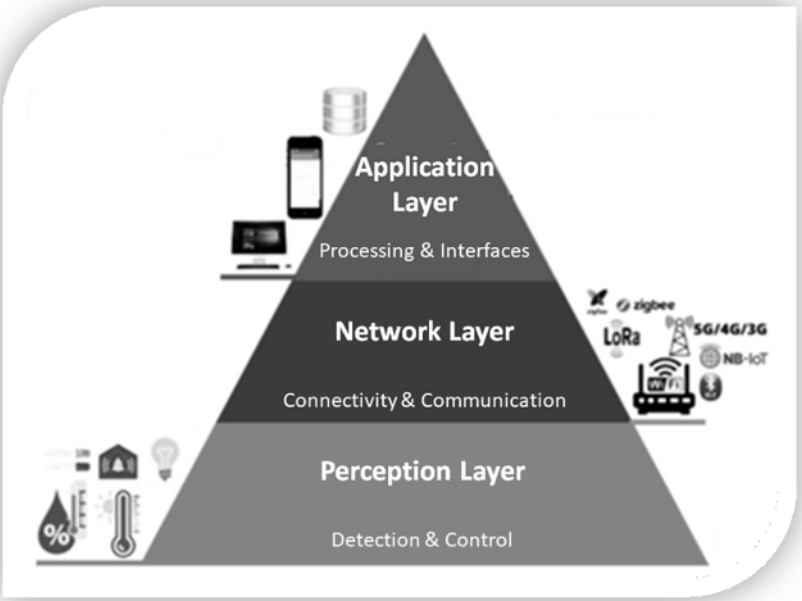

Figure 1.2. *Three-layer IoT architecture*

1.3.1.1. *Perception layer*

The perception layer comprises various hardware devices, such as sensors and actuators, tailored to the specific needs of the application domain. These devices are responsible for detecting and collecting a significant volume of data from the environment. Once collected, data are transmitted to the network layer for processing. This step is essential to ensure efficient interaction between the physical world and digital systems. The role of sensors is key, since they are responsible for measuring parameters such as temperature, humidity or movement, whereas actuators enable interactions with the environment. The quality and accuracy of the data collected depend directly on the performance of these devices. This layer constitutes the first link in the processing chain within IoT architecture. Its proper functioning is crucial to ensuring reliable analyses and decisions. In short, it constitutes the link between the physical world and computer systems.

1.3.1.2. *Network layer*

The network layer plays a central role in IoT architecture by ensuring data transmission between connected devices and servers or the Cloud. It relies on a variety of technologies, such as Wi-Fi, Bluetooth, Zigbee, Low Power Wide Area Network (LPWAN) and 5G, as well as communication protocols such as Bluetooth, NFC (Near Field Communication), Sigfox or LoRa, adapted to specific needs in terms of range, throughput and energy consumption. Whether wireless or wired, these transmission media enable reliable and secure information transfer while adapting to the requirements of the application layer. To put it succinctly, this layer is the essential bridge that connects IoT devices to processing and storage infrastructures, ensuring smooth and efficient communication.

1.3.1.3. *Application layer*

The application layer is the component that provides a user interface for interacting with IoT systems, via mobile applications, industrial management software or other platforms. It enables visualization, analysis and control of the data collected by IoT devices, offering solutions tailored to various fields.

IoT has widespread applications in industrial sectors such as manufacturing, supply chain management, the food industry, smart grids, healthcare and the Internet of Vehicles (IoVs). This layer plays a key role in transforming raw data into actionable information, facilitating decision-making and process optimization in both industrial and consumer environments. In short, it constitutes the final interface which makes IoT systems accessible and useful to users and businesses.

1.3.1.4. *Limitations of the three-layer IoT architecture*

In three-layer IoT architecture, layer 3 (the application layer) has significant limitations: it does not take security into account, making data and systems vulnerable to external threats. In addition, it lacks advanced data management capabilities, including intermediate processing or local storage capabilities. Finally, it does not manage resource optimization, which can lead to inefficiencies and increased latency. These limitations have encouraged evolution towards four-layer and higher architecture models, which incorporate additional features addressing these challenges.

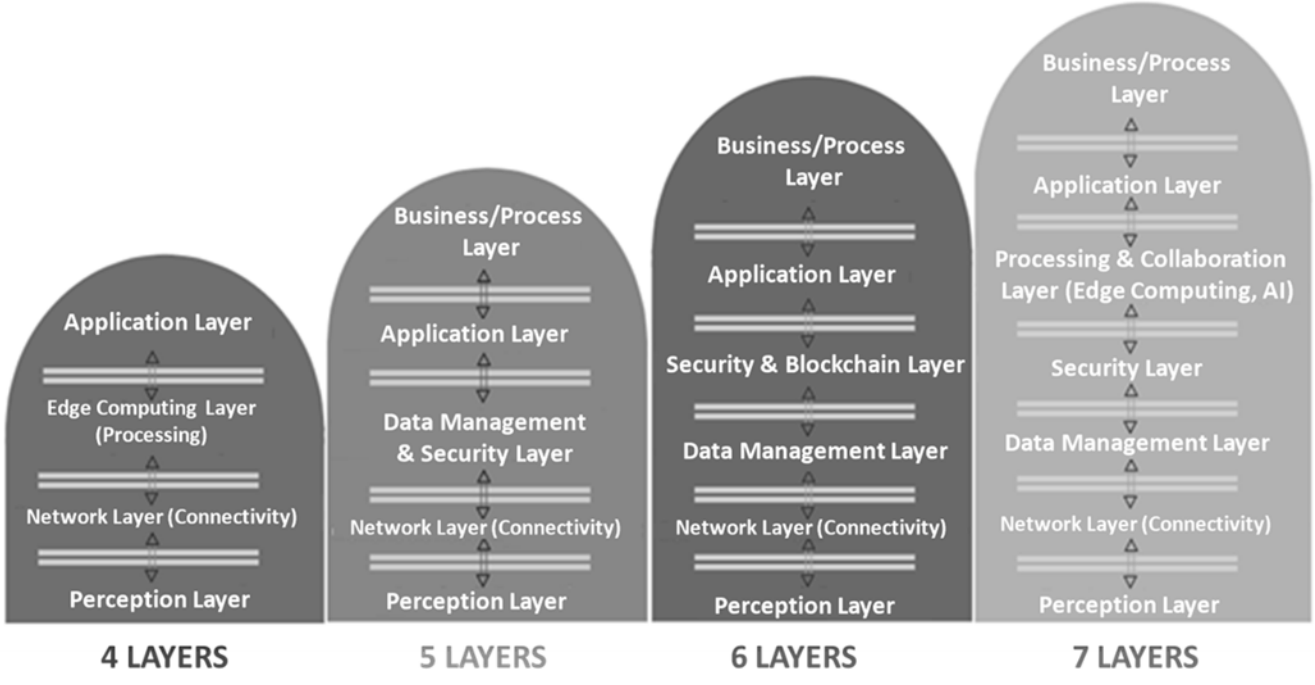

Figure 1.3. *Multi-layered IoT architecture*

1.3.2. *Multi-layered IoT architecture*

The evolution of IoT architecture has adapted to the growing needs of connectivity, data management and security, shifting from simple models to more complex and secure structures. In the 2000s, a three-layer architecture (perception, network, application) served as the basis for simple IoT systems, such as domotics (home automation). With the increase in data volume, a four-layer architecture was introduced in the 2010s, adding an intermediate processing layer (middleware) to manage data storage and analysis via Cloud and Edge Computing, reducing latency and network traffic, although security was still limited (Al-Shareeda et al. 2024).

Between 2015 and 2020, the five-layer architecture emerged to address the challenges of complexity and energy efficiency, integrating a resource management layer to optimize resource allocation, improve quality of service (QoS) and manage energy more efficiently (Saadaoui and Nasri 2014, 2015, 2017). However, security concerns persisted (Al-Fuqaha et al. 2015; Husnoo et al. 2021).

Since 2020, a six-layer architecture has been developed for critical sectors (healthcare, industry, smart cities), adding a data management layer for data filtering, classification and storage, as well as a reinforced security layer with blockchain, data encryption and intrusion detection technologies. This architecture offers increased security for sensitive data and optimized performance through intelligent data management (IDM).

The seven-layer IoT architecture is often used for critical and complex environments, such as Industry 5.0, smart cities or connected health (see Figure 1.3). It adds a new dimension to the architecture by integrating more layers dedicated to security, data management and business aspects.

In parallel, other architectures have emerged to meet specific needs:

– *SOA* (Service-Oriented Architecture): offers a modular and interoperable approach, with a dedicated service layer to provide specific functionalities based on the data collected.

– *Fog/Edge Computing architecture*: introduced to reduce latency and bandwidth, it brings data processing closer to the source thanks to an Edge/Fog layer while retaining a Cloud layer for large-scale processing.

– *Cloud-based IoT architecture*: popularized for its scalability and flexibility, it centralizes data storage, processing and analysis in the Cloud.

– *AI-integrated architecture (AIoT)*: recently developed, it uses an AI processing layer to improve data analysis and decision-making, leveraging AI algorithms.

– *Secure IoT architecture*: developed to meet cybersecurity challenges, it integrates security protocols at each level (network, processing, application) to protect data in transit and at rest.

To conclude, IoT architecture has evolved to adapt to increasing complexity, performance and security requirements. Current trends include the integration of AI, Fog/Edge Computing for decentralized processing, and a greater focus on data protection, particularly in critical sectors. While each architecture presents its own advantages and disadvantages, the choice depends on the specific needs of the IoT application considered.

1.4. Sensor, actuators, gateway and embedded systems

Hardware encompasses the set of objects (things) in the expression "IoT". It represents the essential physical component of a connected object, particularly through sensors. When combined with actuators and embedded systems, these sensors form the technological basis of the IoT. They play a crucial role in enabling connected objects to detect their environment, react to it and act accordingly.

1.4.1. *Sensors*

A sensor is a key electronic device in the IoT, designed to detect and measure real-world physical or chemical phenomena, such as temperature, pressure, movement, shocks, vibrations, position, brightness or even the chemical composition of air or water. Converted into electrical signals, these data constitute the basis of the IoT and enable a variety of applications, ranging from environmental monitoring and domotics (home automation) to industry. Among the most common types of sensors are temperature sensors (used in smart thermostats or industrial systems), humidity sensors (essential for connected agriculture or air conditioning), motion sensors (indispensable for home security or augmented reality) and light sensors (used in smart lighting management). By collecting accurate data, these devices act as the first step in the IoT processing chain, enabling connected systems to perceive and interact with their environment.

1.4.2. *Actuators*

Actuators are essential devices for the IoT, capable of converting electronic signals into physical actions, thereby enabling connected systems to actively interact with their environment. Unlike sensors which measure data, actuators act upon received information, triggering specific actions without human intervention. For example, a

water leak detector connected to a motorized valve can automatically shut off the water in the event of an emergency. Common examples of actuators include electric motors (used in robots or industrial machinery), valves (used in irrigation systems or oil installations) and servomotors (essential for precision robotics). By automating processes and responding in real time, these devices improve the efficiency of IoT systems and contribute to the proactive management of critical situations.

1.4.3. *Gateways*

The gateway plays a central role in the IoT ecosystem. It acts as an intermediary between sensors and network. Its role is to collect the data captured by the sensors, process them if necessary (e.g. by compressing or filtering them), and then transmit them to servers or Cloud platforms for analysis. For example, pollution sensors can send their data via a gateway to the Ministry of the Environment, which exploits information to identify the most polluted areas and make informed decisions. The gateway is therefore essential to ensure reliable and secure communication between IoT devices and central systems.

1.4.4. *Embedded systems*

Embedded systems are miniaturized computers integrated into objects to execute specific tasks. They play a key role in the IoT by processing the data collected by sensors and coordinating the actions of actuators. These systems are exceptionally performant, capable of processing data in real time while consuming little power. They are also ultra reliable, since they have been designed to operate without interruption even in harsh environments. Their design is often custom-made, optimized for specific applications, making them extremely efficient. Common examples include microcontrollers such as ESP32 or Arduino (ideal for simple and inexpensive applications) and single-board computers (SBCs) such as Raspberry Pi (suited to more complex projects requiring increased computing power). These embedded systems constitute the brain of connected objects, ensuring their autonomy and intelligence.

1.5. IoT communication protocols

Communication is a central element of the IoT, connecting the various components in order to enable smooth data exchange. IoT protocols define the rules for transmitting information across various connected devices (Sethi and Sarangi 2017; Çorak et al. 2018; El Alami et al. 2020; Jamuna and Prakash 2021).

Figure 1.4. *Representative IoT communication protocols*

IoT protocols are essential communication standards enabling connected devices to exchange data in a reliable and secure manner. Among the many existing protocols, some stand out due to their importance and specific uses. They can be classified according to their field of application.

1.5.1. *Long-range communication protocols (LPWAN)*

1.5.1.1. *LoRaWAN (long range wide area network)*

LoRaWAN is an LPWAN protocol designed for long-range communications with minimal energy consumption. It is ideal for large-scale IoT applications, such as smart cities, connected agriculture and environmental monitoring. LoRaWAN devices can communicate over distances of up to several kilometers. It is particularly well suited to environments with limited connectivity.

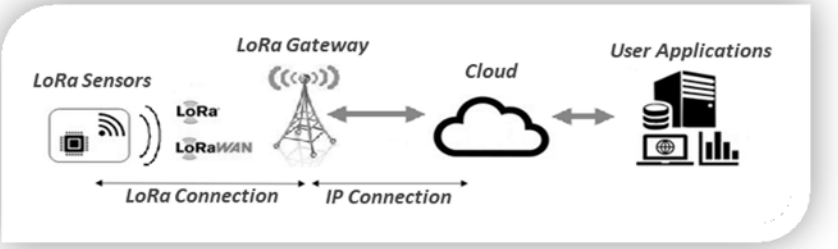

Figure 1.5. *LoRaWAN communication protocol*

1.5.1.2. *NB-IoT (narrowband Internet of Things)*

NB-IoT is a cellular technology specifically designed for low-power, low-data-rate IoT communications. Its key strength lies in its ability to connect a large number of devices across a wide area network while maintaining excellent device battery

life, making it ideal for battery-powered sensors. One of its main advantages is its excellent indoor penetration, enabling it to operate effectively in hard-to-reach environments such as basements, parking garages and industrial buildings. NB-IoT uses existing mobile operator infrastructure, facilitating large-scale deployment without the need for costly new installations. While it does not offer high data rates, it is perfectly suited for applications that transmit small amounts of data at regular intervals, such as smart meters, environmental monitoring and equipment tracking. Its low energy consumption allows for several years of autonomy, thus reducing maintenance. Thanks to its extended range, robustness and energy efficiency, the NB-IoT is the chosen solution for massive IoT networks in urban and industrial environments.

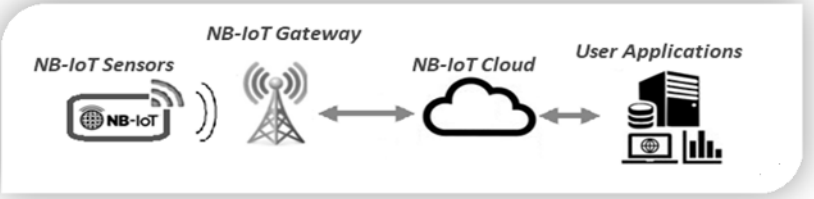

Figure 1.6. *NB-IoT communication protocol*

1.5.1.3. *Sigfox*

Sigfox is another LPWAN protocol, specializing in long-distance communication with minimal energy consumption. It is designed for IoT applications where devices send small amounts of data at spaced intervals, such as smart meters or tracking systems. Sigfox uses a dedicated global network, providing extensive coverage with a lightweight infrastructure. It is ideal for rural or remote environments.

Figure 1.7. *Sigfox communication protocol*

1.5.2. *Short-range wireless communication protocols*

1.5.2.1. *Wi-Fi*

Wi-Fi is a wireless connectivity technology widely used in IoT applications, particularly in home environments where power is readily available. It is particularly well-suited to smart homes, where devices such as security cameras, smart speakers and thermostats can be plugged into the mains. Thanks to its high speed and wide bandwidth, Wi-Fi enables the smooth transmission of large amounts of data, such as video streams or multimedia content. However, it has a limited range, and its relatively high energy consumption makes it less suitable for battery-powered devices or wide area networks. Despite these drawbacks, its ease of installation, native compatibility with most electronic devices and widespread presence in homes make it especially appealing. It is the preferred solution for domotics (home automation) and residential IoT applications with high data demands.

1.5.2.2. *Bluetooth Low Energy*

Bluetooth Low Energy (BLE) is a low-power version of classic Bluetooth, designed for wearable devices and short-range applications. It is widely used with wearables (smartwatches, health sensors) and domotics (home automation) systems. BLE grants fast and secure communication with very low energy consumption. It is also compatible with smartphones, which facilitates its integration into consumer applications.

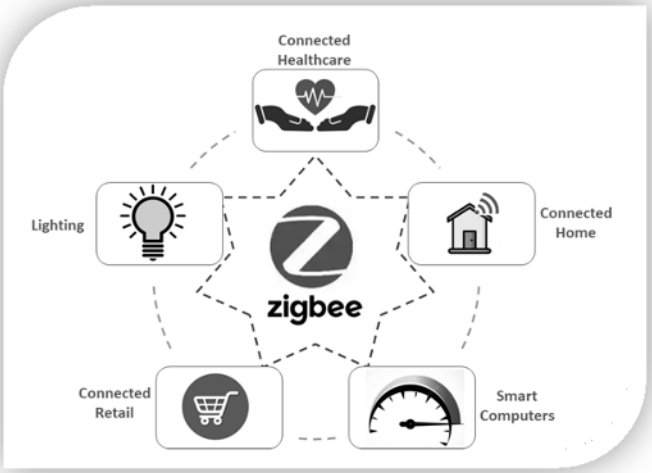

Figure 1.8. *Applications of the Zigbee communication protocol*

1.5.2.3. *Zigbee*

Zigbee is a low-power wireless protocol specifically designed for mesh networks. It allows multiple devices to communicate with one another over short distances, creating a robust and self-organizing network. It is widely used in smart homes to connect devices such as light bulbs, thermostats and sensors. Its low energy consumption makes it a popular choice for both residential and industrial applications.

1.5.3. *Network protocols for IP addressing*

1.5.3.1. *IPv6 over Low-Power Wireless Personal Area Networks*

It enables the integration of IPv6 on low-power wireless networks (Zigbee, Thread). 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) is a protocol specifically designed to enable IPv6 to operate on low-power wireless networks, typical of the IoT. This protocol compresses IPv6 headers to adapt them to the bandwidth and memory constraints of IoT devices.

1.5.3.2. *Thread*

Thread is a wireless communication protocol designed for low-power IoT devices. Based on IPv6 via 6LoWPAN, it enables the creation of reliable, secure and self-healing mesh networks capable of operating efficiently in complex environments. Each network node has a unique IPv6 address, facilitating direct integration with the Internet by means of a gateway. Thread features low energy consumption, robustness and interoperability with other domotics (home automation) technologies. Frequently used in smart homes (such as Google Nest) and in certain light industrial applications, it represents a key technology for the future of the IoT.

1.5.4. *Data and messaging exchange protocols*

1.5.4.1. *Message Queuing Telemetry Transport*

Message Queuing Telemetry Transport (MQTT) is a lightweight and efficient communication protocol based on a publish/subscribe model. It is designed for low-bandwidth, high-latency environments, making it ideal for low-power IoT devices. It works with a central broker to manage messages between devices, ensuring reliable communication. It is widely used in domotics (home automation), industrial and surveillance systems. Its simplicity and low energy consumption make it a popular choice for low-power IoT devices.

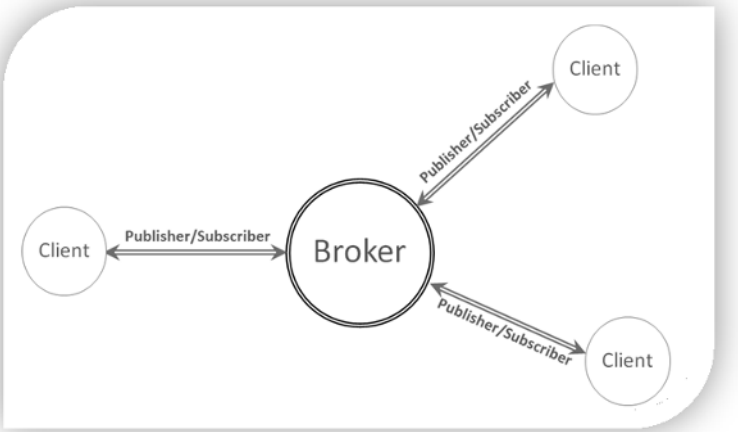

Figure 1.9. *MQTT communications protocol*

1.5.4.2. *Constrained Application Protocol*

Constrained Application Protocol (CoAP) is a protocol designed for resource-constrained devices, such as IoT sensors. It uses a request/response model similar to HTTP, but with a smaller footprint and optimization for low-bandwidth networks. It supports multicast communication and is often used in domotics (home automation) and sensor networks. CoAP is also compatible with HTTP, facilitating integration with web systems.

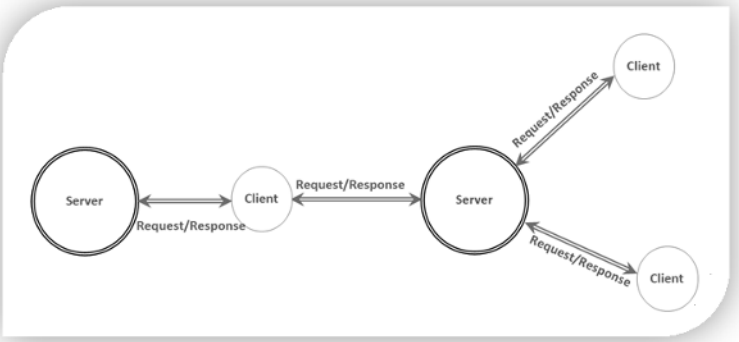

Figure 1.10. *CoAP communication protocol*

1.5.4.3. *HyperText Transfer Protocol/HyperText Transfer Protocol Secure*

HTTP (HyperText Transfer Protocol) and its secure version, HTTPS, are widely used web protocols for IoT communications. While less suitable for low-power devices due to their high energy consumption, they are ideal for applications requiring integration with Cloud services or web interfaces. HTTPS adds a layer of security via SSL/TLS encryption. In IoT systems, it is often used for RESTful APIs.

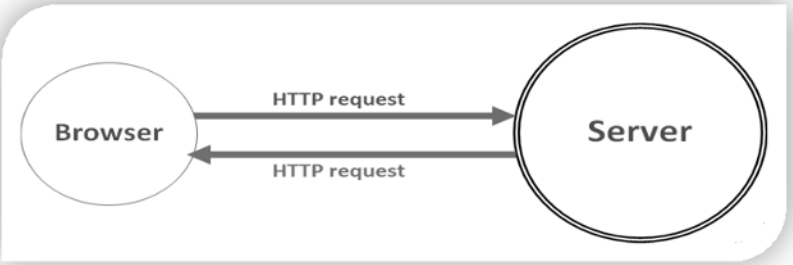

Figure 1.11. *HTTP communication protocol*

1.5.4.4. *Advanced Message Queuing Protocol*

Advanced Message Queuing Protocol (AMQP) is a reliable and secure messaging protocol designed for industrial systems and critical applications. It supports asynchronous message exchange and guarantees data delivery even in the event of network failure. It is often used in environments where reliability and security are essential, such as banking systems or industrial infrastructures. AMQP works with message brokers to manage message queues.

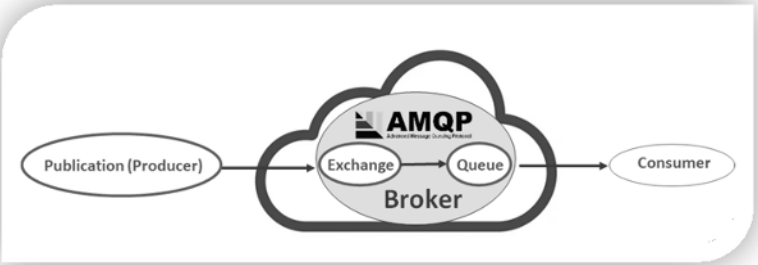

Figure 1.12. *AMQP communication protocol*

1.5.4.5. *Data Distribution Service*

Data Distribution Service (DDS) is a real-time communication protocol designed for critical and distributed systems. It uses a brokerless publish/subscribe model, making it highly efficient for industrial, medical and military applications. DDS guarantees reliable and fast data delivery, even in complex environments. It is frequently used in real-time control systems and highly reliable IoT infrastructures.

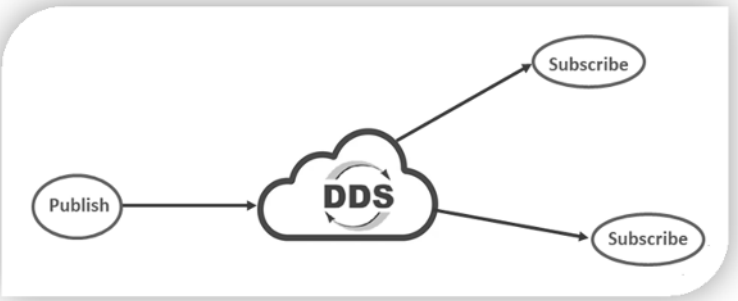

Figure 1.13. *DDS communication protocol*

1.5.4.6. *WebSocket*

WebSocket is a real-time, bidirectional communication protocol that enables continuous interaction between servers and IoT devices. Unlike HTTP, it maintains an open connection, reducing latency and improving efficiency. It is used in applications requiring real-time updates, such as dashboards or monitoring systems. WebSocket is also secured through SSL/TLS encryption.

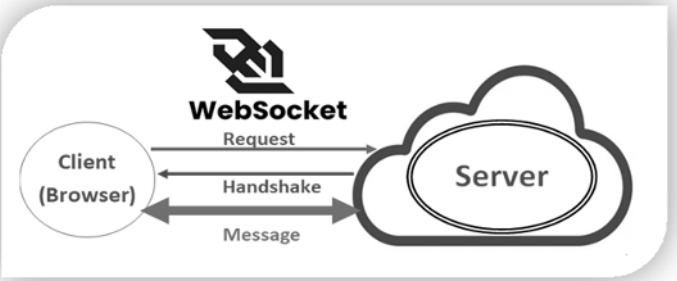

Figure 1.14. *WebSocket communication protocol*

These protocols, each with its own specificities, make it possible to meet the various needs of IoT systems, whether in terms of range, energy consumption, reliability or security.

1.6. Communication medium

The communication medium represents the physical or logical means through which data are transmitted between electronic devices. It plays a key role in the reliability, speed and efficiency of information exchange, particularly in the context of the IoT and connected industry, where connectivity is essential for the digital transformation of factories and industrial processes, in line with the concepts of Industry 4.0 and Industry 5.0. This medium can be classified into two main categories: wired and wireless.

Wired media use cables to ensure data transmission. Among them, the Ethernet cable is widely used for broadband connections due to its stability and low latency, crucial characteristics for industrial applications and Industry 4.0 systems. Fiber optics, on the contrary, can reach extremely high speeds over long distances while being immune to electromagnetic interference, making it the preferred choice for critical infrastructure in connected industries.

In contrast, wireless technologies use radio waves to transmit data. Wi-Fi is commonly used in home and business networks to provide a fast connection without the need for cabling, thereby facilitating the deployment of IoT solutions. Bluetooth is preferred for short-range communications with low energy consumption, namely for connected devices and industrial equipment.

Technologies such as Zigbee are suited to low-power mesh networks, ideal for complex IoT environments, whereas LoRa is optimized for long-range communications with reduced energy consumption, perfect for connected industry applications.

For its part, 5G technology is revolutionizing connectivity by offering high speeds, low latency and increased capacity for connected devices, opening up new perspectives for IoT and Industry 4.0, while laying the foundations for Industry 5.0, which actively integrates AI and human–machine collaboration.

The choice of medium depends on several criteria, including range, speed, energy consumption and environmental constraints such as interference or the presence of obstacles. In order to ensure the smooth exchange of information – whether in an IoT or smart industry context – it must guarantee efficient transmission, adaptability to specific needs and optimal performance.

1.7. IoT application areas: a technological revolution

The IoT is experiencing explosive growth and expanding at an exponential rate, currently impacting numerous sectors. This technological revolution is profoundly transforming the way we live and work by integrating intelligence into diverse aspects of daily life. Through innovative applications in fields such as connected healthcare, smart homes, smart cities, smart industry, wireless sensor networks (WSNs), precision agriculture and many others, the IoT is paving the way for a smarter, more interconnected world (Mourtzis et al. 2018; Haleem and Javaid 2019a, 2019b, 2019c; Oliveira et al. 2019; Keshvarparast et al. 2024).

According to Vermesan et al. (2014), this technology has immense potential to redefine existing infrastructure and establish intelligent, optimized and autonomous ecosystems. By connecting billions of objects and devices, the IoT enables real-time data collection and analysis, promoting informed decision-making and more efficient resource management. This ability to interconnect and optimize systems translates into concrete applications in countless fields (Vilamovska et al. 2009; Domingue et al. 2011; Tao et al. 2018; Almalki and Soufiene 2021). These application areas, which comprise a variety of sectors, illustrate the diversity and scope of possibilities offered by this technology. Here is a detailed exploration of some of these applications.

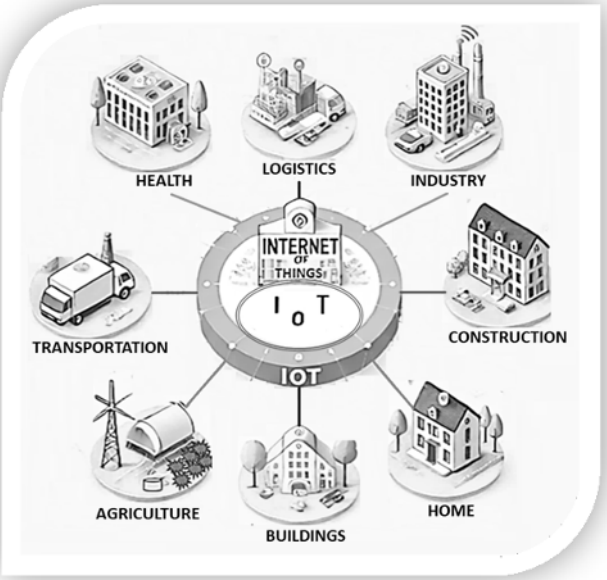

Figure 1.15. *Sectors impacted by innovative technologies*

1.7.1. *Smart home*

The smart home represents a significant advancement in modern societies, providing an automated and connected living environment that enhances comfort, safety and efficiency. These homes integrate automated systems controlled by monitoring, detection and control devices, such as heating, air conditioning, lighting, ventilation and security systems. These systems, often called "gateways", are equipped with sensors and switches interconnected via a central hub. Users can interact with these gateways via mobile interfaces (smartphones, tablets) or computers, leveraging IoT communication networks. The latter plays a key role in domotics (home automation), particularly in strengthening security, privacy, home network management and even the health of its dwellers. For example, sensors can detect water leaks or intrusions, whereas connected devices can monitor indoor air quality.

1.7.2. *Smart cities*

The IoT is pivotal in the development of smart cities, offering innovative solutions to improve citizens' quality of life and optimize urban resource management. Key applications include:

– parking space monitoring: real-time identification of available spaces to reduce traffic congestion;

– infrastructure monitoring: monitoring of vibrations and the condition of buildings, bridges and roads to prevent structural failures;

– noise management: monitoring noise levels in sensitive areas to preserve quality of life;

– smart lighting: adapting public lighting to logical weather conditions and pedestrian or vehicle flows;

– waste management: detection of container fill levels to optimize waste collection;

– smart transportation: real-time traffic management systems, issuing warning messages and diversion suggestions in case of accidents or traffic jams.

These applications rely on technologies such as RFID, WSNs and individual sensors, with bandwidth requirements ranging from low to high, depending on the application. Concrete examples include smart parking, structural health monitoring of buildings, urban noise mapping, waste management and smart transportation systems (Domingue et al. 2011).

1.7.3. *Digital healthcare*

The IoT is transforming the healthcare sector by offering innovative solutions for tracking, identifying and collecting critical data. Key benefits include:

– *patient and staff monitoring*: enhancing hospital workflows by tracking patient and staff movement in real time;

– *identification and authentication*: reducing medical errors through accurate patient identification and efficient electronic medical record management. For instance, identifying newborns in maternity wards helps prevent accidental mix-ups;

– *automatic data collection*: streamlining administrative processes, auditing healthcare operations and managing medical inventories to save time and minimize errors.

IoT sensor devices, such as RFID, NFC (Near Field Communication), WSN, Wi-Fi and Bluetooth, enable real-time monitoring of health indicators such as temperature, blood pressure, heart rate, cholesterol levels and blood glucose. These technologies are used in telemedicine solutions, monitoring compliance with prescribed treatments and issuing an alert in case the patient's health deteriorates. They are applicable to both inpatient and outpatient care, thereby improving the quality and efficiency of healthcare services (Vilamovska et al. 2009; Porkodi and Bhuvaneswari 2014).

1.7.4. *Smart transportation*

The integration of IoT in transportation is revolutionizing the way vehicles interact with one another and their environment. Internet-connected vehicles offer new functionalities that improve safety, traffic flow and the user experience. Thanks to constant connectivity, vehicles can communicate with other connected objects, such as traffic lights, parking facilities or gas stations. These interactions help reduce traffic congestion, optimize routes and provide innovative services, such as predictive maintenance, toll management or access to smart parking facilities. For example, a vehicle can alert its owner of an impending breakdown or suggest an alternative route in real time. These advances contribute to safer, more efficient and more environmentally friendly mobility (Guerrero-Ibanez et al. 2015; Coppola and Morisio 2016).

1.7.5. *Industrial IoT*

The Industrial Internet of Things (IIoT) is transforming production processes by connecting machines, sensors and systems to optimize manufacturing, the supply

chain and resource management (Deshpande and Jogdand 2020; Alabadi et al. 2022). Among its key applications, we can mention:

– *Predictive maintenance*: machines can self-diagnose and alert in case of imminent failure.

– *Environmental monitoring*: monitoring of toxic gas levels, temperature or humidity in factories.

– *Supply chain management*: monitoring storage and transportation conditions to ensure product quality.

– *Worker safety*: monitoring working conditions in hazardous environments.

– *Process automation*: optimization of production lines and reduction of operational costs.

These applications can improve the efficiency, safety and sustainability of industrial operations (Farooq et al. 2015, 2020; Ben-Daya et al. 2017; Shu-Hsien and Yang 2020; Naim et al. 2021).

1.7.6. *Smart agriculture*

The IoT is dramatically altering agriculture by increasing productivity and enhancing crop quality. IoT sensors measure parameters such as soil moisture, temperature, light and CO_2 levels, enabling precise crop management. For example, smart irrigation systems automatically adjust the water supply depending on plant needs. IoT is also used to monitor animal health by measuring heart rate, body temperature and behavior, enabling early disease detection. These technologies undoubtedly contribute to more sustainable agriculture by reducing resource waste and optimizing yields (Farooq et al. 2020).

1.7.7. *Smart environment and agriculture*

The IoT plays a crucial role in optimizing agricultural practices and environmental monitoring, enabling precise and sustainable resource management. Environmental parameters, such as temperature, humidity and soil quality, are essential for maximizing agricultural production. By deploying sensors in the field, farmers can measure these parameters in real time and leverage the data to improve crop efficiency:

– *Automated irrigation*: smart irrigation systems adjust the water supply based on weather conditions and plant needs, reducing resource waste.

– *Greenhouse production*: connected greenhouses use sensors to monitor soil temperature, humidity and nutrient levels. Data are sent to a server for analysis, allowing for optimized growing conditions and increased yields.

– *Pesticide residue detection*: biosensors, such as those based on acetylcholinesterase, can detect pesticide residue in crops. The data collected (sample size, time, location, amount of residue) are analyzed to guarantee crop quality.

– *Product traceability*: a unique QR code can be assigned to each carton of agricultural products. Consumers can scan this code to access detailed information, such as the quantity of pesticides used, via a centralized database.

Regarding environmental concerns, the IoT helps combat air pollution, a major challenge for public health and the climate. For example, electrochemical sensors can measure toxic gas levels on roads, while RFID tags can identify the highest-emission vehicles. These data enable authorities to take targeted measures to reduce emissions and improve air quality (Zhao et al. 2015).

1.7.8. *Supply chain and logistics*

The IoT simplifies and optimizes supply chain processes by providing real-time information on tracking goods, from production to final distribution. Technologies such as RFID (Radio Frequency Identification) and NFC play a central role in this transformation.

– *Goods tracking*: RFID tags make it possible for products to be tracked throughout the supply chain, recording information such as location, temperature and humidity, ensuring product traceability and quality, especially for perishable goods.

– *Inventory management*: data collected by RFID sensors are analyzed to optimize stock levels and anticipate future needs. For example, an IoT-based information transmission system, such as the one proposed by Bo and Guangwen (2009), creates a real-time information network for each product, facilitating inventory management and demand anticipation.

– *Performance improvement*: by providing accurate and up-to-date data, IoT helps companies to analyze past trends and anticipate future demand. This improves operational efficiency and reduces costs associated with inventory shortages or overstocking.

– *Transparency and traceability*: RFID tags can also store information on the quality and origin of products, reinforcing consumer confidence and facilitating regulatory compliance.

In this way, the IoT is transforming the supply chain into a smarter, more transparent and responsive system, capable of adapting to changing market needs while ensuring product quality and traceability (Bo and Guangwen 2009; Ferreira et al. 2010).

1.8. Different extensions of the IoT

The IoT is a catalyst for transformation across many fields, offering innovative solutions to address modern challenges. IoT technology has given rise to numerous specialized extensions, each tailored to specific domains and addressing particular needs in terms of security, latency and reliability. Below is a detailed exploration of these extensions.

1.8.1. *IoV*

The IoV is an IoT application dedicated to smart vehicles and transportation systems. It enables real-time communication between cars, road infrastructure (such as traffic lights and cameras) and traffic management centers. The goal is to improve road safety by detecting potential hazards, optimize traffic flow thanks to dynamic data and support the development of autonomous vehicles. For example, connected cars can share information about weather conditions, accidents or traffic jams, enabling safer and more efficient driving. The IoV relies on technologies such as 5G to guarantee ultra-low latency, essential for real-time decision-making.

1.8.2. *Internet of Medical Things*

The Internet of Medical Things (IoMT) focuses on connected medical devices, transforming the healthcare sector by enabling continuous patient monitoring and remote diagnostics. Devices such as smart watches, connected glucometers and pacemakers collect real-time data and transmit it to healthcare professionals. This permits rapid intervention in case of abnormalities, proactive management of chronic diseases and a reduction in the number of hospitalizations. For example, a diabetic patient can be continuously monitored, with automatic alerts sent to their doctor in case of critical glucose levels. The IoMT also improves healthcare efficiency by automating administrative processes and facilitating the secure sharing of medical data.

1.8.3. *IIoT*

The IIoT applies the principles of the IoT to the industrial sector, connecting machines, sensors and systems with the goal of optimizing production and maintenance. Thanks to embedded sensors, machines can monitor their own condition and predict breakdowns before they occur (predictive maintenance), thereby reducing downtime and repair costs. For example, in a factory, the IIoT can synchronize production lines, adjust settings as needed and monitor product quality in real time. The IIoT also plays a key role in energy resource management, optimizing energy consumption and reducing the environmental impact of industrial activities.

1.8.4. *Internet of Everything*

The Internet of Everything (IoE) goes beyond the IoT by integrating not only connected objects but also people, processes and data. It aims to create interconnected ecosystems where each element interacts intelligently. For example, in a smart city, the IoE can connect transportation systems, public services, citizens and businesses to optimize resource management. Data from environmental sensors, social networks and management systems can be combined to make informed decisions. The IoE fosters closer collaboration between human beings and machines while improving the efficiency and sustainability of systems.

1.8.5. *Internet of Robotic Things*

The Internet of Robotic Things (IoRT) combines the IoT with robotics, enabling robots to collect data via sensors, interact with their environment and make autonomous decisions. These robots are used in fields such as logistics, manufacturing and personal services. For example, in a warehouse, robots equipped with sensors can navigate autonomously, locate products and transport them without human intervention. IoRT is also used in drones for surveillance or delivery missions, where they can analyze their environment in real time and adapt to changing conditions. This extension paves the way for more advanced automation and smarter systems.

1.8.6. *Internet of Agriculture*

The IoA applies the IoT to agriculture to optimize farming practices and improve productivity. Connected sensors monitor soil moisture, weather conditions and plant

health, enabling precise management of irrigation and fertilizers. For example, a farmer can receive alerts when moisture levels are too low and trigger irrigation remotely. The IoA also facilitates livestock monitoring through sensors attached to animals, tracking their health and location. By reducing resource waste and improving yields, the IoA contributes to more sustainable and environmentally friendly agriculture.

1.8.7. *Internet of Behaviors*

The IoB analyzes data collected by the IoT to understand and influence human behavior. It is widely used in marketing to personalize advertising campaigns based on consumer habits. For example, a store can use data from sensors to analyze customer flows and optimize product placement. In the field of human resources, the IoB can monitor employee well-being and suggest measures to improve productivity. However, the IoB raises ethical questions regarding privacy and the use of personal data.

1.8.8. *Internet of Space Things*

The Internet of Space Things (IoST) extends the IoT to space systems by connecting satellites, space stations and other space equipment to optimize communications and space exploration activities. For example, satellites equipped with advanced sensors can monitor weather conditions, climate evolution or seismic activity on Earth in real time. The IoST also enhances communication between space missions and ground stations, enabling more precise and reliable spacecraft control. This technological extension is essential for ambitious projects such as Mars colonization or asteroid mining, which require resilient and autonomous connectivity.

1.9. Conclusion: issues, challenges and prospects for a connected future

The IoT embodies a rapidly growing technological revolution, paving the way for major benefits and diverse applications in almost every field, from industry to everyday life. However, its adoption and large-scale deployment also pose several challenges. These obstacles, both technical and organizational, require careful attention to ensure the success and sustainability of this technology.

One of the first major challenges is interoperability. Indeed, IoT device manufacturers tend to use proprietary technologies, which complicates

communication between devices from different brands. In order to overcome fragmentation, it is essential to standardize protocols and interfaces. This would enable the seamless and harmonious integration of connected objects, promoting an optimal user experience and global interconnectivity.

Another critical issue is identity management and device naming. With billions of connected objects in circulation, each device must be uniquely identifiable on the network. This requires robust, scalable naming systems capable of dynamically managing identities. In addition, data privacy is a major concern. Identification technologies, such as 2D barcodes or RFID tags, are ubiquitous but vulnerable to hacking or unauthorized access. It is imperative to implement advanced security mechanisms to protect sensitive data.

Network security is also an essential pillar of the IoT. Sensors and connected devices transmit data via wired or wireless channels, making them vulnerable to external interference, network congestion or malicious attacks. To ensure the integrity and confidentiality of the information exchanged, reliable transmission protocols and robust encryption techniques are essential. Furthermore, the physical security of connected objects should not be overlooked. These devices, often deployed in open or hard-to-reach environments, are exposed to risks of vandalism or physical damage, which could compromise their operation and service continuity.

A further significant challenge is making the IoT more environmentally friendly. The proliferation of connected devices and the increase in data rates are leading to a noteworthy rise in network energy consumption. To minimize environmental impact, it is crucial to develop more sustainable technologies, such as low-power sensors, autonomous devices and optimized network infrastructures. These innovations will make it possible to reconcile performance and environmental responsibility while meeting the growing demand for connectivity.

At the same time, the IoT is generating an explosion of data, creating both opportunities and analytical challenges. Billions of devices produce continuous streams of information, offering valuable insights for optimizing operations and understanding user behavior. For example, in the agricultural sector, IoT sensors enable the monitoring of environmental conditions and the adjustment of crop cycles to maximize yields. Nevertheless, this massive amount of data requires sophisticated analytical tools to extract actionable trends and transform information into strategic decisions.

Security and privacy are fundamental concerns in the IoT ecosystem. With a multitude of devices handling sensitive data, cybersecurity becomes a top priority. Smart cameras, connected medical devices and other critical pieces of equipment must be protected against malicious intrusions to prevent privacy breaches and

hacking risks. Finding a balance between connectivity and security is essential to building user trust and ensuring widespread IoT adoption.

The IoT also offers unprecedented control over our environment. In the domestic sphere, it makes it possible to remotely manage household appliances, heating systems and lighting via simple and intuitive applications. In the industrial sector, connected machines can detect anomalies in real time, automatically order spare parts and reduce downtime, improving productivity and infrastructure safety.

Finally, the IoT relies on close collaboration between the actors in the ecosystem. Manufacturers, developers, service providers and end-users must work hand in hand to fully exploit the potential of this technology. For instance, in the automotive industry, the integration of connected vehicles requires cooperation between manufacturers, telecommunications operators and software publishers. This synergy is essential to creating innovative, interoperable and sustainable IoT solutions.

To conclude, the IoT represents a multifaceted technological revolution, combining immense opportunities with complex challenges. To maximize its benefits, it is essential to address the issues related to interoperability, security, data management and sustainability while promoting close collaboration among all the actors involved in the ecosystem. Only then will the IoT be able to fully transform our world and meet the growing need for connectivity.