



ILNAS

White Paper

INTERNET OF THINGS (IoT)

TECHNOLOGY, ECONOMIC VIEW
AND TECHNICAL STANDARDIZATION

Version 1.0 · July 2018





COLLABORATION
PARTNER
OFFICE
SERVICE
EXCELLENCE
INDUSTRY

432432

675453

875654

23466

COLLABORATION
PARTNER



White Paper

INTERNET OF THINGS (IoT)

TECHNOLOGY, ECONOMIC VIEW
AND TECHNICAL STANDARDIZATION

Version 1.0 · July 2018

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

 **ANEC**

Agence pour la Normalisation et
l'Économie de la Connaissance

Avec le support de :



LE GOUVERNEMENT
DU GRAND DUCHÉ DE LUXEMBOURG
Ministère de l'Économie



The role of Information and Communication Technologies (ICT) is significantly increasing in our everyday lives and it has a predominant influence on the development of the economy and information society. The positive impact across various economic sectors in the interdisciplinary applications is only possible with the growth of these technologies. In Luxembourg, ICT is largely used for the development of innovative products and services in order to address societal, market, and business challenges.

Today, billions of connected devices are aimed to be interconnected in the Internet of Things (IoT) network using recent computing technologies. This exponentially growing number of things in the IoT opens an era creating new services that can bring noticeable changes to the individual citizens, society, economy and environment and huge number of

business opportunities. Nowadays, IoT is considered to have a potential to advance the quality of life of the citizens and economic growth of the country. Adoption of IoT technology in various domains, such as Smart cities, Smart transportation, Smart logistics, Smart industry, Smart meter and Smart grid improves their current operational efficiency and interaction with the people. Luxembourg is offering an ideal environment for the development of innovative IoT solutions, notably because of its dynamic ICT ecosystem, its qualitative infrastructure for the ICT sector and its central location in Europe. These factors contribute greatly to the implementation of new IoT based solutions and pave the way for a data-driven economy.

To encourage such initiatives, it is necessary to provide insights on relevant concepts, specifications and requirements of new technologies to the national stakeholders. For that reason, this white paper provides the state-of-the-art and examines IoT from three different points of view: basic technological concepts, economic and business prospects, and technical standardization. The first aspect highlights fundamental concepts and broad view of IoT technological landscape together with its driving technologies. It also includes challenges that have to be met in order to unleash the full potential of IoT, notably from technological and regulatory points of view. The second aspect is dedicated to provide a perspective on global trends of IoT business and the potential industries where IoT could have an impact on the economy at large. The third aspect offers an overview of current standardization activities that are being carried out at international level, which will establish the related common technical language, and will focus and improve the required technology's convergence.

In this context, ILNAS, the national standards body, is conducting the national technical standardization strategy, with a strong policy concerning the ICT sector. With associated research and education initiatives, this white paper is only one among several projects that indicates an excellent path that ILNAS is taking to develop the necessary culture about ICT technical standardization at the national level.

Within this framework, Luxembourg will continue to consider technical standardization as a real force multiplier for the ICT sector, directly contributing to the economic growth and in the development of national organizations' competitiveness.

Etienne Schneider

Deputy Prime Minister
Minister of the Economy

Acknowledgements

The working-group (WG) involved to prepare this white paper is:

Name of the contributor	Role	Institution/Organization
Mr. Mario GROTZ	Director General for Research, Intellectual Property and New Technologies	Ministry of the Economy
Mr. Michele GALLO	Director ICT Coordination	Ministry of the Economy
Mr. François THILL	Deputy Executive Advisor	Ministry of the Economy
Mr. Jean-Marie SPAUS	HPC Project Coordination	Ministry of the Economy
Dr. Christian TOCK	Director Sustainable Technologies	Ministry of the Economy
Mr. Jean SCHILTZ	External Consultant Smart Mobility	Ministry of the Economy
Mr. Jean-Marie REIFF	Director	ILNAS
Dr. Jean-Philippe HUMBERT	Deputy Director	ILNAS
Mr. Claude LIESCH	Deputy Director	ILNAS
Dr. Johnatan PECERO	Head of Standardization Department	ANEC G.I.E.
Dr. Shyam WAGLE	Project Officer	ANEC G.I.E.
Mr. Nicolas DOMENJOUR	Project Officer	ANEC G.I.E.
Mr. Benoit POLETTI	General Director	Incert G.I.E.

This working-group would like to thank all the people who have helped and supported us, in different ways, in developing this white paper.

- Ms. Marianne HOFFMANN, Ministry of the Economy
- Mr. Lex KAUFHOLD, Ministry of the Economy
- Mr. Daniel LIEBERMANN, Ministry of the Economy
- Dr. Marcin SEREDYNSKI, E-Bus Competence Center, Luxembourg
- Mr. Stefan LATSCH, Luxair S.A. LuxairCARGO
- Mr. Patrick SILVERIO, Luxair S.A. LuxairCARGO
- Dr. German CASTIGNANI, Motion-S, Luxembourg
- Mr. Manal EL IDRISSE, Motion-S, Luxembourg
- Mr. Guido von SCHEFFER, Motion-S, Luxembourg
- Dr. Francesco VITI, University of Luxembourg

Table of contents

Acknowledgements	7
List of Figures	10
List of Tables	11
Introduction	13
1. Internet of Things – Conceptual overview	17
1.1 IoT building blocks	18
1.2 IoT definitions	20
1.3 IoT basic characteristics	21
1.4 Application domains in IoT	22
1.4.1 Smart City domain	23
1.4.2 Industrial domain	27
1.4.3 Health and well-being domain	29
2. Internet of Things – Technical landscape	31
2.1 Evolution of IoT concept	31
2.2 IoT application structures and driver technologies	33
2.2.1 Collection phase	34
2.2.2 Transmission phase	37
2.2.3 Processing, managing and utilization phase	39
2.3 The concept of Edge, Fog and Roof computing in IoT	42
2.3.1 Edge computing	42
2.3.2 Fog computing	43
2.3.3 Roof computing	44
3. Internet of Things – Challenges	47
3.1 Technical challenges	47
3.1.1 Interoperability	47
3.1.2 Precision	48
3.1.3 Data volume and scalability	48
3.1.4 Internet-connectivity	48
3.2 Security, Privacy and Trust issues	49
3.2.1 Security vulnerabilities in overall IoT system	49
3.2.2 Security vulnerabilities at different layers of IoT architecture	51
3.2.3 Privacy	53
3.2.4 Identity and access management	56
3.2.5 Trust	56
3.3 Sensitivity of security, privacy and regulatory issues in IoT	57
3.4 Regulatory challenges	58
3.4.1 Data ownership and Data collection management	58
3.4.2 GDPR and IoT	58
3.5 Standardization gap	60

4.	Internet of Things – Economic analysis and business prospects	63
4.1	Economic analysis – global outlook	63
4.2	IoT application domains with high impact on economy	65
4.3	Business opportunities, challenges and long-run impact of IoT	67
4.3.1	Strengths and business opportunities in IoT	69
4.3.2	The long-run impact on economy	72
5.	Internet of Things – Technical standardization	77
5.1	Background on technical standardization and the national context	77
5.1.1	Technical standardization and standards	77
5.1.2	Technical standardization and IoT	78
5.1.3	National context of IoT technical standardization	80
5.2	ISO/IEC JTC 1/SC 41 - Internet of Things and related technologies	81
5.2.1	Membership	81
5.2.2	Liaisons	82
5.2.3	Structure and standards	83
5.3	International Telecommunication Union's Telecommunication Standardization Sector (ITU-T)	86
5.3.1	ITU-T SG 20 - Internet of things (IoT) and smart cities and communities (SC&C)	86
5.3.2	ITU-T JCA IoT and SC&C - Joint Coordination Activity on Internet of Things and Smart Cities and Communities	86
5.3.3	ITU-T FG-DPM - Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities	87
5.3.4	Other ITU-T activities related to IoT	87
5.4	European Telecommunications Standards Institute (ETSI)	88
5.4.1	ETSI/TC Smart M2M - Smart Machine-to-Machine Communication	88
5.4.2	Other ETSI activities related to IoT	89
5.5	IoT fora and consortia	90
5.5.1	Third Generation Partnership Project (3GPP)	90
5.5.2	Alliance for Internet of Things Innovation (AIOTI)	90
5.5.3	Association for Automatic Identification and Mobility (AIM)	91
5.5.4	Global Standards One (GS1)	92
5.5.5	Institute of Electrical and Electronics Engineers (IEEE)	92
5.5.6	Internet Engineering Task Force (IETF)	92
5.5.7	Industrial Internet Consortium (IIC)	93
5.5.8	oneM2M	93
5.5.9	Open Geospatial Consortium (OGC)	94
5.5.10	Open Connectivity Foundation (OCF)	95
5.5.11	World Wide Web Consortium (W3C)	95
6.	Conclusions and outlook	97
	References	99

List of Figures

Figure 1	A's and C's concept in IoT	17
Figure 2	IoT building blocks	18
Figure 3	Six smart characteristics to enhance quality of life	24
Figure 4	Schematic representation of the Smart Cities	27
Figure 5	Relation between M2M and IoT	32
Figure 6	IoT application approach	33
Figure 7	Data Flow in IoT Environment	34
Figure 8	Short distance Vs. long distance communication technologies	35
Figure 9	HPC for smart space -mobility application	41
Figure 10	Typical Edge environment in IoT application	43
Figure 11	The Roof federated architecture	44
Figure 12	IoT security concept	50
Figure 13	Projected connected devices by 2019	64
Figure 14	Connectivity dimension calculated as the weighted average of different sub-dimensions	69
Figure 15	M2M cards, per 100 inhabitants	69
Figure 16	RFID used for product identification by enterprises	70
Figure 17	International standardization organizations and their area of competence	78
Figure 18	IoT SDOs and Alliances Landscape	79
Figure 19	ISO/IEC JTC 1/SC 41 membership	82
Figure 20	ISO/IEC JTC 1/SC 41 structure	83
Figure 21	AIOTI working groups	91
Figure 22	Summary of oneM2M Release 2 and 3 features	94

List of Tables

Table 1	IoT components	19
Table 2	IoT definitions	20
Table 3	IoT basic characteristics	21
Table 4	IoT application domains	23
Table 5	Factors and indicators of smart characteristics	24
Table 6	M2M vs. IoT	32
Table 7	M2M applications and technologies by geography and mobility	33
Table 8	Technology references in data collection phase in short range	35
Table 9	Technology references in data collection phase in long range	36
Table 10	Technology references in data transmission phase	38
Table 11	The strategy of Luxembourg with major policy and action levers	40
Table 12	Cloud vs. Edge/Fog vs. Roof	45
Table 13	IoT opportunities	47
Table 14	Set of security requirements	49
Table 15	Security risks in data collection layer	51
Table 16	Security risks in data transmission layer	52
Table 17	Security risks in enabling protocols used for application layer	53
Table 18	Basic principles of privacy	54
Table 19	Communication of information flow in IoT	55
Table 20	Privacy measure examples in IoT	55
Table 21	Sensitivity of security, privacy and regulatory issues in IoT	58
Table 22	IoT implementations where GDPR can affect	59
Table 23	Global trends of IoT market	65
Table 24	IoT application domains with high impact on economy	66
Table 25	Enablers and barriers in IoT businesses	68
Table 26	Settings where IoT can create values in 2025	75
Table 27	ISO/IEC JTC 1/SC 41 liaisons organizations and areas of collaboration	83
Table 28	Standards and projects of ISO/IEC JTC 1/SC 41	85
Table 29	ISO/IEC JTC 1/SC 41 Study Groups and their objectives	85
Table 30	ITU-T SG 20 Study questions and IoT related activities	86
Table 31	ITU-T additional activities related to IoT standardization	87
Table 32	ETSI additional activities related to IoT standardization	89

Introduction

The Internet of Things (IoT) is a promising topic of technical, societal and economic significance [1]. It has the potential to significantly drive **business, technology, and economic growth** over next decade [2]. The IoT is intended for ubiquitous connectivity among different entities, also called **things** [3]. There is a seamless integration among these entities and with human beings. These entities become a part of our life that communicate intelligently with one another to execute daily operations.

The IoT can be viewed from different perspectives [4]. From the **perspective of services provided by things**, it is a world where **things** can automatically communicate to computers and each other providing services to the benefit of the human kind [5]. Similarly, from the **perspective of connectivity**, it is for anyone from anytime, anywhere, i.e. connectivity for anything [4], [6]. From the **perspective of communication**, it is a worldwide network of interconnected objects uniquely addressable based on standard communication protocols [7]. Finally, from the **perspective of networking**, it is the internet evolved from a network of interconnected computers to a network of interconnected objects [8]. Overall, it refers to business process and applications of sensed data, information and content generated from **interconnected world by means of connected devices** that exist in the internet infrastructure.

Adoption of IoT technology in various domains, such as **industries, transport systems, logistics, energy meters, and health & well-being** improves their current **operational efficiency and interaction with the people**. The data generated from various domains helps to create valuable insights for **optimizing operations and quality standards of the citizens**.

The goal of this white paper is to provide a broad view of the developments around IoT and related technologies. To achieve this, a systematic review from the perspectives of three different viewpoints: IoT concepts and technology, economic and business prospects, and technical standardization is presented. The viewpoints provided allow the readers to broadly be able to answer to questions such as:

- What is the concept behind IoT?
- What are the potential application domains of IoT?
- What are the driving technologies of IoT including recent computing technologies devoted to it?
- What are the challenges for IoT?
- What are current trends of IoT and how will IoT impact the economy at large?
- What are the recent developments in IoT related technical standardization?
- Which set of standards are relevant?

The rest of this white paper is organized along these three viewpoints as follows:

Review of IoT basic concepts and its driving technologies:

- **Chapter 1** provides a basic concept of IoT, definitions, fundamental characteristics (Section 1.1, Section 1.2 and Section 1.3) giving summary of major application domains of IoT (Section 1.4) how it can help, by adopting IoT technology, to enhance the efficiency of a traditional approach.
- **Chapter 2** gives technical in-depth analysis across three dimensions.

- The first part of this chapter reviews the evolution of the technology with its supporting technological developments (Section 2.1).
 - The second part of this chapter provides IoT environment landscape and their data interaction phases. In particular, a high-level IoT architecture is provided in the beginning, then driving technologies are illustrated for each phase of data flow together with importance of high performance computing in IoT (Section 2.2).
 - The third, and the final, part of this chapter highlights the importance and comparisons of recent computing technologies introduced for IoT, such as Edge, Fog and Roof computing (Section 2.3).
- **Chapter 3** provides a review of IoT challenges from the perspective of technology, security, privacy and trust, and regulatory issues. In particular, the most prominent issues among many challenges facing by IoT ecosystem are studied.

Economic and business prospects:

- **Chapter 4** first provides insights on global trends of IoT business and the potential industries where IoT technology impacts on the economy at large (Section 4.1 and Section 4.2). The second part of this chapter is dedicated to provide business opportunities, challenges as well as insights on its impact to the economy in the long-run (Section 4.3).

Technical standards watch:

- **Chapter 5** provides a systematic review of the on-going technical standardization activities at the national, EU and international levels. It particularly focuses on the developments within ISO/IEC JTC1/SC 41 - Internet of Things and related technologies as a technical committee, which is one of the most active ones in building standards for IoT based solutions and actively followed by the market. This chapter also analyses activities of IoT and related technologies by different Standards Development Organizations (SDOs), such as ETSI, ITU-T and other fora & consortia.



ECONOMY & BUSINESS PROSPECTS

TECHNOLOGY

TECHNICAL STANDARDIZATION

1

Internet of Things - Conceptual overview

1. Internet of Things – Conceptual overview

Internet of Things (IoT), refers to an **emerging paradigm** consisting of a continuum of uniquely addressable things communicating with each other to form worldwide dynamic networks [9]. The network of **uniquely identifiable connected devices** such as **objects, devices, sensors and everyday items** with computing services is called IoT. However, the term IoT is relatively new, the concept of combining computers and networks to monitor and control the devices already existed around for decades [1]. For example, remotely monitoring meter on the electrical grid via telephone lines was already in commercial use by the late 1970s. It is further became extensive by advanced wireless technology allowed for machine-to-machine enterprise and industrial solutions for equipment monitoring and operation¹, where closed purpose-build networks or proprietary industry specific standards were used rather than **Internet Protocol (IP)** and **Internet standards**. From the beginnings of the use of IP to connect devices in the early 2000s, robust field of research and development into smart object networking led to create the foundation of today's IoT². The term IoT has become popular nowadays to realize the scenarios, where internet connectivity and computing capability extends to a **variety of objects** [1]. The idea behind the IoT could be also represented as shown in Figure 1. The **A's** refer to the globalization of the technology (**anytime, anywhere, any device, any device, any network**, etc.) and **C's** reflects the properties of IoT, such as **collections, convergence, connectivity, computing** and so on. However today's IoT has already reached beyond the range of A's and C's.

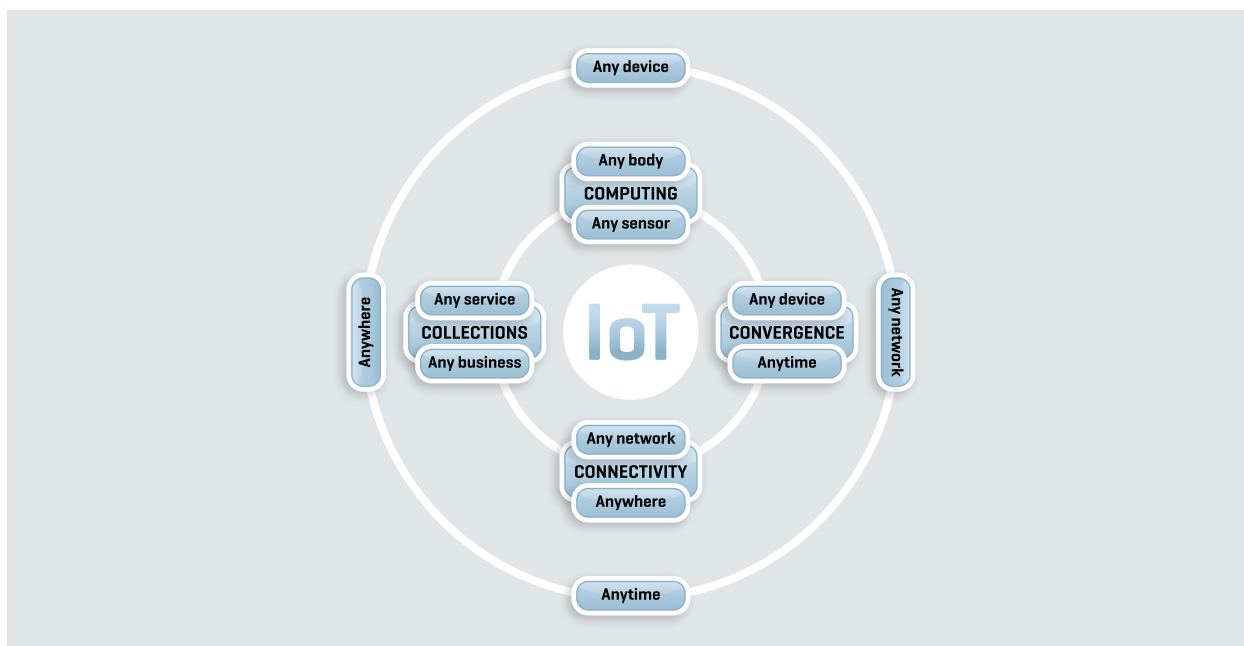


Figure 1: A's and C's concept in IoT [10]

Predictions of several organizations provide a wide range of estimates of the total number of IP-enabled IoT devices to be in operation to the internet by next year from a low of 19 billion to a very optimistic prediction up of to 40 billion and rather continues this growth exponentially for next decade [11]. This growth opens an era of new services that can bring noticeable changes to the **individual citizens, society, economy and environment and huge number of business opportunities**. The rest of this chapter provides basic building blocks of IoT together with its definitions proposed by different organizations and major application domains of IoT.

^{1]} <https://www.automationworld.com/article/topics/cloud-computing/know-difference-between-iiot-and-m2m>

^{2]} <https://tools.ietf.org/html/rfc7452>

1.1 IoT building blocks

The humans in the today's world are surrounded by **basic electronic devices**, smart devices, automated vehicles, smart buildings and so on. These physical devices are **equipped with software**, which are able to provide specific facilities and services based on their designs and purposes. These physical entities can communicate through **powerful communication networks** to overcome the geographical boundaries. Originally, there was a limitations in the number of interactions among these physical entities, which resulted in limited information exchanges and limited control over the connected devices using technologies such as WiFi, Bluetooth, mobile applications. In this context, the **concept of IoT** is introduced to enable full access control in their interaction between physical devices in spite of any location on the earth through the internet [12]. Millions to billions numbers of physical devices are aimed to be interconnected in the IoT network using recent **computing technologies**, such as Edge computing, Fog computing and Roof computing (see Section 2.3 for more detail). The interacting physical devices in IoT should be equipped with device specific embedded software, sensors and network supporting components. The sensors realize the presence of physical entity using device specific embedded software in the surrounding and gather the information required for the interaction. Internet acts as a communication media of various dispersed physical entities. Each physical entity has **unique identification number**. The information gathered from physical devices having unique identification number will be processed using storage servers on web and further will be delivered at right place in right time to be utilized by different applications (Figure 2).

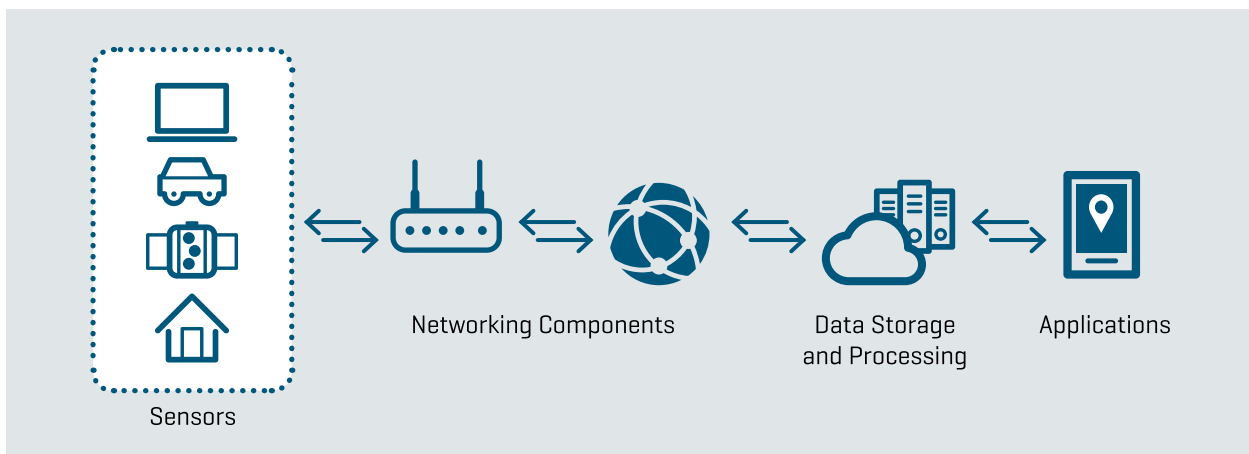


Figure 2: IoT building blocks

The IoT comprises different components as shown in Table 1. The physical objects or devices³ (also called **things**), which can sense to affect the physical environment by means of **actuators**. Human involved in the interactions, for example in home automation; can control the environment via mobile applications. The platforms are used to connect IoT components as shown in Table 1 as a middleware between physical entities and IoT. These entities are **connected by networks** through various means of communication technologies, such as wireline, wireless technologies [10] (further detailed in Chapter 2). Gathered information (**massive volumes of data**) is processed and turned into valuable information to be accessed and utilized by **different applications** running on the IoT components.

³] can be virtual objects such as electronics tickets, books, and wallets

IoT components	Description
Physical objects	Things
Virtual objects	Electronic tickets, books, wallets
Sensors	Sense the physical environment
Actuators	Affect the physical environment
Human	For example, human can control the environment via mobile applications
Networking components	The components are connected together by networks, using various wireless and wireline technologies, standards, and protocols to provide connectivity
Platforms	The middleware used to connect components such as physical objects, human, and services to the IoT. They provide numerous functions such as: <ul style="list-style-type: none"> ● Access to devices ● Ensuring proper installation/behaviour of device ● Interoperable connection to local network, cloud or other devices
Data storage and processing	Cloud services is one example of data storage and processing technology that can be used for: <ul style="list-style-type: none"> ● Processing big data and turning it into valuable information ● Building and running innovative applications ● Optimizing business processes by integrating device data
Applications	Application domains (see Section 1.4 for more detail)

Table 1: IoT components [12]

1.2 IoT definitions

The IoT is difficult to define precisely. It describes a world where anything can be connected and can interact in an intelligent fashion. For the sake of better understanding of the IoT terminology, Table 2 provides definitions of IoT provided by different standard development organizations (SDOs).

ISO/IEC ⁴	<p>“It is an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.”</p>
ITU-T Y.2060 [13]	<p>“A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”</p> <p><i>Note 1</i> – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.</p> <p><i>Note 2</i> – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.</p> <p>“Things: With regard to the Internet of things, these are an object of the physical world (physical devices) or the information world (virtual things), which are capable of being identified and integrated into communication networks.”</p>
IEEE ⁵	<p>“The Internet of Things (IoT) is a framework in which all things have a representation and a presence in the Internet. More specifically, the Internet of Things aims at offering new applications and services bridging the physical and virtual worlds, in which Machine-to-Machine (M2M) communications represents the baseline communication that enables the interactions between Things and applications in the Cloud.”</p>

Table 2: IoT definitions

⁴] <https://www.iso.org/obp/ui/#iso:std:iso:19731:ed-1:v1:en:term:3.21>

⁵] <http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standards-next-steps>

1.3 IoT basic characteristics

The IoT is a complex system with a number of characteristics that can be defined from the perspectives of IoT components/devices used, services provided, usability, and security [14]. Given the evolving character of IoT it is too early to determine its complete features. However, some of the general and key characteristics are highlighted in Table 3:

Smart data collection and smart handling	The IoT is able to distribute sensors widely and collect data quickly and effectively to form a new way of collaboration among connected devices. Smart data processing of such collected data is a key IoT feature. The different kinds of data produced by physical devices of IoT systems can be stream, batch, and asynchronous data. Such data can be processed and used for system feedback, allowing for process improvement, fault detection and incorporation of real-world context into business workflows.
Interconnectivity	The IoT is able to interconnect anything (physical or virtual things) with the help of global information and communication infrastructure. Communication infrastructure ⁶ refers to the backbone of the communications system upon which various broadcasting and telecommunication services are operated. This can be built from copper cable, fiber, or wireless technologies utilizing the radio frequency spectrum, such as microwave and satellite.
Things-related services	The IoT is capable of providing things-related services within the constraints of things, such as privacy protection and semantic consistency between physical and their associated virtual objects. In order to provide things-related services within the constraints of things, both the technologies in physical world and information world are required.
Heterogeneity/diversity	The devices in the IoT should be heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks. Diversity is another characteristic of the IoT. Identifiers in the physical world and the information world are different. In the physical world, the identifiers of physical things of the IoT devices may be different according to applied technologies.
Dynamic changes	The state of devices changes dynamically (for instance, sleeping and waking up, connected and/or disconnected) as well as the context of devices, including location and speed. Moreover, the number of devices can change dynamically.
Enormous scale	The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the number of devices connected to the current internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the generated data and its interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

Table 3: IoT basic characteristics [1], [13], [14]

⁶ <http://www.blackwellreference.com>

1.4 Application domains in IoT

The IoT has huge potential for developing new intelligent applications in nearly every domain, such as **personal, social, societal, medical, environmental and logistics** aspects [9]. The number of application domains has been also increasing due to its ability to perform contextual sensing. It allows, for instance, to collect information of environment, natural phenomena, medical parameters and user habits and then can offer tailored services based on information received. Such phenomenon should enhance the quality of everyday life, and should have a reflective impact on the society and economy irrespective of the application domain. Globally, various applications domains can be categorized in three major areas: **smart city domain, industrial domain, and health and well-being domain** (Table 4). In fact, each domain is partially or completely overlapped but is not isolated from the others since most of the applications are common and share the same resources.

Domain	Sub-domain	Examples
Smart Cities	Smart home/ Smart commercial buildings	Home security system, video surveillance, access management, children protection
		Entertainment, comfortable living
	Smart mobility/ transport and smart tourism	Intelligent transport systems (ITS) - Traffic management, bike/car/van sharing, multi-modal transport, road condition monitoring, parking system
		Connected and automated driving
		Automated adaptive traffic control
		Payment systems, tour guide services
	Utilities	Smart grid: power generation, distribution and management
		Smart meter, smart water management
		Sustainable mobility, Storage services
	Public services, safety and environment monitoring	Public services
		Emergency rescue, personal tracking, emergency plan
		Video/radar/satellite surveillance
		Environmental and territory monitoring
Industrial services	Logistics and product lifetime management	Smart manufacturing
		Identification of material, product, goods or product deterioration
		Warehouse, retail and inventory management
		Shopping operations and fast payment
	Agriculture and breeding	Animal tracking, certification, trade control
		Farm registration management
		Irrigation, monitoring agricultural production and feed
	Industrial processing	Real-time vehicle diagnostics, assemblage process, assistive driving
		Luggage management, boarding operations, mobile tickets
		Monitoring industrial plants

Health well-being	Medical and Healthcare	Medical equipment tracking, secure and access indoor environment management
		Smart hospital services, entertainment services
		Remote monitoring of medical parameters, diagnostics
	Independent living	Elderly assistances, disabled assistance
		Personal home and mobile assistance, social inclusion
		Individual well-being, personal behaviour impact on society

Table 4: IoT application domains [9]

The rest of the section provides brief summary of major application domains of IoT and how IoT can help to enhance the quality of life or efficiency of traditional approach in those domains.

1.4.1 Smart City domain

The city is called smart city when it can operate and provide a management of its services (for instance, energy, transport, waste management, lighting, entertainment) through the widespread usage of ICT technologies [9]. There are many examples how a city can be made smart and improve the life of the citizens. For instance, smart or intelligent services can be created for the citizens to provide effective tools for accurate mobility plan in multimodal transport systems such as public transport and other ride-sharing services. The city can take advantage from intelligent traffic lights and static or mobile sensors spreading in its territory, which can be used to manage the traffic automatically, to monitor and predict the traffic jam situations and to inform vehicle drivers about the possibilities of critical situations and propose alternative routes/means. All the data gathered using sensors [15], at the same time, can help municipalities to perform environmental monitoring and territorial prevention by measuring water level, air pollution, presence of a certain components (for instance, percentage of allergenic pollen or radiation in the air) [16]. Energy optimization can be reached by using smart meter/grid for monitoring and by modifying consumption in the city and buildings using actuators and renewable energies in the production [17]. For instance, the European smart city project⁷ identifies six smart characteristics as indicators of the human life, namely Governance, Economy, Mobility, Environment, People and Living (see Figure 3). The IoT-based technologies can play vital role by providing additional smartness in such human life indicators. Factors and indicators of each smart characteristic are presented in Table 5. The citizen will get better quality standard of life if their authority or municipality can provide the better performance in those indicators.

⁷ <http://www.smart-cities.eu/>

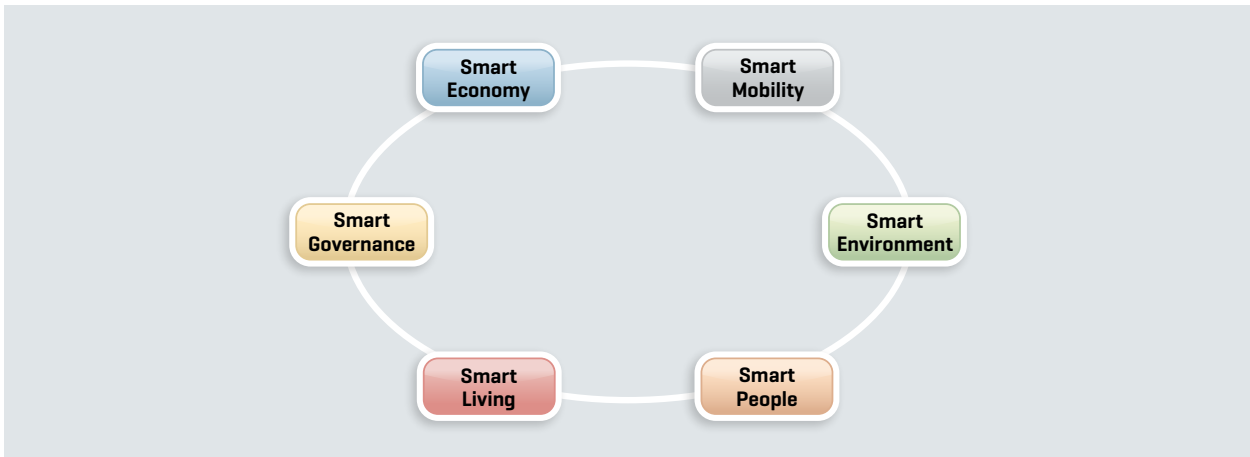


Figure 3: Six smart characteristics to enhance quality of life⁷

Smart Governance	Participation	Smart Environment	Network and environmental monitoring
	Transparency and information accessibility		Energy efficiency
	Public and Social Services		Urban planning and urban refurbishment
	Multi-level governance		Smart buildings and building renovation
Smart Economy	Innovation		Resources management
	Entrepreneurship		Environmental protection
	Local & Global interconnectedness	Smart People	Digital education, creativity
	Productivity		ICT - Enabled working
	Flexibility of labor market		Community building and urban life management
			Inclusive society
Smart Mobility	Traffic management	Smart Living	Tourism, culture and leisure
	Public Transport		Healthcare
	ICT Infrastructure		Security
	Logistics		Technology accessibility
	Accessibility		Welfare & Social inclusion
	Clean, non-motorized options		Public spaces management
	Multimodality		

Table 5: Factors and indicators of smart characteristics⁷

According to Gartner⁸, a Smart City is an urbanized area where multiple sectors cooperate to achieve sustainable outcomes through the analysis of contextual, real-time information shared among sector-specific information and operational technology systems. It subcategorizes the Smart City domain in following subsectors based on types of connecting things:

⁸] Gartner report, 2015, <https://www.gartner.com/newsroom/id/3008917>

1.4.1.1 Smart Homes

The smart homes, also known as home automation, are the residences where IoT technologies are enabled to provide homeowners comfort, security, convenience and energy efficiency by controlling smart devices anywhere, anytime. The users often can control smart home devices by smart applications on their smartphone or other networked devices.

1.4.1.2 Smart commercial buildings

Smart commercial buildings are the buildings, which integrate and account for intelligence services to ensure the drivers for building progression such as energy and efficiency, comfort and satisfaction at lower cost and environmental impact over the building life cycle. The commercially available buildings can be separated into two categories [18]: locally controlled systems through a stationary or wireless interface using the in-home controller and remotely controlled systems through personal computer, mobile applications or telephone of the user. The latter is done with the use of internet connection or connecting with an already existing home security system.

1.4.1.3 Smart transport

It includes IoT based system for managing the traffic system (for instance, intelligent transport systems, connected and automated driving, and automated adaptive traffic control). Thinking of improving a national transportation system not only means of building new roads or repairing aging infrastructure but also in the implementation of technology, mainly network of sensors, microchips or other communication devices that can collect and spread the information for the better functioning of the transport system. The transport systems are further sub-sectored in three domains:

- **Intelligent transport systems (ITS):** The objective of intelligent transport systems (ITS) is to increase the quality of life of the citizens and the environmental sustainability of the cities by optimizing and controlling traffic on public vehicles and on the roads. IoT enabled technologies, such as an ITS helps everyone to reach the destination in time, faster, more safely and in cheaper cost. The ITS adopting the IoT empowers actors of transport system's commuters with intelligent information to make better decisions in choosing appropriate route; optimal driving speed to avoid congestion, appropriate time of the travel; the way of optimizing traffic signals; and so on.
- **Connected and automated driving:** The connected and automated driving is the next big leap in transport technologies, which is expected to be fully functional by 2030. This technology relies on the automation of the vehicle sensing and driving function based on multiple levels of automation, where only passengers exists and driver is no longer required to drive the vehicle. The future automated driving will integrate different technologies, including [19]:
 - Ultrasonic sensors to detect the presence of the obstacles;
 - LIDAR (Light Imaging Detection and Ranging) and/or Radio Detection and Ranging (RADAR) to create a 360-degree field of view to prevent accidents;
 - High definition cameras to spot road hazards in real time, for instance pedestrians or animals;
 - Global navigation Satellite System receivers to provide accurate position of the vehicles;
 - Communication technologies allow interaction of vehicles with the surrounding vehicles, road infrastructures, trusted third parties and remote service providers.
- **Automated adaptive traffic control:** The objective of automated adaptive traffic control is to enhance the management and coordination of traffic flows and use of various cooperative navigation services by drivers. The adoption of automated traffic control relies on collection and analysis of information exchanged

between entities to maintain and build the global traffic control database. The information collected from road sensors is transmitted to the trusted remote data centers for further processing and analysis. The location- and context-based information related to drivers, vehicles, road conditions is taken into account for full automated traffic control.

1.4.1.4 Smart public services

It includes public safety and environmental monitoring related services. The primary objective of public safety is protection of citizens, safeguarding of public and private properties, management of natural disasters, and maintenance of public order. The environmental monitoring includes monitoring the condition of environment, such as measuring the air pollution, detection of the presence of certain components (for instance, percentage of allergenic pollen or radiation in the air), detection of forest fire, measurement of toxic gas or CO₂ emissions from factories and many more. For better management of public services using IoT based technologies, dedicated sensors, smart cameras, global positioning system (GPS) and other wireless technologies are used for real-time tracking, monitoring and localizing.

1.4.1.5 Smart utilities

Utility management using IoT technologies relates to smart resource management of electricity, water, gas, garbage of the citizens. It allows efficient use of existing resources and infrastructures for electricity management (such as in generation, transmission and distribution), efficient disposal of garbage and management of water and electricity. It is also aimed to improve reliability and sustainability of the resources at the peak load. Recent developments being carried out in the utility management are subset of smart meter activities.

- **Smart meter:** The smart meter is capable of transferring electrical, water, gas consumption details of consumers on a real time basis to the utility provider company. Meter readings can be sent remotely over the internet to the utility provider without being physically present at the site to monitor the meter. Two-way communication between meter and the utility providers using IoT based technologies allows gathering several types of information, such as interval data, time-based demand data, service interruption, outage management, service restoration, quality of service monitoring, distribution network analysis, distribution planning, peak demand, demand reduction and customer billing [20]. If the smart meter is programmed it can also force control on the consumption of the devices used in smart environment.
- **Smart grid:** As a means to solve the problems of traditional grid system, the smart grid has been promoted as a promising solution for managing the wastage of electrical energy [21]. It advances the traditional technology to improve in efficiency, effectiveness, reliability, security, and stability of increasing demand of electrical energy. The smart grid further revolutionizes the energy generation, transmission, distribution and consumption. The IoT enabled technology provides interactive real-time network connection to the users and devices via various communication technologies to enhance the overall efficiency of smart grid [22].
- **Smart water management:** Water is a crucial resource in the current world. As a result, nowadays, smart water management is growing in popularity as it gives consumers the ability to easily monitor the water consumption. The smart water sensors track multiple parameters, such as water quality, temperature, pressure, consumption. These sensors are directly communicated to a water utility company, where the data are analysed to provide consumers' water usage patterns. Water leak detectors also can help to detect the faulty pipeline to reduce the consumption of the water.

Figure 4 illustrates how overall characteristics of city ecosystem could be changed in the future with full implementation of IoT-based technologies. The city is equipped with various end devices, such as a network of sensors, cameras, smart meters, screens, speakers, and thermostats, etc. that collect information. The amount of information collected from different sources are referred to as open data, public/private data or Big data depending upon the availability of their source. A common management platform, a city operating system [9],

will be responsible for managing, analysing, sorting, processing and forwarding the information where needed within the city to improve the services according to the citizen needs. This horizontal management layer ensures coordination, interoperability, and optimization of individual services or applications. The authorities or citizens can access the services offered by different platforms using their applications, can consume them and can actively participate by creating additional content that will be further analyzed to properly manage the city. A logical infrastructure provided by such technologies controls and coordinates the physical infrastructure in order to adapt the city services to the actual citizen needs, while making the city sustainable [23].

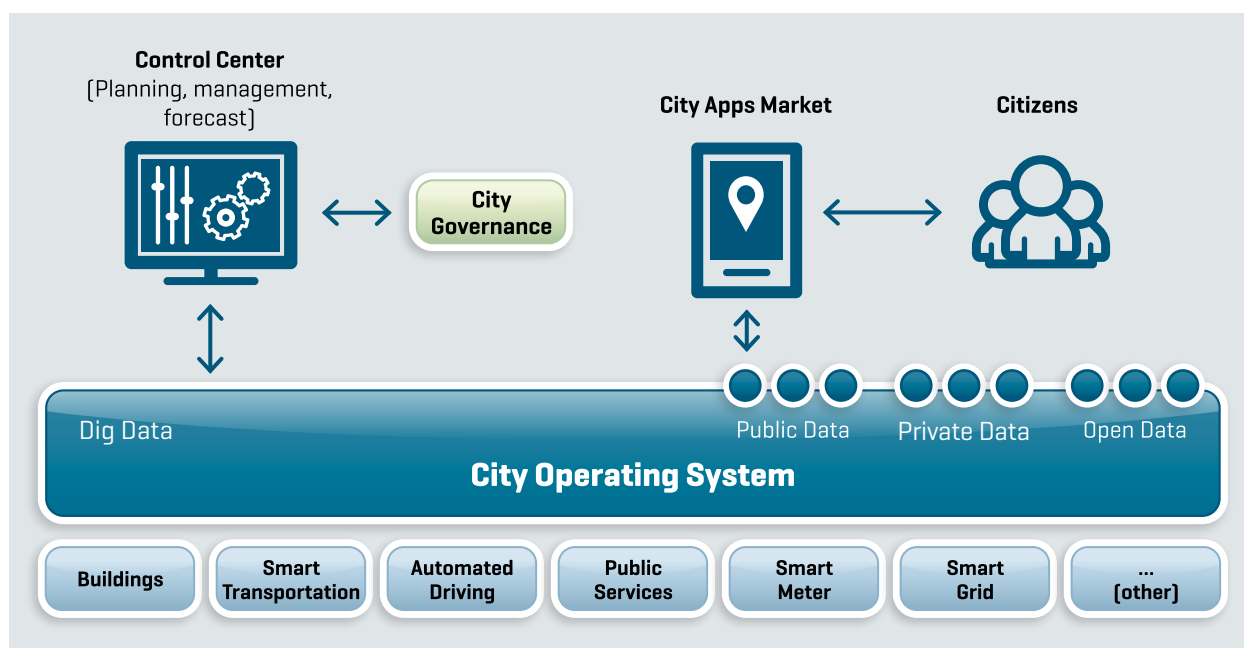


Figure 4: Schematic representation of the Smart Cities [9]

1.4.2 Industrial domain

This domain includes the IoT applications applied to enhance the efficiency, mainly in industrial process, logistic and supply chain management as well as in agriculture and breeding [9]. The industrial domain could be further sub-categorized into smart manufacturing, smart logistics and smart agriculture domains.

1.4.2.1 Smart manufacturing

It is an endeavour to enhance the quality and efficiency of the manufacturing process across entire value chain⁹. In smart manufacturing, digital twin (digital information about each part or product) along with physical part or product accumulates as much data as it can in the process of production and inspection, assembly and test, supply chain in order to handover bundled physical and digital product or service to the end users. It can also be applied to increase the sustainability of product manufacturing, for instance IoT technologies allow monitoring of high-risk industries, such as chemical industries to minimize the emissions of CO₂ or toxic gases in the environment. The smart manufacturing principal guidelines for the conventional industries to become smart industries might be:

- minimization of manual data entry, translation or transformation of information at each process step;
- establishing autonomous diagnostic and decision support distributed nodes at the machine, factory and enterprise levels;

⁹ <https://www.automationworld.com/article/topics/industrial-internet-things/what-smart-about-smart-manufacturing>

- optimizing the schemes that can control acquired data analytics and machine learning algorithms to recommend process adjustments at different levels;
- adoption of machine-to-machine (M2M), application-to-application (A2A) and business-to-business (B2B) integration standards to plug-and-play with hardware and software of multi-vendors.

1.4.2.2 Smart logistics

Getting right product at the right place at the right time in the right condition is the well known requirements for logistics and transportation [24]. The aim of the smart logistics is an efficient transportation of the product lowering cost of the product manufacturer and logistics service providers. It helps in simplifying retail inventory and warehouse by providing accurate knowledge of inventory, reducing inaccuracies in inventory and tracking and tracing of products throughout the journey of their delivery. Optimized route system can support logistics service providers to reduce their operational cost of transportation and to lower the fuel consumption.

The IoT application in smart logistics domain can be considered as use of RFID chips attached to the objects that are used to identify materials and objects, to transmit and record journey of the product (supply chain) and to give the detail of the tracking system, such as 'what', 'where', 'when', and 'why'. Received or shipped times, picked and packed locations, condition of goods during shipment, and availability of materials or goods at specific locations are examples of common information required in tracking system. The supply chain visibility is the near future IoT-enabled solution, which is planned to provide further optimized solutions in logistics. According to Gartner¹⁰, the goal of supply chain visibility is a key capability for becoming demand-driven in a mature value network.

1.4.2.3 Smart agriculture

Smart agriculture is an approach that helps to make agriculture systems more efficient by transforming and reorienting conventional agricultural system through techniques such as sensors, geographic mapping, machine-to-machine connectivity and other smart information platforms. Recent IoT based applications in agriculture, food production are more efficient in terms of saving of energy and water, using fewer resources, for instance in fermentation and manure management, and reducing waste. In addition, it also results in incrementing the productivity of the farmers due to the use of IoT based applications. The popular application domains in smart agriculture are:

- control in the agriculture production and application of drones in feeding;
- identification of particular infected animals or crops to avoid the spread of contagious disease by exact tracing;
- accessible database (global) of animals with the track records of demographics, pedigree of an animal, contracted disease, vaccinations, and veterinary checks, etc.;
- capability of accessing real-time data of animal's health, for instance body temperatures for optimal breeding.

^{10]} Featuring research from Gartner, 2014, <https://www.kinaxis.com/Global/resources/papers/Supply%20Chain%20Visibility%20Gartner%20Newsletter.pdf>

1.4.3 Health and well-being domain

Another essential domain where IoT can play vital role is human health and well-being domain. By introducing intelligent services in conventional health caring system, people's and society's activities can be improved. Some examples of such intelligent services include control patient's health, improvement of quality of life of aged and disabled people. These range from enabling citizens and society to get involved in administration and government decisions, allowing people in order to live independently to maintain their social relationships, or to improve the health and social care [9]. This domain is further sub-categorized into health care and independent living.

1.4.3.1 Healthcare

In the healthcare system, real-time monitoring is possible using advanced sensing devices for medical vital parameters, such as blood pressure, temperature, cholesterol level, and heart rate [9]. These data transmitted using specific communication technologies and are made available to the medical personnel for diagnosis and control of the patient's health. In tele-medicine, the data gathered from patients using wearable devices can be used to monitor the remote (out of the hospital) patient's health. For example, for bulimia (eating disorder) patient in hospital or at his home, sensors could detect the increased temperature, blood pressure or even the odor of vomit of the patients [25]. In case of exercise abuse, such as excessive walking activities, excessive cardio training, sensors could detect those activities compared to walking at normal pace of the patient. This information would be valuable in diagnosis and management of patient's health. The low cost RFID or bar code could be used to track the patient's administrative status at the hospital whether they are still admitted or discharged from the hospital.

1.4.3.2 Independent living

Another application of IoT to improve the quality of life of the citizens is in independent living domain for specific categories of people, such as aging or disabled population. The European commission joint program, Ambient Assisted Living (AAL)¹¹, helps these people to live in their own homes and being active in the society. The key application areas of this project are regular monitoring of the status of aged people and providing medical consultation at home. The real-time monitored data from these people will be able to set off alarms to suggest possible medical check-ups or hospitalization in case of deterioration of health condition or emergency.

^{11]} <http://www.aal-europe.eu/our-projects/>

2

Internet of Things - Technical landscape

2. Internet of Things – Technical landscape

This chapter first provides an overview of evolution of the IoT concept with its supporting technologies (Section 2.1). The second part then provides in depth study of different layers of IoT architecture and driver technologies of each layer (Section 2.2). Finally, the third part overviews the concepts and comparisons of recent computing technologies applicable for IoT (Section 2.3).

2.1 Evolution of IoT concept

The term was first mentioned by Kevin Ashton, co-founder of the Auto-ID Center at MIT, with reference to a global standard system for Radio Frequency Identification (RFID) and other sensors were created [26]. Further, the Electronic Product Code (EPC)¹² was developed aiming to spread use of RFID in worldwide networks [27]. Gradual development of wireless communication systems, such as WiFi, Bluetooth, Near Field Communication (NFC), Wireless Sensor Network (WSN), and cellular technologies helped in its evolution. Today, an IoT system consists of a set of smart devices (building blocks), or **things**, that interact on a collaborative basis to fulfil a common goal [28]. **Things** collect data from the environment, compute, and integrate seamlessly with the physical world. They must be easily locatable, recognizable, addressable and controllable. Because these things are also interconnected through the internet, an almost endless combination can be devised to create innovative products and services. The evolution of IoT is mainly supported by following technological developments:

- **RFID** tags are intelligent bar codes capable to talk with a networked system to track the objects. Technically speaking, RFID tags are chips with antenna that are typically embedded in objects and containing electronically stored data. For the automatic identification and tracking, RFID uses electromagnetic fields. There are two types of RFID tags, namely passive and active tags. Passive tags transmit data when they collect energy from the electromagnetic fields of a nearby RFID reader, whereas active tags contain a local power source and can operate at hundreds of meters from RFID readers.
- **WiFi** (IEEE 802.11x) is a local wireless networking technology that is largely used by IoT devices in home automation (such as in smart homes), whereas mobile wireless networks are used by IoT for geographically dispersed M2M connectivity. Most commonly, WiFi uses the 2.4 GHz frequency band (UHF) and 5 GHz (ISM radio) band for communication. Recently, the WiFi Alliance introduced WiFi HaLow¹³, an extension for WiFi enabling the low power connectivity required for applications using sensors and wearables, such as Smart homes, connected cars and Smart Cities. WiFi HaLow is based on 802.11ah standard and operates in 900 MHz frequency band.
- **NFC**, a Near Field Communication¹⁴, is a communication technology that enables devices to share information wirelessly by putting them in touch or bringing them into proximity with each other. The NFC is broadly used in applications for sharing personal data (such as contacts, business cards, photos, videos), financial transactions, information access in smart posters, etc. It is considered as an evolution of RFID as it is built upon RFID systems adding the possibility of bidirectional communications. There is still lack of adoption of NFC in M2M communications due to the unwillingness among organizations, such as retailers and public transport companies to provide open access to their respective client base. In such cases, infrastructures are explicitly made incompatible with NFC.

¹²] which is a universal identifier to provide a unique identity to every physical object

¹³] <https://www.wi-fi.org/discover-wi-fi/wi-fi-halow>

¹⁴] <https://nfc-forum.org/>

- **Machine-to-Machine (M2M)** communication is often used for remote monitoring. Key components of a M2M system include sensors, RFID, NFC, Bluetooth, WiFi and cellular communication. Figure 5 and Table 6 show the relation between M2M and IoT. Table 7 presents a classification of M2M applications and technologies based on geography and mobility factors.

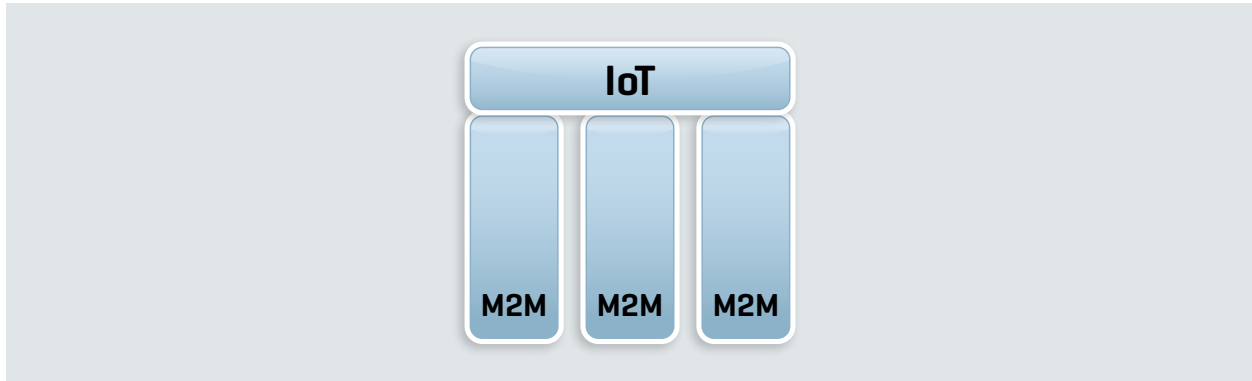


Figure 5: Relation between M2M and IoT

M2M	IoT
Point-to point communication usually embedded within hardware	Multiple communication using IP Networks incorporating with varying communication protocol
Cellular or wired networks are used for main communication	Data delivery is relied on a middle layer hosted in the cloud
Devices do not necessarily rely on an internet connection	Active internet connection is needed in most of the cases
Limited integration options	Unlimited integration options

Table 6: M2M vs. IoT¹⁵

- **Sensor** is a device to convert a physical phenomenon into an electrical signal. It represents part of the interface between the world of electrical devices and the physical world. The other part of this interface is represented by actuators, which convert electrical signals into physical phenomena [29]. For the purposes of IoT, electronic sensors, chemical sensors, and biosensors frequently act as interfaces between the virtual world and the physical world [30]. Sensor data is processed, analyzed, and then provided to the actuators that use this information to influence the physical world environment. The data generated by sensors are transmitted to other electronic devices by a variety of means: wired and wireless, long or short range, high or low power, high or low bandwidth. Ultimately, these collected data are stored in cloud platform for further analysis.

^{15]} <https://www.incognito.com/blog/iot-and-m2m-whats-the-difference/>

	Geographically fixed	Geographically mobile
Geographically dispersed	Application: Smart city, smart meter, smart grid and remote monitoring	Application: Logistics, car automation, eHealth, portable consumer electronics
	Technology required: Public Switched Telephone Network (PSTN), broadband, 2G/3G/4G, power line communication (PLC)	Technology required: 2G/3G/4G, satellite
Geographically concentrated	Application: Smart home, factory automation, eHealth	Application: On-site logistics
	Technology required: Wireless personal area networks (WPAN), wired networks, indoor electrical wiring, WiFi, RFID, NFC	Technology required: WiFi, WPAN

Table 7: M2M applications and technologies by geography and mobility [31]

2.2 IoT application structures and driver technologies

Figure 6 illustrates common approaches to build IoT applications. Vertical approach is largely used in existing ICT infrastructure, where each application is built on its proprietary ICT infrastructure with dedicated devices and managing services, thus resulting in unnecessary redundancy and increase of cost. As an alternative to this approach, a more flexible horizontal approach is suggested [9], where applications will no longer work in isolation, but will share infrastructure, environment and network elements, and a common infrastructure platform will manage the network and the applications. This common platform will abstract across a diverse range of data sources to enable applications to work properly according to the current expectation of the smart environment [32].

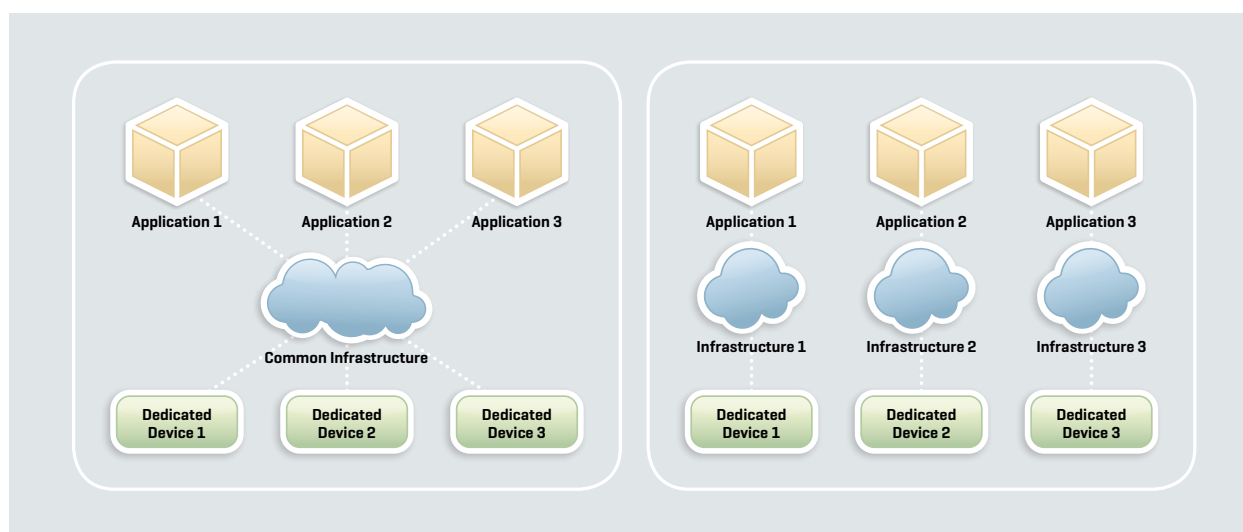


Figure 6: IoT application approach

The IoT environment is driven by technologies shown in Figure 7. These technologies could be classified in three groups supporting the three main phases of data handling in IoT environment, namely data collection phase, data transmission phase, and application phase, including data processing, managing and utilization.

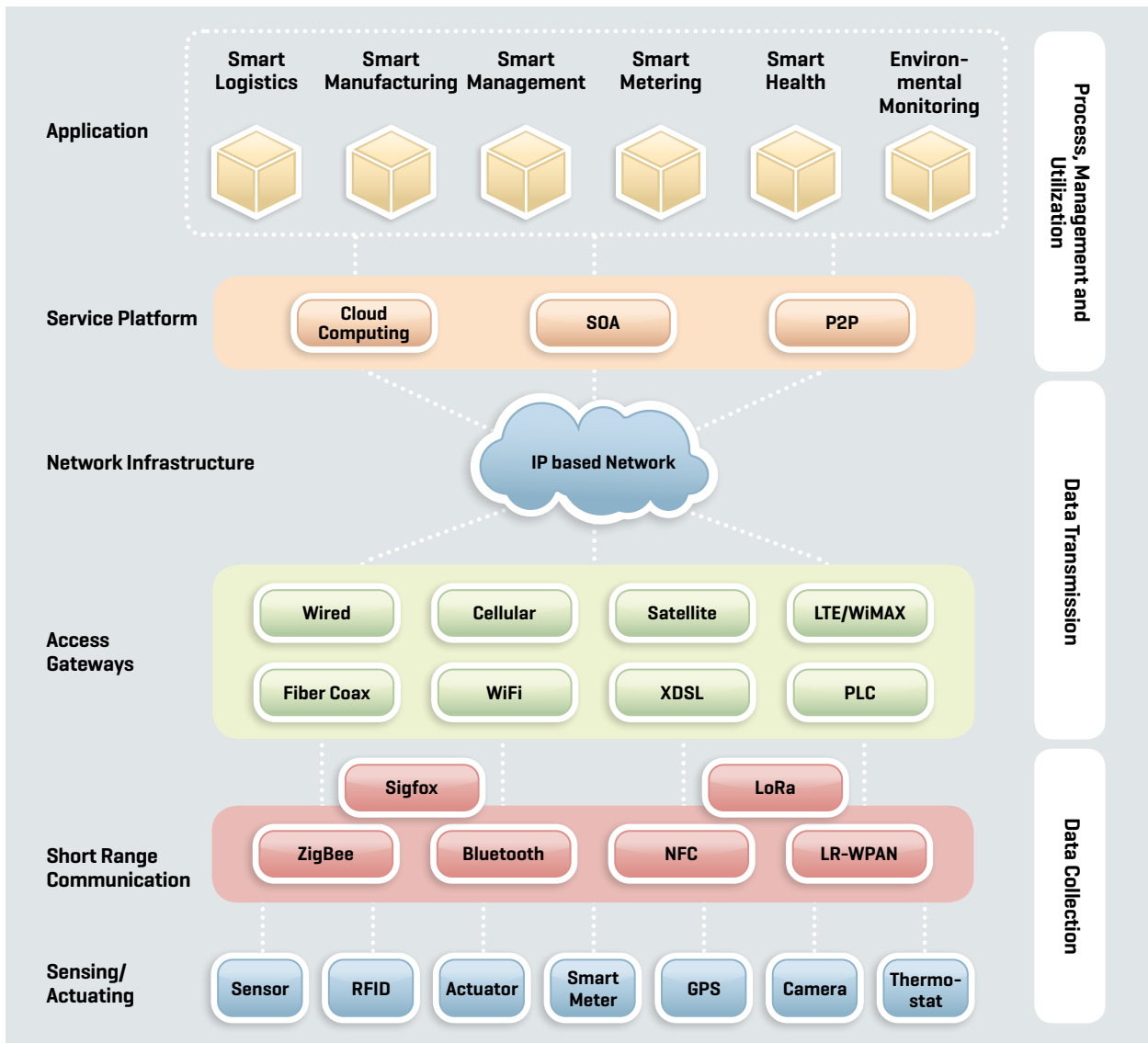


Figure 7: Data flow in IoT environment [9]

2.2.1 Collection phase

This phase corresponds to the procedures for sensing the physical environment and collecting real time physical data. The first step in IoT environment is the collection of information (or data) from the physical environment (things), such as temperature, humidity level, identity, state, etc. As shown in Figure 7, this information could be collected using sensors, RFIDs, actuators, different types of cameras, smart meters, GPS terminals and thermostats, where sensor networks and RFIDs are the most widely used. The information is collected using short-range and cellular communication technologies, some examples are shown in Figure 7. Classification of these communication technologies with respect to distance coverage and speed is shown in Figure 8. Short-ranged communication technologies such as **Bluetooth**, **ZigBee** and **NB-IoT** are open source standard solutions whereas **Z-Wave**, **ANT** are proprietary. Covering longer distance **Sigfox** and **LoRa** are non-cellular technologies, whereas **NB-IoT** and **LTE-M** represent cellular networks. Basic characteristics of commonly deployed short range standard technologies are shown in Table 8.

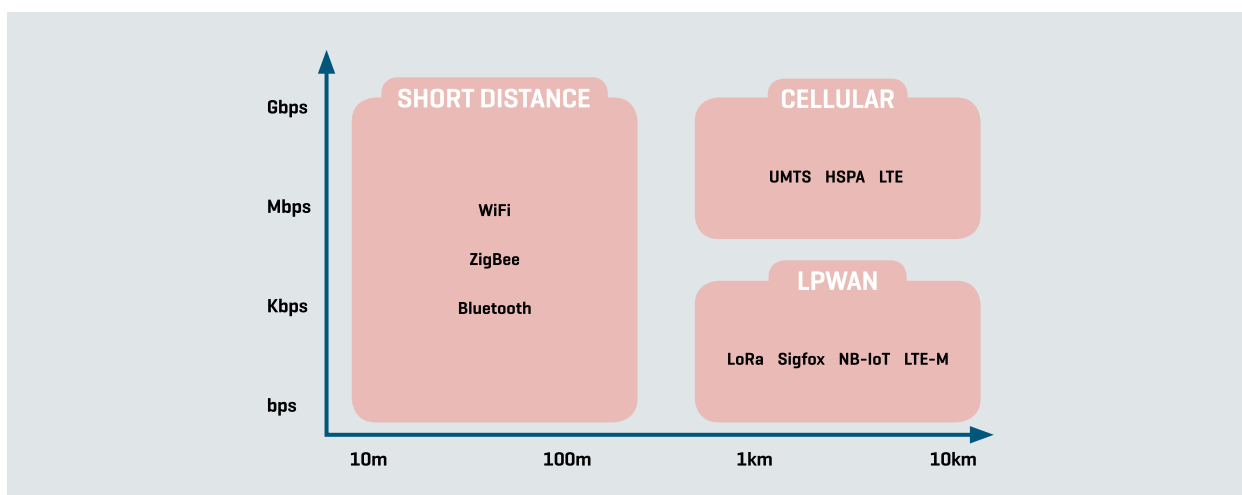


Figure 8: Short distance vs. long distance communication technologies

Technology	Device used	Capabilities	Data rate	Distance Covered	Reference Standard	Example(s) of application(s)
RFID	Book tag, car-sharing cards, RFID passports, RFID badge	Identification, storing, communication	Up to 640 kbps	3–10 m	ISO/IEC 18000	Logistics, transportation, tracking, animal ID, retail, access control, payment
Sensors	Environmental monitoring sensors, wearable sensors, digital cameras	Sensing, storing, processing, communication	250 kbps	10–100 m	LR- WPAN, ZigBee, Wireless HART	Monitoring, intelligent agriculture, surveillance
NFC	Smartphones, ticket stamping machine, parking meter	Communication	106– 424 kbps	<10 cm	ISO/IEC 18092/ECMA-340, ISO/IEC 21481/ECMA-352, ISO/IEC 14443	Sharing/access information, access control, contactless payment
Bluetooth	Smartphones and many other mobile devices	Communication	1– 24 mbps	<150 m	Bluetooth Core Specification Version 4.0 (or higher)	Health and fitness, and in medical monitoring

Table 8: Technology references in data collection phase in short range [33]

The **RFID** has two main types of tags: passive and active. Passive tag can transmit data by using the energy that the reader emits during its passage. Cost wise, they are very affordable since they are very small, inexpensive and have potentially long life. The main drawback of passive tags is that the area in which the tag-reader transmission can take place is limited to 3 m [34]. On the contrary, active tags cover higher distance thanks to their integrated power supply. They also can perform operations that are more complex. Normally, four frequency bands are

used for the transmission of signal between tags and readers: Low-frequency (LF) operating in the 125/134 kHz and 140/148.5 kHz ranges, High-frequency (HF) operating at 13.56 MHz, Ultra-high frequency (UHF) operating at 915 MHz (US) and at 868 MHz (Europe), 2.4 GHz and higher (Microwave tags) [9].

Wireless sensor networks (WSNs) are other essential technologies for collecting data in IoT environment. These networks are well known for gathering and processing data in a large variety of domains, from environmental monitoring [35] to intelligent agriculture [36]. Regardless the network topology, sensors mainly operate in the 2.4 GHz band with a rate of 250 kbps to exchange data. The commonly used standards in WSN communication include LR-WPAN [37], ZigBee [38], Wireless Highway Addressable Remote Transducer Protocol (HART). In the IoT world, the sensor networks exploiting the LR-WPAN standard for energy-efficient wireless communications [37] can play an important role for saving power.

NFC technology is similar to RFID but allows bidirectional communications. Specifically, when two NFC devices are located at a distance smaller than 4 cm, a peer-to-peer communication between them is created, and both devices are allowed to send and receive data. NFC operates within the globally available unlicensed radio frequency ISM band of 13.56 MHz on ISO/IEC 18000-3 air interface at rates ranging from 106 to 424 kbps (Table 8).

Finally, **Bluetooth** technology is also used for sending data among devices located at a short distance. Bluetooth systems operate in the 2.4 GHz band with original data rate of 1 Mbps up to the most recent possible rate of 24 Mbps. It was originally designed to replace wired communications with low power wireless communications. The communication structure using Bluetooth is called piconet [39]. In it, a device assumes the role of master and all the others are slaves, for a maximum of seven slaves. The master decides which slave may access the channel. The new Bluetooth Low-Energy (BLE), also called Bluetooth Smart¹⁶, is a significant protocol for IoT applications. Technically speaking, it offers similar range to Bluetooth and has been designed to offer significantly reduced power consumption.

With the rapid growth of connected devices IoT landscape, low power wide area networks (LPWAN) have become a popular low-rate long-range communication technology [40]. **NB-IoT, SigFox, LoRa, LTE-M** are some leading LPWAN technologies that compete for large-scale IoT deployment, are highlighted in Table 9.

Technology	Governing body	Frequency + Band	Mobility	Data rate (downlink)	Data rate (uplink)	Deployment status
NB-IoT	3GPP	7- 900 MHz licensed or shared	Yes	150 kbps (NB) < 1Mbps	150 kbps (NB) < 1 Mbps	Planned
SigFox	SIGFOX	ISM; 865 -868 / 902 - 928 MHz	No	4x8b/day	100 bps	Deployed since 2009
LoRa	LoRa alliance	ISM; 433/868 (EU) / 780/915 (USA) 902 MHz	No	EU: 30 bps - 50 kbps US: 100 - 900 kbps	EU: 30 bps - 50 kbps US: 100 - 900 kbps	Planned
LTE-M	3GPP	In-Band LTE	Yes	Up to 1 Mbps	Up to 1 Mbps	Planned

Table 9: Technology references in data collection phase in long range

¹⁶ <https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about>

2.2.2 Transmission phase

In the next phase, data collected through sensing needs to be transmitted to the service platform across the network so that applications can access this data. Methods are required for accessing the network through access gateways and heterogeneous technologies. Communication technologies used as major access networks are highlighted in Table 10.

The reference standard among the wired technologies, **Ethernet (IEEE 802.3)**, supports transmission speed from 10 Mbps to 100 Gbps over twisted-pair coppers, coaxial cables, and optical fibers. In wired networks, the need to physically connect devices results in high cost and difficulties in case of changing places. On the other hand, wired networks are the most reliable and robust as they are less susceptible to errors and interference phenomena. Their coverage ranges from 100 m to up to 70 Km.

Among wireless communication technologies, the most common way to access the network is through wireless local area network (WLAN) [41]. There are several wireless technologies with different covering distance and different transmission speed. The **WiFi family (IEEE 802.11a/ b/g/n)** operates in different frequency bands (2.4 GHz or 5 GHz) by implementing different modulation schemes. Data communication rate may reach up to 600 Mbps, supporting distances up to 100 m. To increase the available bandwidth for transmission/reception, the version IEEE 802.11n uses MIMO (multiple-input multiple-output) antennas. IEEE 802.16 family, called **WiMAX**, is the corresponding wireless technologies for the long distances, up to a few kilometres [42]. The frequency band for the WiMAX is 2-66 GHz and its transmission speed can go up to 70 Mbps. This technology is connection-oriented. The broadband technologies, such as **xDSL(x-Digital subscriber line)** are generally used to connect end devices to the internet. The widely used xDSL technologies are asymmetric digital subscriber line (ADSL), ADSL 2+ and very-high-bit-rate digital subscriber line (VDSL).

Another popular access network technology for the IoT is **cellular network**. Global system for mobile communications (GSM), general packet radio services (GPRS), universal mobile telecommunications system (UMTS), high speed packet access (HSPA+) and long term evolution (LTE) networks play a central role in the way of accessing the network. Precisely, recent emerging LTE technologies [42] cover 80 users per sector/MHz (Frequency division duplexing-FDD) and reach up to 300 mbps (downlink)/75 mbps (uplink) maximum transmission speed to provide not only voice services but also other high value services for example.

Satellite communication technologies are used for supporting Internet of Remote Things [43]. They are particularly useful for users located in remote areas who cannot access broadband connections, where deploying terrestrial connection is costly, or as a way to cross the sea/ocean [9]. Basically, a satellite receives a transmission on a frequency band, regenerates the signal, and transmits it over another frequency band. The main drawback of this technology is a propagation delay of 280 ms that is introduced due to the large Earth-satellite distances.

Power line communication (PLC) is another communication technology that carries data by exploiting the electrical power line [44]. Normally, it is applicable for home area networks (HAN) as well as smart meters, but can be considered as an alternative to xDSL providing asymmetrical transmissions (i.e. 2.7 mbps in download and 256 kbps in upload). The significant drawback of this communication technology is the mutual interference among PLC and other technologies, such as radio interference with signals on amateur radio frequencies.

Technology Reference	Standard	Transmission medium	Frequency bands	Data rate	Maximum distance	Limitations
Ethernet u/z	IEEE 802.3	Twisted-pair copper wire, coaxial cable, optical fiber	-	10 mbps to up to 100 gbps	100 m to up to 50–70 km physical connection	Share medium, physical connection among devices
WiFi	IEEE 802.11 a/b/g/n	Wireless	2.5 GHz to 5.0 GHz	up to 600 mbps	up to 100m	Sensitive to the presence of household appliances, interference among WiFi communications
WiMAX	IEEE 802.16 a/d/e/m	Wireless	2–66 GHz	up to 70 mbps	Up to 50–80 km	Low practical data rate, sensitive to weather conditions, high installation and operational costs
xDSL	ADSL, ADSL 2+, VDSL	Twisted-pair, copper wire, coaxial cable	Up to 2.2 MHz	12–55 mbps (d) 1–20 mbps (u)	5.4–1.3 km	Asymmetrical communication
Cellular	GSM, GPRS, UMTS, HSPA+, LTE	Wireless	900–1800 MHz 2100–1900 MHz 800–2600 MHz	9.6 kbps, 56–114 kbps, 56 mbps (d)/22 mbps (u), 300 mbps (d)/75 mbps (u)	Macro/micro/pico/femto cells (10 m to 100 km)	Limited wireless Spectrum
Satellite	BSM, DVB-S	-	4–8 GHz (C band), 10–18 GHz (Ku band), 18–31 GHz (Ka band)	16 kbps to 155 mbps	GEO sat.: 35,786 km, MEO sat.: 500– 15,000 km, LEO sat.: 200–3000 km	280 ms propagation delay, huge launching cost, almost impossible repairing
PLC	HomePlug AV, IEEE 1901	Electrical power system	1–30 MHz	>100 Mbps	Up to 1500 m to the premises up to 100 m between devices	Mutual interference with other technologies

Table 10: Technology references in data transmission phase [9]

2.2.3 Processing, managing and utilization phase

In the last phase of data flow in IoT environment, information is processed and then forwarded to the applications. This phase is responsible for abstracting all the features from objects, networks, and services, and offering a loose coupling of components including service discovery and service composition. One of the major challenges in IoT being to combine heterogeneous service [45], the middle layer service platform plays a crucial role in managing these operations [46].

Adoption of **cloud computing** supports the realization of the full potential of IoT. Generally speaking, cloud is used for the delivery of hosted services over the internet. It gives easy access to virtualized resources, such as a virtual machine (VM) or an application, which can be dynamically allocated without any human intervention. Once in the cloud, the data collected from IoT can be easily accessed by different applications. However, in order to access the cloud to store and retrieve data, IoT objects need to be connected to the internet. Limitations of cloud computing technology in IoT scenario and possible alternative computing techniques are introduced in Section 2.3.

Service-oriented architecture (SOA) is another concept that can be applied for combining heterogeneous service technologies in a single network. Normally, the SOA concept relies on three layers, each responsible for different functionalities [9], [32].

- The first layer is responsible for objects abstraction, i.e., every object or a single functionality implemented by an object is abstracted to represent as a service. In addition, it offers semantic descriptions and procedures to access the objects.
- The second layer is responsible for the services management, providing a way to automatically and dynamically discover them, monitor them, and make their status public. Additionally, it is responsible for remote management of the services, and for maintenance of a correspondence between objects and the services available on them.
- Finally, the third layer provides composition mechanisms for new services, i.e., how to form dynamically and in real-time the new services from a single or set of basic services. Additionally, a repository of services ensures an overall updated view of recently connected instances of service.

Peer-to-peer (P2P) systems [47] represent one of the most important content-centric internet technologies. Notably, peer-to-peer systems are applicable in IoT to implement efficient discovering mechanisms for available capabilities and resources. Many peer-to-peer systems rely on distributed dash tables (DHT) to guarantee the communication flow between peers. DHT are the most promising due to a set of properties they exhibit, such as efficiency, scalability, resilience to node failures, etc.

2.2.3.1 High performance computing [HPC] for IoT

Smart building management, smart mobility, smart logistics and smart manufacturing are some examples of applications using a combination of **IoT and HPC infrastructures**. Indeed, HPC is at the center of progress and innovation in the digital age because it drastically advances the processing ability.

Recently, HPC applications have started to use cloud by various service providers. It is not yet clear what type of HPC-Cloud combination (**cloud HPC or HPC in cloud**) will prevail in the future, but HPC as a service, like many other services in the cloud, would certainly be the major processing technique for the IoT [48].

In Luxembourg, the government supports the development of innovative applications on **HPC and Big Data** to improve the everyday life of the citizens and to strengthen the national economy [49]. The **Third Industrial Revolution of Luxembourg** aims at transforming all industrial sectors into Digital and Smart¹⁷, using Big Data and HPC as one of the means to achieve this goal. The most prominent areas considered in this regard are

¹⁷ <http://www.troisiemerevolutionindustrielle.lu/>

space, personalized medicine, Industry 4.0, Fintech, smart energy, smart mobility, and Smart City. Luxembourg looks forward to become a digital pioneer in Europe in coming years thanks to its policy (Table 11) based on the opportunities offered by the digital transformation:

- World Class HPC & Big Data enabled Hub and Ecosystem;
- Digital -data -friendly regulatory environment;
- Competitive digital advantages in key strategic sectors.

Recognizing the importance of societal and economic benefits that can be derived from HPC enabled applications, France, Italy, Spain and Luxembourg launched an Important Project of Common European Interest (IPCEI¹⁸) aiming to develop and implement next-generation HPC and Big Data technologies and applications to improve the European position in a global digital market [50].

Investment in computing infrastructure	<ul style="list-style-type: none"> ● Initiation of European IPCEI for HPC and Big Data ● Building-out the Luxembourg HPC Ecosystem ● Early access to HPC Capabilities ● Delivering national HPC capabilities ● Enabling the Third Industrial Revolution
Trusted cloud	<ul style="list-style-type: none"> ● Trusted world-class cloud and data infrastructure to be used by Luxembourg companies with wide computing and data handling capacities
Cross-border collaboration	<ul style="list-style-type: none"> ● To support cross-border collaboration on innovative digital experimentation activities, such as HPC and Big Data enabled Testbeds
Addressing regulatory challenges	<ul style="list-style-type: none"> ● To address new regulatory challenges arising from digitization of the industrial fabric, such as privacy issues on data generated from new smart products, or liability of autonomous system

Table 11: The strategy of Luxembourg with major policy and action levers [50]

The objective of the IPCEI initiative is to set-up a secure and trusted pan-European HPC and Big Data ecosystem with the following specific advantages for companies relying on advanced digital technologies [50]:

- State-of-the-art HPC and Big Data enabled infrastructures;
- Low latency and ultra-fast international and national connectivity;
- World-class data centers;
- Preinstalled storage and processing power;
- Specific provision for time-sensitive workloads through real-time computing systems;
- Validating new data driven applications and services using real-life test beds; and
- Fully compliant e-infrastructures respecting the European General Data Protection Regulation (GDPR).

¹⁸] http://europa.eu/rapid/press-release_IP-14-673_en.htm

Figure 9 depicts the smart space – mobility application project, a result of collaboration between the countries involved in the IPCEI in these domains [51]. This project is an example of realization of overall IoT architecture demonstrating:

- how environments will be monitored or sensed through sensing techniques;
- how data are transmitted using communication network; and
- how data are processed to implement predictive decision support systems by particular application.

The connected vehicles or connected cars will be equipped with a large number of sensors, embedded cameras, in-car computers, high precision GPS and satellite receivers, 5G interfaces and short range wireless network to connect to the internet. The vehicles, IoT road sensors, satellite receivers and other sensors exchange data with management and supervising systems to sync up with large databases that constitute a real-time source of information about the local environment, traffic situation, weather conditions, and emergency alerts. HPC and Big Data platform is required to manage all this data that will be used to analyze the geographical position, road condition, state of vehicles, passenger safety and comfort. This data would be also used by predictive driving functions to avoid road hazards and increase passenger safety.

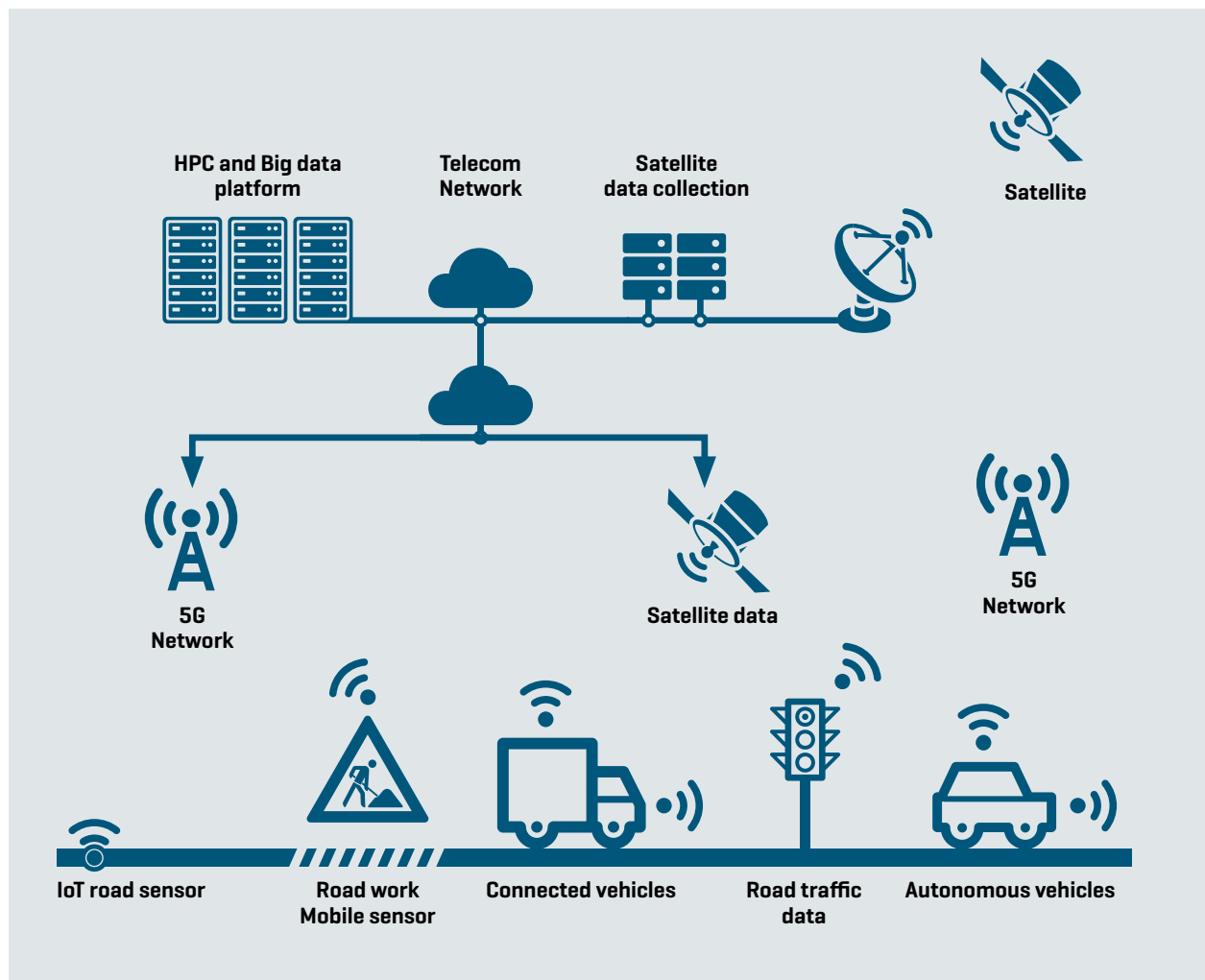


Figure 9: HPC for smart space -mobility application [51]

2.3 The concept of Edge, Fog and Roof computing in IoT

Despite the increasing usage of cloud computing in all sector, there are still unsolved issues due to its inherent problems, such as lack of mobility support, unreliable latency and location awareness [52]. The cloud computing technology is more about providing distributed resources in the core network. Recent computing technologies such as Edge, Fog, and Roof computing can address those problems by providing elastic resources and services to the end users at the edge of the network. This section introduces these three computing technologies in the context of IoT and compares them to cloud computing paradigm.

2.3.1 Edge computing

The **edge** typically consists of sensors, controllers, actuators, tag and tag readers, communication components, gateways and the physical devices [14]. In fact, it is a method of **optimizing cloud computing systems** by performing data processing at the end/edge of the network, near the source of the data, integrating network, computing, storage, and application core capabilities and providing edge intelligent services [53]. It mainly reduces the communications bandwidth needed between sensors and the central data centre by performing analytics and knowledge generation at or near the data source. This approach leverages resources that might not be continuously required to be connected to a network such as smartphones, laptops, tablets and sensors. Edge Computing Consortium (ECC)¹⁹ highlights three major phases to understand the development of edge computing as:

- **Connection:** Numerous heterogeneous, real-time connections between terminals and devices, as well as automatic network deployment and operation and maintenance (O&M) will serve edge computing. As an example, a remote automatic meter reading connected to millions or even tens of millions of electric meters can be considered as a typical application in this phase. In this context, interoperability, security, and reliability of connections should be guaranteed.
- **Smart:** Data analysis and automatic service processing capabilities are applied to the network edge smartly. This capability significantly improves efficiency and reduces costs of data processing. Predictive maintenance of elevators can be considered as a typical application of this phase.
- **Autonomy:** This phase is enabled by recent emerging technologies such as Artificial Intelligence (AI) making possible intelligent automation at the edge. Some examples of such intelligent services include implementing dynamic real-time self-optimization, executing policy adjustments, etc. An unattended factory is a typical application of this phase.

2.3.1.1 Typical Edge Environment in IoT

The **things** in the IoT could be represented by any devices (e.g. physical devices) or entities (e.g. human entities), but all these “things” share a common attribute regardless of the domain in which they reside. Namely, the **things** contain some sort of computing power, either embedded in the physical devices or attached in the form of their actuators or controllers [14]. Most often, physical devices are connected directly to the other physical devices, edge platforms, gateways or to another IoT system. Figure 10 shows typical edge environment in IoT applications. The edge can be as small as a single physical device directly connected to a platform or as big as manufacturing plant comprising all the equipment. Independent local area networks capable of connecting elements in edge gateway or hub act as edge communication media to connect with large networks or cloud based platform. Edge hub is also capable to work offline. Data collected while offline can be uploaded when it is connected. To reduce

¹⁹] <https://www.iotaustralia.org.au/wp-content/uploads/2017/01/White-Paper-of-Edge-Computing-Consortium.pdf>

the volume of the data transfer, edge platform can also store data locally. Edge processing is limited to the needs of edge components functionality [14].

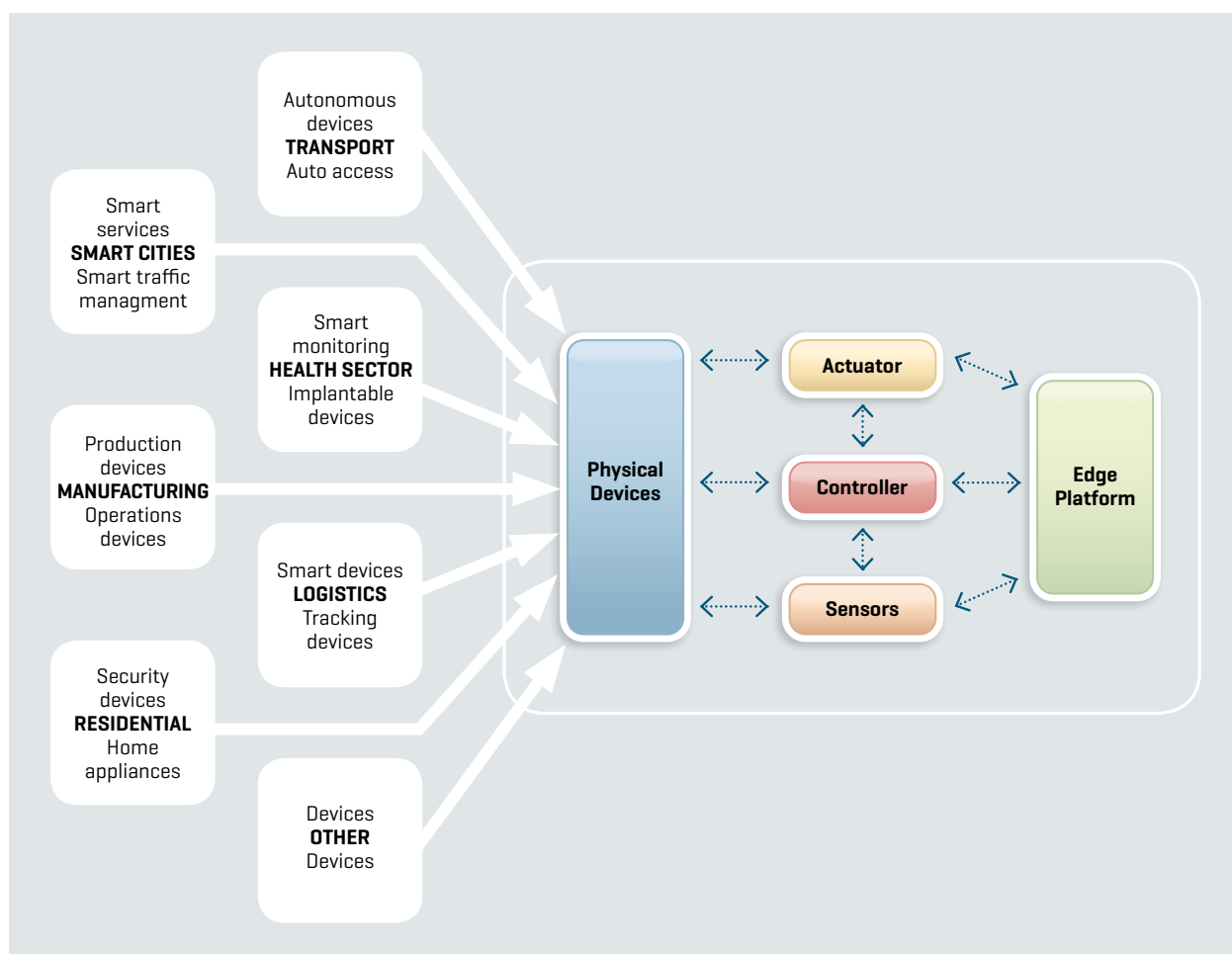


Figure 10: Typical Edge environment in IoT application [14]

2.3.2 Fog computing

Fog computing is considered as an extension of the **cloud computing paradigm** from the core of network to the edge of the network. It accelerates awareness and response to events by eliminating a round trip to the cloud for analysis [54]. It avoids the need for costly bandwidth additions by offloading gigabytes of network traffic from the core network. It also protects sensitive IoT data by analysing the data where it is (i.e. without moving it outside the company). It is a highly virtualized platform to provide computation, storage, and networking services between end devices and traditional cloud servers [52]. The basic characteristics of fog computing are: i) low latency and location awareness; ii) wide-spread geographical distribution; iii) mobility; iv) very large number of nodes, v) predominant role of wireless access, vi) strong presence of streaming and real time applications, vii) heterogeneity. Such characteristics make the fog computing the appropriate platform for a number of critical IoT services and applications, namely Connected Vehicle, Smart Grid, Smart Cities, and, in general, Wireless Sensors and Actuators Networks (WSANs) [55]. The OpenFog²⁰ defines fog computing that as *a system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things.*

^{20]} <https://www.openfogconsortium.org/>

Fog and edge computing in IoT applications are system and network architectures that attempt to collect, analyze, and process data more efficiently than traditional cloud architecture²¹. Both computing technologies involve placing intelligence and processing capabilities down closer to the edge of the network where the data originates. The key difference between the two architectures is where that intelligence and computing power is placed. Fog computing pushes intelligence down to the local area network (LAN) level of network architecture, processing data in a fog node or IoT gateway. Edge computing pushes the intelligence, processing power, and communication capabilities of an edge gateway or appliance directly into devices like programmable automation controllers (PACs). In the comparisons table (see Table 12) of these technologies over cloud computing, fog and edge computing are considered to possess similar characteristics.

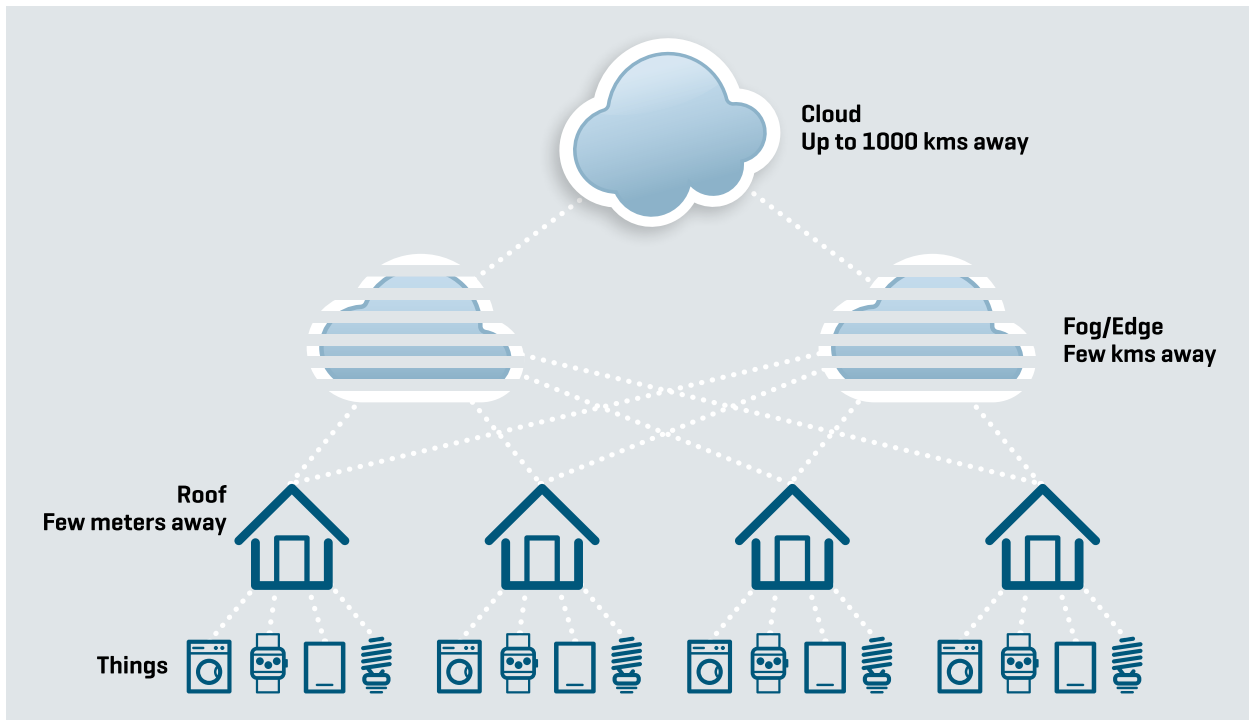


Figure 11: The Roof federated architecture²²

2.3.3 Roof computing

Roof is a recent federated networking and computational paradigm for the IoT available for **Real-time Onsite Operations Facilitation (ROOF)**. This includes next-hop connectivity for the things, real time context building and decision triggers, providing efficient data connectivity to the service/cloud providers, and always-on security²². Standard for an Architectural Framework for Real-time Onsite Operations Facilitation (ROOF) for the Internet of Things²³ originates from the IEEE project P1931.1 working on Roof computing and networking for the data and the devices. The project is expected to cover interoperability, collaboration and autonomous operation of an IoT system with computing required for context building, security, access control, data storage, data aggregation and ability for choosing different application and cloud service providers. In addition, this project is also expected to define how an end user is able to securely provision, commission and decommission the devices. The main objective of this standard is to leverage existing applicable standards and to provide complimentary architectural frameworks defined in broader IoT environments.

²¹] <http://info.opto22.com/fog-vs-edge-computing>

²²] <https://electronicsforu.com/technology-trends/must-read/the-roof-computing/>

²³] <https://standards.ieee.org/develop/project/1931.1.html>

The Roof can be applied in home routers, IoT gateways, mobile phones, personal computing platforms and other embedded platforms that can act as proxy of the things for connectivity to the cloud and the network. Figure 11 reflects the traditional federated architecture that is being practiced since the widespread of Internet. In this architecture, the Roof is a fixed network element that is always reachable as the first hop of the communication channel. It allows strong secure network architecture and enhances robust connectivity to the cloud by providing the things with the required storage and processing capabilities. The Roof bridges the physical world and cyber world by connecting the things and systems to the cloud and building cyber system for the respective physical systems, thus creating highly scalable cyber physical systems for the IoT.

Consideration	Cloud computing	Edge/fog computing	Roof computing
Latency	High	Low	Low
Delay jitter	High	Low	Very low
Location of service	Within the internet	At the edge of local network	At the roof top
Distance to things	Up to thousands of kms	Few kms	Few meters
Deployment numbers	In hundreds	In tens of thousands	Millions to billions
Security	Undefined	Can be defined	Defined
Location awareness	No	Yes	Yes
Implementation cost	Low	High	Medium
Content	Machine data	Internet fringe	Big Data
Drivers	Big data storage and analytics	Support for mobility and to reduce the latency	The things – constrained devices
Applications	Big data storage and analytics	Large distributed IoT applications	Context aware real-time applications

Table 12: Cloud vs. Edge/Fog vs. Roof^{24]}

^{24]} <https://websprout.in/the-roof-computing/>

3

Internet of Things - Challenges

3. Internet of Things – Challenges

IoT promises important benefits in different domains (such as societal, government, economic, research), and it offers numerous, and potentially revolutionary opportunities to the users. Some noticeable opportunities are highlighted in Table 13. The strength of the IoT is powered by different supporting technologies with their distinctive characteristics for the specific applications. However, it is also a source of limitations and challenges.

Cloud based applications	The cloud based secured and flexible smart environment results in cost-effective applications of IoT. The data collected from different environments is analyzed in the cloud server for making decision and prediction of environment parameters.
New business models and diversification of revenue streams	The IoT enables new business opportunities through multiple revenue streams empowering numerous business models. It can radically change the way of approaching customers in the business using smart applications on top of the traditional applications. For example, vending machine providers can also offer an inventory management tool for those who supply goods to refill the machine.
Real-time information	The ability of gathering real-time information from the environment helps organizations to react immediately according to the expectations of the customers. For example, organization can utilize real-time information of product and services in decision making to adapt and improve the operational efficiency and thus reach higher customer satisfaction.
Intelligent operations	The use of intelligence in the smart environment using IoT technologies results in optimal use of resources and maximization of benefits to the organizations. For example, application of machine learning and artificial intelligence in businesses can provide intelligent operation management in the work.

Table 13: IoT opportunities [56]

This chapter describes the challenges of IoT from technological (Section 3.1), security, privacy and trust (Section 3.2 and Section 3.3), regulatory (Section 3.4), and standardizations gaps (Section 3.5) perspectives. The focus of the chapter would be in addressing the most prominent issues among many challenges facing by IoT technology.

3.1 Technical challenges

3.1.1 Interoperability

Interoperability can be considered in various prospects, such as **ability to communicate**, ability to **exchange** the data, and ability to **understand the meaning of exchanged** data between different smart IoT systems or smart environments [56]. Interoperability is one of the critical challenges for IoT technology, where multiple products of different vendors are connected to each other. Indeed, in the current context, most of these products are unable to connect to each other **due to lack of common universal language**. Most of the time, producers or vendors use different communication protocols making it difficult for connecting devices to communicate and exchange data. For example, the products connected in a smart home network, such as refrigerator, microwave, etc. might be the products of different vendors using completely different interconnecting coding. Addressing this challenge necessitates collaboration among multinational vendors in order to design universal interconnecting

coding language and communication infrastructure irrespective of products and vendors specificities. At the same time, this challenge in IoT reflects a **need for standards** allowing the required collaboration of connected devices in smart environments.

3.1.2 Precision

Many IoT based smart environments, and number of devices and their networks are connected worldwide, where precision is one of the critical challenge that need to be addressed [56]. The time is very important in **precision machines** used in very sensitive areas, such as for health and safety of the operators, machine and related business where it will be the cause of danger if timing is off by a millisecond. It is directly or indirectly related with the network latency and available bandwidth in distributed **delay-sensitive environments**. For example, in regards to vehicle-to-vehicle communication in automated smart cars, higher network latency may cause delay in applying car brakes, which may result very risky in life of the people and safety of the car itself.

3.1.3 Data volume and scalability

As mentioned in Section 4.1, **billions of things** (that is about 500% increment in data storage due to additional connected things to the internet) are expected to be connected with each other in coming years [57]. These billions of connected things will generate large amounts of data from different IoT environments. Such important data volumes will require highly scalable computing platforms capable to manage data in terms of collecting, storing, accessing and processing without affecting the performance of the entire application.

Gartner²⁵ predicts that by 2020, 80% of all IoT projects will be a failure at their implementation stage due to **improper and insufficient data collection methods**. In order to avoid such a situation, industries require effective IT system to support the scale of IoT environment. Chapter 2.3 introduced new processing technologies allowing data processing outside the data center combined with massive post-processing at core data center or in the cloud [14]. Another effective solution is a web-scale IT, defined by Gartner as a system-oriented architectural pattern that would enable the rapid and scalable development and delivery of web-based IoT services to the users, where current IoT lacks such web-based capabilities.

3.1.4 Internet-connectivity

The IoT demands flawless and **adequate level of connectivity** among the things. Fast internet speed, robust backup systems, a continuous power supply, scalable and reliable network infrastructure are the key elements of flawless connectivity. The lack of adequate level of connectivity among the connected devices could impact the overall performance of the IoT system. On the other hand, especially in remote areas, limited internet access may cause those areas to be excluded from the IoT system.

²⁵] <https://www.gartner.com/doc/3234018/infrastructure-operations-leaders-prepare-iot>

3.2 Security, Privacy and Trust issues

A secured environment is a **fundamental requirement of IoT**. This requirement covers technological, privacy and ethical aspects. An appropriate level of security of an IoT system will foster users' trust. Security, privacy and trust become particularly challenging issues when the **things** are connected to the global network [3]. Indeed, IoT systems rely heavily on wireless networks, which are well known to be affected by all types of intrusions [58], such as faulty configurations, unauthorized access of routers, interference, jamming, man in the middle attacks, spoofing, DOS attacks, traffic injections, brute-force attacks.

Different sets of requirements were identified in the literature that should guarantee the security of an IoT system (see Table 14). Depending on specific application, all or part of these requirements should be satisfied. Globally, confidentiality, integrity, authorization, authentication, non-repudiation, and availability [59] are the key properties of a secure IoT system. Confidentiality, integrity and availability are particularly important in the context of data exchange between IoT devices.

Set 1 [9]	Set 2 [60]	Set 3 [61]
<ul style="list-style-type: none"> Secure authentication and Authorization, Secure boot strapping of objects and transmission of data, Security of IoT data, Secure access to data by authorized persons 	<ul style="list-style-type: none"> Data authentication, Access control, Attack resiliency, User Privacy 	<ul style="list-style-type: none"> Authentication and access control, and key management, and appropriate secret key algorithms, Secure routing protocols, and intrusion detection technology, Physical security design

Table 14: Set of security requirements

In the rest of the section, the security challenges of an IoT system arising from the adoption of different technologies at each layer of the IoT architecture will be addressed.

3.2.1 Security vulnerabilities in overall IoT system

Having every **things** connected to the global internet infrastructure and **things** communicating with each other brings many security and privacy problems in the overall ecosystem [62]. However, many identified challenges could fit in the frame of the original triad for information security, namely confidentiality, integrity and availability.

- **Confidentiality** is a fundamental challenge for the IoT system as data are generated from various sources and the system access these data dynamically. Proper management of data sources and a capability to handle the classified data from specific device are the key factors to assure confidentiality of the data in IoT system. Current solutions to guarantee confidentiality may not be applicable [3], mainly due to two reasons: big volumes of generated data sources and lack of effective control over dynamically streamed data. Various encryption schemes can be applied to obtain the confidentiality of the communication channel; however, current systematic and asymmetric algorithms should be updated before implementing in IoT based applications [63].

- **Integrity** deals with the first damages or failures of physical devices. Integrity protection includes preservation against sabotage and use of the countermeasure components to protect the device and sent data. Data integrity in IoT system will rely on the robustness and fault tolerance of the entire system. Integrity of the IoT system can be affected by internal and external source as well as by internal process. For example, in sensor networks, many RFIDs remain unattended most of the time. This gives an opportunity to external attackers to either modify data while storing it to the node or while transferring it to the network [3]. Read and write protection using password might be the possible way out to strengthen the integrity of the systems caused by external and internal sources of attacks. Multilevel security (MLS) helps to avoid unauthorized modifications due to internal process, such as malicious running code. A trusted platform module (TPM)²⁶ is another hardware solution proposed for integrity challenges.
- **Availability** of IoT system is highly tied with reliability requirements [64]. To sustain required level of availability, the IoT system should show the levels of performance requested by the application. The adequate level of hardware and software performance used in the IoT network should be able to cope with the requirements of the users. Software availability is the ability of applications to provide the service to everyone at any location simultaneously. Hardware availability refers to the presence of the device all the time. One example of availability challenge could be demonstrated by denial of service (DOS) attack. DOS attacks prevent devices to access resources from the network. Commands for DOS attack can be generated remotely to obstruct the IoT system. DOS attacks in IoT may concern not only the traditional vectors, for instance resources of providers, bandwidth, etc. but also they can affect the data acquisition of wireless communication from IoT node [64]. Moreover, some constrained devices connected in IoT system that may affect the availability in the network, similar to the effect of DOS attacks [65]. Implementation of distributed architecture rather than a centralized one can help to improve the availability of the IoT system [64].

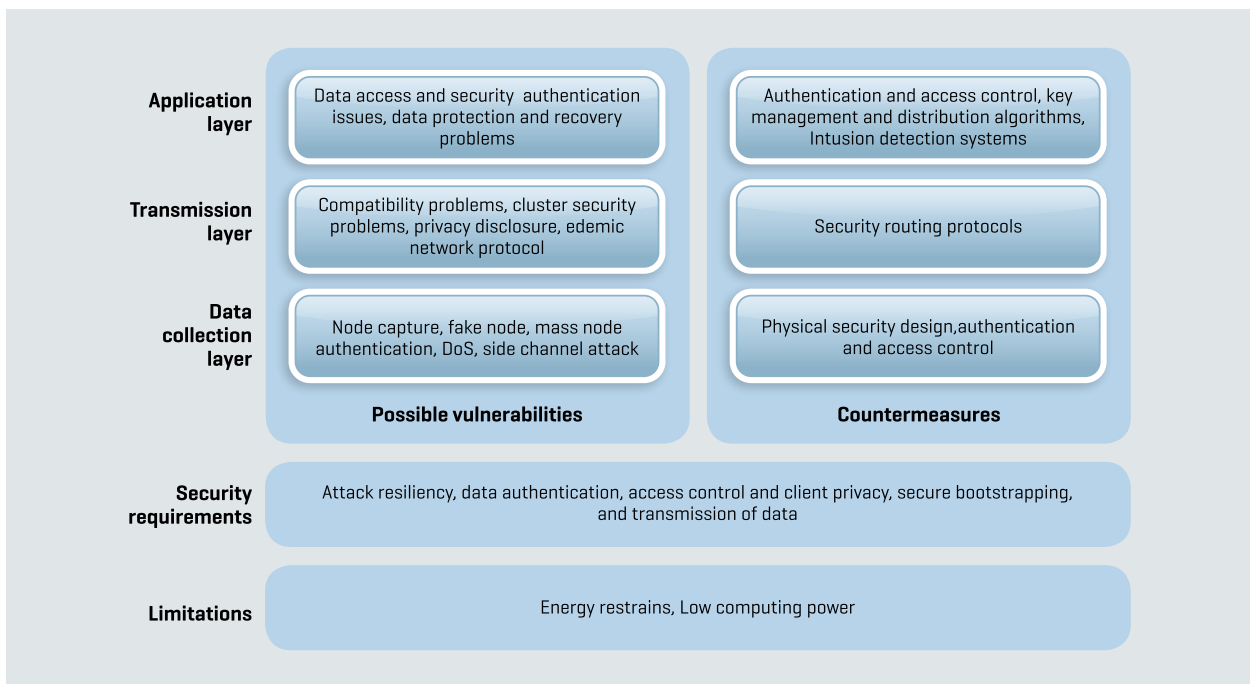


Figure 12: IoT security concept [66]

The IoT security landscape can be realized by its architectural perspective: collection, transmission and application layer [3]. Each layer has own and common security issues that need to be addressed to make a secure IoT system. Some envisions of security concerns [66], in each layer of IoT architecture (Figure 7 in Section 2.2) are highlighted in Figure 12.

²⁶] <https://trustedcomputinggroup.org/>

3.2.2 Security vulnerabilities at different layers of IoT architecture

This section aims at providing a set of the most important security vulnerabilities at different layers of IoT architecture.

3.2.2.1 Data collection layer

This layer has two components: nodes (sensors or controllers) and networks allowing the communication with transport network [67]. The nodes component relies on various sensing and controlling devices, such as pressure, sound, temperature, vibrations sensors. The networks component rely on different communication protocols. Table 15 presents security risks related to the technologies enabling data collection layer.

Enabling technologies	Security risks
WSN [68], [69]	<ul style="list-style-type: none"> Denial of Service (DoS) attack on different layers of the network, traffic analysis, node replication (Sybil attack), general confidentiality concerns; Black hole routing attacks, physical damage / unauthorized manipulation.
RFID [70], [71]	<ul style="list-style-type: none"> Attacks on authenticity, i.e. unauthorized tag disabling; Attacks on integrity, i.e. unauthorized tag cloning; Attacks on confidentiality, i.e. unauthorized tag tracking; Attacks on availability; Personal privacy risks.
WiFi (802.11x) [72]	<ul style="list-style-type: none"> Passive attacks, such as eavesdropping armed with suitable receiving antennas; Active attacks, such as jamming and scrambling attacks.
NFC [73], [74]	<ul style="list-style-type: none"> Denial of Service (DOS), information leakage, traffic sniffing (eavesdropping) in active mode.
Bluetooth [75], [76]	<ul style="list-style-type: none"> Optional or weak encryption, non-secure default settings, weak PIN use, insecure unit keys, flawed integrity protections and predictable number generation; Man-In-The-Middle attacks, data corruption and DOS.
ZigBee [77]	<ul style="list-style-type: none"> Traffic sniffing (eavesdropping), packet decoding, and data manipulation/injection; Physical device damage and key sniffing attacks.
Z-Wave [77], [78]	<ul style="list-style-type: none"> Attack on hard-coded encryption to unveil the content key to unveil the content; Risk on injecting packets to the key exchange process and take control of the device.
6LoWPAN [79]	<ul style="list-style-type: none"> Physical attacks, such as node tampering, destruction and masking; Several type of DOS attack at several OSI layers; Attacks at MAC layer include collision, battery exhaustion and unfairness; An attack against the transport layer.

Table 15: Security risks in data collection layer

3.2.2.2 Data Transmission layer [middleware]

The middleware allows interconnecting and integrating of data collection layer and application layer. This layer in the IoT is also used to interact with cloud technologies and other technologies, such as for example P2P systems. Table 16 provides six categories of services provided by Data Transmission layer depending on the context-awareness, and presents for each category the potential vulnerabilities for security and privacy protection of critical user information [80].

Categories of services based on context awareness	Security risks
Event-based	The events consist of a set of parametric values describing the changes of state. All the participants in the middleware are connected through events. Most of the event-based middleware applications do not consider security requirements.
Service-oriented	It includes security attributes as well as vulnerabilities of service-oriented applications.
Virtual Machine based	It includes vulnerabilities on applications that use virtual infrastructure for the purpose of safe execution.
Agent-based	It includes vulnerabilities on applications running through mobile agents.
Database-oriented	In IoT, the sensor network acts as a virtual relational database system that can be queried by SQL-alike language. It has vulnerabilities related to the relational databases.
Application-oriented	The application-specific middleware cannot satisfy general IoT requirements because of heterogeneity of possible applications.

Table 16: Security risks in data transmission layer [80]

3.2.2.3 Application layer

Due to their specific characteristics, the end devices used in IoT lack the capability to handle high-level protocols, such as HTTP or HTTPS. Table 17 provides some possible security risks for each enabling protocol used in application layer of IoT architecture.

Enabling protocols	Security risks
Message Queue Telemetry Transport (MQTT) [81]	It is a lightweight protocol designed for constrained devices with low bandwidth and high-latency or unreliable networks. The present implementation of MQTT provides support only for identity and authentication policies. Authorization is also not part of MQTT protocol. So, the present security controls provided by MQTT are not sufficient for the IoT network where data anonymization, obfuscation or dynamic context based policies should be dynamically evaluated for each sent message [82].
Extensible Messaging and Presence Protocol (XMPP) [83]	It is an application-oriented specification of the Extensible Markup Language (XML) enabling the near-real-time exchange of structured and extensible data between any two or more network entities. XMPP protocol does not provide end-to-end security. The following order of application protocols is recommended in order to ensure the overall security of application layer: TCP, followed by Transport Layer Security (TLS), Simple Authentication and Security Layer (SASL) and finally XMPP.

Blockchain [84]	It was originally proposed in Bitcoin to solve the double spending problem in a cryptocurrency system. A blockchain can be applied in a distributed and trustless environment and can stand by itself without the need of third party authentication or management [84]. It has recently received a lot of attention in the IoT domain, with the objective to allow autonomous interaction of smart devices without human interventions. However, all the networks connected to the blockchain are not completely trustful. Blockchain offers only pseudo anonymity, because it is possible for adversaries to make inferences about who owns what public keys and thus track the owners of smart devices. As privacy protection is a major concern in the IoT system, additional mechanism should be designed and implemented to prevent the identification of the owners of the smart devices.
-----------------	--

Table 17: Security risks in enabling protocols used for application layer

3.2.3 Privacy

The significant growth of the IoT and data availability during the recent year has tremendously increased the risks to privacy breaches [3]. The primary difference between traditional internet and the IoT is the amount of data being collected by the users. The issue of privacy in IoT starts with the collection of personal data from various environments. Faulty provisioning of data, threatening its confidentiality and integrity, may allow unauthorized users' sensitive data by malicious parties [85]. It might become an obstacle towards the widespread adoption of IoT technology [3]. As discussed in Chapter 2, the basic IoT approaches begin with networks of sensors and actuators. Users will be unwilling to use new technologies without assurance of privacy of connected sensors and systems in such technologies. The ITU report on IoT²⁷ highlights *that concerns about privacy and data protection are widespread, particularly as sensors and smart tags can track a user's movement, habits, and preference on a perpetual basis*. Indeed, information about personal behavior of the users can be misused without their permission for commercial purpose. Moreover, sensors present in a smart phone can be used to evaluate the user, for example, person's health condition, habits, and so on [86]. In automobile industry, it is possible to register the movement of every driver. This data could be relevant to make driving more efficient and safer but at the same time, it is sensitive information, which gives insights about driver's physical condition, driving habits, and so on. Similarly, in smart cities the sensors can control almost everything from water management to power grid control. Almeida et al. [86] suggest that legal framework regarding data protection shall be adjusted according to the nature of the technologies to protect citizens' personal data and increase trust in the IoT. The rules and norms for the four basic principles of privacy are described in Table 18.

²⁷] ITU Internet Reports 2005: The Internet of Things

Privacy principle	The rules and norms to achieve the privacy protection
Notice and consent	Notice and consent are the major intricate issues to work with in IoT. The general formula is to provide an explanation and give people choice to decide how they like their data to be handled. However, in an IoT environment there is hardly any interface between sensors and users, making it challenging if not impossible to apply the same general rule. It is important to explore new possibilities to provide the meaningful information to the users about data gathering, who is responsible and how they can choose the usage of the data.
Data minimization	The concept of data minimization consists in collecting as minimum personal information as possible, which is paradoxical in IoT. In fact, currently sensors are used to monitor and collect as much data as possible from various environments. In this context, designing and controlling the data collection in IoT system is a challenging part. At the end, if the data is misused, the data collection system is liable and accountable for it.
Access to personal data	The personal data collected by any third parties, monitored by IoT system, must be available to the data owner at any time in order to respect his right of access. It is only possible when there is full transparency in the data collection process indicating who is responsible for the data. Given the multiplicity of the involved third parties, this is still a challenge in the IoT ecosystem.
Accountability	It is necessary to define the responsibilities of all the actors involved in the IoT ecosystem. In some exceptional cases, the introduction of a trusted third party, who is located outside the ecosystem, can be considered. This third party will be accountable to provide information and to gather the choice and consent of the users whose personal data might be collected and used by IoT ecosystem.

Table 18: Basic principles of privacy

As mentioned in this context, the information flow is a key concern when it comes to the definition of privacy rules. It is used by individuals, groups, or institutions to determine when, how, and to what extent they are willing to communicate information about themselves to the others²⁸. Table 19 presents six major phases of information flow in IoT as an example.

Information flow	Methods
Sensing	Triangulation Scene analysis Proximity Indirect inference
Identification	Unique identifier detection Facial recognition Vehicle license plate recognition
Storage	Object data Meta data

^{28]} A. F. Weston, Privacy and Freedom. New York: Atheneum, 1967

Processing	Self-contained inferencing Communication and matching Advanced pattern recognition and data analytics
Sharing	Intentional Unintentional
Use	Intentional Unintentional

Table 19: Communication of information flow in IoT [87]

Table 20 uses the same information flow mentioned in Table 19 to show the examples of privacy concerns and possible solutions in IoT [87]. These privacy concerns and solutions are categorized in three different aspects: technical, social and legal protection of privacy.

Phase of information flow	Example(s) of technical protection of privacy	Example(s) of social protection of privacy	Example(s) of legal protection of privacy
Sensing	<ul style="list-style-type: none"> Radio frequency (RF) blocking wallets RFID blocker tags 	<ul style="list-style-type: none"> Socially acceptable use of wearables, such as Google glass 	<ul style="list-style-type: none"> Prohibition of cell phone and camera use at customs
Identification	<ul style="list-style-type: none"> Media access control (MAC) address randomization 	<ul style="list-style-type: none"> Anonymous letters to newspaper editors or postings to online discussion forums 	<ul style="list-style-type: none"> Secret ballots for voting
Storage	<ul style="list-style-type: none"> No physical storage Encryption Ephemeral storage 	<ul style="list-style-type: none"> User social media privacy settings 	<ul style="list-style-type: none"> Formal limits on amount and duration of stored data
Processing	<ul style="list-style-type: none"> Privacy-enhancing technologies: anonymizing, etc. 	<ul style="list-style-type: none"> Privacy-enhancing technologies: anonymizing, etc. 	<ul style="list-style-type: none"> Restrictions of database matching
Sharing	<ul style="list-style-type: none"> Restriction or non-provision of communication facilities 	<ul style="list-style-type: none"> User and application sharing settings 	<ul style="list-style-type: none"> The right to be forgotten Data broker restrictions
Use	<ul style="list-style-type: none"> No provision for input into applications 	<ul style="list-style-type: none"> Accepted business practices and standards such as Electronic Product Code (EPC) guidelines 	<ul style="list-style-type: none"> Prohibition of discriminatory use

Table 20: Privacy measure examples in IoT [87]

3.2.4 Identity and access management

Current identity and access management (IAM) solutions focus on enforcing least access policies while granting access to data, applications and resources [14]. Current IAM systems are not sufficient to handle in storing identities and entities on a large scale in IoT. This limitation results a lack of application integration layers for IoT based applications. So, it is needed to involve enhanced IAM systems, which can discover and manage IoT entities and their identities across different solutions. On the other hand, IoT will require traditional IAM systems to include machine-to-machine (M2M) entities. For example, some of them may use proprietary communication and identification schemes. It will be a challenging part for IAM systems in order to cover identity of all kind of IoT entities.

3.2.5 Trust

Trust is a complex notion²⁹ that can be used in various contexts and no single definition exists in the scientific literature [88], [89]. Multiple existing approaches do not establish metrics and evaluation methodology, and the requirements for trust are strictly related to the identity management and access control issues.

Most of the smart objects of IoT system are exposed in public areas and communicate through wireless networks, which makes them vulnerable to malicious attacks. Indeed, in this context the nodes are communicating with each other establishing social relationships [90] such as friendship, ownership and community. Friends can share services and resources only when they trust each other. The trust level of two friends decides their future interactions. Trust related attacks on a node aim at breaking the social relationships of friendship, thus influencing the entire network. Various trust management protocols or mechanisms are proposed to build the trust level between friends in IoT systems. However, traditional access control models are not suitable in the dynamic and decentralized scenarios of IoT, where the identities are not known in advance. Sicari et. al [89] highlights following issues that are still open in IoT Trust management:

- The introduction of a well-defined trust negotiation language in order to support the semantic interoperability of IoT context;
- The definition of a proper object identity management system;
- The development of a trust negotiation mechanism in order to handle data stream access control.

²⁹] <https://portail-qualite.public.lu/content/dam/qualite/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf>.

3.3 Sensitivity of security, privacy and regulatory issues in IoT

To provide an overview of there level of sensitivity issues in IoT, such as security, privacy and regulatory, summary of these properties are highlighted here. R.H. Weber [62] categorizes different devices used in IoT environment to highlight the sensitivity of each category in security and privacy properties and regulations. Table 21 shows the ratings of each category with respect to the security and privacy properties and regulations.

- **The Integrity** means that the device should be free of malware. It is of high priority in most of the categories of devices used in IoT ecosystem. For processing and identification devices it is considered medium sensitive. Finally, actuators and localization and tracking devices are considered less sensitive toward integrity property.
- **The Authenticity** property is considered a major challenge for communication in IoT ecosystem. Authenticity of sensing and storage devices is equally challenging.
- **The Confidentiality** is another challenging issue for storage, localization and tracking, identification, and communicating devices. It is considered less critical for the end devices, sensing devices and actuators.
- **The Privacy** protection is primary for all devices and equipment involved in the IoT ecosystem. However, end devices and communicating devices are less sensitive compared to the rest five categories listed in the Table 21.
- **The Availability** is vital in localization and tracking, and identification because it guarantees the reactivity of the IoT ecosystem. End devices should be also available compared to other categories of devices in the Table 21 that should not necessarily be available all the time.
- **The Regulatory** issue is already vital for most of the categories of devices, such as in sensing, storing, processing, localization and tracking, and identification. It is going to be even more challenging after the **European General Data Protection Regulation (GDPR)** will enter into force.

Category	Example(s)	Integrity	Authenticity	Confidentiality	Privacy	Availability	Regulation
End devices	Laptops, smart phones, sensors, actuators	High	Low	Low	Medium	Medium	Medium
Sensing	Video, audio, positioning, acceleration, temperature, proximity, RFID readers	High	Medium	Low	High	Low	High
Actuators	-	Low	Low	Low	-	Low	Medium
Storage	Databases, DHT	High	Medium	High	High	Low	High
Processing	Services, sensor networks, network processing	Medium	Low	Low	High	Low	High
Localization and tracking	RFID, cellular network, GPS, sensors	Low	Low	High	High	High	High

Identification	RFID, Barcodes, 2D tags, Biometric, Video	Medium	Low	High	High	High	High
Communicating devices	RFID, cellular network, wired and wireless networks, overlays, infrared	High	High	High	Medium	High	Low

Table 21: Sensitivity of security, privacy and regulatory issues in IoT [62]

3.4 Regulatory challenges

The IoT deals with various amounts and types of data coming from different locations and having different levels of sensitivity. Previous section provided insights on privacy issues in IoT. This section highlights regulatory challenges for the IoT implementation and explains the impact of European General Data Protection Regulation (**GDPR**) on IoT activities.

3.4.1 Data ownership and Data collection management

Several significant regulatory challenges have arisen with respect to data collection, storage, retrieval, and query due to the massive amount of data generation in IoT [14]. There are still open questions about how much and exactly what data to collect and store in IoT system. The questions about data ownership and control of data flow fuel the debate from the regulatory point of view. The issue of data ownership is becoming significantly more complex with the increase of more heterogeneous IoT system including multiple stakeholders of IoT. The corporate users are interested in protecting proprietary business data, trade secrets and limiting liability, for example, from privacy breaches of third party input data they may store, process or consume [14]. End users are particularly interested to control their personal data. But, the current IoT platforms lack robust data right management systems to let data owners know where, how, by whom and for what purposes their data is used in order to enable acceptable level of control over their data. The rest of the section describes the impact of GDPR on IoT activities.

3.4.2 GDPR and IoT

Generally speaking, European Union (EU) laws take form of Directive or Regulation. When it comes to directives, each member state of European Union is free to decide how to transpose it into their national laws. But the Regulations have binding legal force throughout every member state and enter into force on a set date in all the member states [91]. The Data Protection Directive 1995 (95/46/EC), which was responsible for the protection of personal information, is replaced by the European General Data Protection Regulation (GDPR) that entered in force in May 2018. As explained in Chapter 2, all the IoT applications are always about data. This section describes how IoT industry will be affected by the enforcement of GDPR.

The GDPR is about data privacy and the protection of personal data. This means that the regulation has regulatory mandate over all activities or projects where personal data is involved. The regulation ensures the free movement

of personal data between EU member states strengthening the rights of privacy of data subjects as it is expected to give citizens control over their personal data. Thus, it impacts greatly companies that are dealing with personal data. Obviously, the GDPR is expected to have a major impact on IoT industry because it collects and analyzes huge amount of personal information from users. The key elements that distinguish GDPR from Data Protection Directive, 1995 are:

- In the GDPR, the definition of personal data has been further elaborated. Information about location of the data subject, online identifier, and genetic information that were not included in the definition of Data Protection Directive 1995 are included in the GDPR;
- Important penalty in case of violation of the GDPR; and
- Requirements in obtaining consent from data subjects have been strengthened. Specific and clear information should be provided when the consent is requested from the data subject. Easy and simple language should be used in such consent agreement. In addition, data subject has the right to withdraw his consent at any time.

Some examples of IoT applications [92] where GDPR can affect its full implementation are highlighted in Table 22.

<p>Knowing where the data is</p>	<p>Many businesses are unclear about where all of the private, sensitive data resides and who is responsible for taking care of it. Generally, their data are siloed at different layers of the organization, such as in sales department, marketing department, and other services. Under GDPR, the data controller must respond access request of data subject within a month, with the possibility of extending this period in particularly complex situations, which is going to be challenging for all the organizations running in the current traditional data handling approach. On the other hand, GDPR grants different rights to the data subject, such as the right for rectification, the right to be forgotten, the right to restrict data processing, the right to object data processing, or the right to not be evaluated based on automated processing, which would have significant impact on the data management practices in IoT.</p>
<p>Information usage and exchange between IoT devices</p>	<p>The end devices, the things of the IoT environment, send data automatically and communicate with other end devices to work together. There are many cases where the things are supposed to interact and act on the users' behalf. Let's take an example to show how GDPR can affect the implementation process of IoT. A smart fridge in a smart home may connect to the internet in case of food shortage in the fridge and buy the things on behalf of the users. In this case, user's information is exchanged to the various parties. The GDPR's requirement of control of personal data may restrict the implementation of IoT and undermine its success in such domains.</p>
<p>Analysis of data collected from IoT</p>	<p>IoT manufacturers can analyze massive amounts of data generated from IoT environment in order to understand the behavior of the system or users. The analysis of such data may reveal behavior and usage pattern of the user, which can be used for the commercial purpose, i.e. to make more profit. Even if the data collected at the endpoint does not cause any privacy issues, it may become sensitive data after analysis. In the GDPR, this issue is taken into consideration via the extended definition of the personal data. It seems to be one of the biggest challenges introduced by GDPR to IoT industries.</p>

Table 22: IoT implementations where GDPR can affect [92]

3.5 Standardization gap

The IoT, an essential component of this emerging digital world, is a paradigm that involves many information and communication technologies, as explained in previous chapters. The network of connected objects, capable of **capturing and disseminating data**, must allow the development of new innovative services for the benefit of society as a whole, whether to improve the level of service offered in the field such as public, health, transport, and environment. Many challenges remain in order to fully exploit the potential application of this promising paradigm, as explained in Section 1.4. Particularly, in IoT, it is important to ensure a high level of connectivity and interoperability between connected objects as well as to put in place an adequate level of security to protect connected objects from potential malicious uses or to prevent against data privacy. Going further, even though the technology is evolving rapidly, certain IoT applications cannot be further developed without regulatory framework [93]. For example in self-driving cars, technology is already advanced, many auto and technology companies have huge investments in this area but it remains still unclear when and where self-driving cars will be allowed to operate. Specialist Task Force 505: IoT Standards landscaping and IoT European Large Scale Pilots (LSP) provided gap analysis³⁰ in order to give directions for future development of IoT standardization:

- Interoperability will be essential for the deployment of the IoT ecosystem and for ensuring seamless flow of data across sectors and value chains;
- Solutions should be more than technical solutions;
- Existing standards to be refined to address non-technical issues;
- Certification mechanisms are a very important topic;
- Mandatory to complete technological developments;
- Security and privacy are still a limiting factor;
- Regulations and dissemination are needed to ensure users' acceptance;
- Solutions should give advantage to transversal compatibility rather than vertical domain specifics.

Chapter 5 of this white paper is dedicated to provide the standardization activities of international and European standards development organizations (SDOs) in IoT and related technologies domain. This section also provides the overview of IoT reference architectures of different SDOs. Nowadays, many SDOs have already started their collaboration to minimize possible repletion in standardization activities from more than one organizations.

³⁰] <https://portal.etsi.org/STF/stfs/STFHomePages/STF505>

4

Internet of Things – Economic analysis and business prospects

4. Internet of Things – Economic analysis and business prospects

The IoT means the convergence of **embedded computing, broadband and mobile networking**, distributed cloud computing, database architectures, web and mobile user interfaces as well as **integration of business applications** [94]. Its ability to link the physical world by including human to the internet and other data network has profound implications to the society and the economy. As a disruptive innovation it is assumed to improve the business processes within and across sectors³¹. Today, data is mostly used for **abnormality detection** and control but **not for optimization and prediction**, which can provide paramount value in the ecosystem [93], [95], [96]. In the IoT ecosystem, large volume of data is generated across the sectors by various connected devices, e.g., using different sensing devices and wearables. This data (also called **IoT data**) could be used for business process optimization, prediction as well as for the development of new services and products offering opportunities to create meaningful values through **appropriate decision making, and enabling new line of businesses**.

Different players of the IoT ecosystem are working through different initiatives to prepare the required environment to create meaningful value of data worldwide. For example, Luxembourg aims at developing a strong framework for the advancement of (IoT) data driven economy, becoming a trusted (IoT) data hub and building an ecosystem ensuring that data is accessible and usable to position the country in the global data driven economy [50]. The country is considered as an important ICT player with proven competences in availability of high-speed broadband connectivity and cybersecurity. It has already provided significant competitive advantages to the market and continue to progress in that direction. Moreover, it is also investing largely at building ICT infrastructures. Some examples include infrastructure of data centers, development of digital competencies, investing in HPC capabilities and proficiencies (as mentioned in Section 2.2.3.1).

This chapter provides an overview of economic analysis of IoT at large followed by its potential business opportunities. In the first part of this chapter (Section 4.1 and Section 4.2), global analysis of IoT trends as well as its business prospects are highlighted. The second part of this chapter (Section 4.3) presents business opportunities and challenges as well as insights on its impact to the economy in the long run.

4.1 Economic analysis – global outlook

There is lack of sufficient number of studies that addresses deep social, economic, political impacts of the IoT. Most of the existing studies quantify the economic impact of IoT based on the projected number of IoT devices to be connected or investments to them in the coming years. According to Gartner [57], about 11.2 billion connected devices will be in operation to the internet worldwide in 2018, this figure is about 33 % higher compared to 2017, and it will reach around 19 billion by next year. Predictions of several organizations provide a wide range of estimates of total number of IoT devices, from a low of 19 billion to a very optimistic prediction up to 40 billion to be connected to the internet [11], [97]. Nevertheless, in all the cases, the predictions follow the same trend (see Figure 13). The increased number of connected devices, the growth of the sensors market, ubiquitous wireless coverage, and the combination of this technology with other Smart ICT technologies, such as cloud and edge computing, Big Data, etc. lead to various smart applications. Examples include optimized public transport, optimization of energy consumptions using smart meters, real-time and accurate tracking or monitoring of shipment across logistics sector, significant increment in capacity utilization of resources across manufacturing sector etc. Moreover, fast growth of web-connected physical devices, such as smart devices, connected and automated cars, automated farms, and similar developments in various sectors shows the IoT's acceptance, adoption and business applicability is on rise [98].

³¹] <https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination>

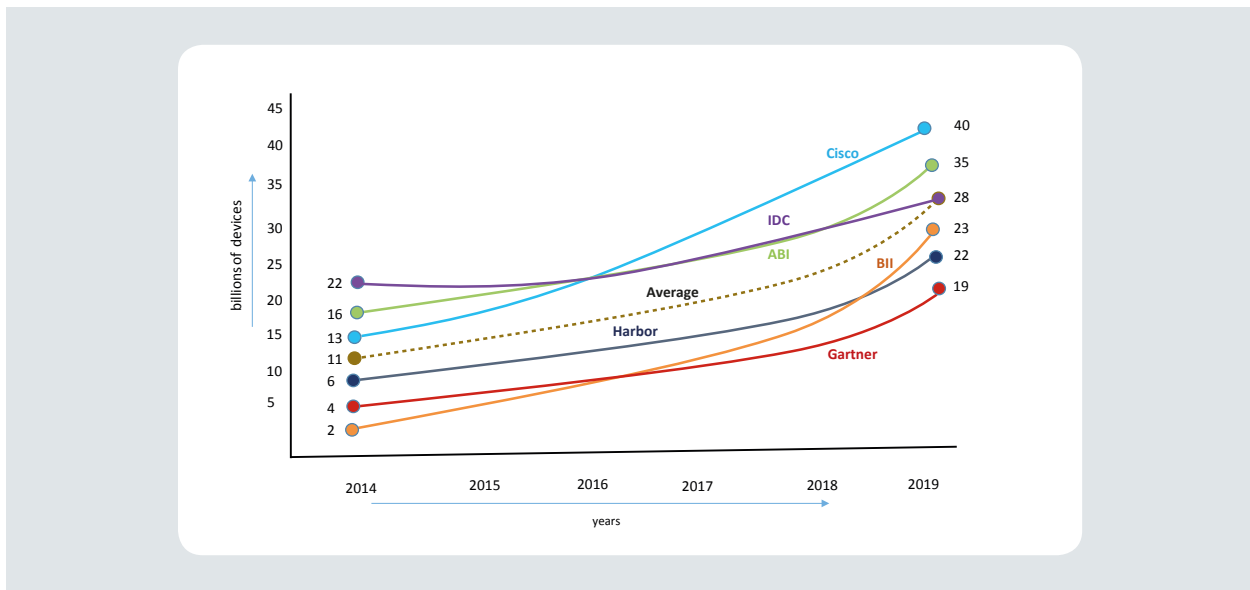


Figure 13: Projected connected devices by 2019 [11]

This growth in IoT opens an era of new services that can bring noticeable changes to the individual citizens, society, economy and environment and huge number of business opportunities. It is also foreseen that IoT will be one of the most compelling technology innovation for the next decade [2]. Its power to transform the way of living, create a business or take a decision instantly is incomparable with other recent technologies. Some global findings on the opportunities generated by IoT in the market according to different studies are listed in Table 23.

Key trends and insights	Explanation
More connected devices than people	<ul style="list-style-type: none"> Even if different organizations provide a wide range of estimates on IoT devices over the next decade, it can be clearly seen from their prediction that IoT connected devices in 2017 has already superseded the population of the world, 7.48 billion [99]. Fast growth of web-connected physical devices, such as smart devices, connected and automated cars, automated farms, and many more sectors shows its acceptance, adoption and business applicability is on rise [98].
Continuous market growth	<ul style="list-style-type: none"> Gartner [57] predicts more than 52% spending on IoT in business from overall IoT spending in 2018. Nearly 1 billion smart meters will be connected globally by most of the energy providers throughout the world to measure and manage the rising demand of energy by 2020 [2]. The continuous global market growth (from \$ 170.57 billion in 2017 to \$ 561.04 billion by 2022 [100]) will positively motivate its stakeholders to invest more in IoT, which helps to create more jobs across many sectors, such as manufacturing industries, transportation, energy as well as healthcare and medical. Global economic impact of \$ 11.1 trillion per year is expected in 2025 due to IoT applications [93].

<p>Opportunity for the established companies and start-ups</p>	<ul style="list-style-type: none"> ● IoT can play vital role to continually build and develop new products in various sectors, such as infrastructure, smart homes, Smart Cities, smart cars and many others for both established companies and start-ups of the country [98]. ● The data used today is used mostly for abnormality detection and control but not for optimization and prediction, which can provide the greatest value in the ecosystem [93], [95], [96]. ● Manufactures, oil and gas companies and other businesses have already seen the initial payoff of IoT technology in their operations [93].
--	---

Table 23: Global trends of IoT market

4.2 IoT application domains with high impact on economy

Enablers for the rise of IoT applications include cheap bandwidth, cheap sensors, cheap processing smartphones, etc. Smartphones in particular provide an easy interface through which people interact with other connected devices and objects. These devices can be seen as the hub to the IoT [31]. Services are offered in numerous different applications, such as navigation, online maps, recommendations for business and pubs. Connectivity in general, has paramount importance in IoT. The lack of adequate level of connectivity to the connected devices could degrade the overall performance of the IoT ecosystem. According to the Mobile Economy Europe report [101], IoT connections across the European countries are expected to reach 6 billion by 2020, which could result in € 1.2 trillion total revenue (including services, hardware and software). Additional value could be created when consumer IoT systems are linked to the business. The data from IoT allow all the organizations to perform unprecedented analysis of business process. It is also stated that use of IoT in business-to-business (B2B) applications will have a greater economic impact than its consumer equivalent [93].

In Europe, the IoT has significant role in realizing the digital future with positive impacts on both economy and society. The European countries and their stakeholders of IoT ecosystem have recognized the importance of IoT and its opportunities, which could result in the increasing number of IoT deployments and creation of new services [101]. European Commission (EC) also supports IoT deployment by huge investment in research and development to improve the quality of lives of the citizens across the Europe. Table 24 illustrates the domains, where IoT has high impact on the economy according to different study reports.

Domains	Projections and impact on economy
Smart Manufacturing	Globally, more than 53 % of smart sensors are expected to be used by manufacturer by 2020 against 35% in 2016. Particular benefits of application of smart sensors include significant increment in capacity utilization, improving safety and minimizing unit cost. In Europe, Industrial IoT is considered as revolutionary technology to advance traditional manufacturing ecosystem.
Smart Transportation	Over 220 million connected cars are expected on the road by 2020. IoT will be a key enabler for driverless cars industry. Particular expected benefits in transportation include improved traffic conditions, optimized fuel consumption, optimized travel routes. In European market, Smart transportation domain will be dominated by automated/ driverless car with active involvement of telecom service providers in the work of traditional carmakers. The local governments also directly support these initiatives. The EC invests around € 100 million and € 139 million respectively for autonomous cars and IoT under Horizon 2020 program.

Smart Utilities	<p>Nearly 1 billion smart meters will be connected by most of the energy providers worldwide to measure and manage the rising demand of energy by 2020. Particular expected benefits include use-based energy to minimize energy transmission losses and outage of power due to excessive demand, cost optimizations by energy savings. The EU aims to replace at least 80% of electricity meters wherever it is cost effective by 2020 [102]. It is also expected that rollout of smart meters and smart grid can reduce emissions and annual household energy consumption by up to 9% in Europe. A major advantage for the consumer due to this concept is that they would be able to access dynamic electricity price contracts. Some of the key assumptions of the EC by 2020 are³²:</p> <ul style="list-style-type: none"> ● Around 200 million smart meters for electricity and 45 million for gas will be rolled out in the EU. It results the potential investment of € 45 billion in this sector. ● Almost 72% of European consumers will have a smart meter for electricity and about 40% for gas. ● Only installing cost of smart meter in the EU will be on average between € 200 and € 250.
Smart Logistics	<p>Sensors placed on shipping containers and parcels will further reduce the associated cost in this business. Use of robots will help to reduce labour costs. Particular expected benefits include real-time and accurate shipment tracking and monitoring, optimized fleet management, and efficient inventory management. According to Eurostat, the EU is the major world trader in medicinal and pharmaceutical products³³ and Luxembourg could be the gateway of these trades for logistics sector to the European and US market. Total export worldwide from 28 member states is at around € 144.2 billion, and EU imports at around € 75.4 billion.</p>
Connected Buildings and Smart Homes	<p>Majority of home devices are expected to be connected to the internet by 2030. IoT will significantly affect the overall building operations. Particular expected benefits include intelligent surveillance, energy saving and monitoring, significant support for improving building operations. In Europe, a range of mobile players and operators has already launched smart home platform for the domestic market. For example, a solution to link consumers to connected objects (for instance, light switches, thermostats, smoke detectors) by telecom service providers gets huge success to control home appliances remotely. New smart home sensors with an updated control hub is another example to be compatible with connected smart home devices.</p>
Healthcare	<p>By 2020, 646 million IoT devices are expected to be used in healthcare industry worldwide. They are used for collecting, and processing data to automatically react to the patients. Particular expected benefits include automated enhanced medical workflow, better and improved out-patients' health monitoring.</p>
Banking, Financial Services & Insurance	<p>IoT will massively disrupt insurance industry by next five years. Most of the companies have already started IoT development and implementing IoT strategies. Particular expected benefits include targeted cross-selling opportunities, users personalization, improved operational efficiencies and risk management.</p>
Oil and Gas Mining	<p>By 2020, 5.4 million IoT sensors, devices and systems are expected to be used in oil extraction sites for tracking and measuring environmental, performance and productivity metrics. Particular benefits expected include safe and efficient workflow operations and automation for predictive maintenance of distribution pipeline networks.</p>
Others	<p>Retail, hospitality, defence, agriculture, and food service are other potential industrial sectors of IoT. 31% of hotels are using next-generation door locks, 33% are having room control devices, 16% are having connected TVs. Spending on drones for military purpose is expected up to \$ 58.7 billion by 2020. More than 310 million IoT devices are expected to be deployed by food service providers including grocery stores, fast food outlets by 2020. In Europe, new technologies are expected as key factors in the development of Smart Cities. The key idea is to better integrate environment, transport, energy and digital networks to have better quality of lives of the citizens.</p>

Table 24: IoT application domains with high impact on economy [2], [101]³⁴

^{32]} <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0864R%2801%29>

^{33]} http://ec.europa.eu/eurostat/statistics-explained/index.php/International_trade_in_medicinal_and_pharmaceutical_products

^{34]} Data included in this table are also taken from different research survey of PwC, Business Insider, SMA Research Survey, and Daintree Networks survey

4.3 Business opportunities, challenges and long-run impact of IoT

As indicated in Chapter 3, the IoT has own pros and cons. Several obstacles need to be addressed to get its maximum economic impact. Some are purely technical, some are structural and behavioural [93], and some are related to regulatory issues. The progress of the IoT is hindered by the complexities associated with these issues.

In fact, addressing these issues at the right time could positively impact business and economy than current IoT market. At the same time, its enablers and barriers should be also analysed before adopting the technology. Some of the enablers and barriers identified by different study reports have been put into the context to aware the stakeholders for its widespread adoption; these are highlighted in the Table 25.

Cost	<p>For widespread of any technologies, cost of its basic hardware must be decreased. In the context of IoT, low cost and low power sensors are essential. Price of micro-electromechanical systems (MEMS) sensors are continuously dropping by 30 - 70 % in the past years [2]. The similar trajectory is needed for RFID tags, and other IoT tracking devices. The other essential requirements for its global market growth are:</p> <ul style="list-style-type: none"> ● rise in high speed networking technologies; ● low cost data communication links; ● low cost of computing and storage devices to capture most of the environmental data into the IoT system.
Maturity of the technology	<p>Although concept of IoT technology is already adopted in the society, including use of sensors in several environments, the adoption of connected device technologies is yet to reach to the full fledge in various domains, such as manufacturing, healthcare and other industrial segments [2]. Additional time may be required for integration, including upgrading legacy equipment, new trainings for staff. For every company, at the stage of IoT revolution, there is still a large degree of uncertainty with respect to what IoT implementation plan to follow. Scarcity on relevant skills and expertise has also added a level of uncertainty to the companies.</p>
Interoperability and Adaptability	<p>Interoperability is a key enabler of IoT technology. Current interoperability issues between IoT devices and systems to work together is critical to realize full benefits of IoT applications. All IoT devices and platforms need to be adaptable to each other. It is predicted that at least 40% of its potential benefits cannot be realized without interoperability [93]. The compatibility technologies, including ZigBee, SigFox, LoRa (see Chapter 3 for more detail) are competing with each other to become a dominant transport mechanism to establish links between connectivity hubs and physical devices. This results in a need of standardized M2M protocols among IoT devices [2]. Full benefits of IoT could be harvested by adopting open standards, or by implementing common systems or platforms, which are able to communicate with each other.</p>
Security, privacy and confidentiality	<p>As mentioned in Chapter 3, the lack of comprehensive network and data security protocols remains critical for every connected IoT devices. The amount of data collected from billions of devices introduces privacy concerns among individuals, and confidentiality and integrity concerns of their data among organizations. Transparency into who, what and how data are being used provides assurance to the users about their data. At the same time, IoT has enormous business potential if these issues are addressed at some extent.</p>

Intellectual property	A common understanding of ownership rights among stakeholders should be clearly defined to unlock the full potential of IoT. The open question remains, for instance in medical devices implanted in a patient's body, who has right on the generated data, the patient or the manufacturer of the device.
Regulatory policy	Growth of particular IoT applications based on current regulatory framework . For example, the technology of autonomous (self-driving) cars is already advanced. There is huge investment of companies in this area but when self-driving cars will be allowed to operate is still unclear from regulatory point of view.
Stakeholders' implications	<p>The IoT has implications for all IoT stakeholders ranging from individuals to organizations. Particularly, it effects following stakeholders of the ecosystems creating new opportunities and risks:</p> <ul style="list-style-type: none"> ● Consumers: For individuals, IoT will be the on-demand source of information. For example, consumers will benefit from IoT-enabled roadways, self-driving cars, real time fleet information and so on, as they travel. Use of smart appliances, reduced cost in energy and on-demand health care at home are some additional examples of IoT benefits. At the same time, privacy concerns, overwhelming information and choices provided to the consumers should be managed carefully in the IoT ecosystem. ● IoT based companies: For companies, IoT technology certainly gives better economic impact for the future. Technology adoption at the right time needs sufficient knowledge about its implications. Early adopters may have better opportunities to create competitive advantages through lower operating cost than later adopters. ● Technology suppliers: Incumbent technology suppliers as well as emerging players have opportunities to create new business models in their favour. The market of IoT components grew more than 100 % in last few years and is expected to increase by 30% a year until 2025. ● Policy makers: As discussed earlier, to reach IoT applications to full potential, three issues – data privacy and usage, security and interoperability should be resolved by policy makers. Apart from policy makers, it is also a responsibility of standardization bodies to facilitate market development and growth through the standardization process. ● Employees: Workers will be affected by different ways with the implementation of the IoT. The demand for workers in some areas, such as food production, security and retail services could be decreased significantly and at the same time IoT can create new opportunities for the workers, such as in installing and maintenance of sensors, cameras and so on for IoT ecosystems.

Table 25: Enablers and barriers in IoT businesses [93]

In the rest of this section, some strengths of the Luxembourg and opportunities for public and private sectors in the country by adopting IoT technology are highlighted.

4.3.1 Strengths and business opportunities in IoT

Internet connectivity (including penetration, speed and specialized telecom infrastructure) could be a potential strength for the country while implementing smarter technologies, such as provided by IoT based businesses. Figure 14 shows the position of the countries in overall internet broadband connectivity (fixed, mobile broadband and speed) in Europe, where Luxembourg holds second position³⁵. The use of M2M cards for different purposes and RFID tags to track easily products of enterprises could be considered as already existing potential market space of the IoT. Figure 15 provides the number of M2M cards per 100 inhabitants in European market, where more than 17 M2M cards are already in use in Luxembourg. Similarly, Figure 16 provides percentage of enterprises using RFID to track their products in the European market. Around 5% enterprises in Luxembourg are using RFID tags for tracking their goods and products.

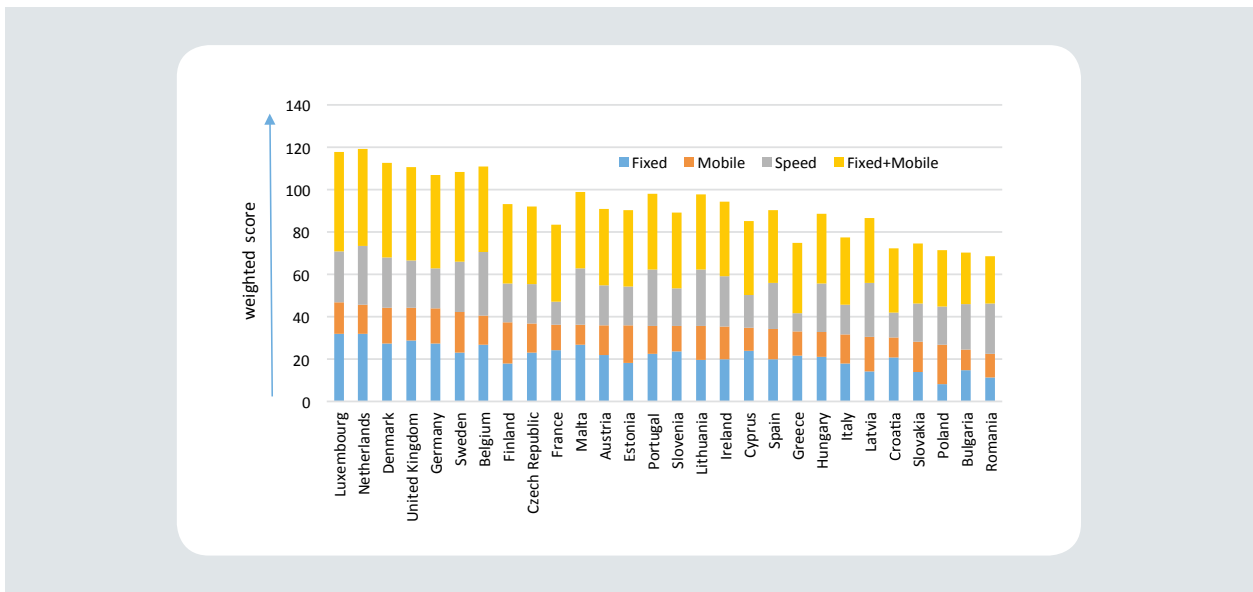


Figure 14: Connectivity dimension calculated as the weighted average of different sub-dimensions [103]

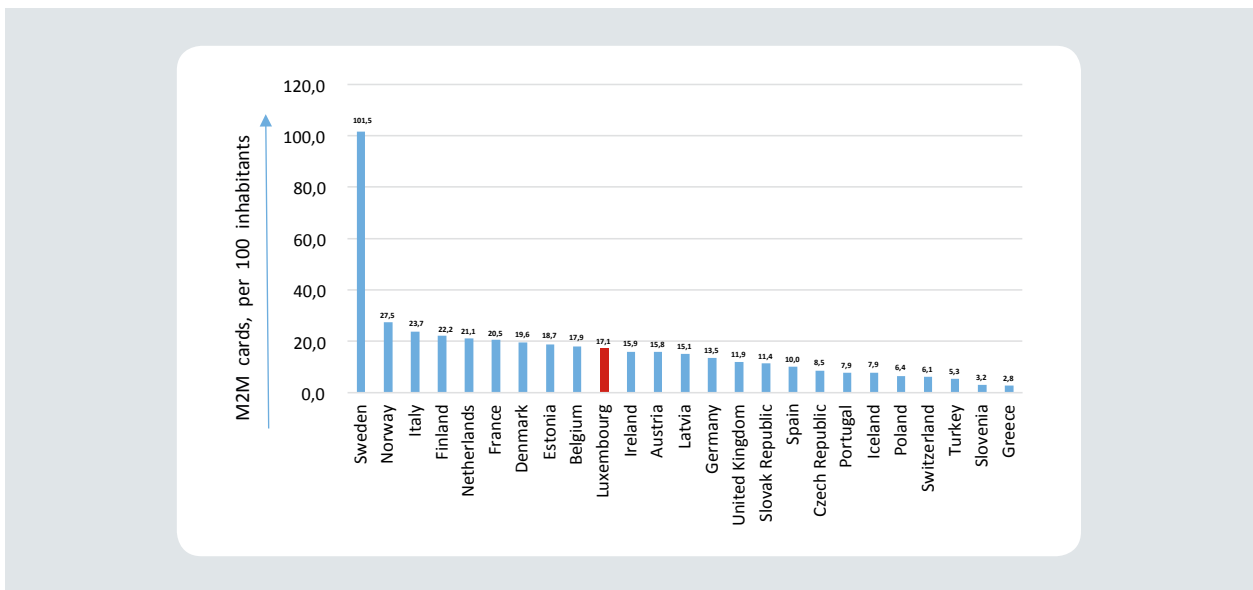


Figure 15: M2M cards, per 100 inhabitants [104]

^{35]} Luxembourg holds highest position if only fixed and mobile broadband are considered as internet connectivity parameters

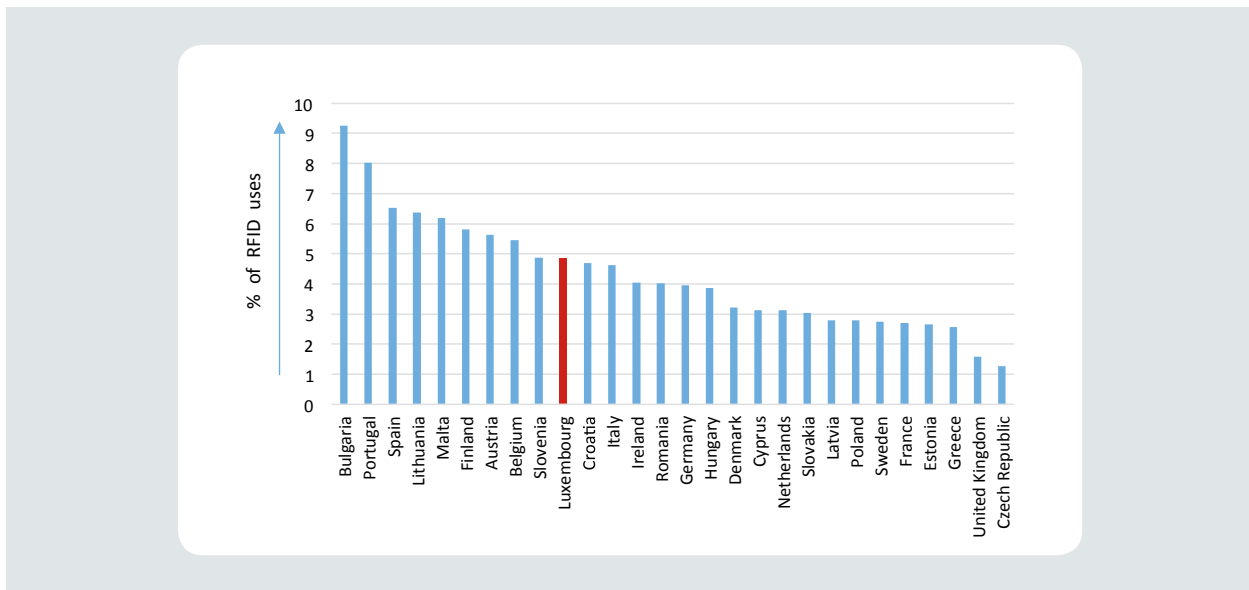


Figure 16: RFID used for product identification by enterprises [105]

Internet connectivity is also important for optimizing mobility or transport systems to increase their operational performance. Smart transport systems, for example, are becoming important application domain of the IoT because it enables vehicles to communicate efficiently with other each other. The IoT would allow developing of new communication network for intelligent mobility, sharing information integrated with existing transport and mobility systems. The sharing economy and services, such as car-as-a-service are gaining attention nowadays as traditional model is rapidly becoming unsustainable due to various problems, such as traffic jam, cost, lack of safety, etc. The IoT is considered as a key enabler for driverless cars industry, allowing to reduce the traffic jams, optimize fuel consumption, and optimize travel routes etc. [101].

Testbeds demonstrate new technologies development to create innovative products and services, show how new technologies can be optimally deployed; generate a measurable impact on new and existing markets. The experimental platform deployed and tested in real-world environment plays an important role in market acceptance. Luxembourg is considered as an ideal testbed for innovative companies due to a number of reasons, such as its central location in Europe, size of the country and agility³⁶. It offers noticeable advantages to create a real-world framework for testing IoT based technologies, e.g., in autonomous cars. Its strong road infrastructure; robust ICT infrastructure and high skilled manpower in this sector along with its central location in Europe are some of them. The digital cross-border testbed signed among Germany, France and Luxembourg last year is another promising example³⁷. This testbed aims at allowing testing of driverless and connected vehicles in a real setting. Its key thematic areas include compatibility of automated driving, link between automation and connectivity, impact and effects of automated and connected driving as well as access and use of data from such environments. Relevant and important data could be collected in real-time in order to analyze the behavior of the vehicles from different environments. The data collected and analyzed could provide tangible examples or precedents of multilateral implementation as an input for further European and international developments. Some benefits include enhanced driving environment perception with sensors, automated driving route optimization, to resolved rebalancing problem in car sharing - getting the car to the next user as soon as the previous user drops off the car, integrated IoT platforms into cars, and enhanced interoperability among different environments³⁸. New smart mobility solutions, services and products could be developed opening a range of opportunities for this sector. For example, real-time car sharing, pay-as-you-drive insurance, reservations/ concierge services, enhanced product design, accurate warranty management system, safety service systems.

³⁶] https://www.luxinnovation.lu/wp-content/uploads/sites/3/2018/01/08285_luxinno_broch_cleantech-200x200_01-2018_web.pdf

³⁷] <https://meco.gouvernement.lu/dam-assets/publications/brochures--livres/2018-05-08-concept-digital-test-bed-ger-fra-lux-v1.pdf>

³⁸] Connected Car Study 2015 -Racing ahead with autonomous cars and digital innovation European Automobile Manufacturers' Association(ACEA)

The Ministry of the Economy, the Chamber of Commerce and Inspiring More Sustainability (IMS) Luxembourg launched strategic plan of Luxembourg **Third Industrial Revolution**³⁹ in 2015, which is inspired by Jeremy Rifkin's social and economic theories. It aims to make the existing economic model more sustainable and interconnected for future generations by working with ICT, energy and transport as part of an intelligent network⁴⁰. As an important milestone of this initiation, the build up and scale up of the **Third Industrial Revolution of Internet of Things (IoT) platform** (according to the Third Industrial Revolution strategy study report^{41, 42}) aims at enabling businesses in Luxembourg by increasing aggregate efficiencies across their value chains, namely **industry, mobility, energy, buildings, food, and finance** [106], [107]. This platform is expected to increase productivity, and minimize marginal costs and ecological footprint of the businesses, to make the nation a leader around the globe shifting to the new economic paradigm and an ecological society [107]. Importantly, the goal is to make Luxembourg businesses more competitive in an emerging global marketplace allowing millions of prosumers connected to the IoT to produce and exchange **things** with each other in the growing sharing economy. Highlights of proposal and suggestions provided in the above mentioned study report are discussed here in six different vertical value chains. For example, transformation of traditional business models could be the main target of Luxembourg in the **industry** value chain to envision the country as an internationally recognized platform for sustainable industrial excellence through innovations. Some of the key IoT implementation in the industries include:

- Smart IoT integration;
- IoT-enabled prognosis in industry and manufacturing;
- Internet of things, services, and networks (IoT, IoS and IoN) for enabling radical makeovers not only in products, but also in the very nature of how a service such as mobility is delivered.

Similarly, **mobility** (transport and logistics) value chain could be another key focus areas of the country, including such links as efficient transportation modes, advanced infrastructure materials and driverless vehicle solutions. IoT platform can be considered to help the nation to shift from a fragmented, carbon intensive individual transport to active mobility combined with renewable energy and multimodal transportation on a driverless road, rail, water, and air mobility internet as in the Vision for 2050. Due to its central geographical location in European market, Luxembourg has high potential opportunities in logistics sector through IoT based solutions. Sensors, RFID placed on logistics supply chain will further reduce the associated cost in this business by providing real-time and accurate shipment tracking and monitoring. It also lies at the heart of the European road and rail network (North-South and East-West railway and motorway corridors). These networks enable easy and uncongested access to the European consumer market.

Smart metering, smart grid, renewable energies could be some other key focus areas of IoT implementation of Luxembourg in **energy** value chain. Luxembourg⁴³ has opted for a large-scale roll out of smart metering - more than 95% smart electricity metering by end of 2019 and more than 90% smart gas metering by end of 2020 with all necessary legal and regulatory framework. *The Energy System 2050* initiative has set forth a vision of a smarter energy in future Luxembourg through different initiatives such as:

- Significant reduction of energy consumption through increased energy efficiency;
- Centralized production and distribution of energy will remain at least a back-up component of the energy system;
- The mobility sector will essentially rely on electricity;
- Innovative ICT solutions will be the basis of a flexible demand side management and thus contribute to an increased flexibility of the energy market(s).

³⁹] <http://www.luxembourg.public.lu/en/actualites/2016/11/15-rifkin/index.html>

⁴⁰] http://imslux.lu/eng/nos-activites/pole-de-specialites/8_the-third-industrial-revolution-in-luxembourg

⁴¹] http://www.troisiemerevolutionindustrielle.lu/wp-content/uploads/2016/11/TIR-CG_Luxembourg-Final-Report_Long-Version.pdf

⁴²] It contains the combined and integrated narrative and proposals of both the Grand Duchy of Luxembourg Working Group and TIR Consulting Group LLC

⁴³] https://ec.europa.eu/commission/sites/beta-political/files/energy-union-factsheet-luxembourg_en.pdf

Buildings connected to the IoT infrastructure would play significant role in data handling, green power production, energy storage, and act as transport and logistics hubs to manage, power, and move economic activity in a smart Luxembourg. Transforming every building into the IoT data center, green micro power generating facility, energy storage site, and automated transportation hub could impressively enhance citizens' economic value by implementing a range of advanced technologies that can dramatically increase aggregate efficiency and productivity and lower marginal cost in the managing, powering, and moving of economic activity.

The concept in **food** value chain is proliferation of wireless smart sensor networks, telematics, geoinformatics, computational visualization, Big Data analytics, drones, robotics, and other automated tools, applications, and smart algorithms for tracking data throughout the entire farming operation for smart farming or Internet of Agriculture food value chain.

The convergence of the communication, renewable energy, and automated transportation and logistics internet on top of the IoT infrastructure enables **finance** value chain to reinvent financial sector. It is going to transform every aspect of financial services, foster new business models, and reshape the industry over the course of the coming decade. The IoT would also be an enabler for issuing of virtual currencies by banks, investment funds, insurance and reinsurance companies in Luxembourg. Favourable tax and regulatory environment of the country for investors, as mentioned below, could attract fund to implement IoT in this sector.

4.3.2 The long-run impact on economy

Viewing the implications of IoT impact how its applications might reduce cost of current operations and improve the quality standard of life through the lens of individual industries or sectors would not be adequate to see the overall values of it for all parties involved in its paradigm [98]. According to McKinsey Global Institute report [93], overall effect of IoT development in the society could be viewed through a lens of **settings** - the physical environments within which the systems can be deployed and where they can capture ways to create value for all parties, i.e. consumers, companies and workers. General speaking, it has defined nine settings: namely **human, home, retail environments, offices, factories, worksites, vehicles, cities** and **outside** where use of IoT could hugely impact globally on economy. Table 26 presents the overview of different settings with their expected economic impact in the future due to adoption of IoT technology. Main numerical facts about IoT in 2025 based on the findings of the above-mentioned report are highlighted here, and could be helpful to establish an IoT implementation plan for businesses:

- IoT has a broader view of potential benefits in vertical and horizontal industries. Global economic impact of \$ 11.1 trillion is expected per year due to IoT applications. The major economically dominant segments will be factories - \$ 3.7 trillion and cities - \$ 1.7 trillion per year in 2025;
- Interoperability is critically important between IoT systems. At least 40% of its benefit cannot be realized without interoperability;
- Business-to-business (B2B) applications of IoT will have greater potential than consumer applications;
- IoT could change the bases of competition and drive new business models for its end users, manufacturers or suppliers;
- The users of IoT (consumers, businesses, and other organizations) could capture most of the potential value (about 90%) over time.

Settings	Description	Example(s)	IoT value(s)	Economic impact in \$
<p>Human - devices attached or inside the human body</p>	<p>Mainly two types of IoT applications fall under human settings, namely health and fitness, and human productivity using IoT technologies. Continuous monitoring of the patients’ health conditions using connected devices attached or inside the human body is the potential transformative change in human health due to IoT in coming years. This impact has been estimated at the impact of \$ 170 billion to 1.6 trillion per year in 2025. Applications of IoT by improved health of users and reduced cost of patients care systems in chronic diseases are expected total societal benefits of worth more than \$ 500 billion per year in 2025. On the other hand, IoT technology can be applied in augmented-reality devices through which data can be displayed for guiding performance of workers in the factory or mobile workers in the field and allowing to stay connected throughout the working hours to work effectively. This impact on human productivity is expected at economic value of \$ 150 to 350 billion globally in 2025.</p>	<p>Wearables and ingestibles to monitor and maintain health and wellness</p>	<p>Increased fitness, disease management, higher productivity</p>	<p>170 billion – 1.6 trillion</p>
<p>Home – residence where people live</p>	<p>A wide range of IoT devices used in the home, including home controller and security systems can significantly impact the global economy in the chore automation. It is estimated that use of IoT could cut 100 hours of labour per year for the typical household, which nearly worth of \$ 135 million per year globally in 2025. Impact on economy due to energy management at home is expected up to \$ 110 per year followed by security, which can have impact more than \$ 20 per year based on injuries and deaths avoided. Economy impact in home due to the IoT applications could reach \$ 200 to 350 billion in total per year in 2025.</p>	<p>Home controller, energy management, and security systems</p>	<p>Control and security</p>	<p>200 – 350 billion</p>

<p>Retail environments - the place for commercial activities</p>	<p>The place where commercial activities take place such as banks, stores, restaurants, self-checkout points, in-store offers, and inventory optimization will be highly positively impacted due to IoT applications in coming years. Automated checkout helps to reduce human resources and other resources related to it. Economy impact of \$ 410 billion to \$ 1.2 trillion is expected per year in 2025.</p>	<p>Banks, stores, restaurants, self-checkout points, in-store offers, inventory optimization</p>	<p>Automated checkout</p>	<p>410 billion – 1.2 trillion</p>
<p>Offices - the workplace of knowledge workers</p>	<p>The work place of knowledge workers will be also highly impacted by IoT technologies. Key benefits of IoT applications in offices are energy saving, and ensuring security using digital security cameras to monitor throughout the activities of office resources ranging from security guards to operators of the building without human intervention. IoT based management is expected to save energy by 20 percent, which could impact of \$ 70 to 150 billion per year including all IoT applications in offices in 2025.</p>	<p>Security and energy consumptions of the building, productivity, and management of the mobile workers</p>	<p>Security and energy management</p>	<p>70 – 150 billion</p>
<p>Factories</p>	<p>Adoption of IoT technology could significantly impact operations of factories. It is expected an economic impact of \$ 1.2 to 3.7 trillion per year in 2025. This estimation includes the benefits of IoT applications in manufacturing as well as hospitals, agriculture environments. In overall 10 to 20 % labor saving is expected due to the IoT.</p>	<p>Places with repetitive work routines, including hospitals, farms, and inventory</p>	<p>Operations and equipment optimization</p>	<p>1.2 – 3.7 trillion</p>
<p>Worksites - custom production environments</p>	<p>Custom production environments are defined as worksites, including construction sites, mines, and oil and gas extraction sites. Use of more than 30,000 sensors in a typical oil-drilling platform for monitoring the performance of several systems shows the applicability of IoT in these areas. Improvement in operations in worksites from IoT applications is expected more than \$ 470 billion per year in 2025. Economic worth of \$ 360 billion is expected in equipment maintenance improvement by the use of IoT. Overall economic impact on worksites per year in 2025 is expected at \$ 160 to 930 billion in 2025.</p>	<p>Oil and gas extraction, mining, prediction, efficiency, and health and safety of the workers,</p>	<p>Operations optimization, health and safety</p>	<p>160 – 930 billion</p>
<p>Vehicles - environment of moving vehicles</p>	<p>This covers all vehicles including cars, trucks, ships, aircraft, and trains. IoT can play significant role to monitor and improve the performance of the vehicles while in use. It is expected that this setting could generate \$ 210 to 740 billion per year due to adoption of IoT technology in 2025.</p>	<p>All the vehicles including cars, trucks, ships, aircraft, and trains</p>	<p>Autonomous vehicles and condition based maintenance</p>	<p>210 – 740 billion</p>

<p>Cities - urban environments</p>	<p>One of the major application of IoT for city is to convert it into smart cities. Cities are the engines of economic growth of the country. The 600 largest cities are expected to produce about 65 percent of global gross domestic product (GDP) growth in the world through 2025, where IoT will have significant impact on it. As described in Section 1.4, cities can benefit from IoT applications in the areas, such as transportation, utilities, public health and safety. IoT application in transportation could be worth more than \$ 800 billion per year across the world in cities in 2025. Public health is the next biggest impacted economy due to IoT for air and water quality improvements, which is expected up to nearly \$ 700 billion per year. Similarly, in utilities management, such as smart meters for management of water and gas resources could be worth up to \$ 69 billion per year globally in 2025. The overall economic impact due to IoT applications is expected \$ 930 billion to 1.7 trillion per year in 2025.</p>	<p>Public spaces and infrastructure, traffic control systems, smart meters, environmental control, resource management</p>	<p>Transportation, utility management and public health</p>	<p>930 billion–1.7 trillion</p>
<p>Outside - between urban environments, and other settings of outside</p>	<p>The settings out of previously mentioned environments, i.e. those activities that take place outdoors between urban environments are considered outside. The activities, including use of IoT for improving the routing of aircrafts, ships, and other vehicles between cities by applying further advanced navigation information, tracking information of goods or containers or packages in transit received from various sensors are included in this setting. Global economic impact of \$ 560 to 850 billion is expected per year in 2025.</p>	<p>Railroad tracks, autonomous cars</p>	<p>Logistics and navigation</p>	<p>560 – 850 billion</p>

Table 26: Settings where IoT can create values in 2025 [2], [98]

5

Internet of Things - Technical standardization

5. Internet of Things – Technical standardization

The rapid growth of connected devices to the internet as well as adoption of IoT technology across business sectors have led to a careful study and development of technical standards. IoT success is highly dependent on the elaboration of interoperable global standards within and across application domains. For example, standard reference architectures and common vocabulary are a prerequisite to develop cost-effective business solutions and enable cooperation between various applications, to cover a wide range of disciplines as mentioned in Section 1.4.

Initiatives in standardization at international as well as European levels will help to increase market confidence in IoT and related technologies. This chapter gives an overview of various developments in the areas of technical standardization. After providing some background details about standardization (Section 5.1), this chapter focuses on ISO/IEC JTC1/SC 41 given that this technical committee is one of the prominent in standardizing in the IoT and related technologies (Section 5.2). Finally, it presents IoT standardization initiatives of ITU-T, ETSI, and other *fora* and *consortia* (Section 5.3 to 5.5).

5.1 Background on technical standardization and the national context

5.1.1 Technical standardization and standards

Technical standardization is widely recognized for its ability to provide technical or qualitative referential for products, services or processes. Technical standards are developed within standardization bodies that bring together all interested stakeholders and are active at different geographical levels in their own areas of competency, as illustrated in Figure 17. The International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) are the three recognized Standards Development Organizations (SDOs) at the international level. Likewise, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) are the three recognized European Standardization Organizations [108]. At national level, each country has one national standards body (NSB) that works for the interests of the country and co-ordinate with European and international standardization organizations. In Luxembourg, ILNAS is the NSB and is member of CEN, CENELEC, ETSI, ISO, IEC and ITU-T.













	General Standardization	Electrotechnical Standardization	Tele-communications Standardization
 International level			
 European level			
 National level			

Figure 17 International standardization organizations and their area of competence [109]

Technical standards provide an effective economic tool for achieving various objectives, such as mutual understanding, reduction of costs, elimination of waste, improvement of efficiency, achievement of compatibility between products and components or access to knowledge about technologies [110]. The application of the fundamental principles stated by the World Trade Organization (WTO), namely transparency, openness, impartiality and consensus, effectiveness and relevance, coherence and development dimension [111], throughout the development of technical standards, also guarantees the legitimacy of these documents. In addition, technical standards play an important role for innovation. As pointed out by the European Commission (EC) in its communication *Europe 2020 Flagship Initiative* [112], “they enable the dissemination of knowledge, the interoperability between new products and services for a platform for further innovation”. It is more relevant in the current context that the world tends to become digitalized and everything becomes connected. Technical standardization is thus a keystone to ensure interoperability of complex ICT systems and it will contribute to minimize the barriers that may still exist to build the future of the digital world.

5.1.2 Technical standardization and IoT

Technical standardization is an effective and indispensable tool to meet most of the challenges as explained in Chapter 3. EC is notably identifying technical standardization as an important element for the development of an IoT single market within the EU [113]. Standards are necessary to ensure interoperability among IoT solutions, which will ensure vendor lock-in problem and stimulate competition in the IoT landscape. Standards can also help in reducing the cost of IoT system realization, thanks to the sharing of research and development costs [114]. Figure 18 depicts the involvement of various SDOs engaged in the process of IoT technical standardization over the past decade.



Figure 18 IoT SDOs and Alliances Landscape [115]

In the following sections, some of the initiatives of SDOs are highlighted. In fact, IoT standardization ecosystem is very rich and complex, which is still in an early phase of deployment where many organizations are developing their own proprietary standard in order to get a better position in the competition. Nevertheless, most of the stakeholder of the IoT ecosystem have now realized the importance of IoT standards convergence to unleash its full potential [115]. The recognized SDOs, with a standards development process relying on the fundamentals principles of the WTO, represent the ideal place to gather IoT stakeholders with the objective of simplifying IoT standardization landscape to fulfil the market requirements.

ITU first published a report on IoT highlighting the key role of technical standardization for its deployment and diffusion in 2005. Following this report, a Joint Coordination Activity on Network Aspects of Identification Systems, including RFID – JCA-NID was established in 2006, which paved the way of IoT technical standardization together with Network Identification Number (NID) and Ubiquitous Sensor Network (USN) [116]. It was then replaced by the Joint Coordination Activity on Internet of Things (JCA-IoT) with the objective of coordinating to the ITU-T's work on IoT in 2011 [117]. ITU-T activities in this field became stronger in 2012 with the creation of the Global Standards Initiative on IoT (IoT-GSI). It aims to promote a unified approach in ITU-T for development of technical standards (recommendations) enabling the IoT on a global scale [118] as well as to serve as an umbrella for IoT standardization worldwide. In July 2015, the Study Group (SG 20) – IoT and its applications including smart cities and communities (SC&C) is created to focus also on smart cities related applications. JCA-IoT terms of reference and title were updated to include coordination of activities regarding Smart Cities and Communities, resulting in the Joint Coordination Activity on Internet of Things and Smart Cities and Communities (JCA-IoT and SC&C). All along this period, a rich ecosystem of IoT-related standards has been developed to fulfil its market demand. ITU-T's current works related to the IoT are detailed in Section 5.3.

Similarly, there are several initiatives of **ISO and IEC** to develop IoT technical standardization through the Joint Technical Committee ISO/IEC JTC 1 dedicated to information technology standardization. Related to IoT, a Working Group (WG) was created on Sensor Networks - ISO/IEC JTC 1/WG 7 in 2009 with the mandate of addressing

emerging areas related to M2M and IoT besides sensor network standardization. A Special Working Group (SWG) on IoT was formed at the end of 2012, in regards to the growing interest of various SDOs in IoT standardization. Its objective was to identify market requirements and standardization gaps in the area of IoT as well as to serve as a coordination group for IoT standardization among ISO/IEC JTC 1 subcommittees⁴⁴ (SC) and with external organizations such as ITU-T. According to the recommendation of this SWG, a new WG – ISO/IEC JTC 1/WG 10 - responsible for the development of foundational standards for IoT (e.g. terms and definitions, reference architecture, etc.) was created in 2014. Acknowledging the growing importance of IoT in the digital world and its strong interdependencies with number of other standardization developments, ISO/IEC JTC 1 decided to create a new **ISO/IEC JTC 1/SC 41 - Internet of Things** and related technologies in November 2016, and recommended transfer of works and liabilities of WGs 7 and 10. Section 5.2 provides details about the organization of ISO/IEC JTC 1/SC 41 as well as its current work programs.

ETSI is one of the most active SDO in IoT standardization, particularly in the frame of its TC Smart M2M - Smart Machine-to-Machine Communication and its involvement in the consortium oneM2M and in the Alliance for Internet of Things Innovation (AIOTI). ETSI/TC SmartM2M is focusing on M2M standardization since it was formed in 2013 as well as in addressing IoT standardization gaps identified in European Commission Large Scale Pilot projects [119] that have been transcribed in a Technical Report (TR) published by ETSI in November 2016⁴⁵. Section 5.4 provides details about IoT-related developments in ETSI, particularly initiatives of ETSI/TC SmartM2M.

Many other SDOs, also referred in this white paper as fora and consortia, are playing an important role in IoT standardization (see Figure 18). They distinguish from recognized SDOs in the sense that they generally do not seek to engage with all interested parties and they do not normally organize public enquiry during the development of the specifications. It is also worth noting that many technologies, that are self-standardized and come into play as a part of IoT, such as sensor networks, RFID, NFC and many other IoT application areas are well covered in terms of standardization. The areas, such as intelligent transport systems, smart homes, smart cities, are leading to an even more complex standardization ecosystem in the current context.

5.1.3 National context of IoT technical standardization

ILNAS, with the support of ANEC G.I.E., manages the National Mirror Committee (NMC) of ISO/IEC JTC 1/SC 41 to participate in the process of technical standardization for registered delegates. The registered delegates involve in the standardization work of ISO/IEC JTC 1/SC 41 by voting and commenting on proposals of the subcommittee and can participate in its international plenary meetings. ILNAS, with the support of ANEC G.I.E., also performs a broader monitoring of IoT standardization activities in order to keep up to date on the area and to inform national stakeholders about its progress.

Indeed, ILNAS, with the support of ANEC G.I.E., works actively on the development of ICT technical standardization. The *Luxembourg Standardization Strategy 2014-2020*⁴⁶, approved by the Minister of the Economy, is based on three pillars where ICT sector is one of the cornerstone. In addition, the *Luxembourg's policy on ICT technical standardization 2015-2020*⁴⁷ guide number of activities to be carried out to strengthen the national ICT sector involvement in standardization. Apart from the management of several NMC and the creation of education⁴⁸ and research⁴⁹ programs in the standardization area, it includes the development of reports informing national market

⁴⁴] ISO/IEC JTC 1 is composed of subcommittees each of them being responsible for the standardization of a specific IT area.

⁴⁵] ETSI TR 103 376 V1.1.1 (2016-10) - SmartM2M; IoT LSP use cases and standards gaps http://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf

⁴⁶] <https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/strategie-normative-2014-2020/luxembourg-standardization-strategy-2014-2020.pdf>

⁴⁷] <https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf>

⁴⁸] <https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/projets-phares-dans-l-education-a-la-normalisation.html>

⁴⁹] <https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/programme-recherche.html>

about the current standardization developments in this sector. For instance, the annual publication of the *Smart ICT Standards Analysis*⁵⁰, which provides an overview of last standardization developments of selected Smart ICT technologies (Cloud Computing, Internet of Things, Big Data and other recent ICT technologies), as well as related Digital Trust standards-based evolution. This analysis is a practical tool available to national stakeholders to identify relevant standardization technical committees in the Smart ICT area, with the objective to offer guidance for a potential future involvement in the standards development process to the national stakeholders [109]. It is worth noting that ILNAS also published a White Paper *Digital Trust for Smart ICT* (last updated in September 2017)⁵¹ to aware national stakeholders in the concept of Smart ICT and related standardization with digital trust requirements for different topics of Smart ICT. In summary, it provides, among other Smart ICT technologies, a state of the art of the IoT, its economic challenges and prospects, the requirement of Digital Trust as an essential factor in performing it, as well as technical standardization related developments as one of the enablers for Digital Trust for Smart ICT [88].

5.2 ISO/IEC JTC 1/SC 41 - Internet of Things and related technologies

The ISO/IEC JTC 1/SC 41 subcommittee on Internet of Things and related technologies aims at serving as the focus and proponent for JTC 1's standardization program on the IoT and related technologies, including Sensor Networks and Wearables technologies. In addition, it aims to provide guidance to JTC 1, IEC, ISO and other IoT related applications developing entities. This section details the latest update of the JTC 1/SC 41, considering membership, liaisons, structure and standards published or under development.

5.2.1 Membership

ISO/IEC JTC 1/SC 41 currently has 25 Participating Members (P-members⁵²), including Luxembourg, and 8 Observing Members (O-members⁵³) [120] as depicted in Figure 19. More than 250 experts from all around the globe contribute their expertise in its standardization activities.

P-Members	O-Members
Australia, Austria, Belgium, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Republic of Korea (Secretariat), Luxembourg , Malaysia, Netherlands, Norway, Russian Federation, Singapore, Sweden, Switzerland, United Kingdom, United States of America.	Argentina, Belarus, Iceland, Iran, Kenya, Mexico, Pakistan, Saudi Arabia.

⁵⁰] <https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2018/standards-analysis-smart-ict-2-0.pdf>

⁵¹] <https://portail-qualite.public.lu/content/dam/qualite/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf>

⁵²] P-members are required to participate actively in the work of the SC. They are voting on all official committee ballots, notably on the standards projects at various stages of their development, as well as participating in all the plenary meetings of the SC.

⁵³] O-members can observe the standards that are being developed, and possibly contribute to the work without any obligation.

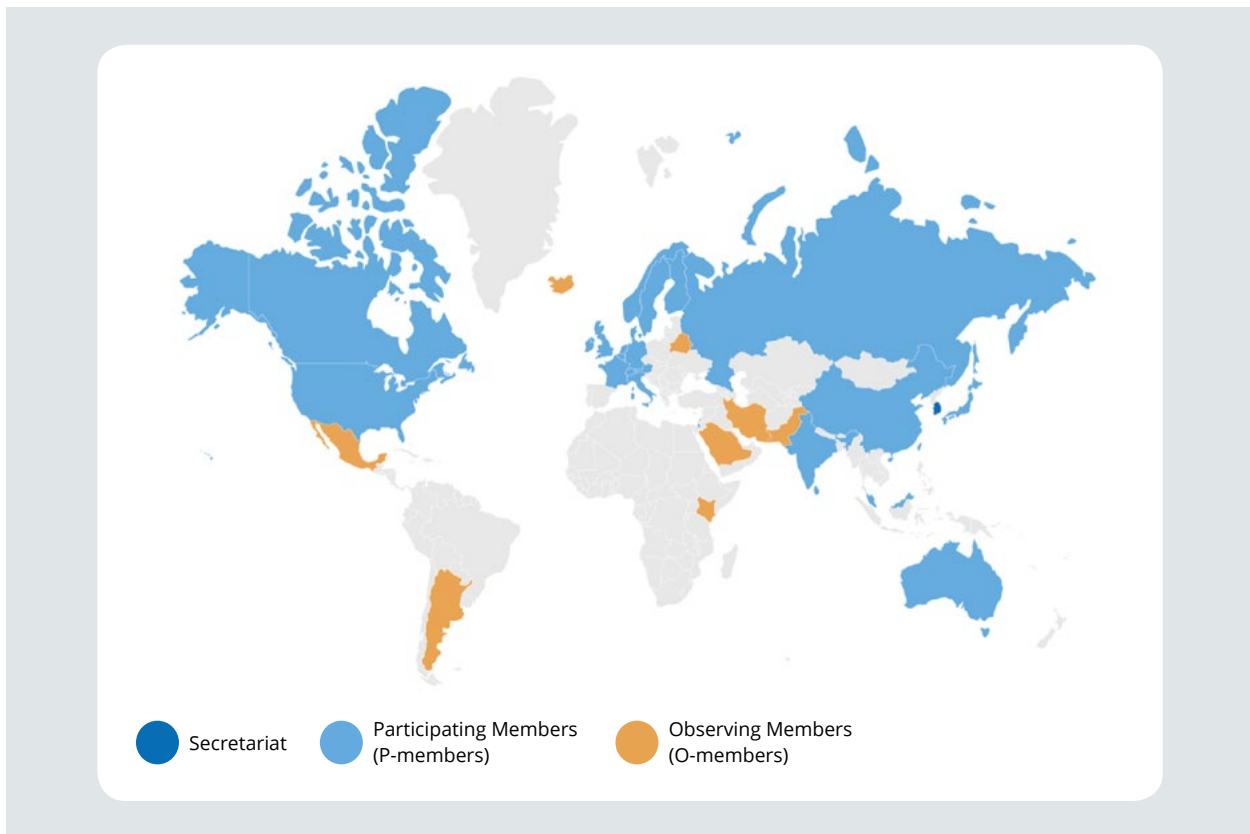


Figure 19: ISO/IEC JTC 1/SC 41 membership (May 2018)

5.2.2 Liaisons

ISO/IEC JTC 1/SC 41 has number of liaisons with different technical committees inside ISO, IEC and ISO/IEC JTC 1 as well as with other SDOs who are active in IoT and related technologies standardization. Main objectives of these liaisons are ensuring close collaboration among SDOs for the development of IoT standards required to the market and avoiding duplication of works. Technical committees and organizations in liaison with JTC 1/SC 41 can access its working drafts, participate in the plenary meetings and put their arguments/suggestions on the draft works in progress. They do also provide regular inputs about their own IoT-related activities. Moreover, other SDOs can propose some of their specifications as a proposition to be accepted as international standards by this subcommittee through a specific procedure.

Table 27 shows some of the active list of liaisons and its areas of collaboration with other SDOs. These organizations actively participate in the process of standardization work of JTC 1/SC 41. In addition, ISO/IEC JTC 1 gets advantage of collaboration and their competencies in different IoT-related areas from different ISO, IEC and ISO/IEC JTC 1 groups including:

- ISO/TC 184 - Automation systems and integration in the Industrial IoT;
- IEC/TC 124 - Wearable Electronic Devices and Technologies in wearable technologies;
- ISO/IEC JTC 1/SC 27 - IT security techniques in the security, privacy and trustworthiness;
- ISO/IEC JTC 1/SC 31 - Automatic identification and data capture techniques (AIDC) in the AIDC, including barcodes, RFID or NFC;
- ISO/IEC JTC 1/SC 38 - Cloud Computing and Distributed Platforms in the edge computing.

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

Table 27: ISO/IEC JTC 1/SC 41 liaisons organizations and areas of collaboration

5.2.3 Structure and standards

As illustrated in Figure 20, ISO/IEC JTC 1/SC 41 is composed of three Working Groups (WG)⁵⁴ and six Study Groups (SG)⁵⁵. Each WG is responsible for developing standards in specific areas, such as defining vocabulary and reference architecture, interoperability standards, and standardization in the areas of applications. Moreover, a Vocabulary Rapporteur ensures the regular update of the IoT-related vocabulary and assists project editors about vocabulary related matters.

5.2.3.1 Working groups (WGs)

WGs and IoT related standards developments along with their scopes are detailed in Table 28⁵⁶.

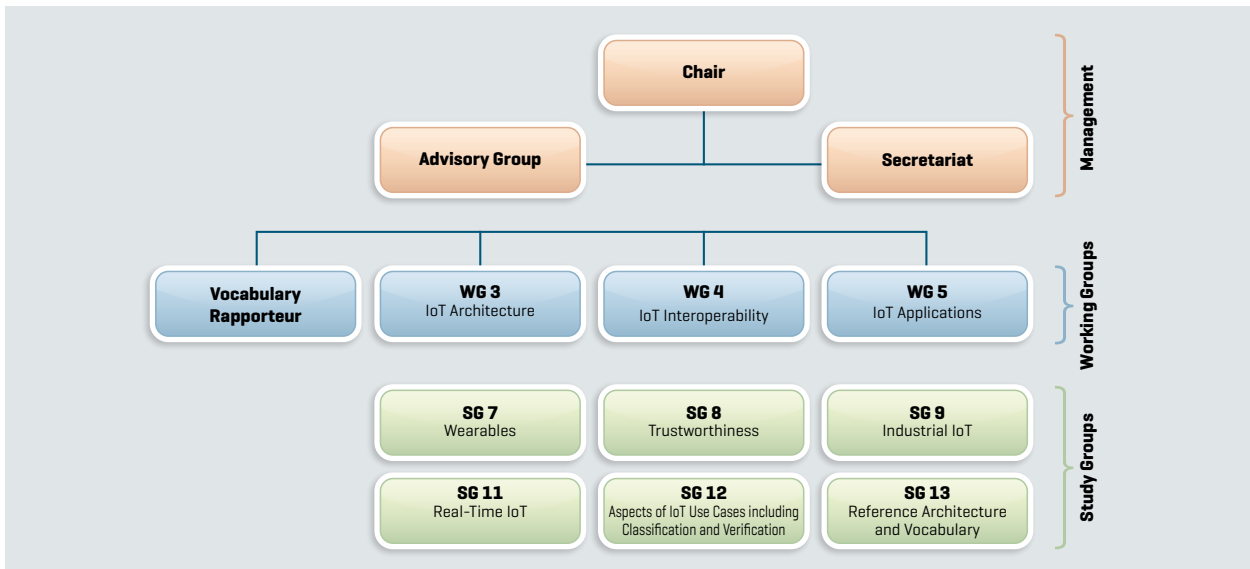


Figure 20: ISO/IEC JTC 1/SC 41 structure (updated in March 2018)

^{54]} A TC or SC can establish Working Groups that are focusing on specific tasks. They are notably responsible to develop the first drafts of the standards or other deliverables [156].

^{55]} Study Groups are set up to support the activities of a TC or SC for a given task. They are disbanded after the completion of their assignment [156]. Note that the meaning of Study Group in ISO and IEC differs from the definition of a Study Group in ITU-T, where a SG is equivalent to a TC.

^{56]} Please visit JTC 1/SC 41 webpage (http://www.iec.ch/dyn/www/?p=103:7:0:::FPS_ORG_ID:20486) for a complete list of standards developed and under development.

Working Group	Reference and title	Scope	Status
WG 3 - IoT Architecture: standardization in the area of IoT vocabulary, architecture, and frameworks	ISO/IEC 20924, Definitions and vocabulary	This draft provides a definition of IoT along with a set of terms and definitions. It represents a terminology foundation for the IoT.	Under development
	ISO/IEC 30141, Internet of Things Reference Architecture (IoT-RA)	This draft specifies general IoT reference architecture defining system characteristics, a conceptual model, a reference model and architecture views of IoT.	Under development
	Technical Report (TR) on IoT Edge Computing	This draft provides basic concepts of IoT edge computing architecture, terminologies, values, characteristics, challenges, use cases and main technologies (including data management, coordination, processing, network functionality, heterogeneous computing, security, hardware / software optimization) of edge computing for IoT systems applications. It is also considered to assist in the identification of potential areas for standardization in edge computing for IoT.	Under development
	ISO/IEC 30147, Methodology for trustworthiness of IoT system / service	This draft provides a methodology to implement and maintain trustworthiness in IoT system/service. The methodology is not targeted to a certain application area of the IoT system/service but for a generic IoT system/service common to various application areas.	Under development
WG 4 - IoT Interoperability: standardization in the area of IoT interoperability, connectivity, conformance and testing.	ISO/IEC 21823-1, Interoperability for Internet of Things Systems - Part 1: Framework	This draft provides an overview of interoperability requirements and a framework for interoperability for IoT systems. It aims to enable IoT systems to be built in such a way that all the entities of the IoT ecosystem are able to exchange information and mutually use the information in an efficient way. The goal of this draft is to ensure that all parties involved in developing and using IoT systems have a common understanding of interoperability as it applies within and out of the various entities.	Under development
	ISO/IEC 21823-2, Interoperability for Internet of Things Systems - Part 2: Transport interoperability	This draft presents a conceptual model for network connection interoperability and requirements for interoperable IoT systems to enable information exchange, peer-to-peer connectivity and seamless communication within and out of the IoT systems.	Under development
	ISO/IEC 21823-3, Interoperability for Internet of Things Systems - Part 3: Semantic interoperability	This draft provides a basic concept of semantic interoperability for IoT systems, as described in the facet model of ISO 21823 Part 1. It also describes technologies supporting for semantic interoperability of IoT systems.	Under development

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

Table 28: Standards and projects of ISO/IEC JTC 1/SC 41 (updated in March 2018)

5.2.3.2 Study Groups (SGs)

Study Groups are formed to study their dedicated IoT related topics and to provide a recommendation to the subcommittee. A recommendation include a report, extension of the study period (if continuation of the study is required), recommendation(s) to assign new projects to the existing WG or creation of new WG(s), etc. to the ISO/IEC JTC 1/SC 41 in a defined timeframe. Highlights of the active SGs under JTC 1/SC 41 are provided in Table 29.

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

Table 29: ISO/IEC JTC 1/SC 41 Study Groups and their objectives (updated in March 2018)

5.3 International Telecommunication Union’s Telecommunication Standardization Sector (ITU-T)

This section provides initiations of **ITU-T’s** activities in technical standardization related to IoT and Smart Cities, particularly current projects of **SG 20**, different focus groups and IoT related works of other SGs.

5.3.1 ITU-T SG 20 - Internet of things (IoT) and smart cities and communities (SC&C)

The objective of this SG 20 is to standardize requirements of IoT technologies. It was initially focused on IoT applications in Smart Cities and Communities (SC&C). This SG is composed of two working parties including study questions dealing with different aspects of IoT standardization, as listed in Table 30.

Study questions	IoT related activities
Q1/20 - End to end connectivity, networks, interoperability, infrastructures and Big Data aspects related to IoT and SC&C	Development of Recommendations concerning interoperability of IoT devices, networks and vertical areas (e.g. smart homes, smart manufacturing, etc.) for reliable IoT communications and services.
Q2/20 - Requirements, capabilities and use cases across verticals	Aims at studying IoT services and applications in different vertical areas .
Q3/20 - Architectures, management, protocols and Quality of Service	Development of Recommendations related to IoT architecture, management mechanisms, protocols and quality of service.
Q4/20 - e/Smart services, applications and supporting platforms	Facilitate the development of e/Smart services and applications among heterogeneous IoT environments .
Q5/20 - Research and emerging technologies, terminology and definitions	Contribute to define a common terminology for IoT.
Q6/20 - Security, Privacy, Trust, and Identification for IoT and SC&C	Development of Recommendations in the areas of security, privacy, trust, and identification for IoT.

Table 30: ITU-T SG 20 Study questions and IoT related activities (updated in March 2018)

5.3.2 ITU-T JCA IoT and SC&C - Joint Coordination Activity on Internet of Things and Smart Cities and Communities

The ITU-T - **Joint Coordination Activity on Internet of Things and Smart Cities and Communities** (JCA IoT and SC&C) coordinates the ITU-T work on IoT and SC&C and ensures cooperation and communication with external bodies working in this field. It also maintains a list of published standards and projects related to IoT⁵⁷. This list includes more than 550 standards by 12 SDOs and covers 25 different activity domains [121] (e.g., IoT, RFID, sensor networks, M2M, identity management, smart cities, geospatial information, etc.).

^{57]} <https://www.itu.int/en/ITU-T/jca/iot/Documents/deliverables/Free-download-IoT-roadmap.doc>

5.3.3 ITU-T FG-DPM - Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities

The **Focus Group on Data Processing and Management** to support IoT and Smart Cities & Communities (FG-DPM) plays a vital role in providing a platform to share views, to develop a series of deliverables, and showcasing initiatives, projects, and standards activities linked to the data processing and management and establishment of IoT ecosystem solutions for data focused cities [122]. It is composed of following five WGs to provide different activities from various aspects of DPM:

- WG1 - Use Cases, Requirements and Applications/Services;
- WG2 - DPM Framework, Architectures and Core Components;
- WG3 - Data sharing, Interoperability and Blockchain;
- WG4 - Security, Privacy and Trust including Governance;
- WG5 - Data Economy, commercialization, and monetization.

FG-DPM is also working on the development of deliverables in different topics, such as IoT and SC&C Applications and Services using DPM, DPM Framework for Data-driven IoT and SC&C, overview of IoT and Blockchain, and Data Governance Framework for IoT and SC&C.

5.3.4 Other ITU-T activities related to IoT

Apart from SG 20, other SGs are also actively involved in the development of Recommendations in this area, as listed in Table 31. Please refer Smart ICT Standards Analysis⁵⁸ for a list of IoT Recommendations⁵⁹.

Study Group	Related areas	Status of work
SG 2 - Operational aspects	Numbering Naming, Addressing and Identification	Active
SG 3 - Economic and policy issues	Tariff, Regulatory aspects, Roaming	Active
SG 11 - Protocols and test specifications	Monitoring, Testing	Active
SG 13 - Future networks (& cloud)	Foundations (overview, terms and definitions, requirements, etc.)	Achieved
SG 16 - Multimedia	IoT applications and services	Achieved
SG 17 - Security	Security, privacy, identity	Active

Table 31: ITU-T additional activities related to IoT standardization (updated in March 2018)

^{58]} <https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2018/standards-analysis-smart-ict-2-0.pdf>

^{59]} <https://www.itu.int/en/ITU-T/publications/Pages/default.aspx>

5.4 European Telecommunications Standards Institute [ETSI]

ETSI has long been involved in IoT standardization. It started working on Machine-to-Machine (M2M) communications with the creation of ETSI/TC M2M technical committee. ETSI has progressively gained importance in the IoT landscape since the creation of this committee. Along with these developments, ETSI is one of the founding member of the 3rd Generation Partnership Project (3GPP) (see Section 5.5.1) and the oneM2M initiative (see Section 5.5.8). It is also actively engaged in the Alliance for Internet of Things Innovation (AIOTI), chairing its WG 3 dedicated to IoT standardization (see Section 5.5.2).

ETSI/TC M2M (ETSI/TC SmartM2M now) is not only focusing on M2M standardization but also on solutions to address IoT standardization gaps identified by European Commission Large Scale Pilot projects [119]. It has now published more than 60 standards directly related to IoT, which are publicly available on ETSI website⁶⁰. Some major standardization activities of ETSI to the IoT related applications are smart appliances, smart metering, smart cities, smart grids, ITS, security, low power supplies and radio spectrum [119].

5.4.1 ETSI/TC Smart M2M - Smart Machine-to-Machine Communication

ETSI/TC - Smart M2M is responsible for providing specifications to M2M services and applications, including IoT and smart cities [123]. It also provides technical specifications on transposition of oneM2M specifications. Some of the published standards related to IoT and M2M are:

- ETSI TR 103 376 - SmartM2M; IoT LSP use cases and standards gaps - published in November 2016⁶¹, which addresses standardization gaps identified in European Commission Large Scale Pilot projects;
- oneM2M releases - release-2015 and release-2016 - both offer a common M2M Service Layer that can be readily embedded within various hardware and software, and rely upon to connect the myriad of devices in the field with M2M application servers worldwide [124];
- The Smart Appliances Reference Ontology (SAREF) - initially published in 2015 and updated in 2016⁶². It provides a reference ontology to serve as an interoperability enabler for appliances relevant for energy efficiency [125], which is mapped with oneM2M Base Ontology and thus runs with oneM2M-compliant communication platforms. ETSI is currently working on extending SAREF Technical Specifications to include semantic models addressing different domains, such as smart cities, industry and manufacturing, smart agriculture and the food chain, automation, eHealth/ageing-well, and wearables [126].

Moreover, **ETSI Specialist Task Force 505**⁶³ published, in close collaboration with AIOTI (see section 5.5.2), two technical reports referenced as ETSI/TC Smart M2M publications:

- ETSI TR 103 375 V1.1.1 (2016-10) - SmartM2M; IoT standards landscape and future evolutions - overviews the IoT standards landscape: requirements, architecture, protocols, tests, etc. to provide the roadmaps of the IoT standards [127].
- ETSI TR 103 376 V1.1.1 (2016-10) - SmartM2M; IoT LSP use cases and standards gaps - studies missing IoT functionalities that have been identified in SDOs, gaps in IoT standardization and proposes some recommendations to overcome these potential gaps [128].

⁶⁰ <http://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&start-Date=1988-01-15&harmonized=0&keyword=IoT&TB=&stdType=&frequency=&mandate=&sort=1>

⁶¹ ETSI TR 103 376 V1.1.1 (2016-10) - SmartM2M; IoT LSP use cases and standards gaps http://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf

⁶² ETSI TS 103 264 V2.1.1 (2017-03) - SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping http://www.etsi.org/deliver/etsi_ts/103200_103299/103264/02.01.01_60/ts_103264v020101p.pdf

⁶³ <https://portal.etsi.org/STF/stfs/STFHomePages/STF505>

5.4.2 Other ETSI activities related to IoT

Apart from above mentioned standardization activities of ETSI/TC SmartM2M, a list of other M2M/IoT related standardization activities of ETSI is presented in Table 32.

Study Groups	IoT-related topics	Status of work
TC ATTM - Access, Terminals, Transmission and Multiplexing committee	Energy efficiency in Smart Cities	Active
TC CYBER - Cyber security	Security of IoT and related technologies and applications	Active
TC ERM - Electromagnetic Compatibility and Radio Spectrum Matters	Low Throughput Networks (LTN) and Radio spectrum	Active
TC ITS - Intelligent Transport Systems	Intelligent Transport Systems (ITS)	Active
TC SmartBAN - Smart Body Area Network	E-health (Body Area Network technologies)	Active
CEN/CLC/ETSI CG-SM - Smart Meters Coordination Group	smart meters	Achieved
CEN/CLC/ETSI CG-SEG - Smart Energy Grid Coordination Group	smart grids	Active
ISG CDP - City Digital Profile	Smart Cities	Active
ISG CIM - Context Information Management	Interoperability for smart city applications	Active
ISG LTN - Low Throughput Networks	Ultra narrowband radio technology for very low data rates for ultra-long autonomy devices	Achieved
ISG OEU - Operational energy Efficiency for Users	Energy efficiency in smart cities	Active
ISG SMT - Surface Mount Technique	Embedded M2M communication modules based on Surface Mount Technology	Achieved

Table 32: ETSI additional activities related to IoT standardization (updated in March 2018)

5.5 IoT fora and consortia

This section highlights the landscape of SDOs working on IoT related standardization in addition to ISO/IEC JTC1, ITU-T and ETSI as illustrated in Figure 18. The term *fora* and *consortia*, used in this whitepaper, means associations regrouping individuals, companies, organizations or governments with a common objective of participating in the creation of *de facto*⁶⁴ standards or technical specifications [129]. Particularly, this section provides overview of fora and consortia having strong relationships with the recognized SDOs presented in the previous sections.

5.5.1 Third Generation Partnership Project [3GPP]

The **Third Generation Partnership Project** (3GPP) is a joint initiation of seven telecommunications standard development organizations, namely ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC in 1994. Its activities include development of reports and specifications that define 3GPP technologies [130], such as UMTS, HSPA+ and LTE. The scope of this project is to prepare, approve and maintain globally applicable technical specifications and technical reports [131] for:

- The 3rd Generation and beyond Mobile System based on the evolved 3GPP core networks, and the radio access technologies supported by the Partners (i.e., UTRA both FDD and TDD modes), to be transposed by the organizational partners into appropriate deliverables (e.g., standards);
- The Global System for Mobile communication (GSM) including GSM evolved radio access technologies (e.g. General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE));
- The IP-Multimedia Subsystem (IMS) developed in an access independent manner.

3GPP specifications represent one of the most important enabler for the IoT in terms of connectivity. 5G is considered as a next major technology step for IoT. Worldwide commercial launch of 5G is expected by 2020⁶⁵.

5.5.2 Alliance for Internet of Things Innovation [AIOTI]

The **Alliance for Internet of Things Innovation** (AIOTI) has been created in 2015 at the initiative of the EC to develop and support cooperation among IoT stakeholders in Europe, with the objective of unleashing the full potential of IoT [132]. More than 200 organizations are already member of AIOTI. It is composed of thirteen working groups to provide research and standardization activities on IoT (see Figure 21).

⁶⁴ "De facto standards" is sometimes used for common solutions and practices that have not been formally developed and agreed upon. In this document, this term is used for technical specifications published by other SDOs than the recognized ones (i.e. ISO, IEC, ITU, CEN, CENELEC and ETSI)

⁶⁵ <https://www.lifewire.com/5g-availability-world-4156244>

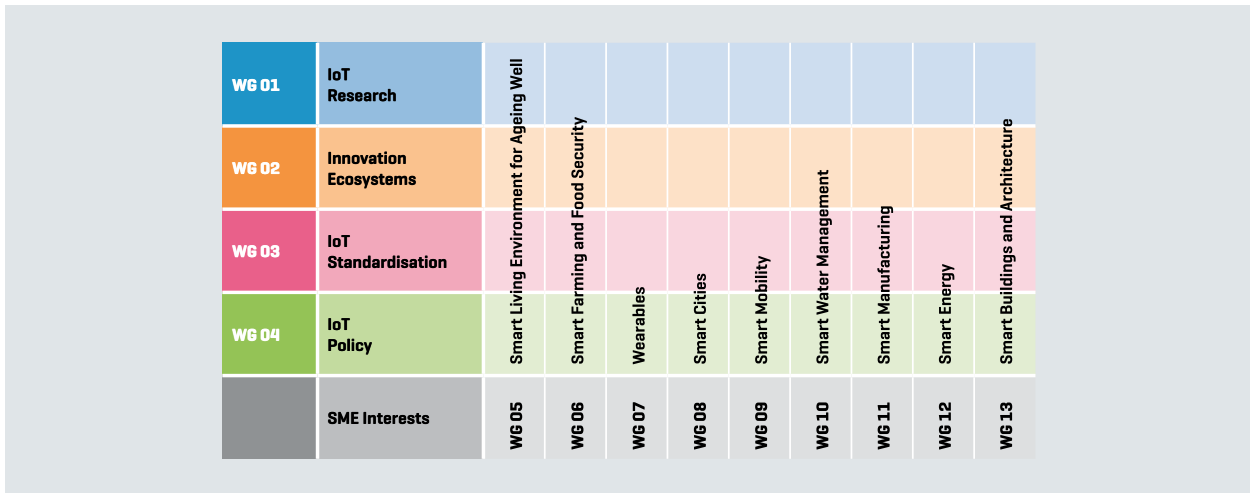


Figure 21: AIOTI working groups

Working group 3 on IoT standardization is chaired by ETSI. Some major deliverables by this WG on IoT standards are:

- IoT Landscape and IoT LSP Standard Framework Concepts – This report provides an overview of SDOs involved in IoT standardization. It offers several ways of visualizing the IoT SDOs landscape in order to simplify and facilitate the usage of information received from various IoT application domains [133].
- IoT High Level Architecture (HLA) provides an initial proposal for a high-level IoT architecture to serve as a basis for discussion within AIOTI, referred to as the AIOTI HLA (High-level architecture) [134].
- IoT Semantic interoperability recommendations provide an overview of the problem statement, value proposition and key techniques pertaining to semantic interoperability within and across the AIOTI Large Scale Pilots. It also provides the details of ongoing standardization work to support in semantic interoperability of IoT [135].

Recent versions of AIOTI WG 3 publications⁶⁶ include updates of the deliverables presented above and new reports. For instance, it published a report on Identifiers in Internet of Things (IoT)⁶⁷ in February 2018 providing a high level discussion about this topic.

5.5.3 Association for Automatic Identification and Mobility (AIM)

Association for Automatic Identification and Mobility (AIM) is an industry association developing specifications for automatic identification and data capture (AIDC) technologies [136]. It is composed of five industry groups. One of them is a joint collaboration of AIM member companies aiming at influencing IoT definition, particularly in the areas of barcode, RFID and other AIDC technologies [137]. AIM has liaised with ISO/IEC JTC 1/SC 41, ISO/IEC JTC 1/SC 31 - Automatic identification and data capture techniques as well as with ETSI. Moreover, AIM is the Registration Authority (RA)⁶⁸ for two international standards, which is responsible for the assignment of unique registration elements required by these standards for maintaining a register of the elements [120]:

- ISO/IEC 15459, Information technology -- Automatic identification and data capture techniques -- Unique identification (composed of six parts)⁶⁹;
- ISO/IEC 29160, Information technology -- Radio frequency identification for item management -- RFID Emblem⁷⁰.

⁶⁶] <https://aioti.eu/aioti-wg03-reports-on-iot-standards/>

⁶⁷] https://aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf

⁶⁸] The RA is a competent body with the requisite infrastructure for ensuring the effective allocation of registration elements required by certain ISO standards. These bodies are designated by ISO to serve as the unique RA for particular standards, which creates a de facto monopoly situation [120].

⁶⁹] http://www.aimglobal.org/?Reg_Authority15459

⁷⁰] http://www.aimglobal.org/?Reg_Authority29160

5.5.4 Global Standards One [GS1]

Global Standards One (GS1) is an industrial consortium, with over a million member organizations, which develops specifications to identify, capture and share supply chain data [138]. Its objective is to provide specifications for an efficient and cost-effective supply chain, allowing different industries (retail, healthcare, transport and logistics, foodservice, technical industries and humanitarian logistics) to track their products and to communicate information about them in an efficient way to their customers, partners and suppliers all along the supply chain process.

GS1 is in liaison with number of SDOs, including ISO/IEC JTC 1/SC 41, ISO/IEC JTC 1/SC 31, ITU-T, AIOTI, IIC and W3C. Number of GS1 specifications has been published as international standards under GS1 and JTC 1/SC 31. GS1 specifications are supporting the development of IoT in different ways [139], such as:

- Specifications to allow identification of real-world entities, making it possible to produce and share data about it;
- Specifications to automatically capture data from real-world entities (e.g., through the use of barcodes or RFID technologies);
- Specifications to share data internally as well as with stakeholders (as an architecture), with the objective of providing electronic business transaction solutions or electronic visibility on physical and digital world all along the supply chain process.

5.5.5 Institute of Electrical and Electronics Engineers [IEEE]

The **Institute of Electrical and Electronics Engineers** (IEEE) is a technical professional organization with thousands of members over 160 countries. The common objective of IEEE is to advance technology in number of areas including IoT with the development of industry specifications⁷¹ [140]. In particular, it launched an IoT initiative in 2014 with the following objectives [141]:

- To serve as a gathering place for the global technical community working on the IoT;
- To provide a platform where professionals learn, share knowledge, and collaborate on this sweeping convergence of technologies, markets, applications, and the Internet.

In this frame, IEEE created an IoT Architecture WG in 2014, which is responsible for the development of standards, registered as IEEE P2413, for an architectural framework of the IoT. The scope of this project is to define an architectural framework for the IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains [142]. The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements. It also provides a blueprint for data abstraction and the quality “quadruple” trust that includes protection, security, privacy, and safety. Furthermore, this standard provides a reference architecture that builds upon a reference model. The reference architecture covers definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems. This standard leverages existing applicable standards and identifies planned or ongoing projects with a similar or overlapping scope.

5.5.6 Internet Engineering Task Force [IETF]

The **Internet Engineering Task Force** (IETF) is an open international community of information technology professionals developing **Requests For Comment** (RFC) that are equivalent to technical specifications. IETF aims at developing the efficiency of the internet as well as to keep it in evolving with the use of last technological developments [143].

⁷¹] A list of IoT related standards is available on IEEE website: <http://standards.ieee.org/innovate/iot/stds.html>

IETF has identified IoT as a topic of particular interest and formed an IETF IoT directorate, which is an advisory group of experts coordinating with IoT related works among IETF working groups and promoting IoT related RFCs within other SDOs [144]. This task force is involving in IoT standardization since 2005, when the first IoT-related WG was created on IPv6 over Low-power WPAN (6LoWPAN). Since then, numbers of IETF WGs have undertaken multiple activities in this area^{72,73}. For instance, one of the most active is a Constrained RESTful Environments (core) WG, which aims to extend the Web architecture to the most constrained networks and embedded devices [145].

5.5.7 Industrial Internet Consortium [IIC]

The **Industrial Internet Consortium (IIC)** was created to identify, aggregate and promote Industrial Internet best practices in 2014. Its members are focused on solving the tough challenges in the Industrial IoT (IIoT): Interoperability through an open framework architecture, security requirements, specifications for standards and more [146]. IIC is not directly developing standards but supports for the current development of standardization in this area.

IIC has provided Industrial Internet Reference Architecture (IIRA) for IIoT systems. In relation with this work, it is worth noting that IIC is actively participating in IIoT interoperability efforts, with the launch of a collaboration with **Plattform Industrie 4.0** (German stakeholders platform that has developed **RAMI 4.0**) to explore potential alignment between their own reference architectures. In this frame, a joint report has been recently published. It maps and aligns two reference architectures that contain similar and complementary elements for addressing IIoT challenges from different perspectives and across different industrial domains [147].

5.5.8 oneM2M

oneM2M is a joint partnership of eight SDOs active in ICT standardization (ARIB - Association of Radio Industries and Businesses-Japan, ATIS - Alliance for Telecommunications Industry Solutions-US, CCSA - China Communications Standards Association, ETSI - European Telecommunications Standards Institute, TIA - Telecommunications Industry Association-US, TSDSI - Telecommunications Standards Development Society- India, TTA - Telecommunications Technology Association-Korea, and TTC - Telecommunication Technology Committee-Japan)⁷⁴. Its objective is to develop technical specifications for a common M2M Service Layer that can be embedded within various hardware and software to connect the wide range of devices worldwide with M2M application servers [124].

This partnership is playing an important role in developing interoperability within and out of the IoT system. Growing number of member organizations (more than 200 member organizations) demonstrates its success to attract and involve organizations active in the M2M/IoT area in different business domains, such as telematics and intelligent transportation, healthcare, utilities, industrial automation or smart homes. Standards release⁷⁵ of oneM2M for basic connectivity between oneM2M and IoT applications are:

- 1st release (January 2015) - provides a common framework for communication service providers to support applications and services;
- 2nd release (September 2016) - provides enhanced security, features for home domain and industrial domain deployment, semantic interoperability, and interworking with popular IoT device ecosystems;
- 3rd release (under development) - will focus on the use of oneM2M for industrial IoT and will include interworking support for industrial technologies and improved support for mobile IoT technologies standardized by 3GPP such as Narrowband IoT (NB-IoT). It will also address Smart Cities and include supporting documentation and tools to assist developers [126].

^{72]} <https://www.ietfjournal.org/internet-of-things-standards-and-guidance-from-the-ietf/>

^{73]} <https://www.ietfjournal.org/rough-guide-to-ietf-101-internet-of-things/>

^{74]} <http://www.onem2m.org/about-onem2m/partners>

^{75]} These specifications are publicly available on oneM2M website (<http://www.onem2m.org/technical/published-documents>) and are also published as ETSI normative documents.

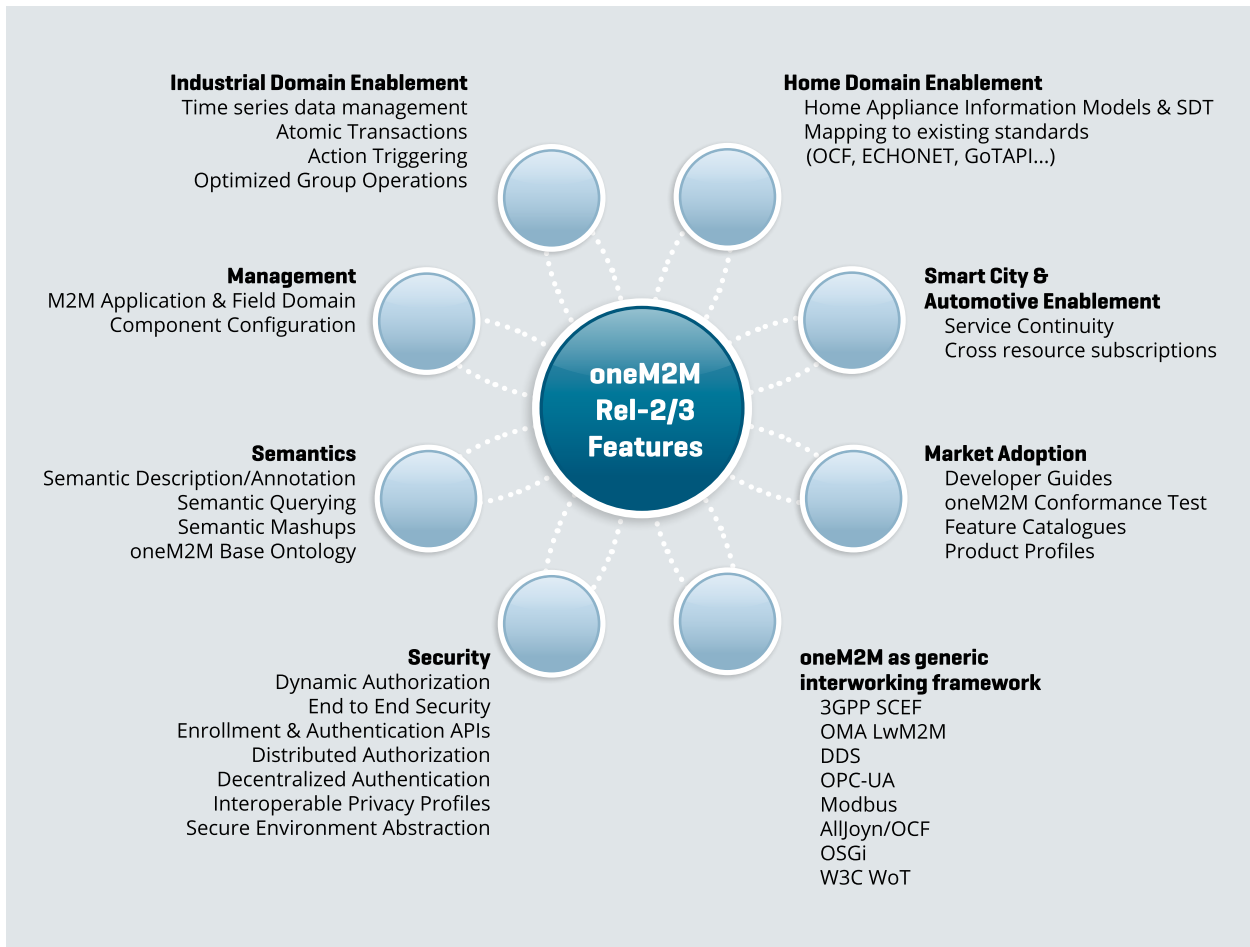


Figure 22: Summary of oneM2M Release 2 and 3 features [148]

5.5.9 Open Geospatial Consortium [OGC]

The Open Geospatial Consortium (OGC) is an industrial consortium of more than 525 member organizations, developing specifications in the geospatial area [149]. OGC mainly covers ten domains: aviation, built environment and 3D, business intelligence, defence and intelligence, emergency response and disaster management, energy and utilities, geoscience and environment, government and spatial data infrastructure, mobile internet and location services, sensor webs [150]. It has liaisons with several ISO and ISO/IEC JTC 1 entities, including ISO/IEC JTC 1/SC 41, ISO/IEC JTC 1/SC 31, ISO/IEC JTC 1/WG 9 - Big Data and ISO/TC 211 - Geographic information/ Geomatics. Number of OGC specifications has been published under ISO/TC 211, such as the Geography Markup Language (GML) published as ISO 19136 in 2007. In regards to the IoT development, OGC is particularly involved in the development of standards supporting sensor technologies, through its Sensor Web Enablement Domain Working Group (SensorWeb DWG)⁷⁶ and its SensorThings Standards Working Group (SensorThings SWG)⁷⁷.

⁷⁶] <http://www.opengeospatial.org/projects/groups/sensorwebdwg>

⁷⁷] <http://www.opengeospatial.org/projects/groups/sensorthings>

5.5.10 Open Connectivity Foundation [OCF]

The Open Connectivity Foundation (OCF) is an industry consortium of more than 350 members, consisting of different companies as well as individuals. Its objective is to develop specifications that define a secure communication and data interoperability framework aiming to connect IoT devices and manage the flow of information among them, regardless the technology used or the service provider [151]. In addition, it is also maintaining Universal Plug and Play (UPnP) specifications, which were originally developed by UPnP Forum [152]. It is collaborating with ISO/IEC JTC 1/SC 41, particularly on standardization process of IoT interoperability and applications. The foundation is also one of the approved Publicly Available Specifications (PAS) Submitter of ISO/IEC JTC 1, meaning that it can submit its specifications as drafts for review and approval as international standards of ISO/IEC JTC 1 [153]. In this frame, OCF proposes its specification for the publication as international standards through the PAS process. JTC 1 is currently in the process of adopting OCF specification (ISO/IEC 30118), which is composed of six parts as:

- Part 1: Core specification;
- Part 2: Security specification;
- Part 3: Bridging specification;
- Part 4: Resource type specification;
- Part 5: Smart home device specification;
- Part 6: Resource to AllJoyn interface mapping specification.

5.5.11 World Wide Web Consortium [W3C]

The World Wide Web Consortium (W3C) is an international community aiming at leading the World Wide Web to its full potential by developing open standards (protocols and guidelines) that ensure the long-term growth of the Web [154]. W3C launched Web of Things (WoT) Working Group⁷⁸ at the end of 2016 to counter the fragmentation of the IoT through standard complementing building blocks (e.g., metadata and APIs) that enable easy integration across IoT platforms and application domains [155]. The WoT WG is working in collaboration with many IoT related SDOs including IETF, oneM2M, OCF and IIC, to develop the following normative specifications:

- WoT Architecture - It is expected to define a high-level architecture for the individual WoT building blocks as well as necessary platform configurations. Furthermore, it confines the deployment scenarios targeted by WoT;
- WoT Thing Description - It is expected to define an ontology and a binding to short names for cross-domain metadata for the WoT, including the data model exposed to applications, as well as security and communications metadata;
- WoT Scripting APIs - It is expected to define a suite of cross-domain APIs for application developers for the WoT.

^{78]} <https://www.w3.org/WoT/WG/>

6

Conclusions and outlook

6. Conclusions and outlook

Information and Communication Technologies (ICT) are becoming essential elements of the global economy as well as today's society and life. Both public and private sectors across the world are transforming their countries and businesses with ICT programs ranging from research and innovation, infrastructure building, and skills development. Internet of Things (IoT) as one of the ICT innovations has attracted unparalleled attention of various stakeholders across the world in the past decade. The IoT is assumed as disruptive innovation to improve the business process within and across sectors. It describes a world where anything can be connected and can interact in an intelligent fashion. Therefore, it is popular to realize the scenarios, where internet connectivity and computing capability extends to a variety of connecting things.

This white paper surveyed the Internet of Things (IoT) technology from three different viewpoints: IoT basic concepts and its driving technologies, economic and business prospect, and technical standards watch.

The first part of **IoT basic concepts and its driving technologies** aimed to provide basic fundamental concept of IoT overviewing started from the basic building blocks of IoT, definitions of IoT provided by different stakeholders along with general characteristics to various application domains of IoT to enhance the quality of life of the citizens. To introduce the driving technologies of IoT, the second part of this study presented its origin, concepts of supporting technologies. The data flow architecture from sensing environment to the use of sensed information by various application domains were described together with highlights of driving technologies in each data flow phase. The importance of new computing concepts were also introduced to understand their relevancy in IoT environment. The strength of the IoT is powered by different technological landscape. At the same time, it owns various limitations due to adoption of such technologies. A primary insight on the most prominent issues among various limitations of the IoT technology from the perspective of technology, security, privacy, trust, regulatory are overviewed together with possible countermeasures to avoid such challenges.

As discussed in the beginning, IoT technologies are applied to enhance the quality of life of the citizens. Its adoption in various value chains is expected to reduce costs of current operations and improve the quality of services provided to the end users. To see its impact to the economy at large, the global trends of IoT technology, business opportunities, challenges as well as insights on its impact in the long-run were summarized in **economic and business prospects** part. According to different reports, smart manufacturing, smart transportation, smart utilities, smart logistics followed by many other sectors, such as connected home, health sectors, banking and financial sectors are the most potential application sectors of IoT.

In IoT, interoperability issue is becoming challenging due to the use of multiple communication languages of different stakeholder of IoT ecosystem. Similarly, availability of security and privacy standards are necessary for efficient implementation of identity management platforms. In this context, technical standardization is expected to play a key role in qualitative development, coherent source of knowledge, and continuous improvement of these technologies with common language of communication among its stakeholders. **Technical standards watch** part of this white paper provided an overview of various developments in the areas of technical standardization. In particular, complete information concerning ISO/IEC JTC 1/SC 41: Internet of Things and related technologies is provided because this technical committee is one of the prominent in standardizing IoT and related technologies. Then, a summary of other initiatives launched by ETSI, ITU-T as well as other fora and consortia is outlined.

In Luxembourg, ILNAS – with the support of ANEC G.I.E. – is actively following the standardization developments of Internet of Things and related technologies, building on the national Policy for ICT Technical Standardization (2015-2020)⁷⁹. The main objectives of this policy are to foster and strengthen the national ICT sector's involvement

⁷⁹ <https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf>

in the standardization work. To achieve this, ILNAS is conducting three intertwined projects: a) developing market interest and involvement, b) promoting and reinforcing market participation, and c) supporting and strengthening the education about standardization and related research activities.

In line with the first project, ILNAS and ANEC G.I.E. – in collaboration with the Ministry of the Economy – is publishing this white paper with the goal of providing a comprehensive analysis of IoT from technological, economic, as well as technical standardization perspectives. Among other outcomes, this white paper aims to create awareness and interest concerning relevant standardization developments within the national market.

Similarly, conforming to the second project, ILNAS is already a P-member of ISO/IEC JTC1/SC 41 in which, 12 experts⁸⁰ are currently building and reinforcing national participation. In addition, ILNAS is closely following the developments of ITU-T, such as SG 20, JCA IoT and SC&C, and FG-DPM, as well as ETSI's TC Smart M2M, and actively transferring relevant information to the market. Interested stakeholders in Luxembourg could involve in the standards development process by becoming delegates (e.g., of ISO/IEC JTC 1/SC 41)⁸¹.

Finally, for the third project, ILNAS is strengthening its relations with the University of Luxembourg (SnT) in order to facilitate standards-related education and research. As part of this partnership, the second edition of the university certificate program "Smart ICT for Business Innovation"⁸² is currently underway. Based on the experiences from these certificate programs, ILNAS and University of Luxembourg aim to launch a full-fledged Master degree "Smart Secure ICT for Business Innovation" where digital trust and technical standardization will be at the heart of the program and be taught transversal to various Smart ICT topics, including IoT.

These three projects will allow the national market to make rapid progress and reap the benefits of technical standardization effectively. They will also serve as a basis for ILNAS to formulate the next national Policy for ICT Technical Standardization (2020-2030) in which IoT will be an integral part.

⁸⁰] As of 1st June 2018: <https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/information-sensibilisation/ilnas-oln-registre-national-delegues-normalisation/ilnas-oln-registre-national-delegues-normalisation.pdf>

⁸¹] <https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation/experts-normalisation.html> [156]

⁸²] <http://smartict.uni.lu>

References

- [1] "The Internet of Things: An Overview, understanding the Issues and Challenges of a More Connected World," October 2015. [Online]. Available: www.internetsociety.org. [Accessed April 2018].
- [2] "Market Pulse Report, Internet of Things (IoT) Discover Key Trends & Insights on Druptive Technologies & Innovations," GrowthEnabler, April, 2017.
- [3] D. Mendez, I. Papapanagiotou and B. Yang, "Internet of Things: Survey on Security and Privacy," Cornell University Library, 2017.
- [4] A. Furness, "A Framework Model for the Internet of Things," GRIFS/CASAGRAS, 2008.
- [5] D. Gil, A. Ferrández, H. Mora-Mora and J. Peral, "Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services," *Sensors*, vol. 16, no. 7, 2016.
- [6] "The internet of Things: ITU Internet report," 2005. [Online]. Available: <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>. [Accessed April 2018].
- [7] "Internet of things in 2020: A Roadmap for the Future," 2016. [Online]. Available: https://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf. [Accessed April 2018].
- [8] A. D. Saint-Exupery, "Internet of Things, Strategic Research Roadmap," European Commission Social Media: Brussels, Belgium, 2009.
- [9] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1-31, 2014.
- [10] R. Gupta, "ABC of Internet of Things: Advancements, Benefits, Challenges, Enablers and Facilities of IoT," in *IEEE Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016.
- [11] J. Greenough, "The Internet of Things is Rising: How the IoT Market will Grow across sectors," Business Insider Intelligence, October 2014.
- [12] I. Bojanova, "What Makes Up the Internet of Things?," *Computing Now*, 2015. [Online]. Available: <https://www.computer.org/web/sensing-iot/content?g=53926943&type=article&urlTitle=what-are-the-components-of-iot->.
- [13] "<https://www.itu.int/ITU-T/>," June 2012. [Online]. Available: <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=en>. [Accessed 10 2017].
- [14] "IoT 2020: Smart and secure IoT platform," 2016. [Online]. Available: <http://www.iec.ch/whitepaper/iotplatform/>. [Accessed September 2017].
- [15] C. Jiming, F. Hannes and L. Xu, "Special Issue: Wireless Sensor and Robot Networks: Algorithms and Experiments," *Computer Communications*, vol. 35, no. 9, pp. 1017-1164, 2012.
- [16] F. M. Al-Turjmanab, H. S. Hassaneina and M. A. Ibnkahlab, "Efficient deployment of wireless sensor networks targeting environment monitoring applications," *Computer Communications*, vol. 36, no. 2, pp. 135-148, 2013.
- [17] E. Ancillotti, R. Bruno and M. Conti, "Review: The role of communication systems in smart grids: Architectures, technical solutions and research challenges," *Computer Communications*, vol. 36, no. 17-18, pp. 1665-1697, 2013.
- [18] S. Bin, L. Yuan and W. Xiaoyi, "Research on Data Mining Models for the Internet of Things," in *International Conference on Image Analysis and and Signal Processing*, 2010.
- [19] A. Chepuru and V. Rao, "A SURVEY ON IOT APPLICATIONS FOR INTELLIGENT TRANSPORT SYSTEMS," *International Journal of Current Engineering and Scientific Research (IJCESR)*, vol. 2, no. 8, pp. 116-127, 2015.
- [20] J. Lloret, J. Tomas, A. Canovas and L. Parra, "An Integrated IoT Architecture for Smart Metering," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 50-57, 2016.
- [21] S. Tonyali, O. Cakmak, K. Akkaya, M. Mahmoud and I. Guvenc, "Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid AMI networks," *IEEE Internet of Things*, vol. 3, no. 5, pp. 709 - 719, 2016.
- [22] Y. Saleem, N. Crespi, M. H. Rehmani and R. Copeland, "Internet of Things-aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," *Cornell University Library*, pp. 1-30, April, 2017.

- [23] F. Calabrese, M. Conti, D. Dahlem, G. D. Lorenzo and S. Phithakkitnukoon, "Special issue on Pervasive Urban Applications," *Pervasive and Mobile Computing*, vol. 9, no. 5, pp. 613-750, 2013.
- [24] D. Uckelmann, "A Definition Approach to Smart Logistics," in *Part of the Lecture Notes in Computer Science book series (LNCS, volume 5174), International Conference on Next Generation Wired/Wireless Networking*, 2008.
- [25] P. A. Laplante and N. Laplante, "The Internet of Things in Healthcare Potential Applications and Challenges," *IT Pro IEEE Compute Society*, pp. 2-4, May/June 2016.
- [26] K. Ashton, "RFID Journal," June 2009. [Online]. Available: <http://www.rfidjournal.com>. [Accessed 23 August 2017].
- [27] GS1 EPC Tag Data Standard 1.6, 2011. [Online]. Available: https://www.gs1.org/sites/default/files/docs/epc/tds_1_6-RatifiedStd-20110922.pdf. [Accessed 09 2017].
- [28] "ILNAS White paper Digital Trust for smart ICT," October 2016. [Online]. Available: <https://portail-qualite.public.lu/fr/publications/confiance-numerique/etudes/white-paper-digital-trust-october-2016.html>.
- [29] J. S. Wilson, "Chapter 1 - Sensor Fundamentals, In Sensor Technology Handbook," in *In Sensor Technology Handbook*, www.sciencedirect.com, 2005, pp. 1-20.
- [30] J. S. Wilson, "Sensors Fundamentals," in *Sensor technology Handbook*, Elsevier, 2014.
- [31] "OECD Digital Economy Outlook 2015," OCED publishing, 2015.
- [32] K. Gama, L. Touseau and D. Donsez, "Combining heterogeneous service technologies for building an Internet of Things middleware," *Computer Communications*, vol. 35, no. 4, pp. 405-417, 2012.
- [33] I. Catherine, R. Tardy, N. Aakvaag, B. Myhre and R. Bahr, "Comparison of wireless techniques applied to environmental sensor monitoring," SINTEF Digital, 2017.
- [34] M. Buzzi, M. Conti, C. Senette and D. Vannozi, "Measuring UHF RFID tag reading for document localization," in *IEEE International Conference on RFID-Technologies and Applications*, 2011.
- [35] F. M. Al-Turjman, H. S. Hassanein and M. A. Ibnkahla, "Efficient deployment of wireless sensor networks targeting environment monitoring applications," *Computer Communications*, vol. 36, no. 2, pp. 135-148, 2013.
- [36] S. Li, S. Peng, W. Chen and X. Lu, "INCOME: Practical land monitoring in precision agriculture with sensor networks," *Computer Communications*, vol. 36, no. 4, pp. 459-467, February 2013.
- [37] N. Fourtya, A. d. Bosscheb and T. Valb, "An advanced study of energy consumption in an IEEE 802.15.4 based network: Everything but the truth on 802.15.4 node lifetime," *Computer Communications*, vol. 35, no. 14, pp. 1759-1767, 2012.
- [38] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications*, vol. 30, no. 7, pp. 1655-1695, 2007.
- [39] R. Bruno, M. Conti and E. Gregori, "Bluetooth: Architecture, Protocols and Scheduling Algorithms," *Cluster Computing*, vol. 5, no. 2, p. 117-131, 2002.
- [40] K. Mekki, E. Bajic, F. Chaxel and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT," *ScienceDirect, ICT Express*, 2017.
- [41] D. Agrawal, H. Gossain, D. Cavalcanti and P. Mohapatra, "Recent advances and evolution of WLAN and WMAN standards [Guest Editorial]," *IEEE Wireless Communications*, vol. 15, no. 5, pp. 54-55, 2008.
- [42] S. Wagle, M. Ade and M. G. Ullah, "Network Transition from WiMAX to LTE," *JOURNAL OF COMPUTING*, vol. 3, no. 1, pp. 66 - 70, 2011.
- [43] M. D. Sanctis, E. Cianca, G. Araniti, I. Bisio and R. Prasad, "Satellite Communications Supporting Internet of Remote Things," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 113-123, February, 2016.
- [44] S. Galli, A. Scaglione and Z. Wang, "Power Line Communications and the Smart Grid," in *IEEE International Conference on Smart Grid Communications*, pp. 303-308, 2010.
- [45] K. Gama, L. Touseau and D. Donsez, "Combining heterogeneous service technologies for building an Internet of Things middleware," *Computer Communications*, vol. 35, no. 4, pp. 405-417, 2012.
- [46] M. Chen, V. C. M. Leung, R. Hjelsvold and X. Huang, "Smart and Interactive Ubiquitous Multimedia Services," *Computer Communications*, vol. 35, no. 15, pp. 1769-1771, 2012.
- [47] A. Passarella, "A survey on content-centric technologies for the current Internet: CDN and P2P solutions," *Computer Communications*, vol. 35, no. 1, pp. 1-32, 2012.

- [48] D. E. Baz, "IoT and the Need for High Performance Computing," in *International Conference on Identification, Information and Knowledge in the Internet of Things*, 2014.
- [49] J.-M. Spaus, "IPCEI on High Performance Computing & Big Data Enabled Applications A European initiative coordinated by Luxembourg Ministry of the Economy," 2014. [Online]. Available: http://amis-uni.lu/wp-content/uploads/2014/10/J-M.-SPAUS-Min.-Economie_Background-note.pdf. [Accessed April 2018].
- [50] J.-M. Spaus, "INDUSTRY 4.0, HPC AND BIG DATA PUTTING IN PLACE A WORLD INFRASTRUCTURE TO SUPPORT THE DIGITALIZATION OF INDUSTRY," 2017. [Online]. Available: <https://www.luxinnovation.lu/wp-content/uploads/sites/3/2017/10/industry-4-0-fedil-final.pdf>.
- [51] "European Commission HPC - Best Use Examples," [Online]. Available: <https://ec.europa.eu/digital-single-market/en/news/high-performance-computing-best-use-examples>.
- [52] S. Yi, C. Li and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," in *ACM Proceedings of the Workshop on Mobile Big Data*, 2015.
- [53] M. M. Gaber, F. Stahl and J. B. Gomes, "Pocket Data Mining Framework," in *Pocket Data Mining Big Data on Small Devices*, Springer International Publishing, 2014, pp. 23-40.
- [54] Cisco and associates, "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are," 2015. [Online]. Available: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf.
- [55] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, "Fog computing and its role in the internet of things," in *ACM MCC workshop on Mobile cloud computing*, 2012.
- [56] A. E. , I. Yaqoob, A. Gani, M. Imran and M. Guizani, "Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 10-16, October 2016.
- [57] "Gartner Report," <https://www.gartner.com/doc/3841268/forecast-analysis-internet-things->, January 2017.
- [58] R. Acharya and K. Asha, "Data integrity and intrusion detection in Wireless Sensor Networks," in *16th IEEE International Conference on Networks*, 2008.
- [59] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar and K. Wehrle, "Security Challenges in the IP-based Internet of Things," *Journal on Wireless Personal*, vol. 61, no. 3, p. 527-542, 2011.
- [60] R. H. Weber, "Internet of Things – New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23-30, 2010.
- [61] K. Zhao and L. Ge, "A survey on the internet of things security," in *IEEE 9th International Conference on Computational Intelligence and Security (CIS)*, 2013.
- [62] C. P. Mayer, "Security and privacy challenges in the internet of things," *Electronic Communications of the EASST*, vol. 17, 2009.
- [63] S. Alam, M. M. Chowdhury and J. Noll, "Interoperability of security enabled internet of things," *Wireless Personal Communications*, vol. 61, no. 3, p. 567-586, 2011.
- [64] R. Roman, J. Zhou and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, p. 2266-2279, 2013.
- [65] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann and K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *Wireless Communications, IEEE*, vol. 20, no. 6, p. 91-98, 2013.
- [66] K. Zhao and L. Ge, "A survey on the internet of things security," in *9th IEEE international conference on Computational Intelligence and Security (CIS)*, 2013.
- [67] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, p. 2481-2501, 2014.
- [68] D. Boyle and T. Newe, "Securing wireless sensor networks: security architectures," *Journal of networks*, vol. 3, no. 1, p. 65-77, 2008.
- [69] T. Borgohain, U. Kumar and S. Sanyal, "Survey of security and privacy issues of internet of things," <https://arxiv.org/ftp/arxiv/papers/1501/1501.02211.pdf>, 2015.
- [70] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," *The Internet of Things*, Springer, p. 389-395, 2010.

- [71] D. Henrici and P. Muller, "Tackling security and privacy issues in radio frequency identification devices," in *International Conference on Pervasive Computing*, Springer, 2004.
- [72] D. Djenouri, L. Khelladi and N. Badache, "A survey of security issues in mobile ad hoc networks," *IEEE communications surveys*, vol. 7, no. 4, p. 2–28, 2005..
- [73] G. Madlmayr, J. Langer, C. Kantner and J. Scharinger, "NFC devices: Security and privacy," in *IEEE Third International Conference on Availability, Reliability and Security*, 2008.
- [74] K. Curran, A. Millar and C. Garvey, "Near field communication," *International Journal of Electrical and Computer Engineering*, vol. 2, no. 3, p. 371, 2012.
- [75] R. Bouhenguel, I. Mahgoub and M. Ilyas, "Bluetooth security in wearable computing applications," in *IEEE International Symposium on High Capacity Optical Networks and Enabling Technologies*, 2008.
- [76] A. Sharma, "Bluetooth security issues: threats and consequences," <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.557.6257>, 2008.
- [77] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis and P. Toivanen, "Security threats in zigbee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons," in *46th IEEE Hawaii System Sciences (HICSS)*, 2013.
- [78] B. Fouladi and S. Ghanoun, "Security evaluation of the z-wave wireless protocol," *Semantic Scholar*, 2013.
- [79] S. Park, K. Kim, S. Chakrabarti and J. Laganier, "Ipv6 over low power wpan security analysis draft-6lowpan-security-analysis-05," tech. rep., IETF Internet Draft, 2011.
- [80] M. A. Razaque, M. Milojevic-Jevric, A. Palade and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of Things*, vol. 3, no. 1, p. 70–95, 2016.
- [81] "MQTT version 3.1. 1," OASIS Std., October, 2014.
- [82] R. Neisse, G. Steri and G. Baldini, "Enforcement of security policy rules for the internet of things," in *IEEE Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2014.
- [83] P. Saint-Andre, "Extensible messaging and presence protocol (xmpp):Core," 2011.
- [84] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," in *IEEE Access (Volume: 4)*, 2016.
- [85] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," *The Internet of Things*, Springer, p. 389–395, 2010.
- [86] V. Almeida, D. Doneda and M. Monteiro, "Governance Challenges for Internet of Things," *IEEE Internet Computing*, vol. 19, no. 4, pp. 56-59, 2015.
- [87] R. P. Minch, "Location Privacy in the Era of the Internet of Things and Big Data Analytics," in *48th Hawaii International Conference on System Sciences*, 2015.
- [88] ILNAS, "White Paper Digital Trust for Smart ICT," September 2017. [Online]. Available: <https://portail-qualite.public.lu/content/dam/qualite/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf>.
- [89] S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, p. 146–164, 2015.
- [90] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," in *ACM international workshop on Self-aware internet of things*, 2012.
- [91] T. E. PARLIAMENT, "Regulation (EU) 2016/679 of the european parliament," *Official Journal of the European Union*, 2016.
- [92] J. Seo, K. Kim, M. Park, M. Park and K. Lee, "An analysis of economic impact on IoT under GDPR," in *International Conference on Information and Communication Technology Convergence (ICTC)*, 2017.
- [93] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs and J. Bughin, "The Internet of Things: Mapping the Value Beyond the Hype," McKinsey Global Institute (MGI), June 2015.
- [94] [Online]. Available: The ThingWorx Guide to the Internet of Things; <http://www.thingworx.com/thingworx-analytics>.
- [95] "The next frontier for innovation, competition, and productivity," McKinsey Global Institute, 2011, May.
- [96] "Open data: Unlocking innovation and performance with liquid information,," McKinsey Global Institute, October, 2013.

- [97] A. Thierer and A. Castillo, "Projecting growth and Economic Impact of Internet of Things," The Mercatus Center at George Mason University, June, 2015.
- [98] P. Szweczyk, "Impact of the Internet of Things on the economy and society," *Wydawnictwo Politechniki Śląskiej*, ISSN: 1641-3466, vol. 93, pp. 461--470, 2016.
- [99] "Population of the World," The World Bank, [Online]. Available: <http://www.worldometers.info/world-population/>. [Accessed April 2018].
- [100] "Internet of Things (IoT) Market by Software Solution (Real-Time Streaming Analytics, Security Solution, Data Management, Remote Monitoring, and Network Bandwidth Management), Service, Platform, Application Area, and Region - Global Forecast to 2022," MarketsandMarkets, June, 2017.
- [101] "The Mobile Economy Europe," GSM Association, 2015.
- [102] "Smart grids and meters," [Online]. Available: <https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters>.
- [103] *European Commission, Digital Scoreboard-connectivity*,
- [104] "Global Economic Outlook," The Organisation for Economic Co-operation and Development (OECD), June 2017.
- [105] *European Commission, Digital Scoreboard - RFID*,
- [106] "The Internet of Things- A New Path to European Prosperity," 2016. [Online]. Available: <https://www.atkearney.com/documents/10192/7125406/The+Internet+of+Things-A+New+Path+to+European+Prosperity.pdf/e5ad6a65-84e5-4c92-b468-200fa4e0b7bc>.
- [107] M. o. t. E. -. Luxembourg, "Third Industrial Revolution Strategy Study," 2016. [Online]. Available: <https://rio.jrc.ec.europa.eu/en/library/third-industrial-revolution-strategy-study>.
- [108] European Parliament and the Council, "Regulation (EU) No 1025/2012 of the European Parliament and of the Council," 2012. [Online]. Available: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF>.
- [109] ILNAS, "Standards Analysis Smart ICT - Luxembourg," 2018. [Online]. Available: <https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2018/standards-analysis-smart-ict-2-0.pdf>.
- [110] CEN-CENELEC, "Standards and your business," 2013. [Online]. Available: https://www.cencenelec.eu/news/publications/Publications/Standards-and-your-business_2013-09.pdf.
- [111] WTO, "Second triennial review of the operation and implementation of the agreement on technical barriers to trade – Annex," 2000. [Online]. Available: <http://docsonline.wto.org/imrd/directdoc.asp?DDFDocuments/t/G/TBT/9.doc>.
- [112] European Commission, "Europe 2020 Flagship Initiative, Innovation Union, COM(2010) 546," 2010. [Online]. Available: https://ec.europa.eu/research/innovation-union/pdf/innovation-union-communication_en.pdf.
- [113] European Commission, "COM(2016) 180 final - COMMISSION STAFF WORKING DOCUMENT - Advancing the Internet of Things in Europe," 2016. [Online]. Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110>.
- [114] BEREC, "BoR (16) 39 - Report on Enabling the Internet of Things," 2016. [Online]. Available: http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5755-berec-report-on-enabling-the-internet-of_0.pdf.
- [115] AIOTI, "IoT LSP Standard Framework Concepts - Release 2.8," 2017. [Online]. Available: https://aioti.eu/wp-content/uploads/2017/06/AIOTI-WG3_sdos_alliances_landscape_-_iot_lsp_standard_framework_concepts_-_release_2_v8.pdf.
- [116] ITU-T, "JCA-NID Background," [Online]. Available: <https://www.itu.int/en/ITU-T/jca/nid/Pages/background.aspx>.
- [117] ITU-T, "JCA-NID," [Online]. Available: <https://www.itu.int/en/ITU-T/jca/nid/Pages/default.aspx>.
- [118] ITU-T, "<https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>," [Online]. Available: <https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>.
- [119] ETSI, "Internet of Things," [Online]. Available: <http://www.etsi.org/technologies-clusters/technologies/internet-of-things>.
- [120] ISO/IEC, "ISO/IEC Directives, Part 1 - Consolidated ISO Supplement — Procedures specific to ISO," 2017. [Online]. Available: https://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/4230452/ISO_IEC_Directives_Part_1_and_

- Consolidated_ISO_Supplement_%2D_2017_%28th_edition%29_%2D_PDF.pdf?nodeid=18905271&vernum=-2.
- [121] ITU-T, "IoT and SC&C Standards Roadmap," 2017. [Online]. Available: <https://www.itu.int/en/ITU-T/jca/iot/Documents/deliverables/Free-download-IoT-roadmap.doc>.
- [122] ITU-T, "Terms of Reference: ITU-T Focus Group on "Data Processing and Management to support IoT and Smart Cities and Communities" (FG-DPM)," 2017. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dpm/Documents/FGDPM_ToRs.docx.
- [123] ETSI, "SmartM2M Activity Report 2016," [Online]. Available: <https://portal.etsi.org/TBSiteMap/SmartM2M/ActivityReport.aspx>.
- [124] oneM2M, "oneM2M - Standards for M2M and the Internet of Things," [Online]. Available: <http://www.onem2m.org/about-onem2m/why-onem2m>.
- [125] ETSI, "ETSI TS 103 264 V2.1.1 (2017-03), SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping," 2015. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/103200_103299/103264/02.01.01_60/ts_103264v020101p.pdf.
- [126] ETSI, "ETSI Work Programme 2017-2018," 2017. [Online]. Available: <http://www.etsi.org/images/files/WorkProgramme/etsi-work-programme-2017-2018.pdf>.
- [127] ETSI, "ETSI TR 103 375 V1.1.1 (2016-10) "SmartM2M; IoT Standards landscape and future evolutions"," 2016. [Online]. Available: https://aioti.eu/wp-content/uploads/2017/03/tr_103375v010101p-Standards-landscape-and-future-evolutions.pdf.
- [128] ETSI, "ETSI TR 103 376 V1.1.1 (2016-10) "SmartM2M; IoT LSP use cases and standards gaps"," 2016. [Online]. Available: https://aioti.eu/wp-content/uploads/2017/03/tr_103376v010101p-LSP-use-cases-and-standards-gaps.pdf.
- [129] ILNAS, "ICT Standards Analysis - Luxembourg - V8.0," 2017. [Online]. Available: <https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/standards-analysis-ict-8-0.pdf>.
- [130] 3GPP, "About 3GPP Home," [Online]. Available: <http://www.3gpp.org/about-3gpp/about-3gpp>.
- [131] 3GPP, "3GPP Scope and Objectives," 2007. [Online]. Available: http://www.3gpp.org/ftp/Inbox/2008_web_files/3GPP_Scopeand0310807.pdf.
- [132] European Commission, "The Alliance for Internet of Things Innovation (AIOTI)," [Online]. Available: <https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti>.
- [133] AIOTI, "IoT LSP Standard Framework Concepts - Release 2.0," 2015. [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11813.
- [134] AIOTI, "High Level Architecture (HLA) - Release 2.0," 2015. [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11812.
- [135] AIOTI, "Semantic Interoperability - Release 2.0," 2015. [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11814.
- [136] AIM, "About AIM," [Online]. Available: http://www.aimglobal.org/?page=About_AIM.
- [137] AIM, "AIM Industry Groups," [Online]. Available: <http://www.aimglobal.org/?page=committees>.
- [138] GS1, "GS1 standards," [Online]. Available: <https://www.gs1.org/standards>.
- [139] GS1, "GS1 and the Internet of Things," 2016. [Online]. Available: <https://www.gs1.org/sites/default/files/images/standards/internet-of-things/gs1-and-the-internet-of-things-iot.pdf>.
- [140] IEEE, "About IEEE," [Online]. Available: <https://www.ieee.org/about/index.html>.
- [141] IEEE, "About the IEEE Internet of Things (IoT) Initiative," [Online]. Available: <https://iot.ieee.org/about.html>.
- [142] IEEE, "Standard for an Architectural Framework for the Internet of Things (IoT)," [Online]. Available: <http://grouper.ieee.org/groups/2413/>.
- [143] IETF, "About IETF," [Online]. Available: <https://www.ietf.org/about/>.
- [144] IETF, "The Internet of Things," [Online]. Available: <https://www.ietf.org/topics/iot/>.
- [145] IETF, "Rough Guide to IETF 101: Internet of Things," 2018. [Online]. Available: <https://www.ietfjournal.org/rough-guide-to-ietf-101-internet-of-things/>.
- [146] IoT Global Network, "IoT Standards," [Online]. Available: <http://www.iotglobalnetwork.com/iotdir/2016/03/30/iic-1286/>.

- [147] IIC and Plattform Industrie 4.0, "Architecture Alignment and Interoperability," 2017. [Online]. Available: http://www.iiconsortium.org/pdf/JTG2_Whitepaper_final_20171205.pdf.
- [148] oneMeM, "oneM2M update zoom on Release 3 - ETSI IoT Week 2017," 2017. [Online]. Available: https://docbox.etsi.org/Workshop/2017/201710_IoTWEEK/WORKSHOP/S00_INTRO/oneM2M_NOKIA_ELLOUMI.pdf.
- [149] OGC, "About OGC," [Online]. Available: <http://www.opengeospatial.org/about>.
- [150] OGC, "Domains that use and develop OGC standards," [Online]. Available: <http://www.opengeospatial.org/domain>.
- [151] OCF, "About Open Connectivity Foundation," [Online]. Available: <https://openconnectivity.org/foundation>.
- [152] OCF, "UPnP Standards & Architecture," [Online]. Available: <https://openconnectivity.org/developer/specifications/upnp-resources/upnp>.
- [153] ISO/IEC JTC 1, "List of approved JTC 1 PAS Submitters," [Online]. Available: <http://isotc.iso.org/livelink/livelink?func=ll&objId=8913248&objAction=browse&sort=name>.
- [154] W3C, "W3C Mission," [Online]. Available: <https://www.w3.org/Consortium/mission>.
- [155] W3C, "Web of Things Working Group Charter," [Online]. Available: <https://www.w3.org/2016/12/wot-wg-2016.html#scope>.
- [156] ISO, "My ISO job - What delegates and experts need to know," 2016. [Online]. Available: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/my_iso_job.pdf.



COLLABORATION
PARTNER
OFFICE
SERVICE
EXCELLENCE
INDUSTRY

COLLABORATION
PARTNER
OFFICE



ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

ANEC

Agence pour la Normalisation
et l'Economie de la Connaissance

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -70 · Fax : (+352) 24 79 43 -70 · E-mail : info@ilnas.etat.lu

www.portail-qualite.lu