en
cs de
sk es

TECH pedia

INTERNET OF THINGS

JORDI SALAZAR, SANTIAGO SILVESTRE

Title: Internet of things
Author: Jordi Salazar, Santiago Silvestre
Published by: Czech Technical University of Prague
Faculty of electrical engineering
Contact address: Technicka 2, Prague 6, Czech Republic
Phone Number: +420 224352084
Print: (only electronic form)
Number of pages: 31
Edition: 1st Edition, 2017

ISBN 978-80-01-06232-6

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Explanatory Notes

	Definition
	Interesting
	Note
	Example
	Summary
	Advantage
	Disadvantage

ANNOTATION

This is an introductory course to the IoT (Internet of things). In the early chapters the basics about the IoT are introduced. Then basics of IPv6 internet protocol that is the most used in IoT environment as well as main applications, the current state of the market and the technologies that enable the existence of the IoT are described. Finally the future challenges that are considered most important are discussed.

OBJECTIVES

At study of this course, students will be able to understand the basics about IT and get a good idea about the possibilities and applications based in this environment.

LITERATURE

[1] R. H. Weber, (2010). "Internet of Things - New Security and Privacy Challenges". Computer Law & Security Review 26: 23-30.

[2] Dave Evans. (2011). How the Next Evolution of the Internet Is Changing Everything. Cisco Internet of Things White Paper.

[3] Stephen E. Deering and Robert M. Hinden (1998). RFC 2460, Internet Protocol, Version 6 (IPv6) Specification.

[4] Charith Perera et. al. (2014). Sensing as a Service Model for Smart Cities Supported by Internet of Things. Transactions on Emerging Telecommunications Technology 25 (1): 81–93.

[5] Ma HD. (2011). “Internet of things: Objectives and scientific challenges”. Journal of computer science and technology 26 (6): 919-924.

[6] In Lee and Kyoochun Lee (2015) “The Internet of Things (IoT): Applications, investments, and challenges for enterprises, *Business Horizons*, 58, 431-440.

[7] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

[8] Ala Al-Fuqaha et al. (2015) “Internet of Things: A survey on enabling technologies, protocols and applications”, *IEEE Communications Surveys & Tutorials*. DOI 10.1109/COMST.2015.2444095

[9] The European Technology Platform on Smart Systems Integration (2008). "Internet of Things in 2020: A Roadmap for the future"

Index

1 What is Internet of Things (IoT)? Definition, history and features of IoT.

This chapter describes some important highlights in the history of the **IoT** (*Internet of things*). Nowadays, the internet-based information architecture allows the exchange of services and goods between all elements, equipment and objects connected to the network. The IoT refers to the networked interconnection of those everyday objects, which are often equipped with some kind of intelligence. In this context, Internet can be also a platform for devices to communicate electronically and share information and specific data with the world around them. So, IoT can be seen as a real evolution of what we know as Internet by adding more extensive interconnectivity, a better perception of the information and more comprehensive smart services. For the most part, the Internet was used for connection-oriented application protocols like **HTTP** (*Hypertext Transfer Protocol)* and **SMTP** (*Simple Mail Transfer Protocol*). However, nowadays a large number of smart devices communicate between themselves and to other control systems. This concept is known as **M2M** (*Machine-to-Machine communications*).

IoT (*Internet of things*) is an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders [1].

Some highlights in the IoT history are the following:

- The term Internet of Things was first used by Kevin Ashton in 1999 that was working in the field of networked **RFID** (*radio frequency identification*) and emerging sensing technologies.
- However, IoT was "born" sometime between 2008 and 2009 [2].
- In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Nowadays there are about 25 billion of devices connected to the IoT. More or less a smart device per person [2].
- The number of smart devices or "things" connected to the IoT is expected to increase to a further 50 billion by 2020.

The IoT introduces a step change in individuals' quality of life by offering a lot of new opportunities to data access, specific services in education, security, health care or transportation among others. On the other hand, it will be a key to increase enterprises' productivity by offering a widely distributed, locally intelligent network of smart devices and new services that can be personalized to customer needs. The IoT brings benefits from improved management and tracking of assets and products, it increases the amount of information data and allows the optimization of equipment and use of resources that can be translated into costs saving. Moreover, it offers the opportunity to create new smart interconnected devices and explore new business models.

2 IPv6 Introduction

This chapter gives a basic introduction to IPv6: Internet protocol version 6, which is necessary for IoT.

2.1 IPv6 Introduction

When we use the Internet for any activity, be it e-mail, data transmission, web browsing, downloading files, images or videos or any other service or application, communication between different network elements and our own computer, laptop or smart phone, uses a protocol: The **IP** ***(Internet protocol)*** which specifies the technical format of packets and the addressing scheme for computers to communicate over a network.

IPv6 (*Internet protocol version 6*) is the most recent version of the IP, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

In order to connect any device to Internet it's necessary to provide an IP address to the device. The first version of an Internet Protocol publicly used was **IPv4** (*Internet protocol version 4*). This protocol was created by the Defense Advanced Research Projects Agency (DARPA). DARPA is an agency of the U.S. Department of Defense responsible for the development of emerging technologies mainly for military applications created in 1958. IPv4 included an addressing system that used numerical identifiers consisting of 32 bits. The use of addresses with a length of 32 bits limits the total number of possible addresses to a number of approximately 4.3 billion addresses for devices connected to internet around the world. The number of devices connected to Internet will be soon bigger than the number of addresses provided by IPv4. For this reason, and in anticipation of the situation, the agency responsible for standardization of Internet protocols: The **IETF** (*Internet Engineering Task Force)* has been working in a new IP version from 1998: The IPv6, the successor protocol that is intended to replace IPv4 was first formally described in Internet standard document RFC 2460 [3].

IPv6 uses a 128-bit address format, allowing 2^{128}, or approximately 3.4 10^{38} addresses, approximately 8 10^{28} times as many as IPv4. While increasing the pool of addresses is one of the most important benefits of IPv6, there are other important technological changes in IPv6 that will improve the IP protocol: easier administration, better multicast routing, a simpler header format and more efficient routing, built-in authentication and privacy support among others.

IPv6 will coexist with the older IPv4 for some time. The deployment of IPv6 will be made gradually in an orderly coexistence with IPv4. Client devices, network equipment, applications, content and services are to be adapted to the new Internet protocol version IPv6. Moreover, the transition from IPv4 to IPv6 will establish a common set of standards between companies, educational systems, around the world.

IPv6 addresses are represented as eight groups of four hexadecimal digits. These groups are separated by colons, but methods to abbreviate this full notation exist. The IPv6 header format is shown by Fig. 1.

Fig. 1. IPv6 Header Format [3]

Structure of IPv6 Header	
Version	4-bit Internet Protocol version number = 6.
Traffic Class	8-bit traffic class field.
Flow Label	20-bit flow label.
Payload Length	16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets.
Next Header	8-bit selector. Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 protocol field
Hop Limit	8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.
Source Address	128-bit address of the originator of the packet
Destination Address	Address 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a routing header is present).

The new features introduced with the IPv6 protocol are basically the following : A new header format, an efficient and hierarchical addressing and routing infrastructure, a much larger address space and stateless and both firewall address configuration, IP security, extensibility, a better Quality of Service (QoS) support and a new protocol for neighboring node interaction.

The IPv6 protocol has solved some of the security problems found in IPv4 networks by adding the **IPsec** ***(IP security)*** as mandatory. As a result, IPv6 is more efficient. IPsec enhances the original IP protocol by providing authenticity, integrity, confidentiality and access control to each IP packet through the use of two

protocols: **AH** (*authentication header*) and **ESP** (*encapsulating security payload*).Moreover, the expansion of the number of bits in the address field to 128 bits offered by IPv6 creates a significant barrier for attackers wanting to conduct comprehensive port scanning. On the other hand, it is possible to bind a public signature key to an IPv6 address: **CGA** (*Cryptographically Generated Address*).

IPv6 offers also improvements on mobility security. Despite that the MobileIP Internet protocol is available in both IPv4 and IPv6, in IPv6 it was built into the protocol instead of being added as a new function in IPv4. This means that any IPv6 node can use a mobile IP both as required. Mobile IPv6 uses two extensions headline: A routing header for registration and a headline target to data delivery between mobile nodes and their corresponding fixed nodes.

3 IoT Applications

In this chapter, some important applications related to the IoT field are described. Main elements of the IoT architecture are introduced and the expected evolution of the IoT market is presented.

3.1 Introduction

The IoT can be seen as a combination of sensors and actuators providing and receiving information that is digitalized and placed into bidirectional networks able to transmit all data to be used by a lot of different services and final users [4].

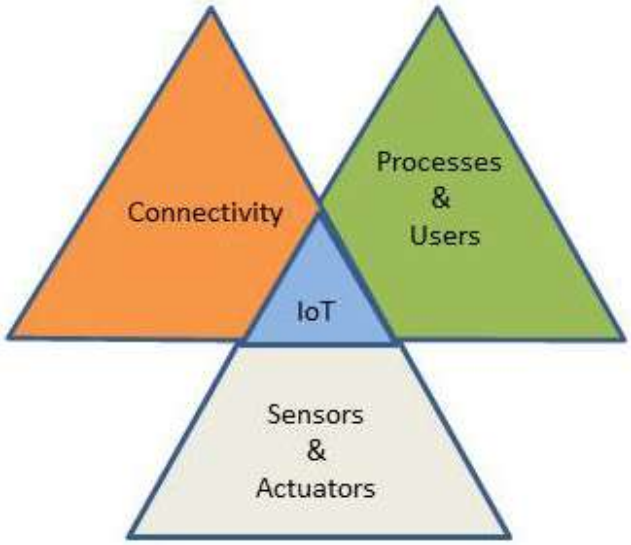

Fig. 2. The IoT Concept.

Multiple sensors can be attached to an object or device in order to measure a broad range of physical variables or phenomena and then transmit all data to the cloud. The sensing can be understood as a service model.

Sensor Classification	
Sensor Data Providers	Business entities that deploy and manage sensors by themselves.
Organizations	Public or Private. Public infrastructures. Commercial organizations. Private corporations: Technology and services providers.
Personal and Households	Mobile phones, smart watches, gyroscopes, cameras, GPS, accelerometers microphones, laptops, food items and household items, such as televisions, cameras, freezers, microwave furnaces, washing machines, smart appliances etc

Nowadays, state of the art devices such as conventional house items as refrigerators or televisions comprise communication and sensing capabilities. These capabilities will be constantly increasing by incorporating smarter communication and sensing tools.

Smart connected products capabilities	
Monitoring	The external environment. The product's condition, operations and usage.
Control	Product functions control. Personalization of the user experience. Programing.
Optimization	Predictive diagnostics. Product performance optimization. Costs reduction.
Autonomy	Autonomous product enhancement and personalization. Self-diagnosis and repair. Coordination operation with other products
Efficient decision making process.	Real-time data for decision making.

The architecture of IoT systems can be divided into four layers: Object sensing layer, data exchange layer, information integration layer, and application service layer [5].

Smart devices can be already connected through traditional Internet. However, the IoT incorporates the sensing layer which reduces the requirements on the capability of those devices and enables the interconnection among them. Sensor data consumers communicate with sensors or sensor owner's through the information integration layer that is responsible of all the communication and transactions. Meanwhile, new requirements and challenges to data exchange, information filtering and integration, definition of new services to users, as well as the complexity of the network architecture Moreover, the use of cloud technologies is exponentially growing. New infrastructure platforms and software applications are offered in the frame of the IoT. Some of the major advantages and benefits of the IoT will be the creation of innovative services with improved performance and value added solutions along with the reduction of data acquisition costs of existing services and the opportunity to create new revenue streams in a context of a sustainable business model. These applications can be oriented to consumers, business, commercials, and survey activities, industrial and scientific community by harnessing the application developers.

Four-layer architecture of IoT	
Object Sensing Layer	Sensing the physical objects and obtaining data.
Data Exchange Layer	Transparent transmission of data through communication networks.
Information Integration Layer	Processing of the uncertain information acquired from the networks, filtering undesired data and integratation of main information into usable knowledge for services and final users.
Application Service Layer	Provides content services to users.

3.2 IoT market

The IoT is an emerging global Internet-based technical architecture facilitating the exchange of goods in a global supply-chain network [1]. As the technology trend shifts towards providing faster data rates and lower latency connectivity the Internet is expected to double in size every 5.3 years and cloud computing can play a key role in that growing. Cloud computing is one of the enabling platforms to support IoT. Most "things" of the real world will be integrated into the virtual world by enabling anytime, anywhere full connectivity.

Cloud computing is a model for enabling access to a shared pool of configurable computing resources by allowing users to take benefit from all existing technologies, without the need for deep knowledge about or expertise with each one of them.

In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. This number is expected to double to 25 billion in 2015 as the number of more smart devices per person increases, and to a further 50 billion by 2020 [2].

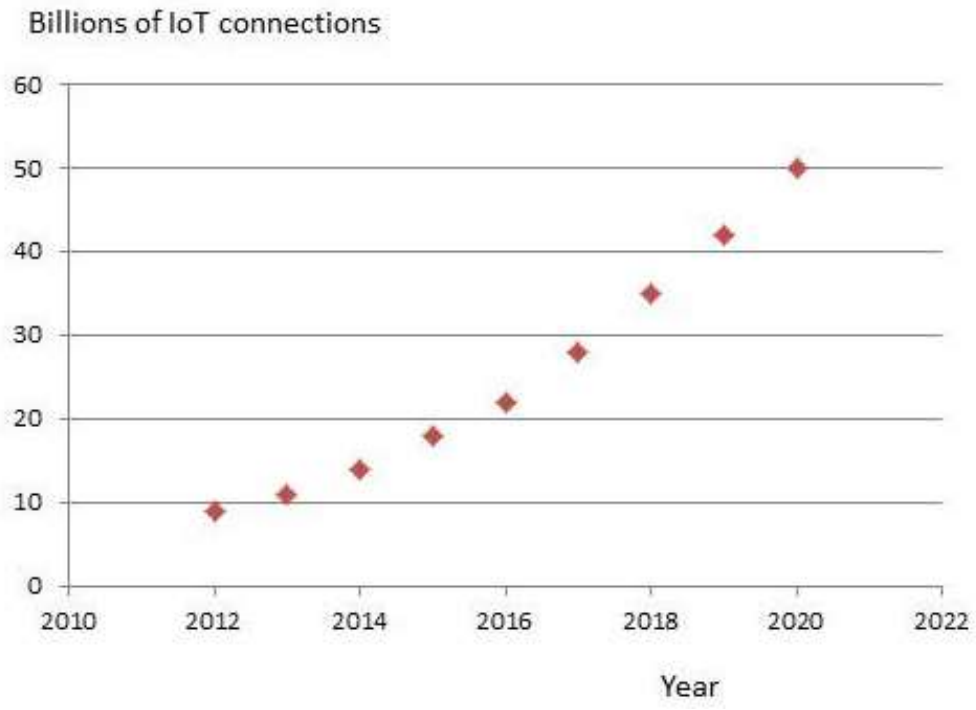

Fig. 1. Number of IoT connections [2].

Connected World.	
31 %	Phones.
29%	Notebook.
10%	Smart Phones.
8%	Smart TV.
5%	Tablets.
5%	Game Players.
5%	Media Players.
5%	eReaders.
3%	Others.

Asia currently has the most M2M connections because of the big effort carried out in some countries as Japan and China. However, American and European technology companies are making an important progress on IoT and they will bring to a market growing in these countries. With the important emergence of the IoT, new regulatory approaches to ensure the privacy and security of users and data must to be defined.

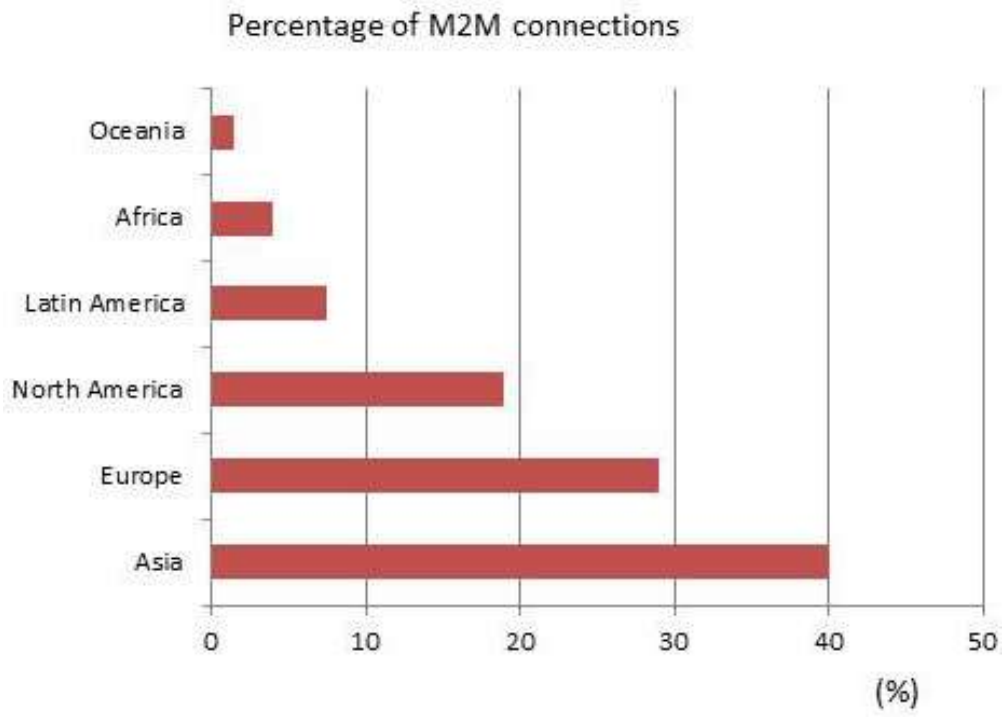

Fig. 1. Percentage of M2M connections [2].

3.3 Applications

The number of applications and services that can provide IoT is practically unlimited and can be adapted to many fields of human activity by facilitating and enhancing their quality of life in multiple ways. This chapter gives a short list of applications and services based on IoT. However, it is just a limited description in order to understand all possible new applications and services that IoT could provide. An estimated value about $19 trillion by 2020 is expected to be achieved by IoT applications and services.

IoT Applications and services:

- Connected intelligent buildings: Improvements in efficiency (energy management and saving) and security (sensors and alarms). Domotic applications including smart sensors and actuators to control home appliances. Health and education services at home. Remote control of treatments for patients. Cable/satellite services. Energy storage/generation systems. Automatic shutdown of electronics when not in use. Smart thermostats. Smoke detectors and alarms. Access control applications. Smart door locks. Sensors built into building infrastructure to guide first responders and assistances. Safety for all family members.

- Smart cities and transportation: Integration of security services. Optimization of public and private transportation. Parking Sensors. Smart management of parking services and traffic in real time. Smart management of traffic lights depending on traffic queues. Locate cars that have overstayed Smart energy grids. Security (cameras, smart sensors, information to citizens). Water management. Parks and Gardens irrigation. Smart garbage cans. Pollution and mobility controls. Get immediate feedback and opinions from citizens. Smart governance. Voting Systems. Accident monitoring, emergency actions coordination.

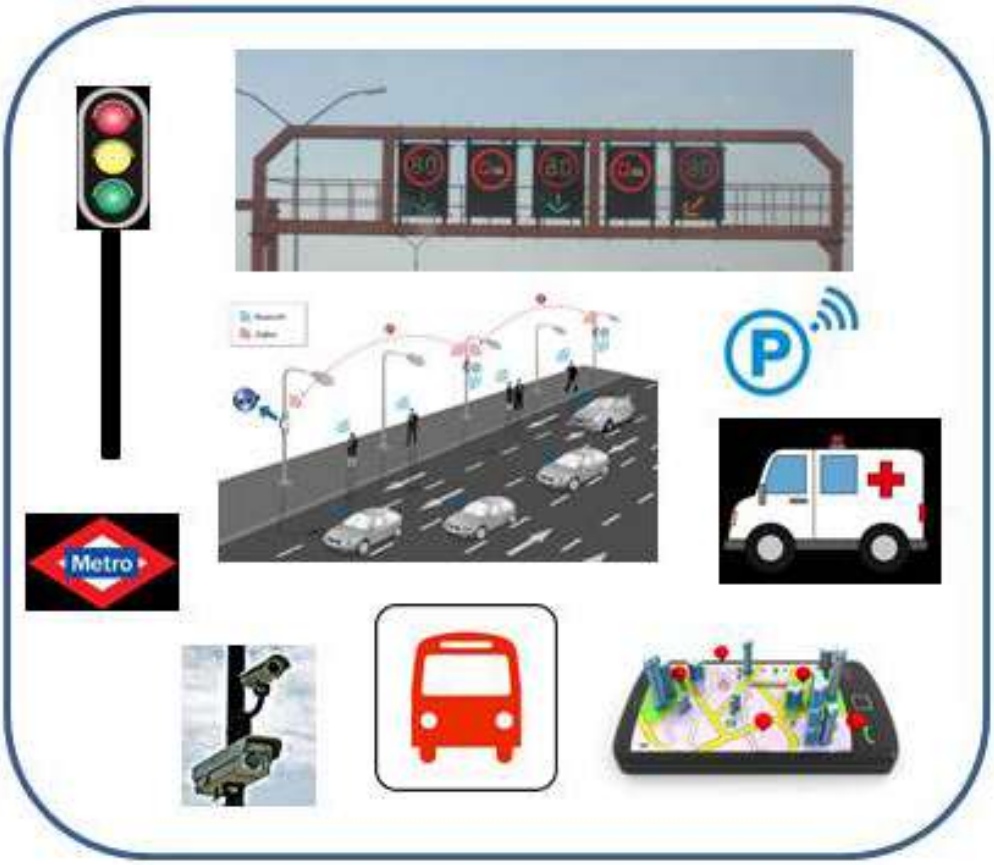

Fig. 1. Example of IoT applications: Smart cities.

- Education: Linking virtual and physical classrooms to make learning more efficient and accessible, e-learning. Access services to virtual libraries and educational portals. Interchange of reports and results in real time. Lifelong learning. Foreign languages learning. Attendance management.

- Consumer electronics: Smart phones. Smart TV. Laptops, computers and tablets. Smart refrigerators, washers and dryers. Smart home theatre systems. Smart appliances. Pet collar sensors. Personalization of the user experience. Autonomous product operation. Personal locators. Smart glasses.

- Health: Monitoring of chronic diseases. Improvement of the quality of care and quality of life for patients. Activity Trackers. Remote diagnostic. Connected bracelets. Interactive belts. Sport and fitness monitoring. Intelligent tags for drugs. Drug usage tracking. Biochips. Brain-computer interfaces. Monitoring eating habits.

- Automotive: Smart Cars. Traffic control. Advance information about what is broken. Wireless monitoring of tire pressure of car. Smart energy management and control. Self-diagnosis. Accelerometers. Position, presence and proximity sensors. Analysis of the best way to go in real time. GPS tracking. Vehicle speed control. Autonomous vehicles using IoT services.

- Agriculture and environment: Measurement and monitoring of environmental pollution (CO_2, noise, contaminant elements presents in ambient). Forecasting climate changes based on smart sensors monitoring. Passive RFID tags attached to agriculture products. Sensors in pallets of products. Waste management. Nutrition calculations.

- Energy services: accurate data on energy consumption. Smart metering. Smart grids. Analysis and prediction of energy consumption behaviours and patterns. Forecasting future energy trends and needs. Wireless sensors networks. Energy harvesting and recycling.

- Smart Connectivity: Data management and service provisioning. Use of social media and social networking. Access to email, voice and video services. Interactive group communication. Real time streaming. Interactive gaming. Augmented reality. Network security monitoring. Wearable user interfaces. Affective computing. Biometric authentication methods. Consumer telematics. M2M communication services. Big data analysis. Virtual reality. Cloud computing services. Ubiquitous computing. Computer vision. Smart antennas.

- Manufacturing: Gas and flow sensors. Smart sensors of humidity, temperature, motion, force, load, leaks/levels. Machine vision. Acoustic and vibration sensing. Compound applications. Smart control of robots. Control and optimization of fabrication processes. Pattern recognition. Machine Learning. Predictive Analytics. Mobile logistics. Warehouse management. Prevent overproduction. Efficient logistics.

- Shopping: Intelligent shopping. RFID and other electronic tags and readers. Barcodes in retail. Inventory control. Control of geographical origin of food and products. Control food quality and safety.

4 Enabling technologies

Successful application of the IoT concept into the real world is possible thanks to advancements in underlying technologies. In this section the most relevant enabling technologies will be stated with the aim to provide a picture of the role they will likely play in the IoT [6, 7].

4.1 Energy

Power and energy storage technologies are enablers for the deployment of IoT applications. Energy issues, in all its phases, from harvesting to conservation and usage, are central to the development of the IoT. These technologies have to provide high power-density energy generation and harvesting solutions which, when used with today's low power nanoelectronics, will enable us to design self-powered intelligent sensor-based wireless identifiable device. There is still a need to research and develop solutions in this area (nanoelectronics, semiconductor, sensor technology, micro systems integration) having as an objective ultra low power devices, and more efficient and compact energy storage like batteries, fuel cells, and printed/polymer batteries, as current devices seem inadequate considering the processing power needed and energy limitations of the future. In addition, system integration will increase efficiency of current systems, and will provide a number of solutions for the future needs.

4.2 Sensors

Sensors are one of the key building blocks of the Internet of Things. As ubiquitous systems, they can be deployed everywhere. They can also be implanted under human skin, in a purse or on a T-shirt. Some can be as small as four millimetres in size, but the data they collect can be received hundreds of miles away. They complement human senses and have become indispensable in a large number of industries, from health care to construction. Sensors have the key advantage that they can anticipate human needs based on information collected about their context. Their intelligence multiplied by numerous networks allows them not only to report about external environment, but also to take action without human intervention.

Miniaturized silicon chips are designed with new capabilities in smaller form factors and better processing performance and efficiency. Costs are falling, following the Moore's Law. The cost of bandwidth has also declined and similarly the processing costs, enabling more devices to be not just connected, but smart enough to know what to do with all the new data they are generating or receiving.

Capabilities such as context awareness and inter-machine communication are considered a high priority for the IoT. Additional priorities are the integration of memory and processing power, the capacity of resisting harsh environments, and an affordable security. Furthermore, the development of ultra low power processors/microcontrollers cores designed specifically for mobile IoT devices and a new class of simple and affordable IoT-centric smart systems will be an enabling factor. The solutions in this respect will range from micro programmed finite state machines to the use of microcontrollers. The choice is a trade-off between flexibility, programmability, silicon area, and power consumption. The devices require some form of non-volatile storage (EEPROM/FRAM/Polymer), independent of whether this will be laser trimmed at the time of manufacture, one time programmable, or electrically rewritable. Rewritable non-volatile memory is clearly preferred for achieving high throughput during production test, and allows concurrently the benefit of user memory, programmability and storage of sensor data.

4.3 Cloud computing

Cloud computing is a model for on-demand access to a shared pool of configurable resources (e.g., computers, networks, servers, storage, applications, services, software) that can be provisioned as Infrastructure as a Service (IaaS) or Software as a Service (SaaS). One of the most important outcomes of the IoT is an enormous amount of data generated from devices connected to the Internet [7]. Many IoT applications require massive data storage, huge processing speed to enable real time decision making, and high-speed broadband networks to stream data, audio, or video. Cloud computing provides an ideal back-end solution for handling huge data streams and processing them for the unprecedented number of IoT devices and humans in real time.

4.4 Communication

New, smart multi frequency band antennas, integrated on-chip and made of new materials are the communication means that will enable the devices to communicate. On-chip antennas must be optimized for size, cost and efficiency, and could come in various forms like coil on chip, printed antennas, embedded antennas, and multiple antenna using different substrates and 3D structures. Modulation schemes and transmission speed are also important issues to be tackled allowing multi-frequency energy efficient communication protocols and transmission rates. The communication protocols will be designed for Web oriented architectures of the IoT platform where all objects, wireless devices, cameras, PCs etc. are combined to analyze location, intent and even emotions over a network. New methods of effectively managing power consumption at different levels of the network design are needed, from network routing down to the architecture of individual devices.

4.5 Integration

Integration of smart devices into packaging, or better, into the products themselves will allow a significant cost saving and increase the Eco friendliness of products. The use of integration of chips and antennas into non-standard substrates like textiles and paper, and the development of new substrates, conducting paths and bonding materials adequate for harsh environments and for ecologically sound disposal will continue. System-in-Package (SiP) technology allows flexible and 3D integration of different elements such as antennas, sensors, active and passive components into the packaging, improving performance and reducing the tag cost. RFID inlays with a strap coupling structure are used to connect the integrated circuit chip and antenna in order to produce a variety of shapes and sizes of labels, instead of direct mounting.

4.6 Standards

IoT devices are quite diverse and measure different parameters and with different conventions and units of measure. Though competing proprietary protocols keep getting proposed, it is likely that open source standards will be one of the ways to get this data to interoperate.

Clearly, open standards are key enablers for the success of wireless communication technologies and, in general, for any kind of Machine-to-Machine communication. However, the need for faster setting of interoperable standards has been recognised an important element for IoT applications deployment. Clarification on the requirements for a unique global identification, naming and resolver is needed. Lack of convergence of the definition of common reference models, reference architecture for the Future Networks, Future Internet and IoT and integration of legacy systems and networks is a challange that has to be addressed in the future.

5 Challenges and barriers of IoT

Many challenging issues still need to be addressed. Addressing these challenges enables service providers and application programmers to implement their services efficiently. In the following paragraphs, we provide a brief discussion of the main challenges faced in the development and deployment phases of the IoT [8].

5.1 Challenges

Reliability

Reliability aims to increase the success rate of IoT service delivery. It has a close relationship with availability as by reliability, we guarantee the availability of information and services over time. Reliability is even more critical and has more stringent requirements when it comes to the field of emergency response applications. In these systems, the critical part is the communication network which must be resilient to failures in order to realize reliable information distribution. Reliability must be implemented in software and hardware throughout all the IoT layers. In order to have an efficient IoT, the underlying communication must be reliable, because for example by an unreliable perception, data gathering, processing, and transmission can lead to long delays, loss of data, and eventually wrong decisions, which can lead to disastrous scenarios and can consequently make the IoT less dependable.

Reliability refers to the proper working of the system based on its specification.

Performance

Evaluating the performance of IoT services is a big challenge since it depends on the performance of many components as well as the performance of the underlying technologies. The IoT, like other systems, needs to continuously develop and improve its services to meet requirements of customers. The IoT devices need to be monitored and evaluated to provide the best possible performance at an affordable price for customers. Many metrics can be used to assess the performance of the IoT including the processing speed, communication speed, device form factor, and cost.

Performance evaluation of the individual underlying protocols and technologies, application layer protocols, and QoS have been reported in the literature, but the lack of a thorough performance evaluation for IoT applications is still an open issue.

Quality of service (**QoS**) is the overall performance of a telephony or computer network, particularly the performance seen by the users of the network.

Interoperability

End-to-end interoperability is another challenge for the IoT due to the need to handle a large number of heterogeneous things that belong to different platforms. Interoperability should be considered by both application developers and IoT device manufactures to ensure the delivery of services for all customers regardless of the specifications of the hardware platform that they use. For example, most of the smartphones nowadays support common communication technologies such as WiFi, NFC, and GSM to guarantee the interoperability in different scenarios. Also, programmers of the IoT should build their applications to allow for adding new functions without causing problems or losing functions while maintaining

integration with different communication technologies. Consequently, interoperability is a significant criterion in designing and building IoT services to meet requirements of customers. Beside variety of protocols, different interpretations of the same standard implemented by different parties presents a challenge for interoperability. To avoid such ambiguities, interoperability testing between different products in a test-bed like ETSI Plugtests would be helpful. PROBE-IT is a research project that aims to ensure the interoperability of validated IoT solutions that conducted interoperability tests like CoAP, 6LoWPAN, and IoT semantic interoperability.

It is a known fact that two different devices might not be interoperable, even if they are following the same standard. This is a major showstopper for wide adoption of IoT technologies. Future tags must integrate different communication standards and protocols that operate at different frequencies and allow different architectur es, centralised or distributed, and be able to communicate with other networks unless global, well defined standards emerge.

Security and Privacy

Security presents a significant challenge for the IoT implementations due to the lack of common standard and architecture for the IoT security. In heterogeneous networks as in the case of the IoT, it is not easy to guarantee the security and privacy of users. The core functionality of the IoT is based on the exchange of information between billions or even trillions of Internet connection objects. One open problem in IoT security that has not been considered in the standards is the distribution of the keys amongst devices. On the other hand, privacy issues and profile access operations between IoT devices without interferences are extremely critical. Still, securing data exchanges is necessary to avoid losing or compromising privacy. The increased number of smart things around us with sensitive data necessitates a transparent and easy access control management in such a way that for example one vendor can just read the data while another is allowed to control the device. In this regard, some solutions have been proposed such as grouping embedded devices into virtual networks and only present desired devices within each virtual network. Another approach is to support access control in the application layer on a per-vendor basis.

Management

The connection of billions or trillions of smart devices presents service providers with daunting issues to manage the Fault, Configuration, Accounting, Performance and Security (FCAPS) aspects of these devices. This management effort necessitates the development of new light-weight management protocols to handle the potential management nightmare that will potentially stem from the deployment of the IoT in the coming years. Managing IoT devices and applications can be an effective factor for growing the IoT deployments. For example, monitoring the M2M communication of the IoT objects is important to ensure all times connectivity for providing on demand services. The Light-weight M2M (LWM2M) is a standard that is being developed by the Open Mobile Alliance to provide interface between M2M devices and M2M Servers to build an application agnostic scheme for the management of a variety of devices. It aims to provide M2M

applications with remote management capabilities of machine-to-machine devices, services, and applications. The NETCONF Light protocol is an Internet Engineering Task Force (IETF) effort for the management of constrained devices provides mechanisms to install, manipulate, and delete the configuration of network devices. It is capable of managing a broad range of devices from resource-constrained to resource-rich devices. The independently developed MASH IoT Platform is an example of a platform that facilitates the management (monitoring, control, and configuration) of IoT assets anywhere in real-time using an IoT dashboard on smartphones. Maintaining compatibility across the IoT layers also needs to be managed to enhance connectivity speed and to ensure service delivery. The Open Mobile Alliance (OMA) Device Management working group is specifying protocols and mechanisms for the management of mobile devices and services in resource constrained environments.

Manufacturing

Manufacturing challenges must be convincingly solved. Costs must be lowered to less than one cent per passive RFID tag, and production must reach extremely high volumes, while the whole production process must have a very limited impact on the environment, be based on strategies for reuse and recycling considering the overall life-cycle of digital devices and other products that might be tagged or sensor-enabled.

5.2 Barriers

But there are also existing barriers for the IoT, especially in the field of regulations, security and safety. Main goal is to better protect the privacy of people and force companies to establish secure ways to manage data and information [8, 9].

Absence of Governance

One major barrier for the widespread adoption of the Internet of Things technology is the absence of governance. Without an impartial governing authority it will be impossible to have a truly global IoT, accepted by states, companies, trade organizations and the common people. Today there is not a unique universal numbering scheme: EPCglobal and the Ubiquitous Networking Lab propose two different, non-compatible ways of identifying objects and there is the risk to have them competing in the coming future over the global market. There is also the need of keeping governance as generic as possible, as having one authority per application field will certainly lead to overlap, confusion and competition between standards. Objects can have different identities in different contexts so having multiple authorities would create a kind of multi-homing, which can lead to disastrous results.

Privacy and Security

In order to have a widespread adoption of any object identification system, there is a need to have a technically sound solution to guarantee privacy and the security of the customers. While in many cases the security has been done as an add-on feature, it is the feeling that the public acceptance for the Internet of Things will happen only when the strong security and privacy solutions are in place. In particular, attacks have to be intercepted, data authenticated, access controlled and the privacy of customers (natural and legal persons) guaranteed. This could be hybrid security mechanisms that for example combine hardware security with key diversification to deliver superior security that makes attacks significantly more difficult or even impossible. The selection of security features and mechanisms will continue to be determined by the impact on business processes; and trade-offs will be made between chip size, cost, functionality, interoperability, security, and privacy.

The security and privacy issues should be addressed by the forthcoming standards which must define different security features to provide confidentiality, integrity, or availability services.

There are also a range of issues related to the identity of people. These must be dealt with in politics and legislation, and they are of crucial importance for the efficient public administrations of the future.

6 Future of IoT

It is possible to identify, for the years to come, four distinct macro-trends that will shape the future of internet technologies, together with the explosion of ubiquitous devices that constitute the future Internet of Things [9]:

1. The first one, sometimes referred as “exaflood” or “data deluge”, is the explosion of the amount of data collected and exchanged. As current networks are ill-suited for this exponential traffic growth, there is a need by all the actors to re-think current networking and storage architectures. It will be imperative to find novel ways and mechanisms to find, fetch, and transmit data. One relevant reason for this data deluge is the explosion in the number of devices collecting and exchanging information as envisioned as the Internet of Things becomes a reality.

The term **exaflood**, coined by Bret Swanson of Progress & Freedom Foundation, refers to the growing torrent of data on the Internet.

2. The energy required to operate the intelligent devices will dramatically decrease. Already today many data centers have reached the maximum level of energy consumption and the acquisition of new devices has necessarily to follow the dismissal of old ones. Therefore, the second trend can be identified covering all devices and systems from the tiniest smart dust to the huge data centers: the search for a zero level of entropy where the device or system will have to harvest its own energy.

3. Miniaturization of devices is also taking place amazingly fast. The objective of a single-electron transistor is getting closer, which seems the ultimate limit, at least until new discoveries in physics.

4. Another important trend is towards autonomic resources. The ever growing complexity of systems will be unmanageable, and will hamper the creation of new services and applications, unless the systems will show self-* properties, such as self-management, self-healing and self-configuration.

As a general trend, as it becomes less expensive to integrate technology into physical objects, we will see more application and adoption of IoT. In consequence, IoT will have major implications for both business-to-business and business-to-consumer companies in the next years.