**Vasco da Costa Pereira**

Licenciado em Ciências da Engenharia Electrotécnica e de Computadores

# Perspectives and Approaches for the Internet of Things

Dissertação para obtenção do Grau de Mestre em

Engenharia Electrotécnica e de Computadores

Orientador: Luís Manuel Camarinha Matos, Professor Doutor, Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa

Júri:

Presidente: Prof. Doutor Tiago Oliveira Machado de Figueiredo Cardoso

Arguente: Prof. Doutora Patrícia Alexandra Pires Macedo

Vogal: Prof. Doutor Luís Manuel Camarinha Matos

**Fevereiro 2014**

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

# Perspectives and Approaches for the Internet of Things

*For my mom.*

*For my dad.*

*For Vicente.*

## ACKNOWLEDGEMENTS

Since the beginning of this thesis, I have always been able to count on the full support of my parents. So in the first place I thank them, and they will always be in first line when it comes to any kind of acknowledgment.

I thank not only to my parents but also the rest of my family for providing the necessary environment into the realization of this thesis.

I have to thank my thesis supervisor, Professor Luis M. Camarinha-Matos, for his support and endless patience in helping me to develop this thesis.

I thank my best and closest friends, who have always supported, either morally or by any kind of contribution to the realization of the thesis: Bruno Luís, Hugo Luís, Claudia Santos, Filipe Pires, João Milho, Andreia Rodrigues, Inês Carvalho, João Silva, João Mendes. Their support was priceless and everything would be much harder without them.

I especially thank João Jacinto, Pedro Fernandes and Catarina Peres for helping me correcting and finding grammatical and structural errors in this thesis.

I especially thank Joana Dias for the help in designing almost all figures in this thesis.

I thank João Nunes, Manuel Mouta and Ricardo Tavares for pointing me the right direction of programming in LabVIEW.

I deeply apologize for the ones not referenced in these acknowledgements.

## ABSTRACT

This thesis was developed based on a scenario in which a CEO of a certain company asked the author to conduct an exploratory work evaluating the potential opportunities and limitations of this emerging area described as the future of the Internet, the Internet of Things (IoT).

The objective is thus to provide the reader with a wide view of the vital points for the implementation and exploitation of the IoT, a technology that promises to deliver a new and wider range of applications to the society.

In this subject there is a need to gather and organize information produced by several researchers and contributors. Due to the fact of being a new area and researchers work independently of each other, the work is scattered and inconsistencies can be found among different projects and publications. As such, in a first stage some definitions are provided and an attempt to clarify concepts is made.

To support and emphasize the exponential growth of IoT, a brief historical overview is provided to the reader. This overview is based on the new trends and expectations that arise every day through news, potential businesses and also in important tools such as Google Trends. Several examples of applications in the context of the IoT, illustrate the benefits, not only in terms of society, but also for business opportunities, safety, and well-being.

The main areas of interest to achieve the IoT such as: hardware, software, modeling, methods of connection, security and integration are studied in this work, in order to provide some insight into current strong and weak points.

As the Internet of Things become a matter of large interest, various research groups are active in exploring and organizing projects in this area. Some of these projects, namely the ones considered the most important, are also presented in this thesis.

Taking into account the facts surrounding this new technology, it becomes quite important to bring them together, clarifying them and trying to open new perspectives for further studies and improvements.

Finally, in order to allow a practical evaluation of the technology, a prototype is developed around the connection of an intelligent object – a small mobile robot – to the Internet.

A set of conclusions and future work directions are then presented which take into account the findings of the bibliographic analysis as well as the acquired experience with the implementation of the prototype.

Keywords: Internet of Things, connection, integration and security technologies.

## RESUMO

Esta tese foi desenvolvida com base num cenário em que um Director Executivo de uma determinada empresa pediu ao autor para realizar um trabalho exploratório, com o objectivo de avaliar o potencial, as oportunidades e limitações desta área emergente e descrita como o futuro da Internet, a Internet of Things (IoT).

O objectivo é então fornecer ao leitor uma ampla visão desta área, focando os pontos vitais para a implementação da IoT e exploração desta nova tecnologia que promete trazer à sociedade uma nova e ampla gama de aplicações.

Nesta área torna-se necessário coleccionar e organizar informação oriunda de vários investigadores e outros intervenientes. Como consequência de ser uma área nova e de os investigadores trabalharem de forma independente, os trabalhos aparecem dispersos e muitas inconsistências podem ser encontradas entre diferentes projectos e publicações. Assim, numa primeira fase algumas definições são fornecidas e uma tentativa de clarificação de conceitos é feita.

Com o intuito de deixar claro o forte crescimento e aposta nesta evolução da Internet, a Internet of Things, é fornecido ao leitor um breve panorama histórico. Tal panorama é estabelecido com base nos factos mais importantes e até mesmo nalgumas das novas tendências e expectativas que surgem todos os dias através de notícias, potenciais negócios e ferramentas importantes, como por exemplo o Google Trends. São apresentados vários exemplos de aplicações no âmbito da IoT, que ilustram os seus benefícios, não só em termos de sociedade, mas também para oportunidades de negócios, segurança e bem-estar.

As principais áreas envolventes da IoT, nomeadamente: hardware, software, modelação, métodos de conexão, segurança, e integração, são estudadas neste trabalho, visando identificar os seus pontos fortes e fracos.

À medida que a Internet of Things se torna um tema de grande interesse, vários grupos de investigação organizam-se com o objectivo de explorar e organizar projectos nesta área. Alguns desses projectos, os considerados mais importantes, são também apresentados nesta tese.

Tendo em conta os factos que cercam esta nova tecnologia, torna-se bastante importante juntá-los, esclarecê-los e assim tentar abrir novas perspectivas com vista a futuros estudos e melhorias em cada uma destas áreas.

Finalmente, e para permitir uma avaliação prática da tecnologia, é desenvolvido um protótipo em torno da conexão dum objecto inteligente – um pequeno robô móvel – à Internet.

Um conjunto de conclusões e linhas de trabalho futuro são então apresentados tendo em atenção quer os resultados da análise bibliográfica, quer a experiência adquirida com a realização do protótipo.

Termos-chave: Internet of Things, tecnologias de conexão, integração, segurança.

# INDEX

## List of Tables

## LIST OF FIGURES

## Acronyms

ACC – Agent Communication Channel;

ACL – Agent Communication Language;

AOP – Agent Oriented Programming;

CPS - Cyber-Physical Systems;

DSRC - Dedicated short-range communications;

FOP – Frame Oriented Programming;

IoT - Internet of Things;

ISP – Internet Service Provider;

LM - Lego Minstorms;

NFC - Near Field Connection;

P2P - Peer-to-peer;

QR code - Quick Response Code;

REST - Representational State Transfer;

SOAP - Simple Object Access Protocol;

XML – eXtensible Markup Language;

WS - Web Services;

WSDL - Web Service Description Language;

WWW - World Wide Web;

# 1. INTRODUCTION

## 1.1 Motivation

The fast development of the Internet and associated technologies, namely regarding the possibility of connection to physical (smart) objects, has opened new perspectives and opportunities for developments that can have a deep impact on the society.

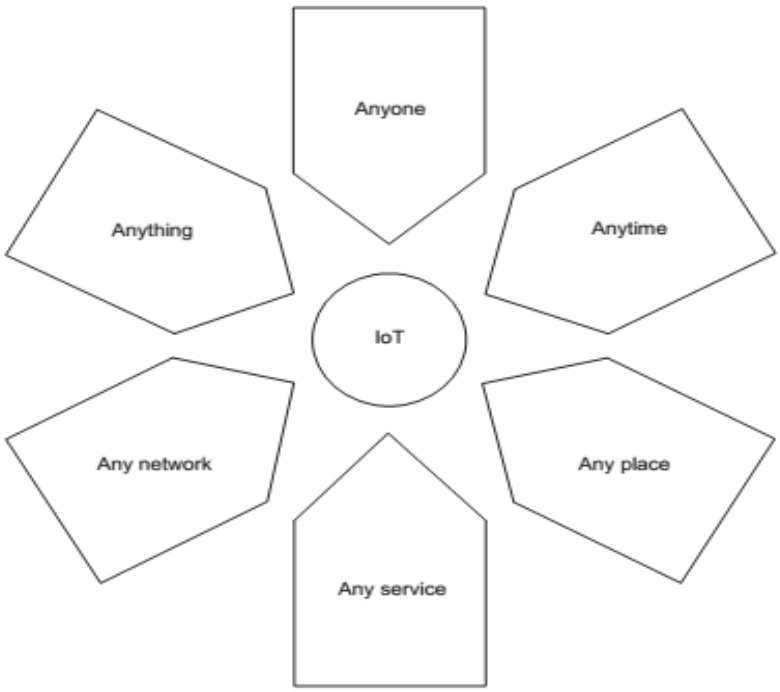


Figure 1-1 – A high-level vision of the Internet of Things

As illustrated in Figure 1-1, Internet of Things (IoT) will include services, networks, and any connectable devices, anyone who intends to use IoT, at any time, in anyplace. These features provide connectivity at a much larger scale than the Internet as we know it today. With the number of objects with capability of connection to the Internet growing exponentially, a new generation of Internet, the IoT, is being established.

In this IoT context, objects will be able to be connected and accessible anytime and anywhere, creating new possibilities for applications, taking full advantage of the access to those objects.

A wide range of application domains, including smart grid, transportation, health care, smart cities, safety, among others can benefit from these new perspectives and better support the needs of our society. This leads to the so called “Vision of IoT”.

“The Internet of Things, sometimes referred to as the Internet of Objects, will change everything—including ourselves. This may seem like a bold statement, but consider the impact the Internet already has had on education, communication, business, science, government, and humanity. Clearly, the Internet is one of the most important and powerful creations in all of human history” (Evans, 2011).

IoT will not only serve the developed countries but if well exploited it can be used as a support tool for the development of smaller and weaker economies, with the potential to boost the economy, education, infrastructures and society in general.

According to a study provided by Cisco referred in “The Internet of Things, How the Next Evolution of the Internet is Changing Everything” (Evans, 2011), IoT can help in the improvement and development of poor areas. Taking the example mentioned in this study, the ability of ubiquitous sensors will allow companies to obtain more detailed information about each area in terms of payments, needs, etc. This will introduce greater efficiency and also reduce prices, which will encourage more companies to negotiate in these areas, thus creating more jobs and developments in existing structures.

Despite the fact of this subject being discussed worldwide, it is still hard to find well-structured information, while each researcher or research group still uses different terms or different meanings to the same term. It is therefore important to gather and clarify relevant concepts and aspects that still lack unity in order to provide consistent information. This work aims to give a contribution in this direction.

## 1.2 Approach

The development of this work is guided by a scenario in which a hypothetical technology-oriented company is interested in making an assessment of the IoT technologies in order to decide if it is worthwhile to invest in this area. For this purpose, the CEO of the company asked the author, a member of the company, to make a survey and perform some exploratory work in order to inform the other members of the R&D department about the potentials, opportunities, and limits of the area.

As such, this thesis approaches the subject as the elaboration of an overview of IoT, exploring not only how IoT could improve daily life and society, but also discussing aspects such has hardware, software, security and connection methods.

The implementation of an experimental prototype is included in this process as a way to gain hands-on experience with this technology.

## 1.3 Structure

The remaining of this document is organized around the following sections:

The second chapter provides a number of concepts and definitions related to the IoT. As mentioned above, information and definitions associated to the IoT still lack unity, being important to clarify the main aspects on this subject. This chapter also provides a historical timeline of IoT development.

Application examples are given, showing how IoT could benefit the society. To emphasize the fast growth of the area, some trends are included.

The third chapter provides a brief overview of the technologies supporting the IoT, including Internet structure, devices, other specific objects, connection methods and their specifications, architectures, programming methods, and integration. One of the most important enablers of the IoT is the capability of supporting a plug-n-play style. The achievement of such ability requires the creation of a proper infra-structure.

On the fourth chapter the issue of security is discussed. Being IoT a global network with billions of “things” connected to it, the need to protect assets and sensible information becomes obvious. Security is important not only to protect data but also to offer confidence in using IoT, allowing people to trust and take advantage of the technology without the fear that their data can be breached, viewed, copied or modified. In case of objects able to act on the physical world, e.g. robots, or actuators, it is also critical that only authorized users can get access to the functionalities of those objects.

In order to provide a practical example on IoT, the fifth chapter introduces a prototype, using a mobile robot and making its functionalities available thought web services. Users can access, via a web browser, to the robot functionalities.

Finally, in the sixth chapter conclusions are presented.

# 2. INTERNET OF THINGS AND RELATED CONCEPTS

This subject has attracted considerable attention in the last years and is addressed by a large number of researchers and developers from different backgrounds. As a consequence, there is already vast literature on the subject but it is almost impossible to find a full consensus regarding terminology and definitions.

Since the first interest taken on the subject, soon researchers realized it would revolutionize the industry and daily life due to the vast scope of applicability of IoT. Potential application areas include intelligent machinery, medicine, business, automotive, smart cities and all simple or complex things we could think connected to Internet, providing new accessibility and ways of use.

It is now possible to come across a large variety of literature, experiences and opinions on future developments in this area. IoT is not a single technology. In fact, it involves a large variety of technological components. Figure 2-1 shows some of these components.

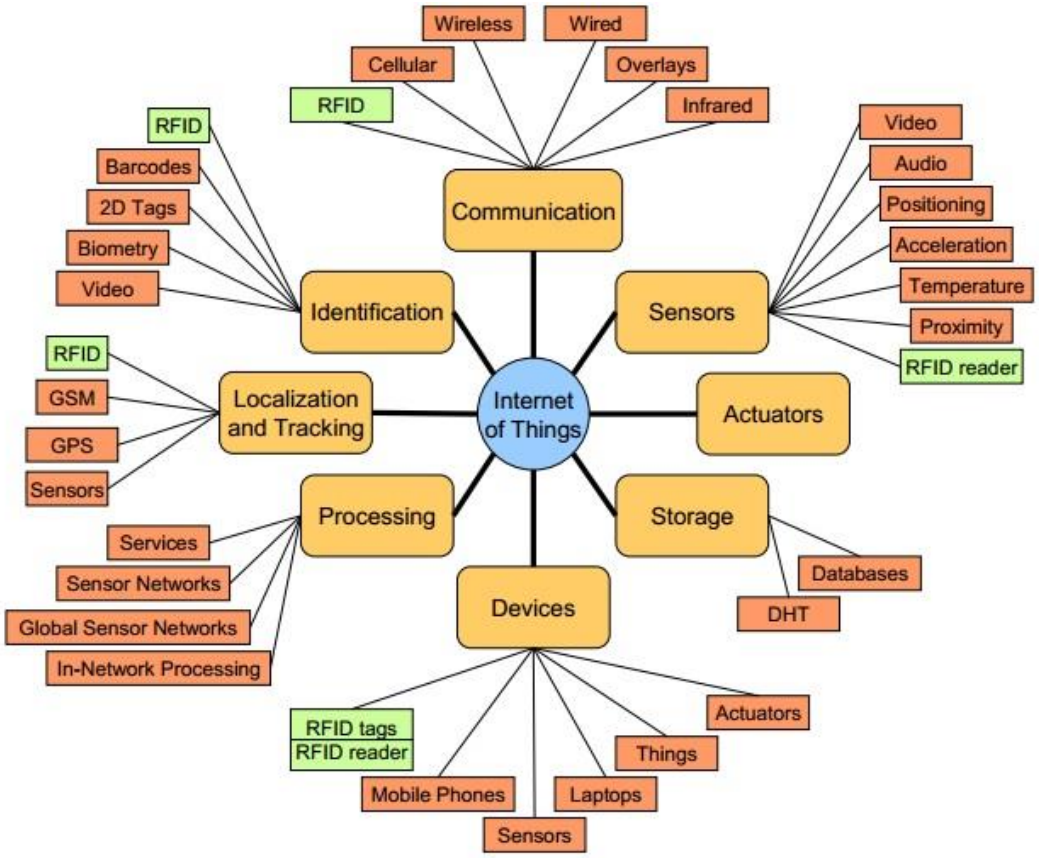


Figure 2-1 - Components involved in IoT systems (Mayer, 2009)

*"Internet of things is not some strange, new phenomenon; on the contrary, it is a natural development of the existing Internet."* (Fältström, 2012)

Some authors consider that IoT is simply a natural evolution of the Internet ( (Paolantonio, 2012), (Pretz, 2013)). It is the next step of a technology that in some ways is already stagnated and in need to respond to the new needs. The evolution represented by IoT is required and happens in a natural way.

## 2.1 Some definitions

In this section we try to clarify some important terms through an attempt to integrate opinions of important authors and other less important and sometimes anonymous people, who are just interested this field.

### *2.1.1 Cyber-Physical Systems*

This term appears sometimes in alternative to IoT, although they are not exactly equivalent. In fact, IoT can be considered a sub-set of Cyber-Physical Systems (CPS). The following definitions can help us getting an idea of what is involved in this concept.

*"Cyber-Physical Systems (CPS) are integrations of computation and physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology"* (Lee, 2007).

*"Cyber-physical systems (CPS) are engineered systems that are built from and depend upon the synergy of computational and physical components. Emerging CPS will be coordinated, distributed, and connected, and must be robust and responsive. The CPS of tomorrow will need to far exceed the systems of today in capability, adaptability, resiliency, safety, security, and usability"* (National Science Foundation, 2013).

*"Cyber-physical systems (CPS) are smart systems that have cyber technologies, both hardware and software, deeply embedded in and interacting with physical components. CPS and the innovative products and technologies they support have the potential to create a source of competitive advantage for the U.S. economy in the 21st century"* (Energetics Incorporated, 2012).

As implicit in the above definitions, CPS represents the integration of physical objects with computational systems. In other words, creating systems that connect computational systems to the physical world and represent the objects of the physical world as appropriate models in the computational world. This allows the development of better automation systems. The next step comes with Internet, combining software, hardware, objects and the network capabilities, exploiting the full advantages of having objects ''presented'' both in physical and cyber worlds.

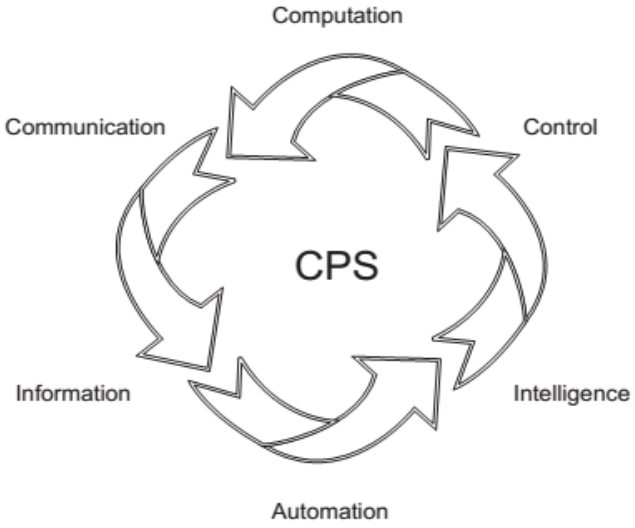


Figure 2-2 - CPS vision

As presented in Figure 2-2, CPS according to the authors mentioned above, includes features like control, intelligence, information, automation, communication, and computing.

### 2.1.2 Internet of Things

Although no common formal definition of IoT exists, various authors have tried to clarify the concept. Some examples:

*"The Internet of Things is a computing concept that describes a future where every day physical objects will be connected to the Internet and will be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it could also include other sensor technologies, other wireless technologies, QR codes, etc"* (Janssen, 2011).

*"In an era of technology were everyone wants to be connected taking advantage of all services provided by the Internet already having a solid network the next improvement is to represent objects we use every day not being restricted by mobility or time, using fully the proprieties each one wants from the objects. Internet of Things is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent inter-faces, and are seamlessly integrated into the information network"* (Sundmaeker, et al., 2010).

*"The basic idea of the IOT is that virtually every physical thing in this world can also become a computer that is connected to the Internet (ITU, 2005). To be more accurate, things do not turn into computers, but they can feature tiny computers. When they do so, they are often called smart things, because they can act smarter than things that have not been tagged"* (Fleisch, 2010).

These definitions clearly bring the idea that the IoT can be considered an Internet that supports "things", providing a virtual space where objects are represented, and access to their actions is provided virtually from anywhere. This integration of the two worlds, virtual and physical, involves issues such as: connection methods, intelligence, and self-configuring abilities.

### 2.1.3 CPS vs IoT

Comparing the notions of CPS and IoT, we can notice that the line that separates them is not quite clear. In this way it is important to discuss what distinguishes them. Let us have a look at the opinion of some researchers in the area:

*"The frontier between CPS and Internet-of-Things has not been clearly identified since both concepts have been driven in parallel from two independent communities, although they have always been closely related"* (Koubâa, Andersso, 2009).

According to (Ma, 2011):

*"Although both IoT and CPS are aimed at increasing the connection between the cyber space and the physical world by using the information sensing and interactive technology, they have obvious differences: the IoT emphasizes the networking, and is aimed at interconnecting all the things in the physical world, thus it is an open network platform and infrastructure; the CPS emphasizes the information exchange and feedback, where the system should give feedback and control the physical world in addition to sensing the physical world, forming a closed-loop system".*

In the slides provided by (Jeschke, 2013) it is simply stated that:

*"Cyber Physical System is the US version of the 'Internet of Things".*

It is true that both definitions cannot be separated due to the fact that they are closely related and even complement each other. The main cause for these terms having drifted apart is that they were developed by two independent scientific communities. However after analyzing the definitions of both CPS and IoT it would not be wise to simply take the idea that they are the same. In fact, if analyzed closely taking the information already presented, IoT can be seen as a subset of CPS. This vision is represented in Figure 2-3.

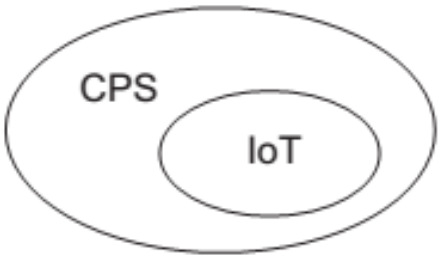


Figure 2-3 – An interpretation of CPS vs. IoT

This interpretation is shared by (Camarinha-Matos, et al., 2013). According to these authors, CPS includes not only "things" connected to the Internet, but also other physical systems with embedded computational power.

### 2.1.4 Things

One key element in the IoT is the notion of “things”. Thus a clarification of “things” becomes necessary when discussing IoT. In Figure 2-4 we have an illustration of some “things” that can be considered in different applications domains.

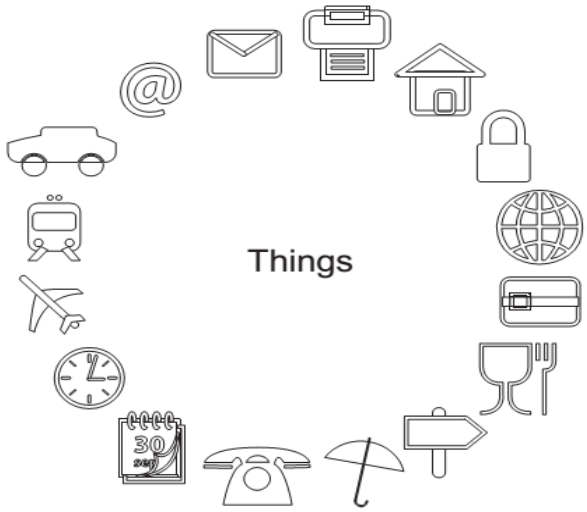


Figure 2-4 – Examples of Things

In IoT, “things” will fit in almost every day life aspect, whether in isolation or integrated in larger systems.

*“In the context of “Internet of Things” a “thing” could be defined as a real/physical or digital/virtual entity that exists and moves in space and time and is capable of being identified.* Things *are commonly identified either by assigned identification numbers, names and/or location addresses”* (Sundmaeker, et al., 2010).

A synonymous that is sometimes used is the term ‘’object’’:

*“Objects are linked through both wired and wireless networks to the Internet. When objects in the IoT can sense the environment, interpret the data, and communicate with each other, they become tools for understanding complexity and for responding to events and irregularities swiftly”* (IoT2012, 2012).

Another relevant point is given in the following statement:

*“IoT is significant because an object that can represent itself digitally becomes something greater than when the object existed by itself. No longer does the object relate just to you, but now it is connected to objects around it, data from a database, etc. When many objects act in unison, they are referred to as having "ambient intelligence"* (Janssen, 2011).

In summary, any object that can be connected to the Internet and get a ‘’digital presence’’ can become an asset to the user, accessible from everywhere through a unique address.

### 2.1.5 Industrial Internet

In line with the IoT concept, the notion of Industrial Internet can be understood as a particular case which by connecting people, data and machines contributes to the optimization of industrial processes.

According to (5 Ways The Industrial Internet Will Change Manufacturing, 2011):

*"The Industrial Internet is enabling this change to be more productive by making the physical world of industry more intelligent. By connecting machines to the Internet via software, data is produced and insight into the manufacturing process is gained. These machines become part of an intelligent network that can automate information and action to optimize plant floor performance".*

In Figure 2-5 we can see a number of features suggested by various researchers (e.g. (Markopoulos, 2011)) to support the Industrial Internet.

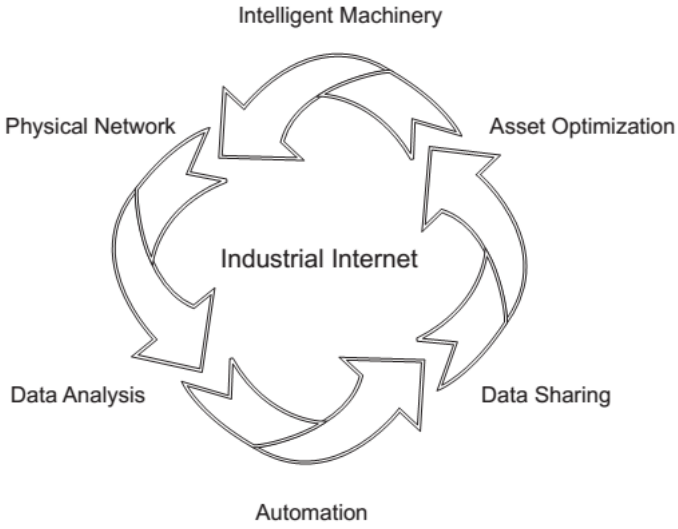


Figure 2-5 - Industrial Internet

This notion also points to increased levels of intelligence of the industrial systems, and intends to establish a bridge between the computational world and industrial machinery.

*"The crucial feature of the industrial Internet is that it installs intelligence above the level of individual machines — enabling remote control, optimization at the level of the entire system, and sophisticated machine-learning algorithms that can work extremely accurately because they take into account vast quantities of data generated by large systems of machines as well as the external context of every individual machine"* (Defining the industrial Internet, 2013).

Industrial internet is thus enabling the optimization of industrial processes through connectivity and increased intelligence, automating processes and providing autonomy to machinery. Industrial Internet will, in this way, increase the productivity, support preventing malfunctions, and cutting unnecessary costs to the company.

### 2.1.6 Sensing Enterprise

One of the most important aspects in human beings is their ability to adapt based on the perception of the surrounding environment, which allows a correct response to changes and adaptation to optimal conditions of comfort. Creating similar ability of analysis for enterprises can prove to be a big improvement.

*"Transformation of the way that business is created, business activity is transacted, business inputs are gathered, processed and factorized, and the outputs of business generate values for customers, business partners and other stakeholders. Shifting the focus and prioritization of enterprises resources and activities - Enterprise networks intersect with object networks and interlaced with knowledge networks"* (Li, 2012).

This author also claims that:

*"Future businesses will operate in a universal business ecosystem in which ICT will become a context for business operation spanning the whole cycle of value from creation to consumption, encompassing both people and things, and seamlessly merging the physical world with the virtual world for the exchange of many different forms of information and the transaction of different types of value"* (Li, 2012).

The vision of Li can be visualized in Figure 2-6.

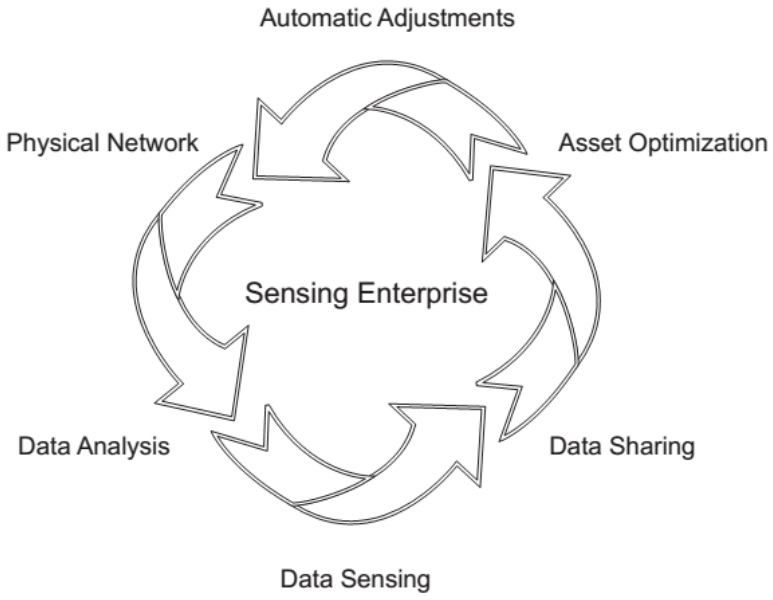


Figure 2-6 - Sensing Enterprise

As illustrated in Figure 2-6 a sensing enterprise is composed of several key aspects to business.
The process of creating a business environment that could sense changes in real time in the world or actuation area is a big and promising project in which many companies are investing in.

Being information one of the most valuable assets, future companies will be able to automatically gather, select and analyze multiple information sources within the area they are inserted in. If we add the capability of this being done in real time, it will likely open new ways of doing business.

### 2.1.7 Ambient Intelligence

"This concept represents electronic-enhanced environments that are sensitive and responsive to the presence of people" (Camarinha-Matos, et al., 2013).

This vision can be illustrated by Figure 2-7. The idea is to adapt personal space to respond intelligently in each different situation

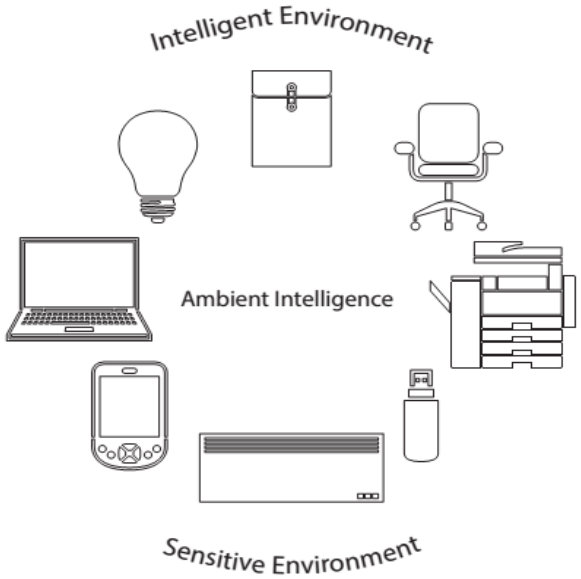


Figure 2-7 - Ambient Intelligence

.

Ambient Intelligence "combines notions such as pervasive computing, embedded systems, context awareness, and human- centric systems interaction" (Camarinha-Matos, et al., 2013).

One on hand, the interactions and cooperation between human and machines will not only make work easier but also faster and more reliable. On the other hand, several applications are emerging in the area of ambient-assisted living, such as elderly assistance.

*"Ambient intelligence is an emerging discipline that brings intelligence to our every-day environments and makes those environments sensitive to us. Ambient intelligence (AmI) research builds upon advances in sensors and sensor networks, pervasive computing, and artificial intelligence. Because these contributing fields have experienced tremendous growth in the last few years, AmI research has strengthened and expanded. Because AmI research is maturing, the resulting technologies promise to revolutionize daily human life by making people's surroundings flexible and adaptive"* (Cook, et al., 2007).

Providing means to sense the environment through sensors, being in this way able to analyze data instantly and adapt basic factors not only in terms of the physical environment but also in the virtual world, this increased intelligence can prove to be a key factor to boost productivity and quality of service.

## 2.2 Brief Historical overview

In this section a brief historical overview is provided, in order to understand the evolution of IoT from its gestation and consequent maturation.

*"Two main periods can be identified in the development of the IoT: IoT gestation and IoT maturation"* (Camarinha-Matos, et al., 2013). These two periods of the IoT evolution are presented next. The timelines show the most significant facts in IoT history. To provide more information on each point of interest, additional information is presented bellow each timeline.

### 2.2.1 IoT Gestation

IoT gestation corresponds to a long period during which a number of breakthroughs contributed to bring IoT to life. To illustrate the IoT gestation phase, Figure 2-8 presents the major milestones that lead to the IoT.

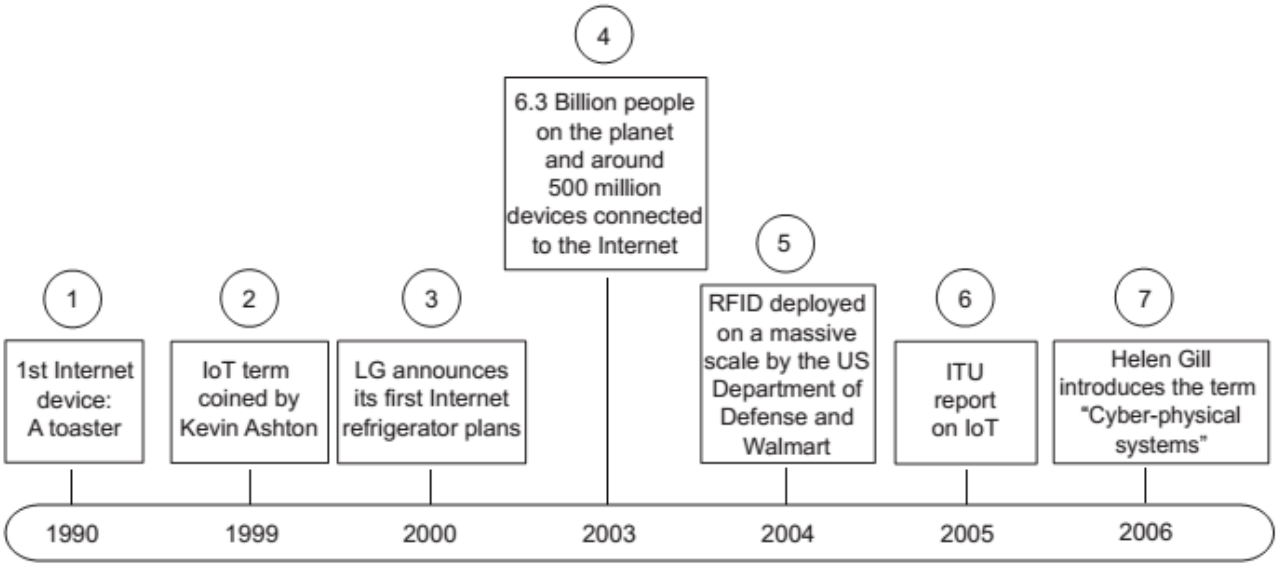


Figure 2-8 - IoT gestation timeline

1

This milestone represents the first time a device was connected to the Internet, a toaster. As simple as this milestone can be seen, it actually marked the first stage of IoT gestation. This device could be turned on and off over the Internet, and the connection was developed by John Romkey (Krikorian, et all. 2004**)**


In 1999 the term Internet of Things was coined by Kevin Ashton, the executive director of the Auto-ID center. This was the first time that the term was used to refer to an Internet capable of integrating devices. “I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at *Procter & Gamble* (P&G) in 1999. Linking the new idea of *RFID* in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight—one that 10 years later, after the Internet of Things has become the title of everything from an article in *Scientific American* to the name of a European Union conference, is still often misunderstood” (Ashton, 2009).


At this stage, LG presented the plans for a new “Internet refrigerator”. This refrigerator could inform, for instance, when the milk or any other product is running out of stock and provide the refilling even before it run out. I consider this milestone important due to the intelligence and autonomy given to a device. A major step towards IoT was the moment a device was provided with intelligence and autonomy.


This milestone emphasizes the fact that at this point there were 500 million devices connected to the Internet, the beginning of an exponential growth which promises to keep the fast pace of evolution of the area.


In 2004 Walmart announced that all its suppliers would have to tag supplies with RFID tags. Similarly, the Department of Defense (USA) took the same action and required that supplies would have to be tagged. These actions led to a better logistics, preventing thefts, among several other advantages. The action of tagging supplies provided real time information about them and although being a one-side information style, it is clearly an IoT feature. Fully developed IoT will allow receiving information about tagged “things”, not only to read information, but also to update and write additional information, creating a structure based on real time information.


This milestone is marked by an important report on IoT. This report was released by the International Telecommunications Union and approached several important subjects of the IoT. It gathered several sections on the Internet, e.g. Internet for mobile generation, telecommunications, integration, ubiquitous networks, visions of the information society, etc. This report also presented information about Internet of Things, its enabling technologies, challenges and opportunities. This publication is considered very important since it promoted the discussion on IoT within the research communities.
The full report can be found at the ITU website:
http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf


At this point in time, IoT had already become an interesting subject to researchers. However one of the most important papers at this time was presented by Helen Gill, in which the perspectives, enabling technology, needed research and challenges to overcome towards the fulfillment of IoT

were discussed. Furthermore, she introduced the term Cyber-Physical Systems in a close relationship to networked systems. “Cyber-physical systems are physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core. Components are networked at every scale. Computing is deeply embedded into every physical component, possibly even into materials. The computational core is an embedded system, usually demands real-time response, and is most often distributed. The behavior of a cyber-physical system is a fully-integrated hybridization of computational (logical), physical, and human action” (CPS: A View from the HCSS Agencies, 2008).

As illustrated in Figure 2-8, the IoT gestation happened at a fast pace particularly in the last decade, as a result of active research on approaches, identification of challenges to be accomplished, and problems to be overcome. In this gestation we also observe discussions on relevant terms such has IoT, CPS, and ubiquitous systems. As a major milestone we have the decision by Walmart and DoD to control their supplies by RFID, which is considered to be a key enabler of IoT.

### 2.2.2 IoT Maturation

In Figure 2-9 the IoT maturation phase is illustrated. As the IoT progressed the discussions and advances became more specific. It started to take form in specific projects, some held by collaborative consortia and others by individual companies. After being at an embryotic stage, IoT quickly started to take shape in terms of software and hardware components and infrastructures.

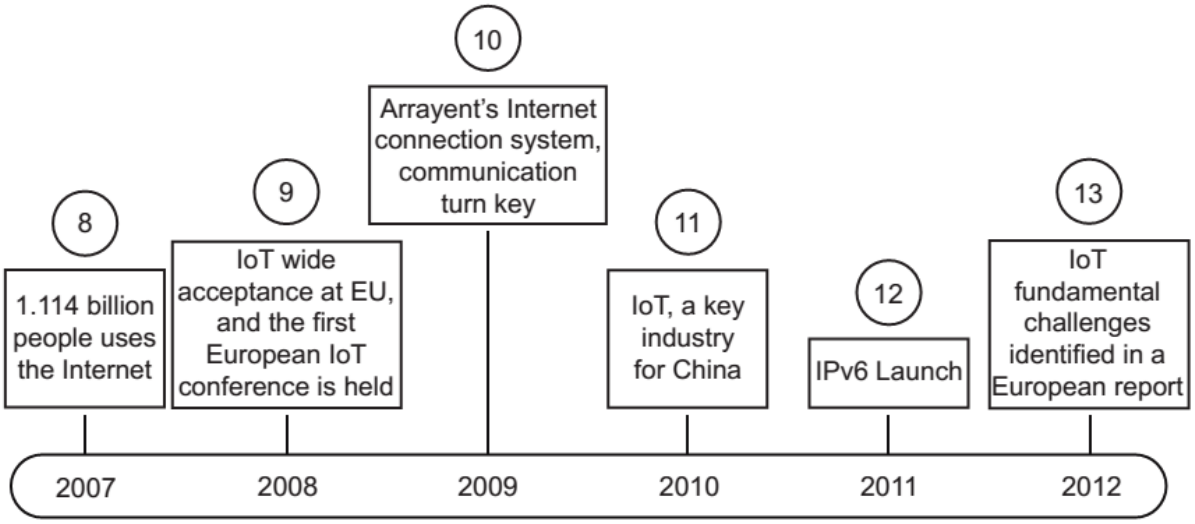


Figure 2-9 - IoT Maturation timeline

In more detail:

8

At this milestone IoT is considered to be born simply by the fact that at this point there were more devices (cellphones, sensors, computer and tablets) connected to the Internet than people. At this milestone there were almost 6.5 billion devices connected to the Internet and 1.114 billion users, which means almost six devices per user.

9

In 2008 the IoT got wide acceptance at EU level, and the first European IoT conference was held. In this conference major subjects such as enablers for the IoT were discussed. Technologies like RFID, short-range communications, real-time location and sensor networks were considered to be enablers of IoT and rising the necessity to explore each technology pros/cons. Results of this conference can be found at http://www.the-internet-of-things.org/iot2008/ (Fleisch, 2008).

10

At this milestone Arrayent introduced “Arrayent Internet-Connect System™”. This communication system can be considered a turnkey in communication terms. Althought not being a major IoT support it provided useful information and ideas to the IoT scene. “The industry’s first turnkey Internet connect system enables electronic product brand owners to connect their products wirelessly to web applications hosted in the Internet cloud... These web applications are used by consumers to monitor and control their electronic devices from any smartphone or web browser” (Dahlberg, 2010).

11

At this milestone the Chinese Premier Wen Jiabao announced the IOT as a key industry for China and presented plans to make major investments in it. The acknowledgement of IoT by China marks the importance given to the IoT subject.

12

In 2011 IPv6 was launched. This protocol is a key enabler for IoT, due to the fact that devices on IoT will be growing exponentially, and thus a new addressing system is needed. Since the IP protocol has its addresses space almost full, a new protocol was necessary. According to Steve Leibson (Leibson, 2008) “We could assign an IPV6 address to every atom on the surface of the Earth, and still have enough addresses left to do another 100+ earths.”

13

In 2012 the European Research Cluster on the Internet of Things (IERC-IoT) released a book identifying the main challenges in the IoT subject. This publication introduced several landmarks to be achieved. Bringing together researchers and several major companies and research communities, this publication introduced several subjects to discussion and a comprehensive overview of potential applications (CASAGRAS2, 2012).

As such, the maturation of IoT evolved from simple principles and in a natural way.

## 2.3 Application examples

IoT promises to support a scope of applications almost infinite. In terms of domains, we can find almost any type of application, many futuristic and other already implemented at the present days. It is therefore almost impossible to describe all cases and scenarios; we can however show that IoT can be used in almost everything in our days.

This section shows the importance and variety of applications of IoT, some of them already accessible with the current technology and others still in need of advances on hardware, software, or architecture. However in each one we can unveil the practical benefits.
The following major areas are briefly analyzed bellow:

- Smart cities;
- Inteligent Buildings;
- Health;
- Agriculture and Animal Farming;
- Industrial Machinery and Autonomous Processes;
- Smart Grid;
- Logistics and Transportation;
- Dangerous Enviroments;
- Public Safety.

The presented domains could be extended to many others, however almost every application derives from these main fields.

### 2.3.1 Smart cities

Smart cities could highly benefit from IoT, saving resources such as energy and decreasing pollution which is already a major problem in our society. Governments and researchers are making major efforts into these areas, with IoT providing the basis for intelligent management of resources, which could be the answer to major problems that affect the entire planet.

Imagine a city were all buildings, automotive, traffic lights, shops, bridges, schools were connected in the same network, sharing information that could be accessed anywhere, maximizing utility services like automatic billings, smart shopping, improving people's life in terms of saving time and comfort. All these objectives can be achieved resorting to sensors and actuators backed up by software capable of interpreting and analyzing data in real time and adjusting the environment to needs. Table 2-1 presents some smart cities areas that could be improved by using the IoT.

Table 2-1 - Application examples in smart cities

| Area | Description | IoT Contribution |
|---|---|---|
| Parking | Parking at rush hours can be a problem. Drivers tend to loose time, gasoline or simply breaking the law by parking in places that are not allowed. | Through sensors distributed over parking spaces that are capable to communicate with the car's onboard computer, could solve the problem. |
| Traffic | Rush hours always imply more traffic; furthermore, constructions on the road, accidents, vehicles malfunctions, will most likely lead to traffic jams. | A real-time traffic monitoring system, supported by updated data, based on the destination could advise the drivers for the different routes, avoiding traffic jams. |

| Area | Description | IoT Contribution |
|---|---|---|
| Waste management | Waste management companies have fixed routes and schedules. However, the waste volume is not the same every day. | Detailed real-time information being provided for utilities on the volume of waste can lead to a more efficient use of resources. |
| Lights management | Usually street lights are always on, according to a fixed schedule, disregarding climate conditions or visibility. | Detailed information about visibility, climate, and people on the street could be useful in terms of energy saving based on networked motion sensors and weather forecast predictions. |
| Transportation system | A big part of population depends on public transports, which sometimes are not as efficient as they could be. | Optimized and automatically adjusted based on information updated in real time routes can help save time and resources, both for companies and users. |
| cityWallet | In our days, payments over the Internet have become a constant. However the payment platforms have associated several downsizes such has security, availability and mobility, | A platform integrating all utility services and payments, having the user described in the Internet associating him to all needed aspects and services used. |

As illustrated in Table 2-1, various problems affecting our cities could be solved or smoothed by IoT. As such, comfort and efficiency would grow and allow to focus on other problems. These solutions can also bring to undeveloped cities more jobs opportunity and a huge boost on local economy.

Examples provided above such as automatic payment and smart lighting can already be found in an advanced stage of development. Siemens offers some solutions within this Smart cities area, namely the cityWallet, or the Smart lighting. At first, these solutions can be thought as an integration platform covering several aspects such as payments, control, etc. However if analyzed with a certain depth, we can conclude that besides integrating several solutions, these platforms include several physical descriptions of “things”, such as: users are represented within the Internet world, therefore their interests can be represented within the cyber world. A few more details:

***cityWallet***: this solution can provide features such as:

- Identity management;
- Mobile payments;
- Loyalty campaign;
- Ticketing;
- Energy services;
- Health services;
- City services;
- Parking.

“A citizen takes the subway and automatically gets a 20% discount because he doesn’t own a car. After leaving the subway, he pays for an electric car rental with the bonus points he was awarded for the energy surplus of the solar panels on his property. At his destination, he parks for free, because he has collected enough eco-points on his cityWallet account to receive free parking for eCars everywhere in the city” (Siemens Convergence Creators GmbH, 2013).

***Smart lighting***:

- Efficient and green operations;
- Command center;
- Optimized maintenance;
- Minimal investments;
- Flexible business models and additional services.

"With intelligent management, municipalities can drive down the energy consumption of their public lighting systems and realize significant savings, all while taking a big step towards becoming the green city of the future" (Siemens Convergence Creators GmbH, 2013).

These proposed solutions allow a wider degree of flexibility and easy integration of new services. There is a great effort into providing secure services and a variety of utilities only possible with the IoT.

### 2.3.2 Intelligent Buildings

Making housing adapted to each one will improve well-being and security, leaving personal environment more healthy and sustainable. In terms of large buildings – office buildings, shopping centers, etc., improvements can also be achieved in terms of environmental conditions, energy management, and security.

Table 2-2 show how buildings could be provided with more autonomy and intelligence through the use of IoT approaches.

Table 2-2 – Application example in Intelligent Buildings

| Area | Description | IoT Contribution |
|---|---|---|
| Energy consumption | Nowadays there is a big waste in terms of energy. | Automatic correction based on sensors, detecting useless energy consumption (e.g. turning lights off when a room is not occupied). |
| Ambient /climate levels | Maximizing comfort levels. | Automatic adjustments in personal environment. Based on the preferences and needs of the user, allowing the increase of the comfort. |
| Art and goods preservation | Works of art such as paintings, old books or any other type of art require specific conditions to be preserved. These conditions generally have to be manually adjusted depending on the environmental conditions. | All these conditions could be adjusted automatically based on environmental or climate change, always allowing the necessary conditions for the preservation of these goods. |
| Safety and security | Detecting certain aspects in the life of the elderly, for instance if they left the house, if they are in need of assistance, if there's a fire or if there's someone unidentified in the house. | IoT can contribute by continuously monitoring our home, making this information available at work or any place through the use of a computer or a cellphone. This type of security is already available, but can be improved with the technology advancements, making sensors more reliable, and tightening up security. Providing real-time information to the competent authorities. |
| Structural building health | Degradation of buildings in their foundations, broken windows, water infiltrations, gas leaks. | Information measured by sensors can automatically lead to repair processes or generation of warnings. |

The most important place for the human beings is their home. Providing several solutions to increase comfort, security, economy, as Table 2-2 refers, can increase the satisfaction levels.
It shall be noted that various solutions for intelligent buildings already exist, but they are usually based on local control units. Having these systems connected to Internet can allow more flexibility of management and open the opportunity for new advanced services.

### 2.3.3 Health

Health is one of the most important aspects in human life.
Some improvements in this sector tracking medical supplies, equipment and medical procedures are show in Table 2-3.

Table 2-3 – Application examples in the Healthcare domain

| Area | Description | IoT contribute |
|---|---|---|
| Patients surveillance | In hospitals or at home there might be patients in need of constant care, like monitoring vital signs, hearth rate beat, emergencies, etc. | A network of specialized sensors available to medical personnel providing constant surveillance on patients based on critical medical information that automatically adjusts drugs dosage, or simply alerting medical staff of an emergency. |
| Medical supplies | The need to track medical supplies from the moment they're made to the distribution, the delivery and the destruction in case of not being used, and most important their preservation and deterioration. | Having medical supplies tagged with the needed information on a data base for instance available to hospital and pharmaceutical companies can facilitate more effective tracking and management. |
| Biodegradable chips | Recording important information about the person like vital sign, habits, temperature pattern, blood pressure, cholesterol levels, and glucose. | Biodegradable chips implemented on people, recording all these information and in case of need, alerting medical personnel. |
| Sports care | Recording useful information each time the user practices sports, helping to improve through changes in habits. | Specialized sensors in conjunction with access to specific data bases can facilitate better monitoring and personal advice. |
| Ultraviolet radiation | High levels of UV can cause skin cancer. | By having real time information based on the location, hours, and position of the sun could allow informing the user when to avoid sun. |

As exemplified in Table 2-3, IoT can facilitate many improvements in the health care scene. IoT can also contribute to safety in medical procedures and real time information of patients, revolutionizing procedures and unlocking new features for medical care.

### 2.3.4 Agriculture and Animal Farming

Optimizing resources in agriculture is very important. In future, as the population grows, it will be necessary to maximize resources and avoid wastes. In Table 2-4 some possible improvements are suggested.

Table 2-4 – Application examples in Agriculture and Animal Farming

| Area | Description | IoT Contribution |
|---|---|---|
| Green houses | Depending on what is being cultivated, adjust the optimal levels of environment to the culture. | Different cultures need different conditions, like temperature or humidity. Automatically adjusting those conditions would contribute to maximize the growing. |
| Meteorological information | Allowing to know when there is a real need to irrigate cultures, based on meteorological information. | Getting real time information about weather forecasts correlated with the information on the cultures and soil information, would allow avoiding wastes in irrigation and thus achieve more productive cultures. |
| Optimal production levels | Optimize the cultures, minimizing the losses. | Instead of producing fixed cultures, information about market saturation or predictable information about tastes would maximize sales and satisfy markets |

| Area | Description | IoT Contribution |
|---|---|---|
| | | without saturation of products. A very simple upgrade easy to implement and with critical information to all the users, such as having a network of producers and market previsions. |
| Animal tracking | Knowing how many animals are there, and where they are. | A small tracker feeding information, with purposes of accounting for taxes, and subsidies from the government. |
| Offspring care | Real time tracking of the health of the animals. | Implemented chip controlling heath of cattle, preventing dangerous epidemics to spread into other animals and preventing infected animals to reach markets, isolating immediately sick animals. |

As illustrated above, IoT can provide autonomy and intelligence on processes, such as optimal levels of production or monitoring animal health and number.

### 2.3.5 Industrial Machineries and Processes

Monitoring malfunctions or making processes more agile are examples of applications in industry. For instance, overheating and malfunctions could be prevented and solved. Some of these improvements are shown in Table 2-5.

Table 2-5 – Application examples in Industrial Machineries and Processes

| Area | Description | IoT Contribution |
|---|---|---|
| Machine auto-diagnosis and assets control | Detecting malfunctions on machineries, and facilitating auto diagnosis. | Through sensors installed in the machines, allowing a faster response to detected problems. Connection to Internet allows remote monitoring. |
| Temperature monitoring | Some goods need a certain environment to be produced or maintained. | Monitoring temperature, raw materials, humidity and adjusting them automatically. |

### 2.3.6 Logistics and Transportation

Optimizing transportation and storage can be achieved through objects identification, and real time information on the transportation network. Table 2-6 shows some examples of major improvements in this area.

Table 2-6 – Application examples in transports and logistics

| Area | Description | IoT Contribution |
|---|---|---|
| Shipment conditions | Optimize shipments in transportation. | Optimize routs based on the shipments needs and status of the transportation network. |
| Track of goods | Knowing where the goods are in real time. | Real time information on the whereabouts of goods, and their conditions. |
| Storage detection | Keep track where the goods are stored, and if there is the need to ask for more in order to have supplies all the time. | Information if there is the need of more or less supplies, always related with the markets demand and degradation of stored products by having a data-base covering all stored goods. |

Logistics and goods transportation require high levels of optimization. As presented in Table 2-6, IoT could support an optimization even greater than the one we have today. Real-time information on routes, goods, and transport lines will take logistics and transports into a whole new level.

### 2.3.7 Smart grid

Being energy one of the most important resources, it needs to be treated with extreme care, aiming at its optimal use. Table 2-7 exemplifies potential management improvements in this field.

Table 2-7 – Application examples in Smart Grid

| Area | Description | IoT Contribute |
|---|---|---|
| Energy management | Increasing efficiency and avoiding waste. | Real time monitoring of production, demand, transport and supply. |
| Demand | Detecting if energy is being distributed according to the needs. | Real time information on the needs of energy. |
| Intelligent monitoring | Detecting leaks in distribution. | Automatically detecting errors and degradation of supply lines. Monitoring the grid lines and providing alerts to supplier's possibility of a faster response. |

Since energy sources, such has electricity, oil, and others are the center of society in our days it is extremely important to maximize the adequate use of these resources.

As in Smart cities, Siemens provides an example of an already developed system capable of dealing with some needs of the smart grid.

***prepaid Energy***:

- Tariff management;
- Charging, rating and usage control;
- Recharging, anytime, anywhere and by any means;
- Customer care.

"Prepaid Energy makes the entire payment process easier. The system supports the usage of physical tokens of a pre-determined value, as used in other existing prepaid systems, but it also allows customers to use an app on a mobile device or tablet to pay exactly the amount they can. Additionally, customers can easily access all their account information and the statistics of their use – giving them full control of their energy budget " (Siemens Convergence Creators GmbH, 2013).

### 2.3.8 Dangerous environments

Sometimes it is necessary to operate in environments hazardous for human beings. In this context, Table 2-8 provides some prospects on how IoT can help improving security in such environments.

Table 2-8 – Application examples in dangerous environments

| Area | Description | IoT Contribute |
|---|---|---|
| Control | Hazardous environments in which sometimes professionals have to act. | Actual work tools like robots already can perform this kind of work. However they'll always need a certain level of human control and in site presence. Reducing the need of this presence is possible by perfecting existing technology and making them connected everywhere, at any time. |
| Studies | Allow scientists to study for example volcanos or high deeps of the sea. | Allows studies to be performed in dangerous environments, and the collect of critical data without endangering human life. |

### 2.3.9 Public safety

Safety is a constant concern on people lives. IoT can contribute greatly to the development of safer environments, by supporting monitoring and alerting functionalities. However it has to be carefully regulated so it does not invade people's privacy or freedom rights.
In Table 2-9 some applications that could become very important in creating a safer environment for everyone are illustrated.

Table 2-9 - Application examples in Public Safety

| Area | Description | IoT Contribute |
|---|---|---|
| Monitoring dangerous criminals | Probation criminals, home detentions. | Based on GPS and sensors, designed to locate and control people of interest based on real-time systems with constant communication with the appropriate authorities (generalization of existing systems). |
| Faster police reaction | Real time monitoring of streets. | Real time monitoring of the streets, in order to allow a faster police response to dangerous situations. |
| Detection of fires | The need of accurate alerts. | Sensors monitoring temperature in forests or any other place. |
| Earthquakes, tsunamis and other calamities | Detection systems are outdated, therefore representing a risk to society. | More accurate systems with real time information of movements on tectonic plates, volcanos or water movements, coordinated with satellites, sensors, and response units. Some of these systems already exist but they can be extended. |

All these applications, although looking very different, share a number of aspects from the point of view of IoT.
They basically require a network connecting all end-points (data collecting, data analysis, and decision making). Even though in our days we can already have some infrastructures with these requirements, they still need improvements to fully unlock the IoT possibilities and open new potential applications.

As the IoT evolves and companies start to develop more specialized software and hardware, we can already see some breakthroughs available in the market, or at least in an advanced development state. In spite of being only small applications, it is already possible to have a small taste of the IoT potential.

According to the New York Times, which releases a top 10 products every year, the Table 2-10 provides information on what were considered the most important ones in 2009:

Table 2-10 - IoT products (Macmanus, 2009)

| Product | Developer | Description | URL | Date |
|---|---|---|---|---|
| IBM's sensor solutions | IBM | Sensors used in horticultural supply chain in order to track progress of shipment, from the moment they're collected to the retailer. | http://www.ibm.com/developerworks/websphere/techjournal/0911_hanis/0911_hanis.html | 2009 |
| Arduino | Arduino | Open-source platform for hardware and software. Intended to casual user and professionals interested in creating interactive objects or environments. | http://www.arduino.cc/ | 2009 |
| Mir:ror | Violet | Detects objects possibiliting to trigger applications and multimedia content. This ''mirror'' simply reacts to RFID tag placed in the object. | http://www.violet.net/ | 2009 |
| WideNoise | WEIDENOISE | Application that samples decibel noise levels and allows to share with WideNoise community in and | http://www.widetag.com/widenoise/ | 2009 |

| Product | Developer | Description | URL | Date |
|---|---|---|---|---|
| | | interactive map. | | |
| ioBridge | ioBridge | It is a web platform for remote control and monitoring, trying to respond to the need for interfacing physical devices with the Internet | http://www.iobridge.com/ | 2009 |

## 2.4 Trends, expectations, and strategic movements

This section intends to illustrate some trends, expectations, and strategic movements made by companies in order to prepare for IoT. As it will be shown, the awareness by the public and companies let us foresee a strong future for the IoT and the opening of all kind of opportunities for business and research.

### 2.4.1 Trends and expectations

As the IoT grows, as shown in Figure 2-10, after 2009 the interest on the subject suddenly grew almost at an exponential rate, not only by interest of the common user but also by the major companies and governments involved in IoT. Gartner contributed with a hype cycle on IoT. A hype cycle shows the interest on a subject from the discovery until the loss of interest by the community that matches with the stabilization of interest on the subject. Through an analysis of the IoT Hype cycle, as presented in Figure 2-10, we can observe the biggest discoveries.

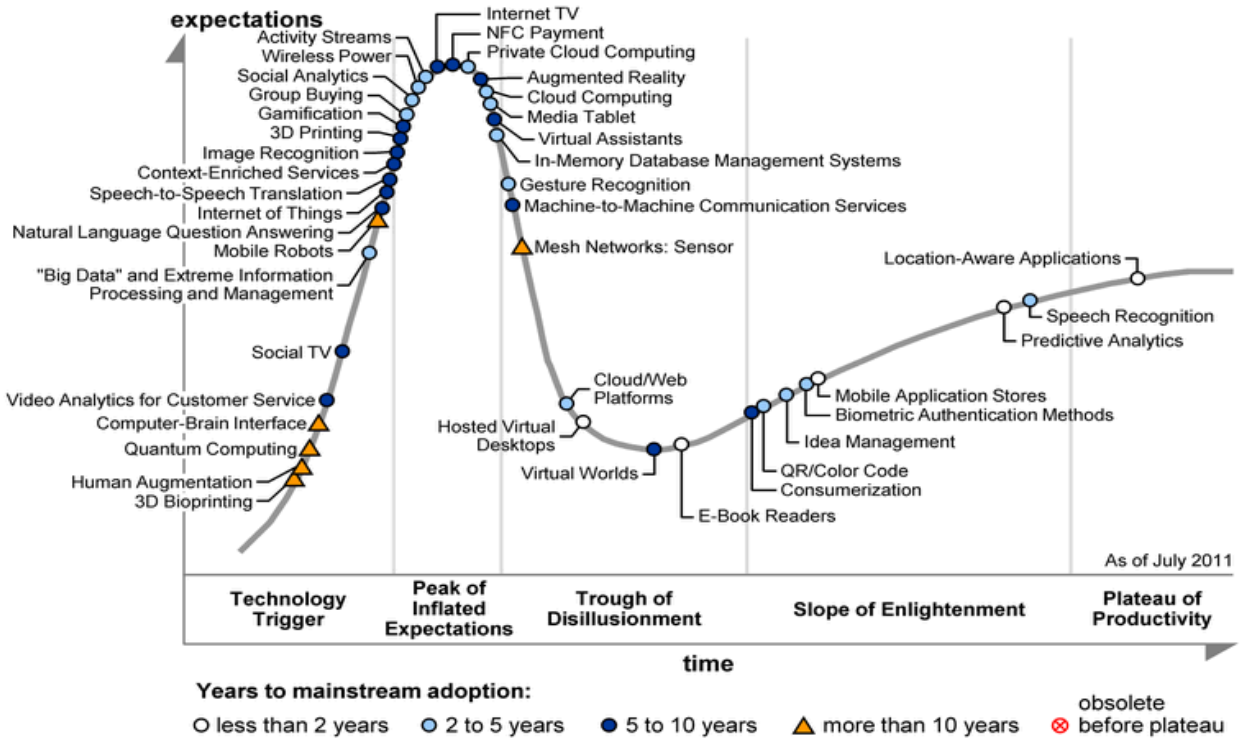


Figure 2-10 - Hype cycle of IoT by Gartner

As illustrated in Figure 2-10 the interest on IoT grew exponentially with the evolution of hardware and software and is probably reaching the pick in 2013. The interest is likely to decay after an intense period of expansion, even with the fact that technology continues to evolve, people tend to lose interest after the first approach and start to expect the final product to be delivered. In this period the interest will be mainly taken by companies and researchers.

Using Google Trends (analysis tool that analyses trends based on search queries), we obtain a chart that also shows the growth of the IoT interest (Figure 2-11). Due to the growing expectation and curiosity we observe an awaking on interest by the average user of Internet. This leaves no doubt that the fast development and natural evolution of the technology makes the interest continue to rise on the near future.

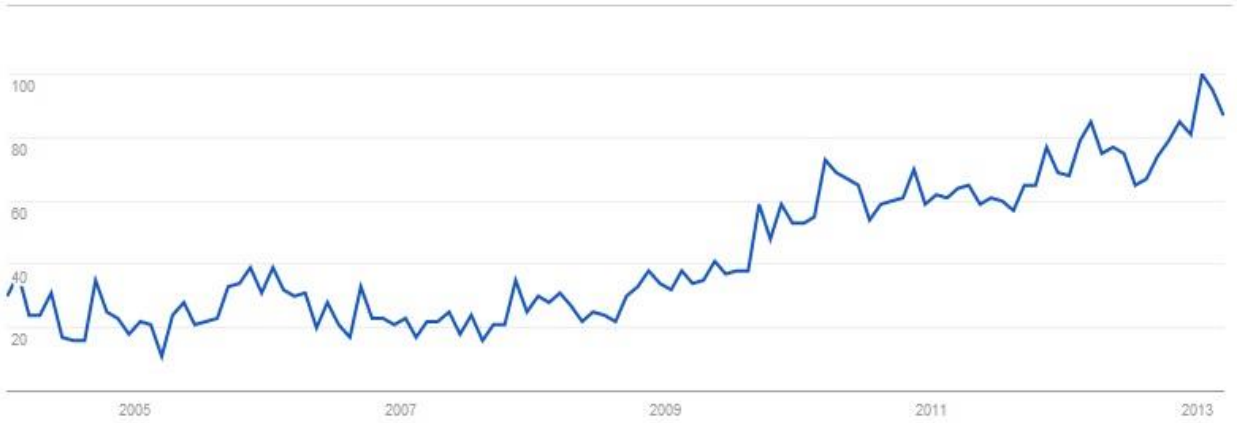


Figure 2-11 - Google trends graph for Internet of Things

According to Cisco, this interest on IoT can be explained with the evolutionary states that the Internet, and by consequence the IoT, have suffered. Cisco estimated the number of devices connected to the IoT.

Today there are almost 2.5 billion devices connected to the Internet. As the research and applications advance moving towards larger IoT, it is estimated that in 2020 there will be 50 to 100 billion devices connected to the Internet as referred in Figure 2-12. A remarkable milestone happened between 2003 and 2010 when the Internet became more populated than global society, i.e. when the number of connected objects outnumbered the world's population.

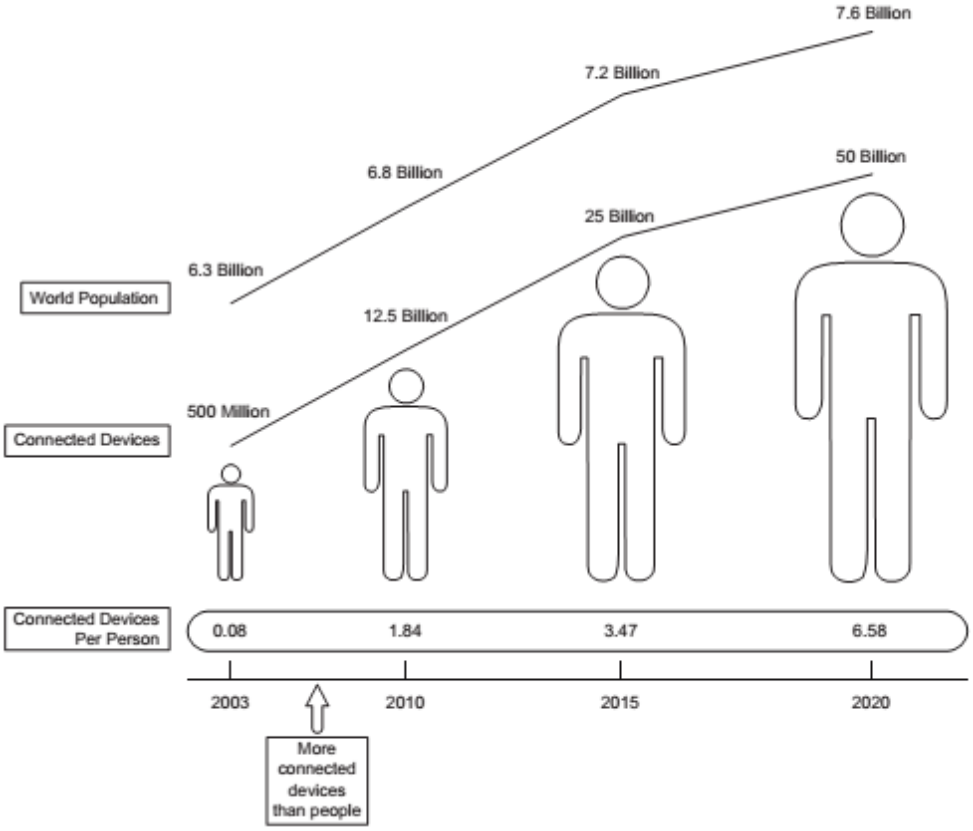


Figure 2-12 - Expectation of Objects in IoT (adapted from (Evans, 2011))

Figure 2-12 illustrates perfectly the fast growth of devices in the IoT. Currently, there are more objects connected to the Internet than people living on Earth.

Research perspectives come from all over the world. For instance, Auto-ID Labs has formed a network of seven research labs, that research on IoT and more specifically on RFID and Wireless Sensor Networks (Santucci, 2010). Hewlett-Packard presented a project for a Central Nervous System for the Earth which combines nanotechnology with electronics to develop sensors, including many potential applications such as intelligent buildings, traffic patterns, shipments, etc. (Hewlett-Packard Development Company, 2010).
After an initial period of slow development, industry seems to have realized that they could benefit greatly from IoT, making processes faster, and more independent.
One of the most important steps in the IoT evolution is the need of communication between everyone involved in the subject. There is the need to create a sound base of concepts, exchange ideas, and a mentality change by the average user.
Another interesting trend is presented in Figure 2-13, which shows that the number of conferences dedicated to IoT tends to grow every year.

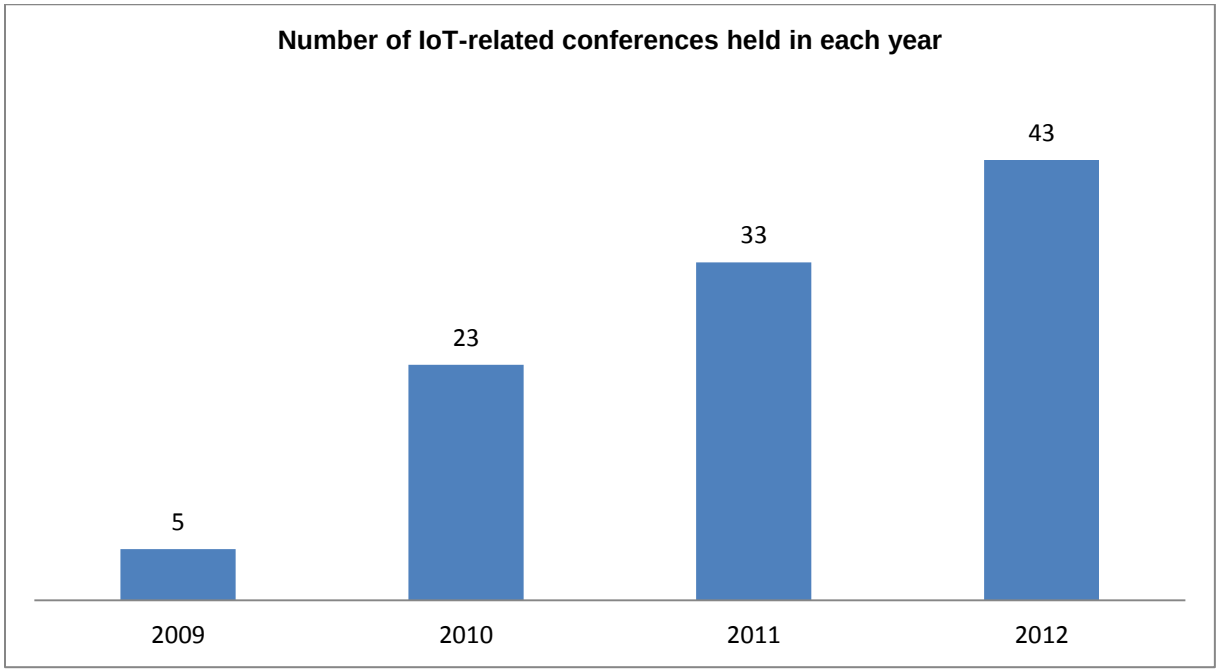


Figure 2-13 - Number of IoT-related conferences held between 2009 and 2012 adapted from (Presson, 2012)

Table 2-11 includes some information about the relevant conferences in which the most important aspects of IoT are discussed and proposals/solutions are presented.

Table 2-11 - Relevant IoT conferences

| Name | Date | Description | URL |
|---|---|---|---|
| IoT Week 2013 - The Event on IoT technologies and Innovation and Businesses | 16-20, June 2013 in Helsinki | This conference aims to unite the IoT community, offering a platform to present all the relevant research topics, opportunities, political and societal insights. This community also aims to provide the participants with networking opportunities. The general topics discussed in this gather were: presentations focusing IoT from the global point of view; IoT researchs such as IoT architecture, IP, technologies, etc; solutions as a core for smar cities concept; IoT entrepreneurship and business models. | http://www.iot-week.eu/ |
| Rotterdam Internet of Things Days | 9-12, April 2013 in Netherlands | Rotterdam Internet of Things Day intends to explain the IoT to anyone interested. In this conference the IoT is explained, since it is a common sense that IoT will have a major impact on society, it is extremely important to educate the common user. It is asked the participants to experience and share ideas, concerns and thoughts on this future technology. | http://iotrotterdam.nl |

| | | | |
|---|---|---|---|
| Special session at IEEE Photonics Conference 2013: Photonics and the Internet of Things | 12-16, October 2014 in San Diego, California USA | The predictions of devices connected to the IoT point to more than 100 billion wireless devices in 2020. This prediction makes this conference extremely important since it aims to introduce the IoT current state of work, contribute with related works and researches, identify future challenges in the area. Contributions on the IoT area are also invited into participation, namely on areas such as: energy harvesting and supply; low power communications, communication technologies relevant to the IoT. | http://www.ipc-ieee.org/ |
| IEEE World Forum on Internet of Things 2014 | March 2014, Seoul, South Korea | This upcoming conference presents clarification sessions, tutorials, and an industrial exhibition. Participants are invited to submit technical papers for presentation. This conference promises to gather some important figures within the IoT area. | http://sites.ieee.org/wf-iot/ |
| The 2013 IEEE International Conference on Internet of Things (iThings2013) | Nov. 13-16 in Munich, Germany | This conference intends to provide a forum in which researchers, engineers and practitioners can present proposals, advances, and innovations within IoT areas such as: foundations, systems, infrastructures, tools and applications. It is important to mention that this is the sixth conference of the same organization, which provides the conference a certain responsibility and credibility among the IoT community. | http://www.china-iot.net/iThings2013.htm |
| China International Energy Harvesting Summit 2013 | 5-6 December 2013, in Shanghai, China | Even being endorsed by a private company this conference aims into bringing to the ioT discussion some major companies and specialists to discuss technologies, challenges, applications in energy area. | http://www.iotevents.org/china-international-energy-harvesting-summit-2013 |
| Accelerating the Open Source IoT ecosystem | 22 November 2013, UK, London | This conference focus on the open source theme and it is designed to bring together all the interested in Open Source IoT/M2M ecosystem. This conference approached several important issues such as: privacy, security, data and interoperability. | http://www.eventbrite.co.uk/e/accelerating-the-open-source-iot-ecosystem-tickets-8444444561 |
| 2013 M2M HACKFEST | 26-28 November 2013, UK, London | This event can be considered a conference however, it proposes a different approach. It aims to gather teams or individual developers to develop solutions, addressing issues affecting the industry. This way, it provides an environment extremely important to the IoT, the collaboration. | http://iotevents.org/2013-m2m-hackfest |

As Table 2-11 illustrates we have been watching a huge growth in conferences about IoT. These conferences intend to unify the community into working together to achieve the full potential of IoT.

### 2.4.2 Strategic movements by companies

Complementing the information on trends and the recent ‘’gold rush’’ to the IoT subject, we can find several relevant news on the growth and strategic takeovers from companies that believe that the future is on the IoT.

In a Cisco report we are able to find predictions of the values at stake associated with the IoT. This study claims that the associated values that IoT will bring to involved sectors, is a huge motivation to the researchers. Cisco's predicts that the IoT will generate $14.4 trillion (Bradley, et al., 2013). In this study it is also estimated that a company that does not embrace IoT will probably loose more than a year of profit in a 10 years space.

Resently ARM, a chip manufacture bought the Sensinode, with prospects to introduce products and research in IoT. ARM is specialized in researching technology involving the IoT, while Sensinode is a company pioneer in creating low-cost, low-power Internet connected devices. Full article can be read in http://www.computerweekly.com/news/2240204209/ARM-buys-Sensinode-for-internet-of-things-push.

Within the company's world besides takeovers, we have been watching several alliances rising. For instance M2M magazine released information about an alliance between ThingWorx and SPIMSENSE. ThingWorx develops M2M application platforms while SPIMESENSE offers solutions for planning, building and deploying customized M2M and IoT applications. This alliance allows the two companies to progress in the near future with the IoT. Full article can be read in http://www.machinetomachinemagazine.com/2013/08/27/thingworx-expands-globally-with-spimsense-technologies/.

Another interesting piece of news about IoT future came from COMPUTERWORLD UK, in which Gartner stated that the IoT should not be ignored by business. The IoT concept is considered to be a key enabler to the business due to an increasing number of devices, communication and technology involved. "Gartner defines the Internet of Things as the network of physical objects that contain embedded technology to communicate and interact with their internal states or the external environment." (Savvas, 2013).

These examples confirm the trends described along this thesis, proving the value and possibilities considered by the companies from the moment they realized the advantages of IoT.

### 2.4.3 Conclusions on IoT awareness

All the facts presented on sub-chapter 2.4.1 and 2.4.2 let no doubt on the IoT awareness by all affected areas and interested parties. The associated values at stake, improvements, security, and all other benefits make the IoT a necessity for everyone. To avoid the IoT is almost like saying no to the progress.

Accordingly to Cisco the five main factors increasing the values associated to the IoT are:

- Innovation – Increasing the return on research and innovation investments, reducing time to market, creating new business models and opportunities;
- Customer experience – increasing the lifetime of customer and adding more customers;
- Supply chain and logistics, including waste elimination – improve utility services to a new and more efficient level;
- Asset utilization, including reduced costs – expense on goods reduced and improving business process;
- Employee productivity and efficiency – more productive labor.

(Bradley, et al., 2013)
The IoT potential is also analyzed in this study:

Table 2-12 - IoT potential (Bradley, et al., 2013)

| 2013 (without IoT) | 2022 (Potential with IoT) |
|---|---|
| Automated assembly machines are expensive and complicated to create and install. | Reduced costs as automated tools become less expensive to manufacture and implement. |
| Inefficient management. | Automated management of available resources. |
| Quality controls rely on human perception and dexterity. | Sensors help workers improve product quality. |
| Vulnerable to breakdowns, security threats, and natural disasters. | Automated detection and self-healing improves reliability of the electricity network, and other services. |
| Inefficient use of key inputs for production. Lack of flexibility among assembly locations. | Reduced waste (materials, energy). Greater freedom and agility to reallocate production and optimize inputs. |
| Missed or unidentified sales opportunities. | Increased sales from real-time market assessments and reactions. |
| Inefficient geographical selling. | Increased sales from location-based selling. |
| Little holistic assessment of customers' wants and needs. | Increased sales from improved coordination with other products and services (two-sided markets). |

The table presented above points some examples of critical improvements that IoT enables.
Therefore, everyone is trying to keep up with this evolution. All the benefits that IoT will bring are crucial to company's survival.
Past this point, it is impossible to deny the IoT importance, not only by the natural evolution of technology but also by necessity.

## 2.5 Projects and research

The fast development of the Internet and consequently the gestation and maturation of IoT got the attention of leading countries very early in the IoT gestation. Researchers understood the benefits that connectivity could bring and the new perspectives that could be opened. The development phases that the internet has experienced can be described making clear how this evolution awaken the interest on the subject.
In Figure 2-14 major development phases are illustrated.

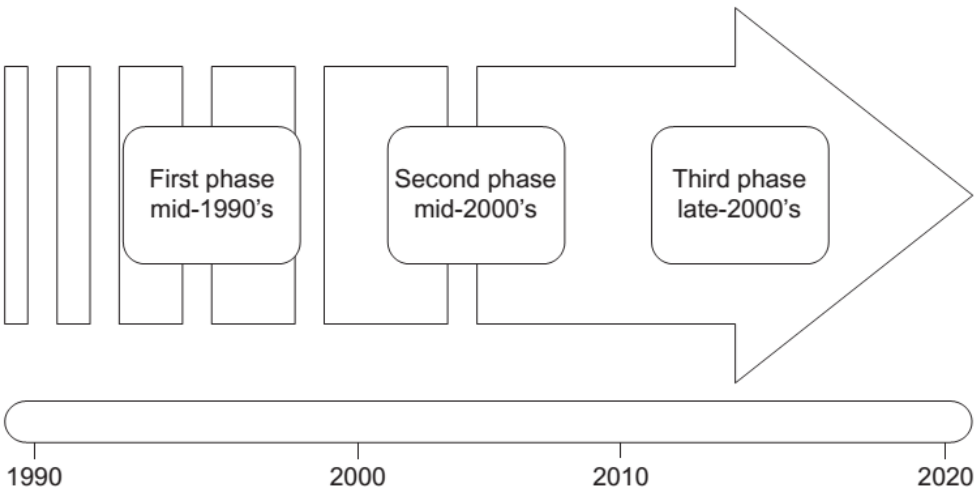


Figure 2-14 – The three development phases of Internet

According to Figure 2-14 the three main phases can be detailed as follows:

- First phase:
  - Internet was a way to collect and disseminating information;
  - It was used by people, to people;
  - The principal technology was WWW.

- Second phase:
  - Internet started to take shape into communities, involving people, goods and services;
  - It was used by people, to people;
  - The principal technology was the search engine.

- Third phase:
  - Internet evolved into a data collector of the real world;
  - Used by people and “things”;
  - The principal technology was an analytical engine that processes huge amounts of data.

In the first phase Internet provided a mean to do research, share documents and analyze raw data in scientific communities. In this phase, general public were still unaware of the Internet. In the second phase Internet turned into a tool used by not only the scientific community but also by the average user. In this phase Internet provided services like shopping, gamming, news feed, banking, etc. The contributions of this phase opened new challenges and debates about what could be accomplished. In this second phase, Internet started to evolve into the IoT. In the third phase industrial machinery, sensors, and most of connectable objects gained connectivity and autonomy to perform some tasks. With the rising interest on IoT, all parties interested and capable of investing in research acknowledged the importance and the need to keep up with this evolution. This third phase can have unknown effects on society, however most of them are expected to be benefic to people.

Another important view, besides the one provided above, is the Cisco’s vision of the evolution of the Internet into the IoT. Accordingly to Cisco (Evans, 2011) the first step was the research phase, when the Internet was called ARPANET, in which, during this time it was primarily used by academics and for research purposes. The second phase was characterized by the domain called ‘’gold rush’’. In this stage companies became aware of the improvements that Internet could bring, namely for advertising. The third phase was the explosion of services in the Internet. In this paper, Cisco considers a fourth stage of evolution, in which we are now, the called ‘’social Internet’’ where companies like Facebook, Twitter and others have become very popular, allowing people to share information and socialize via Internet.

### 2.5.1 EU perspective and research on IoT

With the new perspectives of IoT, the EU soon realized that this is one field with high potential and impact on European and world wide society.
IoT-I started in 2010 bringing together European countries into discussion as well as many multinational companies to work together in IoT vision. Analyzing the companies that joined the IoT effort (Table 2-13) we can visualize the strong effort put in research in the field:

Table 2-13 – Examples of major companies doing research on IoT (European Union, 2010)

| Company | Country |
|---|---|
| Ericsson | Sweden |
| NEC Europe Ltd | United Kingdom |
| SAP | Germany |
| Universität zu Lübeck | Germany |
| CEA | France |

| Company | Country |
|---|---|
| Alcatel Lucent | Germany |
| Thales Research & Technology | United Kingdom |
| Universitat St Gallen | Switzerland |
| Ericsson AB | Sweden |
| Alexandra Instituttet | Denmark |
| Universität Zürich | Switzerland |
| Telenor ASA | Norway |
| Hitachi Europe Ltd | United Kingdom |
| VDI/VDE IT | Germany |

Together, this community pursued several goals, however the most important were:

- Creating a joint vision adequate to all contributors;
- Contributing to an economical sustainable research basis;
- Creating measures so that all contributors can adopt IoT.

The projects presented in Table 2-14 are some examples, showing the effort put in research. Other important projects can also be found in http://www.rfid-in-action.eu/cerp-iot.

Table 2-14 – Some EU projects on IoT

| Acronym | Title | Funds | Description | Date | URl |
|---|---|---|---|---|---|
| IoT-i | Internet of Things Initiative | FP7 | Building a platform that will unify the diversity of companies and engineering disciplines working on the various projects. | 2010-2013 | http://www.sprint-iot.eu/ |
| IoT-A | Internet of Things Architecture | FP7 | Designing protocols, algorithms and interfaces. | 2010-2013 | http://www.iot-a.eu/public |
| ASPIRE | Advanced sensors and lightweight programmable middlware for innovative RFID enterprise applications | FP7 | This project aims to research and provide a massive change in the RFID scheme through a deployment of a new middleware. | 2008-2010 | http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=9833713 |
| PRIME | Privacy and Identity Management for Europe | FP7 | Bringing sustainable privacy and identity management to future networks and services. | 2008-2011 | http://primelife.ercim.eu/ |
| AMI-4-SME | Ambient Intelligence Technology for Systemic Innovation in Manufacturing SMEs | European Consortium (ATB, CARSA & DERI) | Innovate industrial processes, focusing on the human factor applying new approaches using intelligent environments. | 2005-2008 | http://www.ami4sme.org/ |
| BRIDGE | Building Radio Frequency IDentification for the Global Environment | FP7 | Project with the objective of resolving barriers to the introduction of RFID. | 2006-2009 | http://www.bridge-project.eu/ |
| CoBIs | Collaborative Business items | IST | Creating a platform with the objective of dealing with processes at a certain point of business instead of a centralized system. | 2004-2007 | http://www.cobis-online.de/ |
| CONFIDENCE | Ubiquitous Care System to Support Independent Living | FP7 | Develop and integrate technologies to build a care system to detect abnormal events such as falls or emergency situations especially to elder people. | 2008-2011 | http://www.confidence-eu.org/ |

| Acronym | Title | Funds | Description | Date | URI |
|---|---|---|---|---|---|
| DYNAMITE | Dynamic Decisions in Maintenance | FP6 | Monitoring machinery predicting the need of maintenance. | 2005-2009 | http://cordis.europa.eu/projects/rcn/75606_en.html |
| PROMISE | Product orientated manufacturing systems including RFID technology | FP6 | Managing the product life cycle creating information on the product at all phases of the lifecycle, improving service quality, efficiency and sustainability. | 2004-2008 | http://www.promise.no/ |

IoT continues to be a very important subject in the new research program HORIZON 2020.

### 2.5.2 USA perspective and research on IoT

USA also started its own IoT (or CPS as mentioned in their community of researchers) program by enabling funds to support projects.
The NSF predicts that IoT will exceed Internet as we know it today in all its key aspects like adaptability, safety, reliability, stability, functionality, etc. After several reports on this matter presented to the US government in 2007, the Cyber-Physical System (CPS) program was created and managed by NSF's Directorates for Computer and Information Science and Engineering (CISE) and Engineering focusing on the IoT matter (Table 2-15).
The USA CPS program focuses on three key subjects:

- Foundations;
- Methods and Tools;
- Components.

The program managers strongly believe that these subjects will provide a stronger IoT rather than an uncontrolled growth similar to the Internet. This means that USA is putting effort in not making the same mistakes as in early Internet developments.

For these new efforts, the US government supports researchers with large amounts of money:

- Small Projects:
  - $200.000/year up to three years;
- Medium Projects:
  - $500.000/year up to three years;
- Large Projects:
  - $1.000.000/year up to three years.

It does not only support big projects but also small and individual projects, what can prove to be a very useful bet in research since all contributions are valid, and like in the past, some of the biggest advances in the Internet were made by individual projects and researchers.

In Table 2-15 some of the USA projects in the field of IoT are summarized.

Table 2-15 – USA projects on IoT

| Acronym | Title | Funds | Description | Date | URl |
|---|---|---|---|---|---|
| ExCAPE | Expedition in Computer Augmented Program Engineering | NSF | The ExCAPE plan is to produce a range of design tools, these will allow end users to for instance program robots by demonstrating example behaviors, and that provide smart assistance for expert programmers to meet challenges in multicore programming. | - | https://excape.cis.upenn.edu/index.html |
| | Foundations of Secure Cyber Physical Systems | NSF | Cyber-physical systems regulating critical infrastructures, such as electrical grids and water networks, which are increasingly geographically distributed, necessitating communication between remote sensors, actuators and controllers. | 2011-2015 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=1136174 |
| | Towards robust cyber-physical systems | NSF | The objective of this research is to develop the theoretical foundations of robust Cyber-physical systems. Robustness is the property ensuring that slight perturbations in the cyber, physical, or in the interaction between the cyber and the physical components, e.g., noise in sensor measurements, causes only slight changes in the system execution. | 2010-2013 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=1035916 |
| | Closing the gap in Controller Synthesis | NSF | Automatic controller synthesis algorithms hold the promise of producing correct-by-construction systems, obviating the need for costly post facto verification. However, there is currently a gap between theoretical foundations of controller synthesis and their practical implementations on hardware and software platforms. This project addresses challenges in closing the gap in control synthesis. | 2009-2012 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=0953994 |
| CSR-EHCS | Collaborative Research: An Anytime Approach to Real-Time Embedded Control | NSF | Cyber-physical systems will soon become ubiquitous. One of the major challenges that such systems pose is that the control algorithms that modulate the interaction with the physical world have traditionally assumed availability of unlimited computational resources. However, in cyber-physical systems, control tasks are executed on shared processors that can only provide time-varying and uncertain computational resources. | 2008-2012 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=0834771 |
| | A CPS Approach to Robot Design | NSF | With the aim of accelerating innovation in a wide range of domains including stroke rehabilitation and prosthetic limbs, the project is developing new control concepts and modeling and simulation technologies for robotics. | 2011-2015 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=1136099&HistoricalAwards=false |
| | Co-Design of Multimodal CPS Architectures and Adaptive Controllers | NSF | The focus of this project is the efficient implementation of multiple control and non-control automotive applications in a distributed embedded system (DES) with a goal of developing safe, dependable, and secure Automotive CPS. | 2011-2015 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=1135630&HistoricalAwards=false |
| | Logical Foundations of Cyber-Physical Systems | NSF | This project seeks to develop logical foundations for cyber-physical systems (CPS), i.e., systems that combine cyber aspects such as communication and computer control with | 2011-2016 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=105424 |

| Acronym | Title | Funds | Description | Date | URl |
|---|---|---|---|---|---|
| | | | physical aspects such as movement in space. | | 6&HistoricalAwards=false |
| | Efficient Mapping and Management of Applications onto Cyber-Physical Systems | NSF | Full potential of CPS isn't being used to full potential due to the difficulty to program, and even more to deploy. The project is developing CPSISA, an abstraction layer or intermediate representation to facilitate CPS applications expressing their compute/sense/actuate requirements to lower-level mapping and management layers. The project is also exploring methods of providing a Device Attribute Catalog (DAC) that summarizes regions available CPS nodes and their capabilities. Third, this research is improving and exploiting the ability to model, predict, and control the mobility of CPS nodes. | 2011-2014 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=1135874&HistoricalAwards=false |
| Physically Coupled Software | Design and Run-time Techniques for Physically Coupled Software | NSF | This project seeks to establish the scientific principles governing software for such physically-coupled systems by focusing on four challenges in the context of distributed sensing and control applications. | 2008-2012 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=0820061 |
| CAREER | Automated Synthesis of Embedded Control Software | NSF | Effort towards the development of embedded control software that is correct by design. | 2006-2010 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=0717188 |
| SGER | Event-triggered control over sensor/actuator wireless networks | NSF | Research effort towards the integration of sensing, computation and actuation over wireless networks. | 2008-2009 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=0841216 |
| CSR - EHS | Formal Methods for Control and Real-Time Scheduling Co-Design | NSF | Computational tools for automated synthesis of real-time schedulers enforcing control, timing, scheduling and power consumption requirements are being built. | 2006-2009 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=0712502 |
| iSEE | Integrated Simulation and Emulation Platform for Security Experimentation | NSF | This project proposes to build iSEE - integrated Simulation and Emulation platform for security Experimentation, as software supporting research infrastructure used for cyber security research and development. iSEE allows for the concurrent modeling, experimentation and evaluation of CPS that range from a fully simulated to a fully implemented system. | 2011-2014 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=1127396&HistoricalAwards=false |
| | Self-Sustaining CPS for Structural Monitoring | NSF | This project proposes to design a self-sustaining, wireless structural monitoring system. | 2010-2013 | http://www.nsf.gov/awardsearch/showAward?AWD_ID=1035627&HistoricalAwards=false |

These projects focus on a wide range of aspects of IoT, including infrastructures, software, autonomous systems, self-sustainable systems, integration and control.

### 2.5.3 China's perspective and research on IoT

*"Internet + Internet of Things = Wisdom of the Earth."*
(Jiabao, 2010)

The rapid growth of China broke several barriers to development in their economics and social well-fair. This rapid growth also created several problems to social infrastructures which couldn't keep the fast pace of growing. With problems accumulating, China realized that IoT could help to overpass some of these problems, not only in technology terms but also as a development tool. In 2009, premier Wen Jiabao visited the Chinese Academy of Sciences (CAS) with the proposal to start the initiative of ''Sensing China" which had the goal to research and accelerate the development of IoT, establishing a research facility known as "Sensing China center" (Jingyue, Liu. 2012).
China's research is based on improving infrastructures, software and hardware already available, but also to establish new foundations to the implementation of CPS and consequently IoT (Table 2-16).

Table 2-16 - China projects (INOUE, et al., 2011)

| **Area** | **IoT expected contribution** |
|---|---|
| Manufacturing | • Intelligent control of processes;<br>• Inspections;<br>• Management. |
| Agriculture | • Real-time monitoring;<br>• Adjustments of temperature, humidity and illumination. |
| Logistics | • Monitoring and adjustments of goods, containers, vehicles and personnel;<br>• Traceability of food and chemicals. |
| Power distribution | • Monitoring the state of transmission and equipment;<br>• Remote meter reading. |
| Transportation | • Traffic volume;<br>• Parking management. |
| Public safety | • Monitoring commercial areas;<br>• Monitoring buildings. |
| Environmental | • Water and air quality;<br>• Monitoring pollution. |
| Disasters | • Early warning of natural disasters. |
| Housing | • Safety and security of residential areas;<br>• Energy management. |
| Health | • Monitoring vital signs;<br>• Health management of individuals. |

As mentioned above in Table 2-16, China is betting on projects that will be able to provide support in key aspects such as agriculture, health, housing, safety, which are problems affecting their society and are in need of a stronger solution. Premier Wen encouraged his provinces to make their own move on IoT, giving each province the ability to create its own research center, and implementing models and projects, emerging therefore independent research on each city, making this feature one of the reasons why China

is advancing so fast. The huge competition between provinces and the large amount of funds to support research was consequence of this research movement started by Premier Wen.
Companies started to be attracted to these independent projects due to their appeal in terms of business opportunities, boosting China's economy by attracting investors and creating work places.

Besides having its own IoT program, China also created international relations in order to have a wider research possibility. For instance, in 2011 the EU and China created the *EU-China IoT Advisory Group.* This partnership intends to cooperate in many areas within the IoT such as:

- Strategy;
- Architecture;
- Smart City;
- Standardization;
- Privacy and Governance.

This group promotes research and communication between China and EU (EU-China IoT Cooperation, 2013).

### *2.5.4* Japan's perspectives and research on IoT

Being a highly developed country, Japan has all the necessary conditions to lead the IoT research. Even more, due to the capability of research and advances in technology matters, Japan released IoT applications sooner than Europe. (Sa, 2011). In 2004, Japan's Ministry of Internal Affairs and Communications (MIC) created the u-Japan Policy in order to accelerate the development.

To continuously being able to fund research, u-Japan Policy is based on developing some high consumed areas in Japan:

- Vending machines: These machines can be found in almost every corner in Japan's streets. Upgrading these machines passes by implementing an e-wallet system, real-time information on supplies, and preventing underage to buy certain products.
- Transportation management: improving safety and reducing fuel consumption. This system intends to provide all transportations with a navigation service able to issue warnings, emergency situations, real-time location to reduce rescue and assistance time delays.
- Mobile payments: A platform able to integrate several services and a one-time authentication.
- Surveillance: surveillance systems used mostly by municipality services such as: nuclear facilities, service maintenance, sewage monitoring, etc.

Information adapted from (Sa, 2011).

In Japan we can already find several IoT solutions implemented. Japan focused in upgrading the systems that were based in the existent technologies, to make them more easily developed and upgraded to respond to the new challenges. Besides this upgrade in structures, Japan is also giving high importance to ubiquitous networks, enabling the possibility of access "anytime, anywhere, by anything and by anyone".

Currently the main focuses of Japan regarding IoT are:

- Safety and legal standards;
- Operational and organization structure;
- Educations systems;
- Educating on operation/maintenance;

- Models for investment and operation.

Besides doing its own research, Japan is also betting in creating joint research. CEA-Leti announced a partnership between Europe and Japanese companies (not only private companies but also universities, research institutes, etc.). This partnership aims to research a cloud project involving "things". This project is called "ClouT project" and, according to (Berst, 2013), it will develop the needed infrastructures to support services, tools and applications. ClouT project is based in the cloud technology (a relatively new concept which involves a network of several computers connected in a real-time communication), and intends to support and enhance several areas in need of advances such as: transportation, safety, management, and emergencies. ClouT project stands out from other projects since it intends to allow private users to create, manage and share their own applications. This project also involves the users into the development and research since the applications are tested in a public basis and it is expected to generate feedback allowing, in this way, to continuously improve the project. Thus, creating a more personalized infrastructure, closer to the user needs.

### *2.5.5* Other research and collaboration worldwide on IoT

Besides contributing to IoT in joint research initiatives, various countries are betting also on individual work in order to answer their country's own problems. We find proposals and reports from almost every country that realized that IoT evolution is an important key to developments at all levels. Hoping not being left behind and based on their capability in terms of resources and economic capability, Table 2-17 shows some projects active in various Universities:

Table 2-17 – Other IoT research groups (IOT-i, 2012)

| Country | Where can be found | URL |
|---|---|---|
| Algeria | Université Badji Mokhtar se Annaba | www.lri-annaba.net |
| Argentina | Ministry of Science, Technology and Productive Innovation (MINCyT) | www.mincyt.gov.ar |
| Australia | Forum for European-Australian Science and Technology Cooperation<br>Australian National University (FEAST) | http://www.montroix.com/feast/ |
| Azerbaijan | Baku Business Training Centre (BBTC) | www.bbtc.az |
| Brazil | Brazilian Bureau for Enhancing the International Cooperation with the European Union (B.BICE) | www.bbice.unb.br |
| Canada | Communication Research Centre (CRC) | www.crc.ca/ncp |
| Chile | Pontificia Universidad Catolica | www.ing.puc.cl |
| Egypt | Ministry of Communication and Information Technology International Relations Division (MCIT) | www.mcit.gov.eg |
| India | Ministry of Communicatons and Information Technologies (MIT) International Cooperation Division Dpt of Information Technology | http://deity.gov.in/ |
| Israel | Israel Europe R&D Directorate for the European Framework Program | www.iserd.org.il |
| Jordan | Higher Council for Science and Technology (HCST) | www.hcst.gov.jo |
| Lebanon | Arab Open University (AOU) | www.euinp.org.lb |
| Mexico | Tecnologico de Monterrey | www.itesm.mx |
| Morocco | Ministere de l'education Nationale, de l'Enseignement Superieur, devla Formation des Cadres et de la Recherche Scientifique | www.pin.edunet.ma |
| New Zealand | Facilitating Research Cooperation between Europe and New Zealand (FRENZ) | www.frenz.org.nz |
| South Africa | SAP / Meraka Unit for Technology Development | www.esastap.org.za |
| Tunisia | Ministry of Higher Education, Scientific Research and Technology (MHESRT) | www.isi.rnu.tn |

As represented in Table 2-17 even less developed countries are involved in IoT research, even if being smaller in terms of economy and ability to do research. We also can find some projects addressing interoperability and standardization between all interested parts on IoT. One example is the project

CASAGRAS2, which is a supporting action on IoT standardization, joining several countries like: USA, China, Korea, Japan, India, Russia, Brazil and Malaysia. The goal is to address issues like foundations and co-operation necessary to realize the IoT. This project intends to discuss issues such as:

- IoT Governance;
- IoT identification coding;
- Standards;
- Regulation;
- Policy and intellectual property;
- IoT architecture;
- Services and applications
- Awareness & education & training.

### 2.5.6 How is the IoT being referenced on YouTube

The next table (Table 2-18) references several videos available on YouTube which illustrate the IoT development.

Table 2-18 - IoT vision explained in videos

| Provider | Name of the video | Description | Link |
|---|---|---|---|
| DigitalAgendaEU | Internet of Things Europe – The movie: Imagine everything was link. | This presentation summarizes the essence of the Internet of Things, problems that could be solved by IoT, and how IoT could support people and not the opposite. | http://www.youtube.com/watch?v=nDBup8KLEtk |
| Eli the computer Guy | Introduction to the Internet of Things | This video explains the IoT to the average user. It explains the paradigm, the technology that will support the IoT, possible applications and how people could benefit from the applications provided by IoT. | http://www.youtube.com/watch?v=RCIyoqqzI6c |
| xdadevelopers | The Internet of Things – The Next Frontier for Developers | This presentation explains the concept of IoT, in terms of "things", applications, opportunities and trends. | http://www.youtube.com/watch?v=RlDIdHZ1XTk |
| IBM | The Internet of Things | In this video released by IBM, it is possible to visualize an assessment of future applications. It is possible to observe part of a day of a user with the support of IoT. It is also possible to obtain information about the integrated system that IoT will create in a natural way, due to the need for organization. | http://www.youtube.com/watch?v=sfEbMV295Kk&feature=youtu.be |
| Fwthinking | The Internet of Things \| Fw:Thinking | This video analyzes trends, such as growth. It shows a detailed example of the introduction of intelligence, and how IoT adapts and responds to each user. | http://www.youtube.com/watch?v=LVlT4sX6uVs |
| OreillyMedia | Fluent 2012: Tom Hughes-Croucher, ''Creating the Internet of Things with JavaScript'' | In this video, we see the needs of the IoT in terms of research: energy, structures, data flow, etc. | http://www.youtube.com/watch?v=PrWPHww1KoM |

# 3. SUPPORT TECHNOLOGIES

This chapter provides a review of the technologies underpinning the Internet of Things. This summary covers not only the new technologies but also those that are already in use and which may allow an easier passage from the Internet to the Internet of Things. Despite all the work still needed in this area, some solutions are already viable and facilitate this development. Nevertheless issues such as integration, sustainability, security, and upgrading existing infrastructures, still need the attention of researchers.

## 3.1 Internet

The Internet is the foundation of the Internet of Things. This huge infrastructure of information and media services can be accessed and used by anyone nowadays, and can be considered as the starting point for IoT. The Internet has evolved from a simple infrastructure, which had the sole purpose of sharing documents. Over time, the Internet has evolved into what we have today, as a result of multiple research activities.

With billions of users this evolution occurred naturally, but needs have changed and new barriers and challenges emerged. These developments led to the IoT, the next generation Internet that promises great improvements to society and the solution of various problems.

### 3.1.1 Brief history of Internet

The Internet is a global system that connects people, including private users, businesses, academic, and governments, providing services such as: information sharing, media, services, etc. The Internet can be described as a network that connects millions of devices around the world, usually desktops and portable devices such as phones and tablets.

In 1957, the U.S. launched the Advanced Research Projects Agency (ARPA), which established in 1969 the "ARPANET". The purpose of the "ARPANET" was to allow seamless communication between various points of interest in case of a nuclear attack. The general public only had access to the Internet around 1990.

The Internet as we know it today came to light in the hands of Tim Berners-Lee, with the help of CERN. CERN researched and created a protocol called hypertext, allowing connecting Internet contents based on hyperlinks.

By the end of 1993, the Internet contained 130 sites, and in 1995, it had more than 3,000. In 1998, there were more than 2.2 million websites.

In our days Internet is a network of networks, where private users, companies, governments can join and take advantages of being connect to this world. In this “world” they can share various resources like archives, documents, media, databases, etc. Internet relies on public, cooperative and self-sustainable bases, accessible to everyone owning a computer or a device capable of accessing the World Wide Web (WWW).

### 3.1.2 Basic aspects on the Internet

The Internet is an open network of computing devices. The Internet backbones are the servers that allow to store and transmit information. The devices used to access the Internet are called hosts or end devices, to allow access to the Internet these devices contain all the necessary software, which provides the protocols needed to be able to access the Internet and use all the services that it provides.

The Internet can be distinguished from other types of communication due to the use of TCP / IP protocol (Transmission Control Protocol / Internet Protocol). Strictly speaking, the Internet is itself a communication protocol. This protocol standardizes the communication regardless of the system used (Linux, Windows, Mac OS), so users are not required to be connected with other users sharing the same type of system.

Each node of the network is identified by an IP address, a numerical label assigned to each connected device, creating in this way a sort of a map on the network used to identify devices.

The DNS (Domain Name Service) is a system designed to assign names to the resources on the Internet. The main advantage is that the DNS translates IP addresses to labels that can be more easily understood and memorized by humans. Thus, we can see DNS as a database of hostnames. This system is based on a client / server architecture that responds to the request of users to access a certain page or Web service. When the DNS server receives a request it searches in its database the corresponding address.

The WWW is based on HTTP, which is a protocol on top of IP. HTTP allows the download of documents available in the Internet.

"*Data on the Internet is sent in "packets", which are basically small blocks of data. Each packet has a header that describes its origin and destination (like an envelope with a sender and recipient address). This information allows the network equipment to determine the best path to send a packet at given moment*" (McNamee, et al., 2012).

In this way the information available on the Internet is not accessed via a pre-defined path but rather by a dynamic packet switching mechanism. This switching allows information to be transmitted and received via different paths, providing a greater degree of flexibility.

The most used software to access the Internet is the Web Browser, which is used to retrieve, send and present information available on WWW. Each web page has an identifier attached, the URL (Uniform Resource Locator). We can think of URL as an understandable address, used to easily identify a Web resource. URL is a formatted string consisting of three different parts, the network protocol, the host name and the resource location.

Hosts in the past were connected to the Internet through cables, but nowadays there are also wireless connections. An important category of stakeholders in the Internet are the Internet Service Providers (ISP). An ISP is a business organization, usually a telecom company, that connects customers to customers of other ISPs. This company ensures that all the necessary protocols for Internet browsing are provided to the user.

Another important element is the router, a device that forwards data packets between networks. For instance, between a local area network and the Internet. An example is the home or office router that passes information between home computers (home network) or office computers (office network) and the Internet (via a connection to an ISP).

## 3.2 Devices or ‘’things’’

A device is a generic term to represent most of the “things” that can be connected to the IoT.

Nowadays it is possible to find some base technologies that can already support the IoT. However, more development is still necessary in order to reach the full advantage of IoT. The biggest problem with current technologies is the standardization; different devices can only be used in certain situations and require large integration effort. Creating standards for various classes of devices could facilitate the IoT to spread, allowing a much wider range of opportunities and flexibility.

Another issue is the amount of energy consumption of these devices. In IoT a device can be required to be on and stay connected for a long period of time (sensors and actuators for instance). This means a high consumption which has consequences in operational cost or affect the autonomy of devices in case of wireless connections. Therefore, the development of low consumption devices and more effective energy storage is an important enabler for IoT.

On the following tables, some of the “things” that can be connected (already available or expected in a near future) are described. In order to classify “things” we need to clarify some key aspects that suits IoT. In this way an effort was made in this thesis to clarify and classify “things” in a number of categories based on the proprieties: mobility, active/passive, dependent/independent and wired/wireless. However these categories, may change in time due to the constant evolution of the capabilities of “things”.

Classification category:

- Mobility – Classification about the mobility of the “things”, if it has to be stationary or mobile in the physical space. The mobility issue can be considered for instance in: a device in a transport vehicle, providing information about the conditions of the goods or the mechanical parts of the vehicle. Which means, that this “thing” is able to move instead of being stationary.

- Active/Passive – Clarification about the objects interaction with the surrounding environment. Active objects can sense the environment and adapt to it without human intervention depending upon their specific design and programming. Passive objects are not provided with this ability; they can only sense, analyze and ask for instructions. The capability of being active means that the “thing” only depends on itself to read surrounding conditions and act by itself, meanwhile, a passive “Things” needs to have permission from a third party, for instance, in a system where a temperature sensor depends on the specifications of the user, at the moment to change the environment it has to ask permission to the main system, which on its turn monitors all the environment.

- Independent/Dependent – Specifies if the object depends the other “things” or can act by itself. This means that an object or “things” does not depend on other “things” to act. This definition implies that a “thing” has the capability to act directly, without the need to order another “thing” or to be ordered, we can take the example of a programmable alarm clock, the user can program the clock located at this home over his phone, and the clock after programmed does not depend on any other device to work.

- Wired/Wireless – Indicates the type of connection of the object with the Internet, if it is by wires or wireless. This notion intends to clarify the type of connection, which have a huge impact on the mobility, however, it is important to have this clarification, since the type of connection has a great impact depending on the case it is inserted in.

Some “things” can enter in more than one category. Ultimately, “things” will only be distinguished in terms of its use. The evolution will likely allow most objects to be mobile, wireless, active and independent.

The tables of the following sub-chapters present some examples of “things”, characterizing and presenting them according to the categories described above.

### 3.2.1 Home automation

Due to the need of comfort and increased automation at home, this is one of the fastest growing IoT areas. Table 3-1 provides a brief overview of “things” included in the home automation area.
Table 3-1 – Examples of objects characteristics in home automation

| Things | Proprieties | Description |
|---|---|---|
| Air Conditioning | • Mobility – Stationary;<br>• Active;<br>• Dependent;<br>• Wired or Wireless. | Based on sensors and programmed logic. Storing information about ideal conditions, and being able to automatically adapt to each situation. When connected to Internet it allows remote command. |
| Television | • Mobility – Stationary;<br>• Active;<br>• Independent;<br>• Wired or Wireless. | A television able to store information about user, the favorite programs, access to the internet, and able to give feedback to the companies about preferences of the user. |
| Refrigerator | • Mobility – Stationary;<br>• Active;<br>• Dependent;<br>• Wired or Wireless. | Sensing and storage unit able to provide information about the conditions of products and able to provide automatic suggestions to buy products. |
| Surveillance system | • Mobility – Stationary and/or Mobile;<br>• Active;<br>• Dependent;<br>• Wired or Wireless. | Based on motion sensors, detection sensors, biometrics; the surveillance system can detect presence of intruders and activate adequate measures depending on the situations. It can be applied in home, car, or other environments. The connection to Internet also allows remote access to information about situations. |
| Safety box | • Mobility – Stationary and/or Mobile;<br>• Passive;<br>• Dependent;<br>• Wired. | Knowing our precious belonging kept in a safety box is secure can be a relief for some. This way, having the ability to control the content of our safety box from a smartphone could be a great utility for users. |
| Keyless doors | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wireless | A simple way to lock our doors, and a mean ensure that we left all doors closed, without going back. |
| Smart water analyzer | • Mobility - Stationary and/or Mobile;<br>• Active;<br>• Independent;<br>• Wired. | A gadget that would provide a complete analysis to the water we consume, not only to drink or cook, but also for instance in our pool, or any other water we use on our daily life. This gadget depending on the purpose of the water could provide an analysis on whether the water is within the specific parameter to consume or use. |
| Auto adjustment sounds | • Mobility – Stationary;<br>• Active;<br>• Independent;<br>• Wired. | A gadget that could adjust for instance the sound of speakers depending the room acoustic, the number of persons in the room, etc. |

### 3.2.2 Smart cities

Intelligent or smart cities are environments designed in order to offer improved living conditions in terms of organization, security and all other aspects such as mobility, time saving, energy consumption, etc. Table 3-2 describes some of those things that could possibly improve these aspects.

Table 3-2 – Examples of objects characteristics in smart cities

| **Things** | **Proprieties** | **Description** |
|---|---|---|
| Localization system | • Mobility – Mobile;<br>• Active;<br>• Dependent;<br>• Wired or Wireless. | A system within a city, capable of tracking persons of interest based on cameras, sensors, and biometrics. Could be useful in tracking lost children, avoiding crimes, and detecting general problems. |
| Smart lighting | • Mobility – Stationary;<br>• Active;<br>• Dependent;<br>• Wired or Wireless. | Automatic adjustment of timers in traffic lights depending on the traffic affluence or overcrowding. When connected to Internet, it allows more intelligent decision making, based on global information about traffic conditions. This technology can also be used in city lights, etc. |
| Automatic payments | • Mobility – Stationary;<br>• Active;<br>• Dependent;<br>• Wireless. | A system similar of the used on tolls, but extended to city related payments, like sanitation, parking spaces, etc. |
| Smart grid | • Mobility – Stationary;<br>• Active;<br>• Dependent;<br>• Wireless. | In this case, smart grid could be thought as a smart system allowing users to manage the energy consumption, avoiding wastes and unnecessary energy. This system would also provide a mean to the utility companies. Allowing to avoid extra expenses such as live maintenance in cases that would be needed and a tighter control of users. |
| Smart Parking | • Mobility – Stationary;<br>• Active;<br>• Independent;<br>• Wireless | A smart parking based on sensors to locate free parking spaces. Avoiding this way waste of gasoline and reducing pollution. |
| Dynamic advertising | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wireless | A smart advertising based on people choices, for instance, by accessing a smartphone web browser, advertising boards could present specific information to the user, or campaigns of a certain shop within user range. |

### 3.2.3 Personal gadgets

In terms of personal devices adapted to the Internet of Things, gadgets will become objects with more capabilities relevant to the user, i.e. providing a new range of applications, which can be useful in many cases. As illustrated in Table 3-3, we can find new applications for almost all devices used daily.

Table 3-3 – Examples of objects characteristics in personal gadgets

| Things | Proprieties | Description |
|---|---|---|
| Smartphone | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wireless. | Smartphones already have functions that illustrate the concept of IoT however they still haven't achieved their full potential. Smartphones could be able to store information and provide automatic adjustments or advices to user based on regular activities; like suggesting a restaurant, providing alternative routes, automatically selecting advertisements, etc, based on location. |
| Medical Chip | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wireless. | An integrated medical Chip with the ability to measure the host condition and able to report emergencies directly to doctors allowing to proper execute prevention medicine. |
| Smart Watch | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wireless. | Automatically adjust time zones, provide information like weather or in some cases for instance for sports; provide heath rates, distances travelled, timers on alimentations, etc. |
| Key chains | • Mobility – Mobile;<br>• Active;<br>• Dependent;<br>• Wireless. | Locate anytime, anywhere the location of important keys. |
| All-in-one Remote | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wireless. | A remote control able to integrate all aspects that can be adjusted within our personal space or personal Things. The remote could for instance check is we locked our car, or if it needs maintenance. It would allow with a single click to turn off lights or redirect the air conditioner. |

With the introduction of the Internet of Things, the capabilities of personal gadgets will assume a new role with a wide range of attributes and user applications. Another example already in an advanced stage of development is the Google glasses connected to Internet. This technology allows interactions with the physical world through the use of a pair of glasses connected to Internet. This object can support services such as interactive maps, video calls, music, etc. More information about Google Glasses can be viewed in http://www.google.com/glass/start/.

### 3.2.4 Health equipment

As with the other "things" mentioned above, also medical objects will have new capabilities within IoT. In Table 3-4 we can see a number of health-related equipment. Providing such objects with intelligence and autonomy can represent a big step to increased quality of life.

Table 3-4 – Examples of objects characteristics in health-related equipment

| Things | Proprieties | Description |
|---|---|---|
| Pacemaker | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wireless. | Pacemaker with ability to connect wirelessly, providing live information alerting for emergencies, or special attention needed by the patient. |
| Intravenous and Infusion Equipment | • Mobility – Mobile;<br>• Active;<br>• Dependent;<br>• Wired. | After being diagnosed, the patient may need special dosages and changing on medicines. A system remotely controlled by medical personal could allow controlling dosages and changing medicine. |
| Health surveillance system | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wired/Wireless. | Some patients need special attention such as elder patients, mental, or intensive care. A surveillance system adapted to each situation could improve health care and reduce mortality. |
| Medical triage | • Mobility – Mobile;<br>• Active;<br>• Dependent;<br>• Wired. | Automatic scan based on sensors reading specific biometric features could save time in triage and speed the processes up by categorizing certain symptoms. Connection of devices to Internet allows access to further information and thus better decision-making. |
| Heart rate monitor | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wired and/or Wireless. | Life supporting monitors capable to connect to Internet alerting for emergencies or anomalies. |
| Blood Pressure equipment | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• Wired/wireless | A smart blood pressure machine, instead of the usual readers, could easily keep records in medical staff databases. Thus, it would avoid patients to have to go to medical facilities. For instance, if the daily readings of a patient are abnormal, medication could be suggested or an emergency team dispatched. |
| Urine analysis | • Mobility – Stationary;<br>• Active;<br>• Independent;<br>• Wired/wireless | An automatic reader placed in the toilet could detect anomalies and issue warnings to the user, and perhaps keep detailed records to be presented to medical personnel. |
| Medicine smart reminder | • Mobility – Mobile;<br>• Active;<br>• Independent;<br>• wireless | Many people have to take medicines on a daily basis. A smart storage (similarly to the manual one used in our days), however with the constant control of medical staff, able to refill when necessary, and providing information about time and schedules. |

All these objects can highly benefit from IoT, such as the possibility of prevention and alerting for dangerous cases and also preventing from an escalating condition on the patient.

## 3.3 Connection modes

There is a need to separate and clarify object connection types. Connection can be specified by proximity, interaction and continuity of data transmitted/received. In the following sections an effort was made to classify the various cases. For each connection type the characteristics are described and based on that, some examples are given.

### 3.3.1 Connection on demand

Connect on Demand mode implies that it only happens when required. This means that the communication does not happen until there is a change of state or the user needs to communicate with the object. This type of connection is commonly found when there is the need to identify objects or receive information about them. In addition, it is also possible to store information or update the object's status.

Some cases:

#### 3.3.1.1 *RFID*

RFID is an old technology, however, due to recent advances in this field, it has opened a new range of applications.

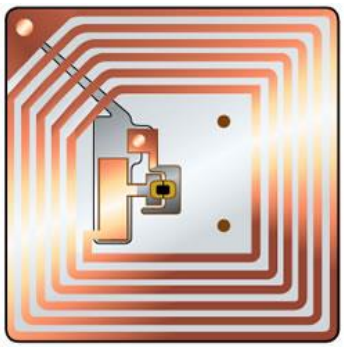

Figure 3-1 - RFID TAG

This technology is just one of many in the field of Auto-ID. RFID tag (Figure 3-1) is able to store, collect and transmit information about a particular item, providing a unique ID for the object and allowing it to identify itself when needed. The integrated circuit containing the data regarding the product is attached to an antenna that allows the transmission of information to a reader (Figure 3-2), which in turn forwards the information to the receiver.
There are different types of tags, as shown in Table 3-5.

Table 3-5 - RFID tag types (ILIE-ZUDOR, et al., 2006)

| Type of tag | Characteristics |
|---|---|
| Passive | • Power is obtained from the reader;<br>• Reader sends electromagnetic waves inducing the tag's antenna that reflects the signal transmitted and adds information. |
| Semi-Passive | • Uses a battery to maintain memory in the tag or power the electronics that enable the tag to modulate the reflected signal;<br>• Communicates in the same method, as the other passive tags. |
| Active | • Powered by an internal battery, used to run the microchip's circuitry and to broadcast a signal to the reader;<br>• Generally ensures a longer read range than passive tags;<br>• More expensive than passive tags;<br>• The batteries must be replaced periodically. |

The needed readers also change according to each situation, as described in Table 3-6.

Table 3-6 - RFID readers types (ILIE-ZUDOR, et al., 2006)

| Type of reader | Characteristics |
|---|---|
| Read | • Only reads data from the tag usually a micro-controller-based unit with a wound output coil, peak detector hardware, comparators, and firmware designed to transmit energy to a tag and read information back from it by detecting the backscatter modulation;<br>• Different types for different protocols, frequencies and standards exist. |
| Read/write | • Reads and writes data from/on the tag. |

Different types of readers can read/write or read. The specific reader to use in each case depends, thus, on the requirements of the application.

Figure 3-2 – RFID reader example

RFID technology has several advantages and problems. On the advantage side we have:

- Tag detection does not require human intervention;
- RFID has longer detection range than barcodes;
- Tags can read, and write information;
- Tags are less sensible to weather, damage and other conditions;
- Can be combined with other sensors;

- Reduce inventory control;
- Improve mobility.

On the disadvantages side we have:

- Lack of standardization;
- Price;
- Collision of information, such as multiple tags being recognized;
- Faulty detection, the readers are prone to fail the reading;
- Possibility of virus attack.

#### 3.3.1.2 Quick Response Code

Quick Response Code (QR code) is a two-dimensional graphical symbol, invented in 1994 by a Toyota group. Due to its widespread and use acknowledgment it was approved as ISO standard in 2000.

Figure 3-3 – A QR Code Example

The QR code (Figure 3-3) manages up to 100 times more information than the standard barcode due to its encryption type. The QR code is a coded image, which stores information which can be accessed by using the appropriate decoding software.

QR codes can:

- Tolerate a certain degree of damage without losing information;
- Be encrypted to only being able to be read by an unique reader;
- Be used to link symbols to external functions;
- Restore data and correct errors;
- Can be interpreted by various devices, including smartphones or tablets.

Figure 3-4 - QR Code reader example

There are many processes of encoding QR codes, and thus in spite of their advantages over bar codes, they have not yet been fully accepted by the general public despite being an ISO standard. One advantage is the possibility of QR codes being read in almost all devices (Figure 3-4).

#### 3.3.1.3 *SMART CARD*

Figure 3-5 - Smart Cards

The Smart Cards technology (Figure 3-5) came to light in 1976 by the hand of Michel Ugon who invented the first microprocessor chip. Since then, this technology has undergone several improvements in terms of safety, size and capabilities. The Smart Card is generally a shaped card made of polycarbonate and similar derivatives, and has integrated circuits. These smart cards can provide identification, authentication, and data storage. This technology allows communication without contact. Entering the field of action of the reader it is possible to access information and perform transactions. In the future, these chips could be made available to other applications such as in smart clothes, or even inserted in the human skin for identification or for automatic payments. The wide range of applications related to smart cards can be almost endless.

### 3.3.2 Connection when within range

This type of connection requires proximity between two objects. Two or more objects should be within the radius of action in order to establish communication. This means that the data is not flowing constantly, but only when the objects can interact.

Some examples:

#### 3.3.2.1 NEAR FIELD COMMUNICATIONS

The NFC is a contactless proximity technology, which was initially developed by Philips and Sony. NFC provides connection between devices, easy installation and allowing data communication simply approaching two devices. NFC can be used for ticketing, access to personal data, mobile entertainment, etc.

NFC is based on the principles of the RFID technology and usually operates within 10 cm using the specific transmission modules supporting technology standards, being possible to provide communication for a certain degree of security. The NFC supports up to 424 Kbits / s, and can be configured to be active or passive and is usually configured in peer-to-peer mode.

In terms of research, the "NFC Forum," aims to continue the research on this technology bringing together scientists and practitioners in the evolution of this communication way. This forum focuses mainly on:

- Directing the future developments of the NFC technology, by proposing technical specifications for data structures, protocols, etc.;
- Providing technical recommendations and reference designs to form the basis for interoperability between devices and interoperability with services;
- Establishing conformity testing and issuing conformance certificates;
- Proposing applications and use cases of NFC technology;
- Driving market adoption of NFC by initiating promotional activities such as a website, press releases, educational workshops, and support for members on tradeshows.

Examples of use of NFC can be found in automatic tolls, in parking spaces or for instance in some security checkpoints for identification.

#### 3.3.2.2 BLUETOOTH

Bluetooth was developed around 1994 by Ericsson. Its main objective was to eliminate wires for communication between certain devices. Bluetooth is a mean of communication used for establishing communication between two endpoints, despite being low cost, it provides security functions. This type of communication is typically configured in an ad-hoc mode. It operates in 2.4GHz frequency, and can establish a communication between two devices up to 10m to 100m and allows data rates up to 723 Kbps. Its components are quite small and can be deployed with most other devices.

Nowadays, Bluetooth can be found in almost all mobile devices (mobile phones, tablets, TVs, cars, appliances, etc.), and is used to share information between these devices, or to access information available in certain areas, such as museums, information desks at airports, or information about products, for example in commercial areas.

#### 3.3.2.3 Dedicated short-range communications

The dedicated short-range communications (DSRC) is a wireless communication method, and available in one-way or two-way communication at a certain distance. It was designed specifically for mobile use, and especially to improve the security and other specific applications.
In the U.S. we find DSRC using 75MHz of spectrum in the 5.0GHz band. In Europe it is allocated 30MHz of spectrum in the 5.9GHz that allows specific companies to monitor this frequency, allowing no interference between communications and a certain degree of safety. This technology is mainly used in electronic tolls, but may have other possible applications, such as:

- Emergency warnings;
- Automatic cruise control;

- Collision warnings;
- Vehicles inspection;
- Parking payments.

This technology is also being adapted for many other applications, such as providing information to blind people, allowing warnings of proximity of objects or points of danger, for example, in the street, providing information about the color of the traffic light, or the presence of a crosswalk. This type of communication can also be used to provide real-time information about the traffic, through the use of sensors that enable communication with onboard computers for instance, informing the driver on accidents, road hazards, speed limits, etc.

### 3.3.3 Wireless permanent connections

The connection is continuously available without the requirement of being established. Being a wireless connection makes this type of communication very attractive because of the mobility and availability it provides. However this type of connection tends to spend a lot of energy. Its installation reduces some costs of hardware, and allows a considerably large data stream.

Examples:

#### 3.3.3.1 3G

3G technology comes from the evolution of the GSM system. Third generation is the term used for this mobile communication. The 3G is used worldwide by almost all mobile phone carriers, has security solutions and provides up to 2 Mbps data stream. Due to the large use of 3G there are already implementations of its evolution: 3.5G and 3.75G. The 3G is normally used by telecommunications companies, but it can also be used in many other applications:

- Mobile Tv;
- GPS systems;
- Video conferences;
- Location services.

Even being telecommunication, its primary application it can be adapted to meet the specifications of IoT.

#### 3.3.3.2 WI-FI

Wireless communication is considered nowadays one of the most important means of communication.
Using an integrated modem, Internet can be accessed at anytime, anywhere as long has the place has wireless coverage. Wireless communication is a great facilitator for the IoT, since one of the major aspects of IoT is being able to connect objects to the Internet anywhere.

Wi-Fi has been designed specifically to act as wireless Ethernet, the rapid development allowed to obtain better results than other types of connections based on the fact that Wi-Fi does not need much physical support and is based on open source which means anyone can help improve.

Today's wireless runs at 2.4GHz spectrum, but with the high usage it is already near its full capacity. The solution is to move in the 5 GHz spectrum, also allowing increased bandwidth, faster connections, and greater reliability.

The rapid development of Internet and telecommunications made Wi-Fi Internet connection preferred. Besides having a huge mobility and independence characteristics, its cost is much lower than the wired version. The connection needs only that two stations recognize each other and establish a network.

The Wi-Fi has already several variants. The version currently used is 802.11, and suffers constantly changes due to the type of platform being open source. The original 802.11 standard has evolved into 802.11b, a supplement that provides a significant improvement in the speed of communication. One variant researched is 802.11q. This version provides nearly 54 Mbps and is allocated in the 5GHz frequency. These improvements however may require some changes in terms of hardware, but it is already possible to find equipment that can support both versions 802.11a and 802.11b.

### 3.3.4 Wired continuous connection

This type of connection provides a permanent connection to the Internet through a physical cable.
As it is a method based on wires, the mobility is highly limited. However, it can be useful in certain situations, particularly if the location of “things” is static. For example, in the case of devices that provide information about the environment, or warning sensors.
As described in the next section, this medium has evolved from ISDN and DSL, being important to have a little insight into their evolution.

#### 3.3.4.1 DSL connection

Digital Subscriber Line is a type of connection through a phone line, but with greater speed than dial-up. This type of connection requires a special modem. DSL evolved into ADSL (Asymmetric Digital Subscriber Lines), which is optimized for a faster connection, due to the fact that the line is asymmetric, providing a greater capacity to receive and transmit data.

#### 3.3.4.2 ISDN connection

Integrated Services Digital Network is considered to be an upgrade of the phone line used to access the Internet. This development enables faster communication and allows the use of the telephone and the Internet at the same time through the use of two different lines which means that the data does not have to be converted to analog.

#### 3.3.4.3 Optical fiber connection

Optical Fiber connection is used to support many applications such as: LAN, WAN, Storage Area Network (SAN), among others. The connection is provided by optical cable and can be a huge competitor to the wireless connection since it allows a plug-n-play connection, which means that the installation is basically to plug the device. Optical fiber connection has a huge power of data transmission, in our days, this type of connection can reach almost 500MHz. Optical fiber is also immune to electrical interferences since it’s functioning does not depend on electricity.

## 3.4 Network topology

The topology of a network refers to the way how the network is organized.
On top of Internet different topologies can be considered when we focus on the logical relationships among a subset of nodes.

Examples:

### 3.4.1 Client/Server topology

Client/server topology is exemplified in Figure 3-6.

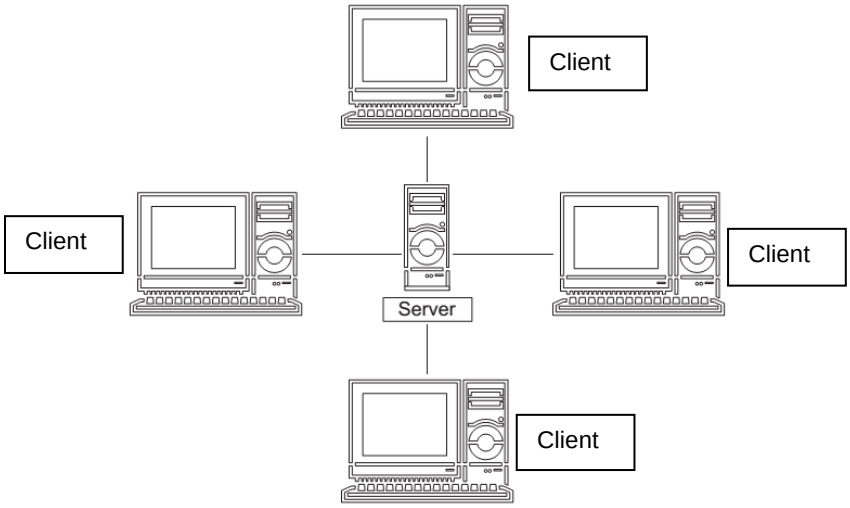


Figure 3-6 - Client/Server Topology

This type of topology has two different types of participants, the client and the server.
The client is connected to the network and asks the server to run some tasks. While the server is connected to the network it has the sole purpose of executing tasks to the clients. The server is capable of multi-tasking which means it can receive multiple requests and is capable of prioritizing each application and thus being able to satisfy various clients.

In terms of security, this type of topology can provide a high degree of protection since all features are located in the same place, however, it has some costs in terms of maintenance. In this way, proper protections, protocols and all the necessary service characteristics are implemented in the server, while each end-point (client) has the responsibility to protect its own device.

### 3.4.2 Peer to peer topology

In P2P topology each computer plays both the role of client and server when needed. This topology allows the sharing of resources and information, without the need for a physical server. The P2P topology is illustrated in Figure 3-7.

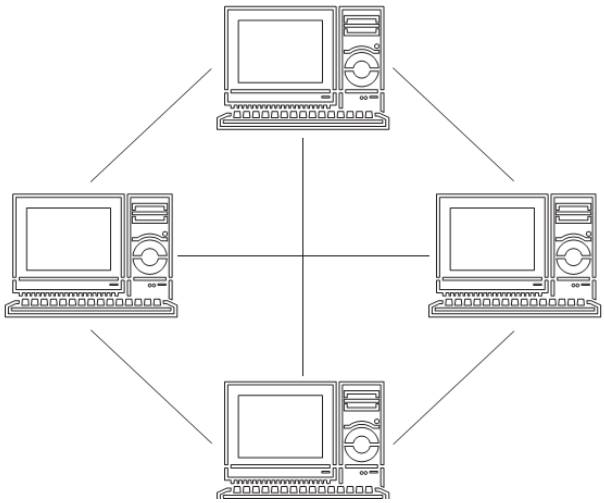

Figure 3-7 – P2P configuration

In this case, each computer can join a communication as a client participant or as a contributing server, depending on the needs at the moment. The fact that each computer can act both as client or server makes the network more difficult to manage and less secure. However, this topology requires less cost than others; the only maintenance necessary is on the computer itself.

P2P is often confused with the sharing of information or files among users, but it is in reality a collaborative network.

In this type of topology it is difficult to manage the growth of the network, since any computer can join this network type.

### 3.4.3 Mesh topology

Mesh topology is illustrated in Figure 3-8.

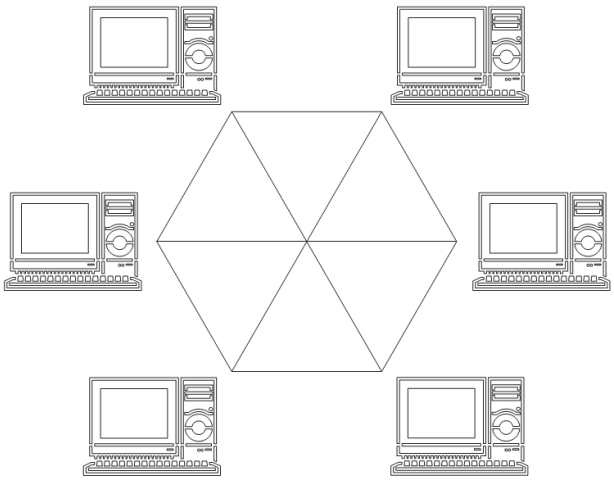

Figure 3-8 - Mesh Topology

It is a topology in which each node acquires not only the data but also help on data to be transmitted. Each node acts as a transmitter to other nodes, collaborating in the propagation of information in the network. In mesh networks information flows, jumping from node to node. This property allows the network to continue to function even if a node is blocked or leave the network. Therefore, in this type of topology information can always find a different route, using different nodes.

This network is more difficult to manage and organize. This type of topology is rarely used in open networks and is more common in intranets.

## 3.5 Representing ‘’things” in the cyber space

Deciding on the best way to represent "things" over the Internet is an important challenge. A number of available options can be adapted to the IoT. Each solution has as its advantages and disadvantages depending on the situation. The need to represent objects, their services, and any other aspects that the IoT has to offer is very important and has to consider the specific characteristics of each application case.

Some relevant approaches include:

- Web Services based modeling;
- Agents-oriented modeling;
- Frame-oriented modeling.

### 3.5.1 Web Services

Web Services (WS) are a solution often used in systems integration and communication between different applications. This approach allows to represent applications or systems as a set of services, offering standardized way to interact with those services from any point on the Internet.

The basic technologies used by WS are XML and SOAP; the data transport is done over HTTP or HTTPS. (Baltopoulos, 2005)

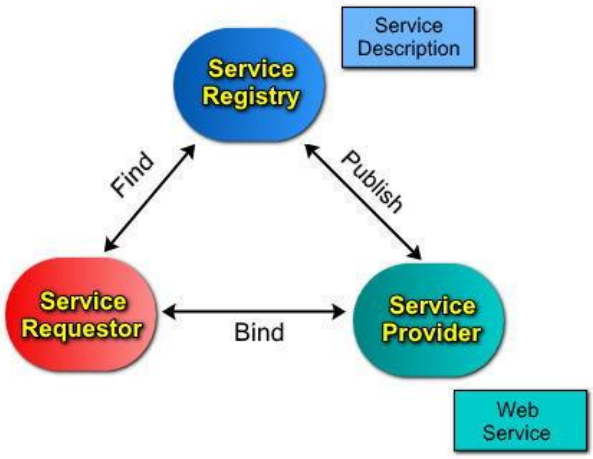


Figure 3-9 - Web Services architecture. (Brittenham, 2010)

As illustrated in Figure 3-9, WS includes three main components: service provider, service registry, and service requester (or client):

- Service registry acts as a mediator between the service request and the service provider;
- Service provider publishes the requested service in the Service registry;
- Service requester that asked service registry for a certain action binds to the service provider.

(Adapted from (Gunzer, 2002)).

When a client requests a service, this requires finding it in the service registry and then binding it to the service provider.

Following this approach, an object could be described in terms of services it provides. In other words, each functionality provided by a "thing" would be available as a service, providing a high level of abstraction in terms of describing objects.

However, security is still a concern in WS, not because of lack of solutions, but rather due to the fact that there is no consensus on which solution to use. Some examples of mechanics to handle security include:

- W3C XML Encryption: used to encrypt and decrypt information;
- W3C XML Signature: used to provide integrity , signature assurance and non-repudiation;
- WS-Security Tokens: tokens provide a mechanism for conveying security with SOAP message, such as username tokens used to provide means to identify the user;
- W3C WS-Addressing: protection against replay attacks;
- Other standards including IETF SSL/TLS, SSL/TLS with client authentication and other authentication methods.

The specific type of security mechanism is decided in each project taking into to account the objectives, and other constrains. Besides the needs to take under consideration in each project individually, there are some considerations that can be taken such as, for instance:

- The message sender specifies the processing intermediaries in the SOAP (Simple Object Access Protocol) message header;
- The message sender can encrypt message headers and sign them using the XML Signature standard;
- Each part of the SOAP message can be given a different signature that corresponds to the intended processing intermediary;
- The message sender can utilize XKMS (XML Key Management Specification) to distribute and register public keys for each processing intermediary;
- Upon receipt of the message, each processing intermediary inspects the signed SOAP headers using an XKMS public key and validates the signature;
- After validation, each processing intermediary may then utilize XML encryption to decrypt the SOAP headers and the corresponding message component.

(Government of Hong Kong, 2008).

Companies like IBM and Microsoft, in collaboration with the W3C and OASIS, are putting a lot of effort in terms of research in the framework of WS, striving to provide standards that facilitate the integration and thus, providing a stronger and safer solution.

"*The SOPA specifications, like the WSDL specifications, were first released as a joint effort by IBM and Microsoft and have also been submitted to the W3C organization to become standard. It defines the structure of SOAP messages, a model for exchanging SOAP messages and how SOAP messages over HTTP can be used for Remote Procedure Calls (RPC)*" (Telektronikk, 2002).

These referred, companies strongly believe that Web Services are a solution able to respond to several subjects and problems when addressing the representation paradigm.
To provide a further insight on how could "things" be described in WS, an example is provided in which a temperature sensor is described along with some capabilities. In this case, the sensor possesses several

attributes and is able to realize several functions, such as: regulate temperature or use an auto adjustment mode scenario.

There are several steps needed to create and deploy a WS. The first step is to create a server project, which means to define the dependencies and the structure of the project.

Next, we have to declare in any adequate programming language the methods (or operations) that the client can access.

```
@WebService()
public class Sensor {

    @WebMethod(operationName = "Sensor")
    public location(@WebParam(name = "location")
    String LimitUp, @WebParam(name = " limitUp ")
    String LimitDown, @WebParam(name = " limitDown ")
    String CurrentValue, @WebParam(name = " current_Value ")
    int GetTemperature, @WebParam(name = " get_temp ")
    int DefineRangeTemperature, @WebParam(name = " set_Limits ")
    String AutoAdjustMode, @WebParam(name = " autoAdjust ")

    String Sensor)
}
```

Figure 3-10 - Representation of the sensor in WS

The information about the sensor is stored in a database. In this way, the information about the sensor (location, temperature limits, current temperature, get temperature, set limits and auto adjustment mode) can be accessed when needed. The code provided in Figure 3-10, is the actual representation of the sensor. This example code, describes the sensor and its characteristics. From this point on, the sensor can be called a “thing”.

```
@WebMethod(operationName = "returnSensor")
    public String returnSensor () {
    StringBuilder sb = new StringBuilder();
    String sid;
    String sLocation;
    String sLimitUp;
    String sLimitDown;
    String sCurrent_Value;
    String sget_temp;
    String sset_Limits;
    String sautoAdjus;
```

Figure 3-11 - Information kept about the sensor

At this point (Figure 3-11), all the information of the sensor would be available. The user could access individually to each sensor depending on a location or identification, which would be unique for each sensor.

```
/**
     * Web service operation
     */
    @WebMethod(operationName = "AutoAdjust")
    public int AutoAdjust(@WebParam(name = "IdSensor")
    int IdSensor) {

    try{
        Class.forName("org.sqlite.JDBC");
        Connection conn =
DriverManager.getConnection("jdbc:sqlite:sensor.db");
        Statement stat = conn.createStatement();
        ResultSet query = stat.executeQuery("select * from sensors where pid
= "+IdSensor+";");
        query.next();

        int i =Integer.parseInt(query.getString(1));

        stat.executeUpdate("update from sensors where pid = "+Idsensor+";");
        conn.close();
        return 1;

        }
```

Figure 3-12 - Auto adjustment operation in WS

The code in Figure 3-12 allows the user, with a simple button click, to change the status of the sensor auto adjust mode, from active to inactive or the inverse action. While on auto adjustment mode, the sensor would take regular readings of the temperature within a certain time interval, and automatically adjust temperature.

The following step is to publish our WS, which means, making it available to be used. Thus the last step is to create a client application, so the user can access the WS provided.

```
@WebService()
public class User {

    /**
     * Web service operation
     */
    @WebMethod(operationName = "Sensor")
    public int location(@WebParam(name = "Location")
    String LimitUp, @WebParam(name = "LimitUp")
    String LimitDown, @WebParam(name = "LimitDown")
    String Current_Value, @WebParam(name = "Current_Value ")
    String get_temp, @WebParam(name = " get_temp ")
    String set_Limits, @WebParam(name = " set_Limits ")
    String autoAdjus, @WebParam(name = " autoAdjus")
```

Figure 3-13 - Interaction between the User and the WS

The code in Figure 3-13 would provide the user a way to interact with the sensor, namely to change temperature limits, get information on the temperature and activate/deactivate the automatic adjustment mode.

Adapted from (Ursini, 2011).

### 3.5.2 Agents

Programming through agents has become very attractive in some domains due to their specific characteristics, which are particularly interesting when developing autonomous systems.

*"An agent is an entity that:*

- *Acts on behalf of others in an autonomous fashion*
- *Performs its actions in some level of proactivity and reactivity*
- *Exhibits some levels of the key attributes of learning, co-operation and mobility"*

(Green, et al., 2007).

The main characteristics of agents include:

- Autonomy: each agent takes its own decisions based on its goals;
- Heterogeneity: agents don't know what other agents goals are;
- Sociability: agents can interact between them in order to achieve their goals;
- Reactivity: agents react to changes in their environment;
- Persistency: agents modify their reaction to achieve a goal.

A programmed environment based on agents can easily be compared with a real society, where agents act according to the needs for which they were programmed and organize themselves to achieve their own goals. Agents have the ability to react to events within certain parameters and act in accordance with an implementation plan, which may be regarded as guidelines to comply with the event. Thus, the agent is an entity created by a programmer who is able to perform tasks independently, based on its internal programming and interactions with the surrounding environment.
Relevant features of intelligent agents can be observed in Figure 3-14:

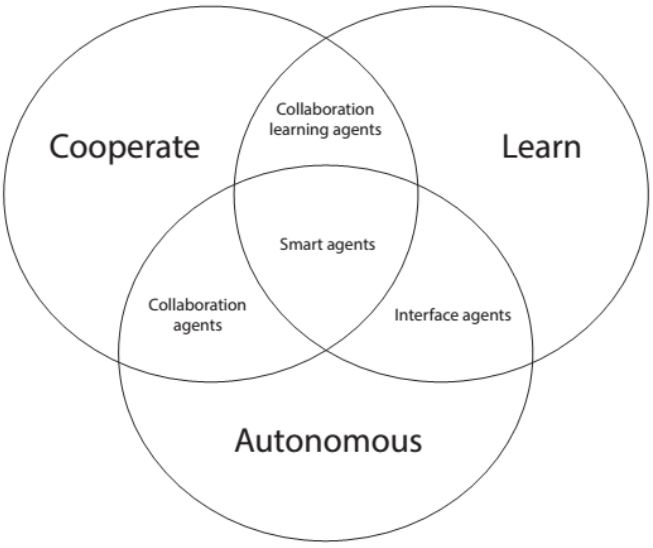


Figure 3-14 - Intelligent agents characteristics

Agents can "blend" into the environment where they live, through interaction, collaboration and learning. For the case of having an environment with more than one agent, that environment can be described as a multi-agent system. A multi-agent system is an environment in which there are several different agents.

In order to interact with each other, agents use a specific language – Agent Communication Language.

In the case of multi-agent systems there are some tools that can be used for their development.
One popular example is: Jade - Java Agent DEvelopment Framework, a system used to create multiple agents and agent containers. Each Jade platform is required to have two specific components:

- AMS – Agent Management System which can be viewed like the authority in the platform and can destroy or create other agents, shutdown containers or the platform;
- DF – Directory Facilitator that acts as a directory of services those agents can use.

(Information adapted from (Dalpiaz, 2011)).

Using this approach, objects, and especially smart objects, could be represented in the cyberspace by agents that model the functionality and behavior of those objects.

Although agent-based approaches are quite popular when developing advanced local automation systems, the approach is not so easy when we deal with distributed systems. This is due to the fact that most existing platforms are not robust enough to operate over Internet. Nevertheless, at prototype level, and considering the characteristics of intelligent agents mentioned above, they offer an interesting conceptual modelling environment.

As in the previous section, it is useful to describe a theoretical case in order to approach the AOP (Agent Oriented Programming), providing the reader insight on how could a “thing” be modeled as an Agent. In this way, same as in the previous section, a temperature sensor will be described in AOP.

At this point, and in order to understand the underpinned mechanisms, it is useful to provide some insights on AOP concepts.

To program an Agent a platform is required, and by platform it is meant:

- A place where Agents live;
- Agent communication services;
- Agent directory services;
- Agent management:
    - Creation and termination;
    - Security;

Since in this case, the actual matter is the IoT (several “things” interacting), it is useful to exemplify the sensor within a multiple-agent platform, which means, an environment capable of dealing with multiple agents. Therefore the following text will explain the JADE platform.

JADE is suitable to develop multi-Agents systems and applications. As shown in Figure 3-15, this platform is composed of several containers. A container is an instance of JADE, and can contain several Agents. The platform has a special container (a main container). This container must always be active and all secondary containers must register with it, creating in this way a hierarchy.

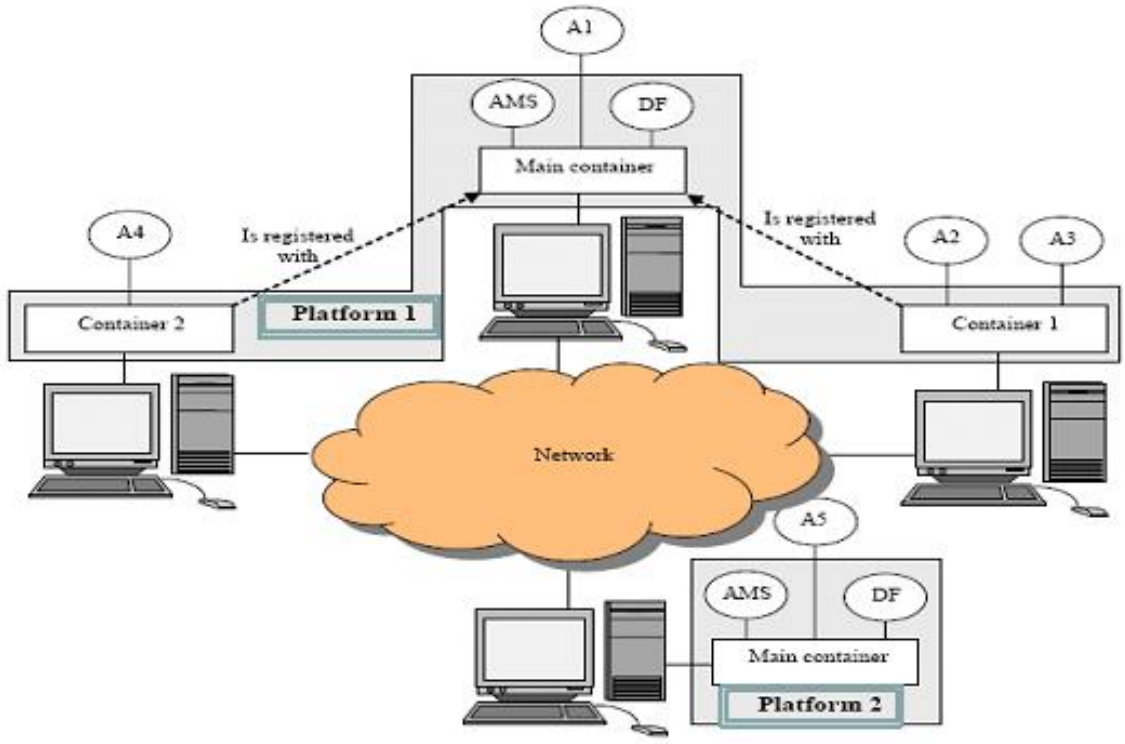


Figure 3-15 –Multiple Agent environment example (Yu, 2012).

In Main container:

- AMS (Agent Management System) – This system provide a naming service and represents the highest authority in the platform;

- DF (Directory Facilitator) – This service provides a mapping mechanism in which an Agent can find other Agents, thus providing the services it requires in order to achieve its goal.

Adapted from (Yu, 2012).

Agents communicate through the Agent Communication Channel (ACC). ACC provides the means to exchange messages between Agents, and platforms.

Now, we can explain how Agents works as an entity. To program an Agent it is needed:

- setup() – Which initializes and registers the Agent in the AMS system;
- addBehaviour() – This function adds a behavior;
- action() – This function defines the actions;
- Send/Receive messages.

Adapted from (Yu, 2012).

In our case, we have a temperature sensor able to perform automatic adjustments. The sensor will register in AMS, handle the messages, test the action and then take a decision.

```
public class AgentSensor extends Agent {
    private AID responderAID;

    public void RegisterInDF() {
        DFAgentDescription dfd = new DFAgentDescription();
        DF.setName(getAID());
        ServiceDescription sd = new ServiceDescription();
        sd.setType("AgentSensor");
        sd.setName(getLocalName());
        dfd.addServices(sd);
        try {
            DFService.register(this, dfd);
        } catch (FIPAException fe) {
            fe.printStackTrace();
        }
    }
```

Figure 3-16 - Sensor as an agent registering in DF

In the code above (Figure 3-16), the sensor, as an agent, is able to monitor the temperature and perform an action, to activate or deactivate the auto-adjustment mode. It is described by a name, services it can provide, location, and a type. The code represents how the sensor would register in the DF.

```
    @Override
    protected void setup() {
        RegisterInDF();
        FindResponder();
        addBehaviour(new InitiatorBehaviour(this,
PrepareInitialMessage(responderAID)));

        MessageTemplate mt =
MessageTemplate.MatchPerformative(ACLMessage.REQUEST);
        addBehaviour(new ResponderBehaviour(this, mt));
    }
```

Figure 3-17 - Initial setup of an agent

At this point (Figure 3-17), the Agent Sensor tries to register itself in the AMS, creating in this way an acknowledgment of its place in the Agents hierarchy.

```
public ACLMessage PrepareInitialMessage(AID targetAgent) {

    Operation operation = new Operation(Automatic Adjustment);
    ACLMessage msg = new ACLMessage(ACLMessage.REQUEST);
    msg.addReceiver(targetAgent);
    msg.setProtocol(InteractionProtocol.FIPA_REQUEST);
    try {
        msg.setContentObject(operation);
    } catch (Exception e) {
        System.out.println(e.getMessage());
    }
    return msg;
}
```

Figure 3-18 - ACL message example

This ACL message (Agent Communication Language) prepares the message to be sent by the Agent to the standard communications used in the platform.

```
private class InitiatorBehavior extends AchieveREInitiator {

    public InitiatorBehaviour(Agent ag, ACLMessage msg) {
        super(ag, msg);
    }
```

Figure 3-19 - Agent initiating a behavior

As said previously, this initiatorBehavior (Figure 3-20) adds an action to the queue (a behavior line up).

```
    @Override
    protected void handleAgree(ACLMessage agreeMsg) {
        System.out.println("AGREE");
    }

    @Override
    protected void handleInform(ACLMessage informMsg) {
        System.out.println("Message Inform");
        try {
            Operation oper = (Operation) informMsg.getContentObject();
        } catch (Exception e) {
            System.out.println(e.getMessage());
        }
    }
```

Figure 3-20 - Handling messages

As already referred above, ACL codes messages to be transmitted such as: messages of concepts, actions and predicates. (ACL messages information adapted from (Université de Montréal, 2004)).

```
    @Override
    protected ACLMessage handleRequest(ACLMessage requestMsg)
    {
        Operation oper;
        System.out.println("Agent " + requestMsg.getSender() + " sent
message" + requestMsg.getContent());
        try {
            oper = (Operation) requestMsg.getContentObject();

            if (oper.GetOperation().get_Temperature ||
                  oper.GetOperation().temperature is within limits) {
               ACLMessage response = requestMsg.createReply();
               response.setPerformative(ACLMessage.AGREE);
               return response;
            }
        }
        ACLMessage response = requestMsg.createReply();
        response.setPerformative(ACLMessage.REFUSE);
        response.setContent("The temperature is already optimal");
        return response;
    }
```

Figure 3-21 - Agent interaction with environment

At this point, the Agent will test the environment, and take an action if required. Which means that if the temperature is below/above the desired value it will automatically adjust.

```
  @Override
  protected void takeDown() {
     try {
        DFService.deregister(this);
     } catch (FIPAException fe) {
        fe.printStackTrace();
     }
  }
```

Figure 3-23 - Elimination of an agent

The code illustrated (Figure 3-23) is how the Agent is terminated, ending in this way, its representation and services.

### 3.5.3 Frame Oriented Programming

Frame Oriented Programming (FOP) is also a viable option for the representation of “things” in the cyberspace. FOP can be described as a mechanism used to encapsulate information about a particular object, including attributes and functionalities. In this way all the information related to a given object is described in an encapsulated form, the “frame”.

“*These features include object identity, complex objects, inheritance, polymorphic types, query methods, encapsulation, and others*” (Kifer, et al., 1995).

Frames can be organized in a hierarchy that defines how the frames are related to each other and to form a taxonomy of classes with inheritance mechanisms along the hierarchy. Figure 3-22 illustrates the hierarchy of a program based in frame.

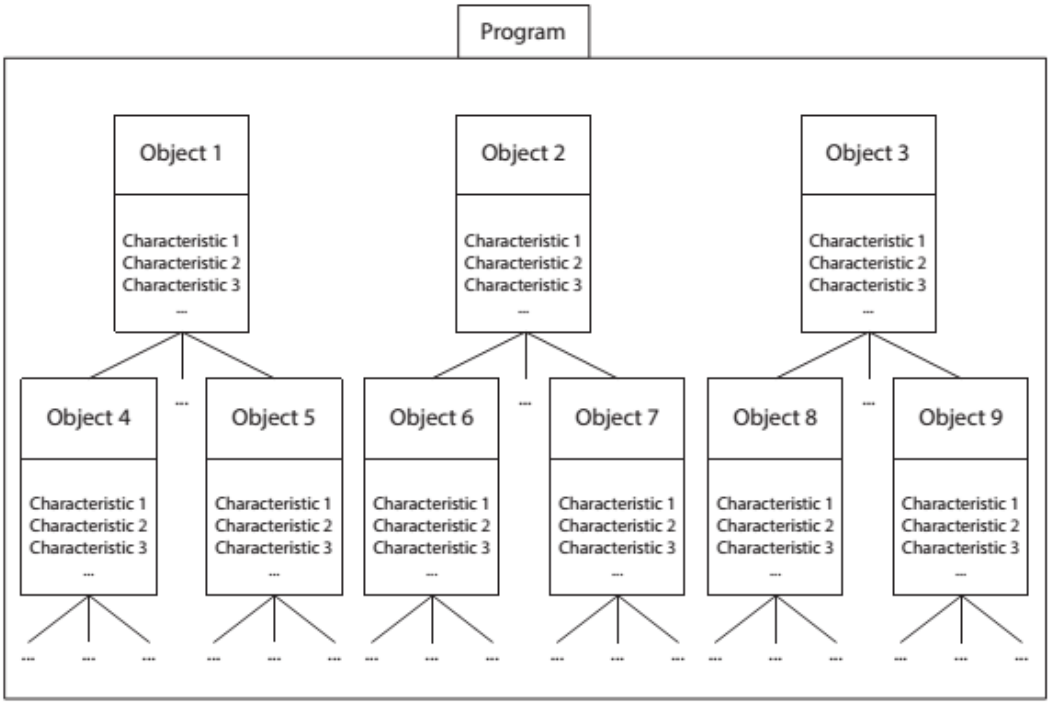


Figure 3-22 - Frames hierarchy

As shown in Figure 3-22, defined objects may relate to another previously included in the hierarchy due to its ability to apply inheritance.

To provide a higher insight on Frame Oriented Programming, we will use the same example as in sub-chapter Web Services and sub-chapter Agents. In this way, the following example code represents a temperature sensor, with some characteristics and functions.

| | Sensor | |
|---|---|---|
| Slots | localization | Living room |
| | limits | 25-30 |
| | time-Interval | 900(s) |
| | current_Value | 26 |
| Methods | get_temp | |
| | set_Limits | |
| | get_Localization | |
| | autoAdjust | |

Figure 3-23 - Sensor modeled in FOP

As illustrated in Figure 3-23, the table represents a single sensor, with its own slots, which contain values, and methods to be used with a certain trigger or order. The table represents a Frame, and it is used to organize the information on the sensor.
To model the presented information, we need to create the Frame, which means, we need to define the sensor:

```
% FRAMES E RELATIONS


?- new_frame(SensorMonitoring).
?- new_frame(Sensor).
?- new_relation(belongs_to,intransitive,none,nil).
?- new_slot(Sensor,belongs_to,SensorMonitoring).
?- new_slot(Sensor,location,'Room1').
?- new_slot(Sensor,limitUp,32).
?- new_slot(Sensor,limitDown,24).
?- new_slot(Sensor,current_Value,0).
?- new_slot(Sensor,get_temp,0).
?- new_slot(Sensor,set_Limits,0).
?- new_slot(Sensor,autoAdjust,'Inactive').
```

Figure 3-24 - Sensor relation and attributes

In the code above (Figure 3-24), written in Golog (a frame engine on top of Prolog), the sensor frame is created, with the necessary attributes and methods. A relation is also created. If we think in this sensor as part of a system, it is needed to specify it within the hierarchy of sensors. In this case we distinguish sensors by location.

```
% DEMONS AND METHODS


?- new_demon(autoAdjust,state,test_active,if_write,before,alter_value).
?- new_demon(autoAdjust,state,test_inactive,if_write,before,alter_value).
?- new_demon(Sensor,set_limits,test_limits,if_write,after,side_effect).
?- new_demon(Sensor,get_limits,test_limits,if_write,after,side_effect).
?- new_demon(Sensor,get_temp,test_temp,if_write,after,side_effect).
```

Figure 3-25 - Sensor demons and methods

The demons declared in Figure 3-25 are used to react to certain situations. In this example case, it is appropriat to provide the program with demons to properly react to changes in the temperature, or if the case, to activate auto-adjustments. These demons test the temperature; if too high or too low, the program will trigger the proper measure, which means to regulate the temperature to the limits set previously by the user.

```
% INTERFACE
showMenuSensor(_,Value,Value1,Value2,Value3):-
  write('================================================================'),nl,
  write('==          Welcome to Sensor Monitoring system             =='),nl,
  write('================================================================'),nl,
  write('= Control:'),nl,
  write('= Set Temperature Limits: '),write(Value),nl,
  write('================================================================'),nl,
  write('= Additional Info:'),nl,
  write('= Read Temperature:'),write(Value1),nl,
  write('= Get Sensor Location:'),write(Value2),nl,
  write('================================================================'),nl,
  write('= 1- AutoAdjustment'),nl,
  write('= 2- Activate'),nl,
  write('= 3- Deactivate'),nl,
  write('= s- Exit'),nl,
  write('================================================================'),nl,
  nl.

execute(C,X):-
  C=1,nl,menu1(X),pc1(X);
  C=2,nl,menu2,pc1(X);
  C=3,nl,menu3,pc1(X);
  C=s,nl,write('Program Closed'),abort;

% Function to initiate the sensor system

pc1(X):-X=Sensor,
    get_value(Sensor,location,Value),
    get_value(Sensor,current_Value,Value1),
    get_value(Sensor,location,Value2),
    showMenuSensor(X,Value,Value1,Value2,Value3),read(C),execute(C,X).



  menu1(X):- write('GetTemp:'),nl,read(temp),
       call_method_1(Sensor,current_Value,temp).

  menu2:- call_method_2(Sensor,AutoAdjust,activate).

  menu3:- call_method_3(Sensor,AutoAdjust,deactivate).

  menu4:- call_method_4(Sensor,limitUp,temp).

  menu6:- call_method_6(Sensor,limitDown,temp).
```

Figure 3-26 - Possible interface

The menu presented in Figure 3-26, represents a possible interaction by the user with the system.

The methods described below in Figure 3-27 - Methods definition, are used to support the various function, such as: read temperature values, increase temperature, decrease, set temperature limits and activate or deactivate the auto adjustment mode.

```
% METHOD DEFENITION
  GetTemp(X,temp):- X=Sensor,
                    new_value(Sensor,temp).

  increaseTemp(X,temp):- X=Sensor,
                    get_value(operacao,estado,Y),
                    temp=<23,
                    new_value(Sensor,limitDown,temp).

  decreaseTemp(X,temp):- X=Sensor,
                    get_value(Sensor,limitUp,temp),
                    temp=>34,
                    new_value(Sensor,limitUp,temp),

  SetLimits(F,temp,X):- X=Sensor,
                    new_value(Sensor,limitUp,temp),
                    new_value(Sensor,limitDown,temp).

  AutoAdjustActivate(X):- new_value(Sensor,autoAdjust,'Active').

  AutoAdjustDesactivate(X):- new_value(Sensor,autoAdjust,'Inactive').
```

Figure 3-27 - Methods definition

The demons programmed below (Figure 3-28) are functions triggered upon certain situations. These demons are designed to test values and take the appropriated measures, which in our case depend on temperature readings.

```
%DEMONS
   test_active(X,Y,T,_):-
              T='Active',
              new_value(Sensor,autoAdjust,T).

          test_inactive(X,Y,T,_):-
              T='Inactive',
              new_value(Sensor,autoAdjust,T).

   test_limitUp(X,Y,T,Z):- get_value(SensorMonotoring,tipo,X),
              X=Sensor,
              get_value(Sensor,limitUp,temp),
              T>limitUp,
              write('Temperature is above the limit:').

   test_limitDown(X,Y,V,Z):- get_value(SensorMonotoring,tipo,X),
              X=Sensor,
              get_value(Sensor,limitUp,temp),
              T<limitUp,
              write('Temperature is below the limit:').
```

Figure 3-28 - Demons definition

All the presented code has the sole purpose of demonstrating how a sensor could be modeled in the cyber-space according to the IoT vision. If a sensor was modeled in this way, and made available to be used in the Internet, we could, at that moment assert that the sensor had become a “thing”.

The information used to create this case was adapted from the course notes from MDE (Data Modeling in Engineering) by (Camarinha-Matos, 2009).

### 3.5.4 Conclusions on representing “things” in the cyberspace

In the previous sections, we proposed a scenario in which a temperature sensor was represented, based on three solutions such as: WS, Agents and Frames. This section aims to provide the reader with the advantages / disadvantages of each representation encountered in the exemplified implementation.

Even as a simple example, it is possible to draw several conclusions about each type of representation.
In a first approximation, all three are viable solutions for the representation of the sensor. WS approach is based on requests from the user, which means that the system only uses the appropriate resources, however, in AOP and FOP, all features are available permanently in the system, thus making the system heavier.

In turn, the FOP option turns out to be much more understandable and easy to implement. The “thing” is easier to describe and can be considered a much more organized and understandable programming model.

AOP, in this case, has a higher degree of autonomy, however, the system may become slower.

Another matter in terms of programming with FOP, is that it was possible to implement more functions with less code than in WS and Agents. May thus, seem that the object is much better described in FOP, however, in AOP and WS it is only necessary to describe the functions that are intended to implement.

For this particular case, which was a simple example, all three solutions can be used to implement the sensor. However, in an environment with a higher amount of mostly active sensors, the type of representation would have to be decided with basis on a more careful analysis.

Let us consider for example, a system capable of controlling various sensors, with different applications, and different decisions to be made.
In this case, each sensor could easily be described in frames, with the appropriate demons and functions, providing a flexible and easy way to represent all functionalities. If WS were chosen, besides becoming slower due to all the capabilities, new functionalities could easily be added. If Agents were chosen the system would have a wider independence from the user, being able to coordinate all system by itself, requiring minimal attention from the user, however, hierarchy could become a problem.

Table 3-7 - Comparison between WS vs FOP vs AOP implementation

| | Learning | Understanding | Scalability | Integration | Complexity | Autonomy | Flexibility |
|---|---|---|---|---|---|---|---|
| AOP | | | | • | | • | • |
| WS | • | • | • | • | • | • | • |
| FOP | • | • | | | • | | |

In Table 3-7, the several characteristics found regarding the three types of representation described above are illustrated.

As already stated, each case has to be thoroughly analyzed, measuring the pros and cons posed by each type of programming. Please note that in discussion only the ‘’representation power” of each mechanism

is being considered. In a real application we would also need to consider the availability of robust solutions to operate on Internet, in which case, WS would probably be the winner.

## 3.6 Integration

*"Innovative architecture and platforms are needed to support highly complex and interconnected cyber-physical systems. A key consideration is how to enable development and application of comprehensive architectural frameworks that include both the physical and cyber elements of CPS"* (Energetics Incorporated, 2013)

Integration is a subject that is becoming more and more important as systems become more complex and involve the interoperation of different technologies. Ultimately, integration in the context of IoT is supposed to hide all technologies, protocols, complexity and architecture from the point of view of the user, allowing the ability to plug-n-play anytime and anywhere independently of the software or hardware used. But this objective faces tough challenges. If a device needs to be connected with certain software that is not related to another, problems can arise in terms of integration. Middleware can help solving some compatibility problems. However middleware solutions are not totally standardized.
This chapter provides a brief overview of the integration problems and approaches in IoT.

In a report released by Energetics Incorporated (Energetics Incorporated, 2013), the authors have described the main characteristics of the integration scheme. The information presented in the following bullets proposes some innovative ideas, marked as indispensable to a successful IoT integration.

Main transformative ideas proposed by Energetics Incorporated in (Energetics Incorporated, 2013):

- Architecture and Platforms
    - Create an application-specific open-source platform that the CPS community can collaboratively populate and strengthen;
    - Utilize a platform for interoperability, allowing for automatic negotiation of function and capabilities;
    - Develop a layered architecture that is not subverted by issues of time, (e.g., a three layered architecture encompassing communications, utility, and value added);
    - Utilize abstractions that encapsulate multiple aspects (e.g., functional, behavioral, timing, quality of service, quality of control) and multiple layers (e.g., application, network, and physical layers);
    - Utilize plug and play components that produce predictable results, even for unanticipated interactions
    - Employ automatic adapting and reconfiguring architecture in response to failed/aging/drifting components;
    - Deploy architecture containing multi-level "safety nets" and security defenses.
- Intelligence and Cognition
    - Incorporate understanding of human intent into input (in real-time);
    - Develop components with extreme intelligence, allowing components to act as individuals in a human organizations (e.g., reporting status or skills to a component "manager");
    - Employ intelligent system designs that are able to decide in real-time when to violate certain constraints in order to protect other constraints.

- Unique Functionalities and Applications
    - Enable multi-dimensional applications to comprehensively interact with our four dimensional world, unleashing dramatic innovation;
    - Share middleware across CPS domains;
    - Deploy embedded technologies that can evolve with integration.

These ideas provide the main ground rules to the IoT infrastructure. This infrastructure needs to be: flexible, adaptive, self-sustainable, and modular.

Instead of starting research from scratch, using the current technology as a starting point, it is possible to make adjustments in order to respond to the new needs. The idea of using current technology as a starting point is also supported in *Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems* (Vermesan, et al., 2013).
This document refers the IoT-A (IoT Architecture) as a project that aims to promote an evolutionary approach than starting from the scratch (more information about this project can be viewed in http://www.iot-a.eu/public).

### 3.6.1 IoT-A Reference Model

As referred above, the IoT-A is an architecture aiming to provide full scale integration in the IoT domain.
It is important to refer this model in a higher detail, due to the fact that it is a model fully adapted to the IoT. Besides being still an ongoing research, it can be considered an achievement in the integration models.

This model is based on modules, each one with its specific function, as illustrated in Figure 3-29.

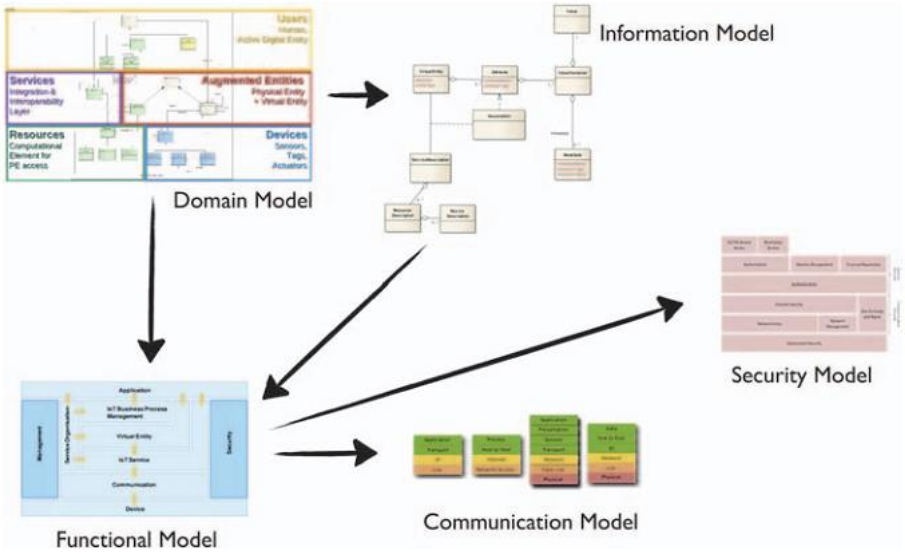


Figure 3-29 - IoT-A Reference Model modules (Vermesan, et al., 2013).

According to Figure 3-29:

- Domain Model: creates the common grounds needed to establish a context. Depending on the context, the underlying levels are enabled for each specific object and the appropriate mechanisms provided. Thus, offering a standardized way to interact with different “things”.

- Information Model: Defines a structure of attributes and information specific to each type of object.

- Functional Model: this module is probably the most important module, since it contains all the necessary functionality groups.

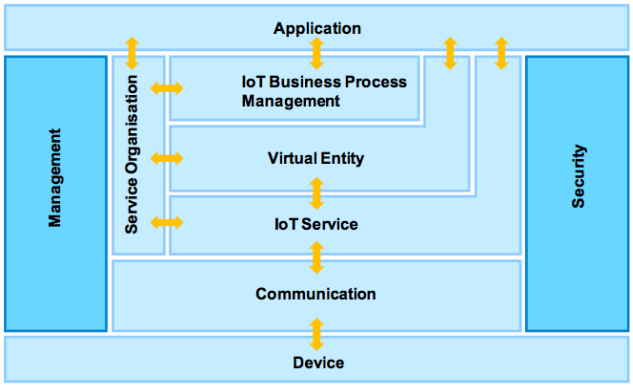


Figure 3-30 - IoT-A Functional Model

- Communication Model: responsible to provide all the communications.

- Security Model: this component provides the appropriated security. Some features may be general, and some specific to each “thing”.

This approach is based on the middleware we have in our days.

The efforts put in this architecture, lead us to believe that this model can be a strong candidate to the IoT architecture.

### 3.6.2 Middleware

IoT demands a relatively complex architecture to cope with a diversity of components and services. The common goal of all the middleware development initiatives is to provide a framework which can enable an adaptation layer to support a plug-n-play mode. The aim is that IoT devices are able to communicate with other devices anywhere in the world. The middleware in IoT provides the bond between heterogeneous devices such as sensors, aggregators, actuators, and a diverse range of applications, preserving security and privacy. Providing means to interaction is an easy and very simplistic way to describe the Middleware function.

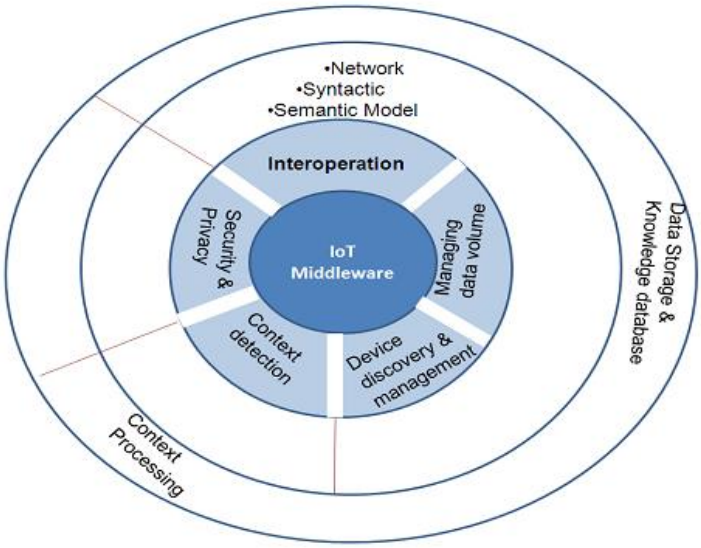


Figure 3-31 - Middleware abstraction (Bandyopadhyay, et al.,2011)

As illustrated in Figure 3-31, the middleware component establishes a bond among the several layers needed to the structure of the Internet. It can be viewed, as a platform that provides a certain level of abstraction capable of integrating all devices.
Several issues lead to the need of this middleware including:

- Interoperation;
- Context detection;
- Device discovery and management;
- Security and management;
- Managing large data volumes.

Context detection characterizes the situation of an entity in its surrounding environment.
Device discovery and management enables the ability of devices to discover other devices thus allowing interaction between them.
Security and privacy is the element responsible for managing security and privacy in the system, providing the necessary tools to keep the data flows secure.
Managing large data volumes is an important module in middleware structure. Due to the fast growing of the number of devices on the network, it is imperative to create methods to index, identify and collect data. The main problem with this module is the querying, indexing and modeling, due to the large number of devices and the terabytes of information potentially flowing in the network.

Interoperation issues can be divided into three categories:

I. Network, which defines the protocols used to establish communication, data type and transportation;
II. Syntactic structure, which defines the type of format and structure used to exchange information among “things”;
III. Semantics, which defines the means and rules for understanding the information.

In the following illustration (Figure 3-32) we can observe the role of the middleware element in the Internet of Things context.

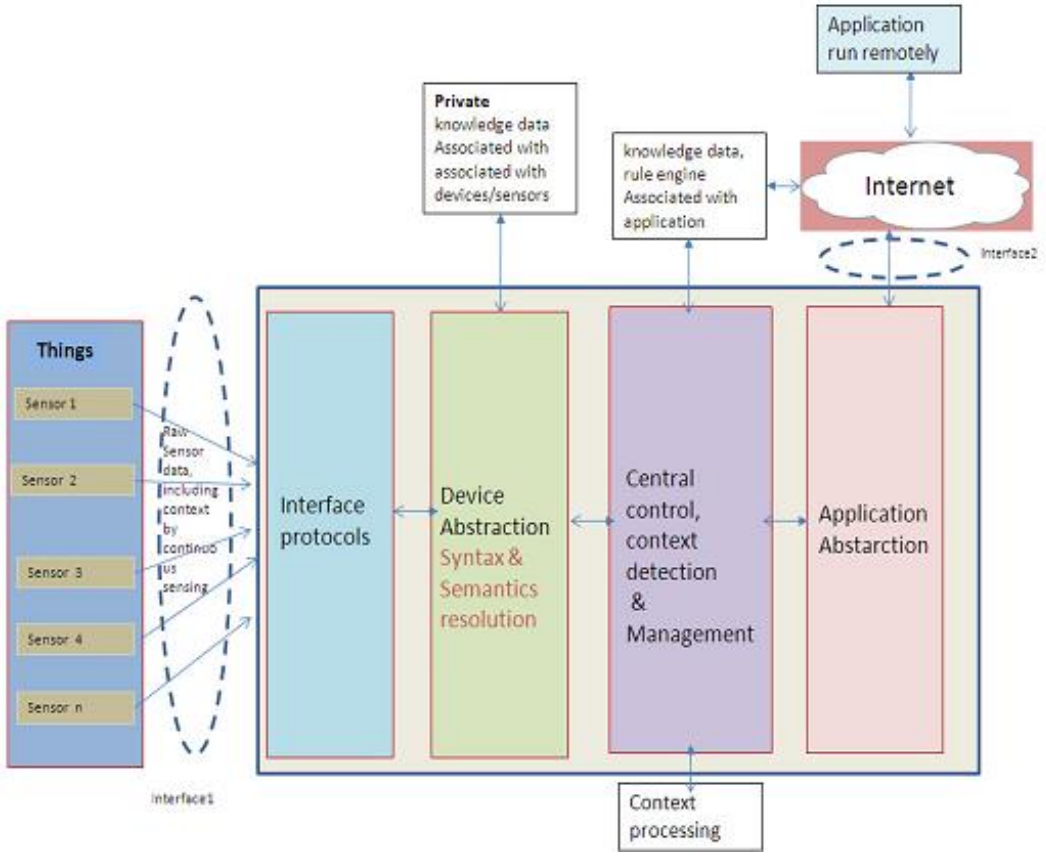


Figure 3-32 - Middleware layers (Role of Middleware For Internet of Things: A Study, 2011)

As illustrated in Figure 3-32, the middleware component provides support and all necessary modules for the correct functioning of the Internet of Things, including interface tools, device abstraction, control, context detection and an application abstraction layer. “Things” communicate with the middleware infrastructure.
Nowadays, we can already find some middleware solutions. However they are addressed to certain systems with specific proprieties. Like with other technologies, the biggest issue for the IoT realization is standardization. To fully achieve IoT all devices, software and end users must be able to connect between them without losing information, incompatibility problems, and assuring security and privacy.

In Table 3-8 relevant features from different middleware solutions are shown. The selection of a specific solution naturally has to take into account the desired characteristics.

Table 3-8 - Middleware features (Role of Middleware For Internet of Things: A Study, 2011)

| Designation | Device Management | Interoperation | Portability | Security and privacy |
|---|---|---|---|---|
| HYDRA | • | • | • | • |
| ISMB | • | | • | |
| ASPIRE | • | | • | |
| UBIWARE | • | | • | |
| UBISOAP | • | • | • | |
| UBIROAD | • | • | • | • |
| GSN | • | | • | • |
| SMEPP | • | | • | |
| SOCRATES | • | • | • | • |
| SIRENA | • | • | • | • |
| WHEREX | • | • | • | |

These different middleware choices need to be fully adapted in order to provide the integration that IoT requires, or else, there will always be integration problems, since it will be necessary more than one structure.

It is still premature to try to fully describe the functional needs of the integration type required. It is still uncertain the specific requirements, how will objects behave and fit within the architecture, how will network sensors interact with the end-points, how will addresses be treated, etc. All these questions need to be clarified and explained within the IoT context, only in this way the actual needs of the system will be known.

### 3.6.3 Web services as an integration solution

Besides being a way to represent “things” in the cyber world, WS can also provide a mean to integrate “things”. Web Services can act as a way to bind the physical world with the cyber world, thus, making the necessary bridge to relate the both worlds.

WS can be a very efficient and fast solution to solve compatibility issues and thus help integration. Although much work remains to be done on the WS area, they already provide a very acceptable level of abstraction such as in: routing support, resources and switching abstract API. WS can provide a high level of abstraction to devices. Which means that Service Request only has to ask a certain service, abstracting in that way the knowledge on the necessary conditions to execute the task associated.

Two types of web services seem to be suited for integration:

#### *3.6.3.1* WS-* (SOAP-based)

In this case services are declared using WSDL (Web Service Description Language) and correspond to the most common form of WS used nowadays. SOAP (Simple Object Access Protocol) is like an envelope that carries message contents over diverse transport protocols. It is XML-based and provides a standardized way to access services.
Being the most used approach, it offers some WS-* standards, such as for addressing, discovery, and security.

#### *3.6.3.2* RestFul

This approach is based on RESTful resources identified by URLs and is based on the Representational State Transfer (REST). A REST WS is inspired on the concept of “resource”, which is anything that can be identified by an URL. REST services require less infrastructure than SOAP.

Even sharing the same goal, these two methods should be applied in different situations, while the WS-* is suggested for enterprise applications, the restful can be used for applications that do not require much security such as ad hoc networks or sharing files.

#### *3.6.3.3* WS-* VS RestFUL

Because of its applicability, it is useful to compare WS-* and RESTful. There is a very interesting study done on this subject, showing the differences, pros and cons, trying to compare these two types of WS (Guinard, et al., 2012). This study tested the implementation of WS-* and RESTful by organizing two separate groups of students who were instructed for the first time in the WS-* and RESTful. Students were assessed during the whole time via surveys to collect results and opinions. Each group received some tasks, such as programming services in REST and WS-*. This study provided important conclusions on these architectures, which can help solving the integration problem. The main findings of this study are illustrated in Figure 3-33.

| **REST** ($N = 69$) | # |
|---|---|
| Easy to understand, learn, and implement | 36 |
| Lightweight | 27 |
| Easy to use for clients | 25 |
| More scalable | 21 |
| No libraries required | 17 |
| Accessible in browser and bookmarkable | 14 |
| Reuses HTTP functionality (e.g., caching) | 10 |
| **WS-*** ($N = 69$) | # |
| WSDL allows to publish a WS-* interface | 31 |
| Allows for more complex operations | 24 |
| Offers better security | 19 |
| Provides higher level of abstraction | 11 |
| Has more features | 10 |

Figure 3-33 - Ws-* vs RESTful services (Guinard, et al., 2012)

As shown in Figure 3-33, students consider that RESTful is easier to learn and implement, more lightweight, simpler in terms of interface, and very affordable. While the WS-* services allow more complex operations, provide more security and a higher level of abstraction.

Regarding the types of applications more adequate for each case, Figure 3-34 summarizes the collected opinions.

| **REST** (N=37) | # |
|---|---|
| For simple applications, with atomic functionality | 23 |
| For Web applications and Mashups | 14 |
| If security is not a core requirement | 8 |
| For user-centered applications | 6 |
| For heterogeneous environments | 6 |
| **WS-*** (N=37) | # |
| For secure applications | 20 |
| When contracts on message formats are needed | 16 |

Figure 3-34 – REST vs WS-* application characteristics (Guinard, et al., 2012)

### 3.6.4 Agents and frames

As in WS, FOP and AOP can also provide a way to establish a bridge between the cyber world and the physical world. Even having been described in the previous section as a way to represent “things”, these programming paradigms provide a high level of abstraction, allowing the integration of “things”.

The differentiation between AOP and FOP from WS was intentional, since WS are already used to provide integration at a certain level.

By using AOP and FOP, it is possible to represent physical objects in the cyber world, providing inputs and expecting outputs in a bidirectional way (cyber to physical and physical to cyber).

Representing “things” using these programming languages can help surpass some integration issues, since today hardware is already able to support such programming representations. However representing “things” means only a part of the solution to the problem. The IoT assumes a high level of intelligence associated with “things”. Even knowing that FOP and AOP can provide a high degree of autonomy, it has to be in a much larger scale. Having provided information on the previous sub-chapters about AOP and FOP, it was important to refer these technologies as an integration method, keeping in mind that these technologies could only solve part of the problem, since it will always be required supporting hardware, able to respond all the requirements and needs.

Issues that could become a problem:

Agents:

Agents can become a solid solution in IoT, but in large environments and with a great deal of autonomy to interact, the organization of these systems can become a big problem, and instead of solving the problems could bring even more. Since agents are autonomous entities, we can imagine problems in terms of hierarchy, conflicts between agents with the same objectives, etc. Organizing agents could be thought as creating a virtual society from scratch similar to any physical society. However, the main practical problem, at the current stage, is that existing platforms are not robust enough to operate over the Internet.

Frames:

When considering FOP has a solution, we find ourselves with the problem of abstraction. Each object needs to be characterized in detail in each appropriated frame. Thus, it would be necessary to characterize all things, making the architecture very heavy in terms of information. Another issue is the availability or not of suitable FOP platforms to work on Internet.

### 3.6.5 Concluding remarks

As implicit in IoT, the hardware always requires a software complement. Thus, WS, AOP and FOP can be taken in consideration to respond to this need in terms of abstraction.
The current state of the art in middleware, already includes various architectures, however all solutions fail in some aspects of integration. None of them fully covers all the necessary aspects such as security, integration, abstraction and portability. Therefore, research in this area needs to continue in order to develop a middleware layer able to meet all the conditions to support IoT.
The main focus of research goes to the architectural solution. In the previous sub-chapters, AOP, WS and FOP were highlighted, because these programming paradigms can help in terms of abstraction.

Another issue in terms of middleware for IoT is if it will have a central or distributed structure. In case of a distributed one, the various middleware subsystems need to be 100% compatible between them. Having a central middleware able to handle all protocols may seem very unlikely. However, it could more easily solve problems of interoperability, integration, etc. The problem with having a single structure is that it would have to be a highly complex one, with high costs in terms of maintenance.
The trend in the use of web services as the backbone for the IoT is still growing due to its ready to use "feature".

The past experience in integration, suggests that the correct way to the integrating issue in IoT should be in a modular way. Thus, providing a flexible way to attend the specific needs of each “thing”. Having the context and identification of each “thing” well set, all secondary modules (security, features, mobility, etc.) can easily provide the functions required, abstracting from all the unnecessary details.

# 4 SECURITY

*"In the Internet of Things vision, every physical object has a virtual component that can produce and consume services. Such extreme interconnection will bring unprecedented convenience and economy, but it will also require novel approaches to ensure its safe and ethical use"* (Roman, et al., 2011).

Security is a field with a constant growth. What we consider safe today may not be tomorrow. This growth requires a constant need for research in order to be prepared for situations before they can cause real damage. The fact that Internet has become the largest public data network with a volume of information constantly growing every day, gives rise to new risks and dangers on a constant basis. Attacks on sensitive data such as financial data or personal information have become very common and, hence, the need for greater protection, safeguarding the interests of each being stolen, damaged, viewed or copied.

In the context of IoT it is impossible to avoid the security subject, since the IoT will be able to support billions of devices and deal with huge amounts of information. This fact makes essential to ensure a high degree of security to protect data and communication channels. However, the existing protection mechanisms were developed to serve the existing infrastructures and not to work on IoT. There is, therefore, a need for further research in this area.

Even being considered outdated, existing security measures can be used as the starting point for creating new bases of security for the Internet of Things. Therefore researchers have a starting point to develop based on the specific security threats that exist.

During this chapter an overview in terms of safety issues is provided. There is also an overview of the types of attacks and vulnerabilities that can be exploited, both in software and in hardware. Finally, some solutions that can be used as a basis for further research as well as other approaches already fully adapted to IoT are presented and described.

## 4.1 Turning point of security awareness

The biggest turning point on Internet security happened after a known hacker named Kevin Mitnick have committed the greatest crime of computer science in the U.S. Mitnick stole about eighty million dollars in intellectual property and source code from several companies (Adapted from (Meriwether, 1995)). This event made private and corporate parties to realize, that their information was far more valuable and far more worthwhile to protect then to be left without safety. Nowadays, almost all critical information available on the Internet is in some way protected. The stolen information can be used in many different ways. The average user may be a victim of identity theft, theft of money, passwords and credit card numbers stolen. Companies can be victims of unauthorized access to secret information, such as contracts, databases of customers and processes classified as secret.

One of the most popular solutions to protect data are antivirus. Antivirus possess databases that contain information on how to combat each type of viruses and attacks. When as a new virus emerges in the virtual world it is catalogued and a solution begins to be searched.

Also in IoT, users need to be certain that privacy is a top priority, thus excluding the risk of information leakage while companies need to be safe from information theft. Furthermore, since IoT deals with physical objects, the risk of unauthorized use of those objects brings new concerns.

## 4.2 IoT context

As the Internet evolves into IoT, security also needs to evolve to be able to respond to new needs. The IoT is based on new protocols and communication standards that will bring new security risks, both in hardware and in software. Since IoT involves the interaction between the virtual and physical world, it will lead to new types of security threats. IoT will allow interactions between several critical infrastructures such as: smart buildings, automotive, medical, and military infrastructures, etc. The information value and being high profile targets make all IoT infrastructures extremely sensitive to attacks. This fact implies the need of a high degree of security since an attack at such structures could cripple systems in a dangerous way.

## 4.3 Attack types

To better understand the attacks on the Internet, let us first consider their typology and the types of attackers. The attacks come from various types of “cyber criminals'', each type being characterized by several features, contexts and purposes. The attacks are generally suited to each situation and may occur in almost any type of network protocol and software. The attacks rely heavily on the network topology, and the type of software.

Normally, the attacks involve several steps, in which the attacker can gain full access to our system.

- Step 1: Reconnaissance and enumeration;
  The goal of this first step is to learn about our system vulnerabilities, such as: credentials, software, and settings. This reconnaissance is often made thought fraudulent emails, or fraudulent web pages.

- Step 2: Intrusion and advanced attacks;
  After learning about the system vulnerabilities, the attacker can now begin to exploit those vulnerabilities. These attacks are normally made by denial-of-service (DoS) such as: ping flood attacks, smurf attacks, ping-of-death, among others*.

- Step 3: Malware insertion;

  After having a certain control of the system, the next step is to insert malware, which is software secretly inserted in the system with the goal to remotely control our system or even destroying it.

Adapted from (DELL SonicWALL, 2012).

*Note: The goal of DoS is to deny users access to certain resources. DoS is usually done against users, hosts and networks. These attacks can for instance generate errors to fill logs consuming disk space or deny users to use their computer. Ping-of-death and smurf attacks are types of network attacks, and involve a resource exhaustion or corruption of the system runtime.

In Table 4-1 the differences between each type of striker are briefly represented.

Table 4-1 – Types of actors involved in attacks

| Designation | Purpose |
|---|---|
| Hackers | The name given to cyber criminals that try to steal information with a specific intention other than just destroy or cause chaos. |
| Crackers | Crackers goal is simply the destruction, or causing damage by crashing web pages, destroying data bases and disrupting business and personal information. |
| Unaware staff | Employees that simply ignore safety rules, such as changing passwords, downloading unsecured software and other human errors that compromise and leave innumerous vulnerabilities in the network. |
| Disgruntled staff | Vengeful staff that inflict on purpose damage to the company's network. This group is especially harmful since they know the value of the information and security procedures. |
| Snoops | Unaware staff, snoops are only curious; they try to access data leaving the network unsecure to eventual attacks. |

As shown in Table 4-1, each attacker has a certain purpose or just careless (indirect attacker). Some intend only to cause damage to structures or simply steal data and do nothing with it, others intend to profit from the attacks, whether it be stealing information and then sell it. In other cases the attacks can happen due to lack of precaution on the part of employees. In all cases, attacks can be very harmful for users or companies. Attacks from these groups come in many forms, depending on the objectives (Table 4-2). Each type of attack is very specific.

Table 4-2 – Attack types performed by attackers

| Designation | Purpose |
|---|---|
| Virus | Also known as security treats, viruses are programs specifically designed to replicate and spread in the system when certain events (like pressing a key on keyboard) trigger them. They can have several effects that go from stealing information to simply destroying it. |
| Trojan Horses | A Trojan horse is actually a transportation mode to the virus. It allows virus to disguise as a useful software to the user however, as soon as they download information and run the programs, Trojan horses release virus destroying information, copying it, or doing any other function they were programmed for. |
| Vandalism | Vandals are usually found in downloaded applets, with the simple function to destroy the system. |
| Reconnaissance attacks | This type of attack can be viewed as a gathering of information by the hackers to later on access systems based on collected information, |
| DoS Attacks | It is a type of attack used to block the users, preventing them to use their system. |
| DDoS Attacks | It is a variation of DoS, instead affecting one system they can spread through other systems associated with the infected one. |
| Data Interception | It is the action of eavesdropping on information flowing in the network. |
| Social Engineering | The act of obtaining private information by non-technical methods, like using social networks or misleading staff to obtain information. |
| Spam | Is the action of sending information to a system filling it with useless information, preventing the normal usage of the computer since it consumes most resources. |
| Phising | It is an attempt to acquire information such as usernames, passwords, details on credit cards, addresses, etc. |
| Session hijacking | The hacker is able to impersonate a user, being this way able to access, data such as credit cards, passwords, email accounts, etc. |
| Directory browsing | The hacker is able to retrieve list of directories. |
| Java Decompilation | It is the ability to decompile Java Bytecode, reveling sensitive information. |
| SQL injection | Using typical SQL code, hackers can access tables, i.e. retrieve passwords, usernames, etc. |

## 4.4 Security at the network architecture level

Several authors consider that security has to be implemented from the beginning, i.e. while designing the network. Networks are typically designed based on the OSI model which besides being relatively safe, offers great features such as modularity, flexibility, ease of use and standardization protocols. However, this model can be complemented in order to introduce additional features or modifications. Some of the features of the OSI model include:

- Restrict access – only trusted users are granted access;
- Confidentiality – information flowing in the network is granted to remain confidential;
- Authentication – ensure that the user really is who they say they are;
- Integrity – provides means to ensure that the message is not modified;
- Non- repudiation – ensure that the user can't deny that he accessed the network.

These features allow protecting the information flow, ensuring that only authorized personnel can access data and prevent the destruction or corruption of communication. Network security, often starts during its conception in network design.

### 4.4.1 Layered security

The OSI model is organized into seven layers. Each layer has its own security and allows the flow of information from the seventh layer reaching down to the first layer and back to the seventh layer starting from the first layer. The layers of the OSI model are:

- Layer 1 – Physical layer: defines the physical characteristics of the network;
- Layer 2 – Data link layer: where data packets are encoded and decoded;
- Layer 3 – Network layer: protocols for routing and switching;
- Layer 4 – Transport layer: provides de transport of data as well as error recovery and flow control;
- Layer 5 – Session layer: manages connections;
- Layer 6 – Presentation layer: formats data to proper coding avoiding compatibility problems;
- Layer 7 – Application layer: supports applications at the user end.

Each of these layers includes a specific protection type.

## 4.5 Hardware vulnerabilities

The fact that the IoT is based on the connection with physical objects, makes it important to study their vulnerabilities, in order to improve their safety, and to be able to protect the future structure of the Internet. IoT will certainly be very dependent upon wireless communication systems, which means that there is no physical barriers between the network and the attacker, and thus a higher degree of vulnerability.

### *4.5.1* RFID

Systems based on RFID technology can be considered very insecure. These devices are based on the electromagnetic spectrum for their operation and can be easily corrupted. When thinking on a larger scale

such as in supply chains, a hospital or a military operation, such disturbances could cause enormous damage.

Tags can continue to be read by readers that use the same frequency and therefore allow anyone to view the stored information. In some cases, tags can be associated with additional information, such as credit card numbers or personal information, which hackers can easily access. Thus, several points of RFID security should be revised and improved:

- Secure data access;
- Secure access on the system.

The above implies the need to provide security in the communication channel and thus it is necessary to provide some sort of identification of authorized users. The aim would be to have a secure communication for this technology so that only the authorized users of the RFID tag could use it.

### *4.5.2* 3G

3G and other equivalent communication technologies, have major security flaws. The bandwidth used for this type of communication is shared by all users and so the frequencies used for communication are common knowledge, which makes it very hard to hide and secure. The complexity of the network that supports 3G technologies is also very high, and an increase in the complexity brings an increased risk, not only due to the complexity but also due to the multiple access points of the network that can be exploited.

Even though some of these problems are rather complex, they are key issues that must be solved in order to have a functional and secure IoT. The bullets provided below intend to introduce some of these issues that are considered the most important and that are being addressed in different initiatives:

- Authentication – the wide range of users covered by 3G can impose problems in authentication, however this is a feature that can increase greatly the security and privacy;
- Integrity – Files transfer as well as text messages or chat need to ensure that the data is carried without modification;
- Confidentiality – Keeping information restricted to the sender and the receiver.

### *4.5.3* NFC

As a way of communicating without contact, NFC can be easily corrupted, since it operates at a public frequency. Most of the attacks on NFC could be avoided by protecting the channel, encoding packets or providing mechanisms to verify packaging between the sender and receiver. However, it is very difficult to provide security to this type of communication because their packages cannot be protected when in circulation. NFC is particularly susceptible to:

- Eavesdropping – which is almost impossible to be avoided;
- Data corruption – since the communication is made through an open channel, it is very easy to corrupt, modify and insert data.

Addressing these issues is a priority for researchers, focusing on protecting channels, encryption and hardware protection.

### *4.5.4* WiFi

Being a form of wireless communication it is susceptible to almost all attacks that other forms of wireless communication may suffer. However, due to their state much more evolved than other technologies, WiFi can provide much more security. Several techniques can be applied such as the protection of channels, encryption, signal hiding, etc.
Wireless communication should deserve special attention, since it is the strongest candidate for communication in IoT. Wireless communication contains the following points:

- Transmission of data by radio frequency;
- Access points;
- Client devices;
- User.

Each of these points may be susceptible to attacks. Transmissions are difficult to protect, access points may be unprotected or lack proper protections, and users may not be aware of protection mechanisms to protect their data.

### *4.5.5* QR code

The vulnerabilities affecting the QR Code can only come through hidden code at his creation, i.e., if we create the QR code in a safe place it is virtually impossible to attack through this medium. Attacks however may arise through reading a QR code that was created to destabilize or attack a system. In this case, the QR code is read and redirects to a page of hazardous contents or even force the download of malicious software allowing the hacker to gain control.

## 4.6 Software vulnerabilities

Programming forms can also be quite susceptible to suffer attacks. It is useless to try to assign each programming type certain modes of attacks, since in general they all suffer the same. Code may suffer from:

- Exploiting errors;
- Exploiting validation forms;
- Error handling;
- Code injection.

When the code contains programming errors, the hacker can exploit these mistakes, taking advantage to have access to the system. Often forms available online to gather data may contain errors in programming; these errors allow hackers to access the information. Sometimes, the programmer does not code correctly the way how the program will handle errors, thus leading to the creation of so-called backdoors. Another problem is when the programmer does not protect the program against code injection; whenever it is possible, hackers attempt to enter their own code, which makes the system vulnerable to attacks. So it is not about the type of coding, but the way how the code is being protected from attacks.

## 4.7 Hardware and software solutions

Once the types of attack are identified, appropriate protection methods can be attempted (Table 4-3) to be implemented.

Table 4-3 – Some security solutions

| Designation | Function |
|---|---|
| Protocols | When setting up new networks, usually some protocols are imposed to ensure security, whether verbal protocols with users or integrated security in the network, like passwords, or encryption; in order to prevent unauthorized accesses or security breaches. |
| Hardware choices | Some types of hardware already have embedded security; despite being more expensive it can greatly improve security in systems. |
| Anti-virus | The most common protection against virus. A very effective solution due to the contribution of users that warn about new treats allowing the search for a solution. |
| Firewalls | A firewall can be thought as a package of protocols ready to use in networks; these packages can include virus scan, intruder blockers, identify system vulnerabilities. |
| Detection systems | This type of system allows to detect intruders, using methods like detecting users that try to force entrance or leave ‘’footprints’’. |
| Encryption | Encryption ensures the information is only available to the system that possesses the decryption key. |
| Upgrading software | Older software like OS XP, and Vista provide lesser protection when compared with their successors Windows 7 and 8. |

With the constant evolution of threats it is almost impossible to protect our information in absolute terms; what is safe today will not be tomorrow. This implies a constant supervision and continuous research efforts, addressing the dangers as they arise.

## 4.8 Specific work on IoT security

The previous section is based on existing solutions to the security problems we face these days. Despite the fact that these solutions can be, to some, adapted for IoT, it does not imply that we do not need to consider the specific needs of IoT. There are already some views of safety that are fully adapted to the IoT. Several projects have already developed some solutions but it is still necessary to spend much more time on this research.

### 4.8.1 Some relevant work

Conferences to discuss these problems began to occur, linking researchers with various views on the security problem. Besides developing specific security solutions is also important to establish standards so that all devices can share the same security, making it easier in managing the network and integration. Some of the main issues in securing IoT systems include:

- Facing IoT uncontrolled growth;
- Deployment on simple devices;
- Supporting advanced features;
- Easy to manage systems.

Without the integration of all devices, advanced features and easy management, the IoT makes no sense. Among others, these issues were discussed in the IoT Week 2013 in Finland. From this conference, some interesting aspects are highlighted in Table 4-4.

Table 4-4 - Security proposals Adapted from (IoT Week 2012, 2012)

| Proposal designation | Support | Description | URL |
|---|---|---|---|
| BUTLER's Privacy and Security vision | FP7 | Flexible infrastructure to implement Privacy Regulation and Business Requirements. | http://www.iot-butler.eu/ |
| Privacy by design (PdB) | Private | Deal with privacy issues. | http://privacybydesign.ca/ |
| Capability Based Approaches to Authentication and Authorization | EU funded Project, and several private companies | IoT supporting systems, plug-n-play solutions. | http://www.iot-week.eu/iot-week-2012/programme-1/tuesday-1/presentations/privacy-security-workshop/IERC%20AC5%20IoT-Sec-Priv_IoT-Work_contribution.pdf |
| User-side Utility-Driven Privacy Management in IoT | FP7 | Privacy and authentication | http://www.iot-week.eu/iot-week-2012/programme-1/tuesday-1/presentations/privacy-security-workshop/Papaioannou_OpenIoT_Privacy_June2012.pdf |
| IoT Security & ''privacy'' Standardization activies and results in ITU-T | Private investors, governments, universities | Standards, identification, data protecting | http://www.itu.int/en/Pages/default.aspx |

The works mentioned in Table 4-4, focus mainly on authentication, standards, data protection, solutions for plug-n-play, privacy issues, etc. A few more details on these proposals:

***BUTLER's Privacy and Security vision:***

BUTLER's vision proposes a flexible infrastructure to implement privacy and business security. This vision intends to implement standards in security, providing a basis to standardization and it is based on two principles:

- Minimum disclosure principle:

  The basis of this principle is that the data and the user's identity is kept protected. It is a vision in which the user does not trust in peers communications, and only accepts the disclosure of data if the service provider is able to assure protection and the service provides value to the user.

- Ethic of Knowledge:

  The collected data are only revealed when needed, i.e. only revealed on the basis of a "need to know". The collector will protect information and data should not be used fraudulently.

These two principles are based on the need for privacy and secure access to data.

Open issues of BUTLER'S vision:

- End-to-end security is not yet addressed in IoT;
- Attacks on the physical layer;
- Identity linking
- Anonymity
- Secure deployment for billions of objects;
- User interface.

Adapted from (Castanier, 2012)

These aspects clearly indicate a need for further research.

***Privacy by Design:***

PbD proposes security based on the following seven principles:

- Proactive measures;
- By default, this means that PbD seeks the maximum degree of security in any IT device;
- Embedded, PbD is embedded into the design of the system;
- Positive – Sum, accommodates all legitimate interests and objectives;
- Lifecycle protection;
- Visibility and transparency;
- Respect of privacy.

As we can easily understand through the analysis of the above points, the PbD bets in a proactive system as a solution to data protection and privacy. To open the discussion with these terms, the PbD proposed some standards in matters of protection, prevention, investigation and detection. Adapted from (Fabiano, 2012).

***Capability Based Approaches to Authentication and Authorization:***

This is a project funded by the European Commission, which focuses on securing interaction between all IoT participants: “things”, humans and applications. Key subjects for this project are:

- Interaction patterns:
    - Planned;
    - Long-lived;
    - Short.
- IoT world:
    - Short-lived;
    - Casual;
    - Spontaneous.
- Context:
    - Actions;
    - Requests;
    - Data sources.

The project is intended to protect all interactions between people and “things”. These interactions can go from the life cycle of the “thing”, the context in which they are inserted, and the type of actions they perform. Based on these aspects, the research is focused on certain key points:

- Face IoT scalability;
- Deployed on simple devices;
- Flexible;
- Support advanced features;
- Secure;
- Easy to manage.

Currently, models of traditional access control, or RBAC (Role Based Access Control) and ABAC (Attribute Based Access Control) fail in terms of scaling. These models require a great effort on their

management, the identification of “things” can become very complex due to their quantity, and also bring several other associated security issues.

Having that background information, researchers started to develop a more advanced identification system able to meet all necessary requirements. Examples:

Capability Based Authorization Positive points are:

- Principle of Least Authority (PoLA) is default, this principle is based on providing users only the privileges required for their work;
- More access control;
- Less security issues;
- Capable of externalizing the authorization process;
- No need to manage issues related to complexity of subjects identities.

And why Capability based authorization in IoT?

- Many objects accessing resources;
- Ability to easily delegate tasks to other objects;
- Offload management of external subject’s dynamics.

Adapted from (Capability Based Approaches to Authentication and Authorization, 2012)

### *4.8.2* Hardware security research

This section presents some research in terms of hardware in order to support safety of the IoT. Table 4-5 show some relevant projects.

Table 4-5 – Examples of IoT security research in hardware

| Acronym | Description | Target | URL |
|---|---|---|---|
| ISO/IEC 14443 | Architecture for contactless proximity cards | Information flow protection (AES) | http://www.iso.org |
| IEC 62591 (WirelessHART) | Protocol for industrial wireless sensor networks | Encryption, authentication, key management | http://www.hartcomm.org/ |
| GS1 keys | Identification system | Unique identifier definition | www.gs1.org/gsmp/kc/epcglobal |
| ucode | Hardware-agnostic identifier | Unique identifier definition | www.uidcenter.org |

Adapted from (Roman, et al., 2011)

Issues such as information flow, encryption, identification, and other issues are being investigated in various projects to ensure safety at all levels.

### *4.8.3* Software cryptography and protocols research

In terms of data security, encryption and specific security protocols may be the solution. Although there are already some solutions, since the data stream in the IoT will be much greater than that found on the traditional Internet, there are several other issues that need to be revised. The main difficulty in this case is to meet all the required standards. In this sub-chapter some solutions are presented.

**Lightweight Cryptography**

Lightweight Cryptography is a protocol specifically designed for environments that include RFID tags, sensors, smart cards, etc. Even being on a research state, it has already been discussed as a possible standard, and it has already proved to have superior capabilities than the current cryptography used in the Internet. This protocol intends to replace the usual Internet security systems with fully adapted solutions to the IoT. For instance:

In Internet AES (Advanced Encryption Standard) is used; for the IoT, CLEFIA (Clef means key in French), and PRESENT, among others were proposed. These new ‘’blocks’’ intend to provide encryption in IoT.

The hash functions are suggested to be replaced with a new cryptography hash algorithm “SHA-3”, which is expected to be a general purpose hash function. A new Public Key Cryptography, with the objective of replacing the conventional RSA (Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman), and the ECC (Elliptic curve cryptography) are also proposed.

Note:

- Symmetric-key algorithm – Class of algorithms used to cypher and decipher text;
- Hash functions – It is an algorithm that generates data has a shortening to original data;
- Public Key Cryptography – It is an algorithm that generates two keys, a public one and a private one, these two keys are mathematical related.

Adapted from (Katagi, Moriai, 2011).

**Permutation Based Cryptography for IoT**

The objective of this project is to simplify cryptography in the IoT domain. In the report presented by STMicroelectronics and NXP Semiconductors to CIoT (Cryptography for the Internet of Things) in 2012, some solutions were presented:

- Adoption of Datagram Transport Layer Security: a protocol designed to provide privacy in communications;
- The use of just one permutation in hashing, authentication, random number generation and key functions.

This “one permutation” solution, allows a faster response time, improved processing time and a flexible and multipurpose keys. Adapted from (Bertoni, *et all*, 2012).

The projects presented above intend to provide a strong basis to cryptography for the IoT, however it is also important to discuss solutions based on the IP.

“*As billions of smart objects are expected to come to life and IPv4 addresses have eventually reached depletion, IPv6 has been identified as a candidate for smart-object communication. The deployment of the IoT raises many security issues coming from (i) the very nature of smart objects, e.g., the adoption of lightweight cryptographic algorithms, in terms of processing and memory requirements; and (ii) the use of standard protocols, e.g., the need to minimize the amount of data exchanged between nodes*” (Cirani, et al., 2013).

In the IP context, several solutions are being researched, and it is important that these solutions fit the IoT ideology and technology. Among the solutions being proposed, we can find some that are very important, such as:

- IKEv2/IPsec – The Internet Key exchange, it is a protocol able to exchange authenticated keys, and resides in the network layer in the OSI model;

- HIP – Host Identity Protocol – Is also able to exchange keys and also resides in the network layer in the OSI model;

- TLS – Transport Layer Security, is a data oriented protocol to provide security for TCP at the transport layer;

- DTLS – Datagram Transport Layer Security, this protocol also provides security in transport layer, however it targets the UDP;

- PANA - Protocol for Carrying Authentication for Network Access, enables the network authentication between clients and the infrastructure;

- EAP – Extensible Authentication Protocol, an authentication framework able to support multiple authentication methods.

Adapted from (Heer, et al., 2011).

Lightweight cryptography can contribute greatly to the security of “things” because of its efficiency and lightweight. By its turn, security based on IP can be easily reused and adapted to other objects.
At this point it is still important to gain more practical experience in order to identify the solutions.

# 5 A DEMONSTRATION CASE

This chapter describes all the implementation of a small illustrative example of connecting a mobile robot to Internet using RESTful WS. For this demonstration the following components were used:

- Hardware:
  - Lego Mindstorms, http://mindstorms.lego.com/en-us/default.aspx.
- Software:
  - LabVIEW 2011.

The Lego Mindstorms consists of various hardware components, which allow the user a wide range of possibilities for different configurations. The various individual parts that are provided in the kit allow the creation of multiple robots with varied functionalities.

The chosen environment for programming the Lego Mindstorms was LabVIEW. This system, besides providing a specific module for programming the Lego Mindstorms, also supports the creation of web services to make the created services available on Internet.

## 5.1 Lego Mindstorms module

Each Lego Mindstorms provides the following set of pieces:

- 1 NXT micro-computer – that acts as the brain of the robot;
- 2 Touch Sensors – that makes the robot feel;
- 1 Ultrasonic Sensor – that makes the robot 'see' - and detect motion;
- 1 Color Sensor – that can detect different colors, and light settings;
- Interactive servo motors with built-in rotation sensors.

These parts offer a great degree of freedom to the programmer, thereby allowing a wide range of functions that can be implemented.

Being a very flexible tool, Lego Mindstorms offers the possibility to be programmed in various types of programming languages, so the user is not bound to a specific one. It includes:

- NXT-G;
- C#;
- BricxCC;
- Not eXactly C;
- Robotlab;
- Robot Operating System (ROS);
- ROBOTC.

These programming environments all differ from each other. However they all allow a very flexible way to program Lego Mindstorms. The Lego Mindstorm allows a wide range of personalization. For communication with the computer it can use cable or Bluetooth.

## 5.2 LabVIEW

LabVIEW is a programming environment used by engineers and scientists which provides a graphical programming style and is used to design and deploy systems. It is a flexible platform that allows integration with other systems already implemented. Through a graphical programming style, it allows users to quickly deploy solutions, using reduced programming and a high level of abstraction.
This software was chosen for this experiment because it has all the modules required to design and implement an example within the IoT.

For this demonstration a specific module of LabVIEW, the LabVIEW NXT Module 2011 was used. This module provide the necessary tools to develop programs for the Lego Mindstorms robot. LabVIEW also provides a tool that allows the use of RESTful web services, thus allowing the publication of user-created services.

## 5.3 Context of IoT

In our experiment of connecting a “thing” to Internet it was used the Lego Mindstorms programmed in LabVIEW. After certain features were programmed, they were made available through web services, so the user can access the robot capabilities from anywhere, anytime. These features are implemented by programming in NXT and can be used to control the robot through a form.
Having a computer to serve as a server, allows thereby to order the robot to perform the actions that a remote user requests. These can be commands of motion, increase of speed or object detection. The robot is used by the remote user through a web browser, just by entering the URL of the service. The server receives commands through the RESTful Web services and communicates with the robot.
The implemented experiment demonstrates the usefulness of the Internet of Things, leaving no doubt that these features could be expanded, including any example provided in the previous chapters, thus giving the user a useful experience, within the vast world of the Internet of Things.

## *5.4* Implementation

In order to better understand the performed implementation, the information provided in this section can be complemented with the provided by National Instruments (Shenkeshi, et al., 2013), available online at www.ni.com. Figure 5-1 shows the robot used to implement this experiment on IoT.

Figure 5-1 - Robot Lego Mindstorm

Figure 5-2 shows the image of the sensor used to detect objects.

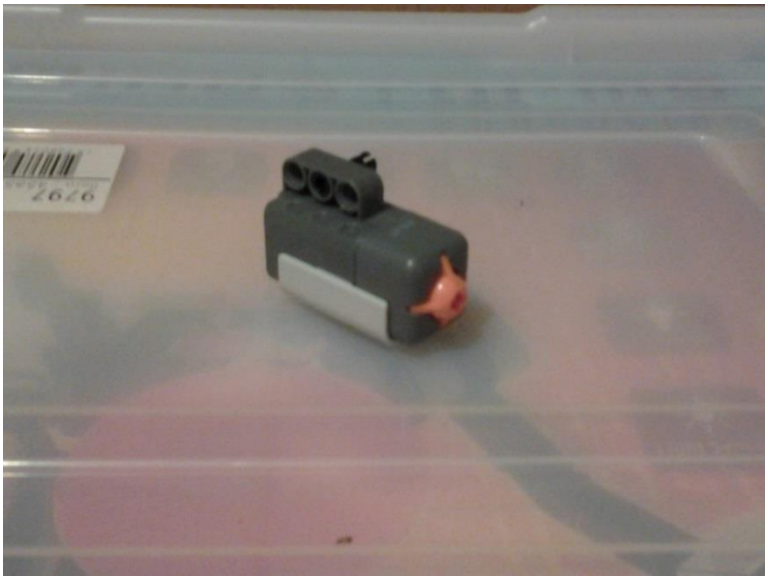

Figure 5-2 - Sensor used for object detection

To control the robot we used a simple remote panel created in LabVIEW. The implemented commands and their interface are shown in Figure 5-3.


Figure 5-3 - Remote panel

In this case, the robot is controlled by the arrow keys to move, and other specific keys to increase/decrease engine speed and detect objects. The actions activation is based on events. Each event is activated through a button. For movement we use the arrow keys, to stop the engines we use the "Ctrl" key and for the detection of objects we use the "Home" key.

LabVIEW provides the necessary tools to program this system. All functions are provided by blocks, which means we can use:

- Structures (Figure 5-4):

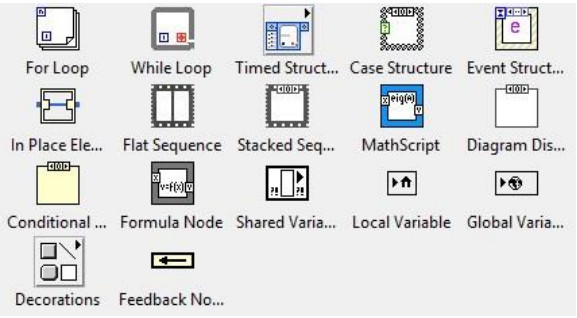


Figure 5-4 - LabVIEW structures

- Numeric functions (Figure 5-5):

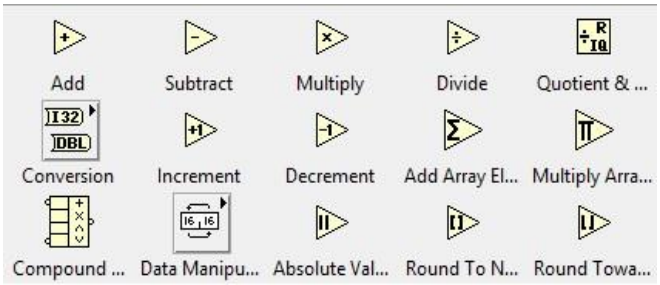


Figure 5-5 - LabVIEW numeric functions

- Comparison (Figure 5-6):

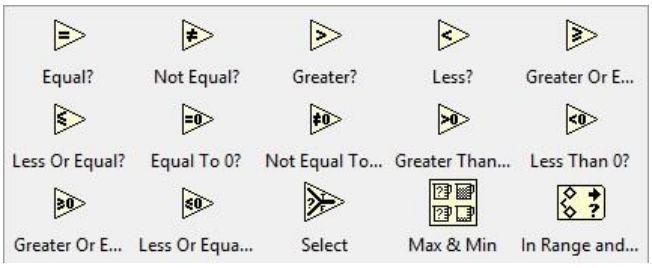


Figure 5-6 - LabVIEW comparison functions

- NXT functions (Figure 5-7):

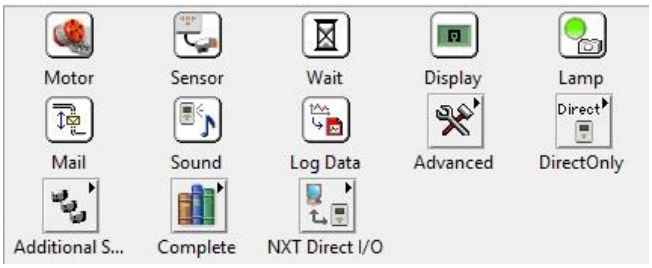


Figure 5-7 - LabVIEW NXT module

LabVIEW provides more modules, however these ones were the ones used to program the robot.

Using an event structure, it is possible to manage events. In this case it was chosen to have an event by pressing a certain key, which means that depending on the key pressed it runs a certain action. This structure has the purpose of detecting which key is pressed. After detecting the key, it points to a certain action. This action runs in a case structure, which activates a certain movement or action (such as detect objects) by enabling a certain port, which is connected to a certain motor, or sensor.

To get a better insight on the flow of the program, it is illustrated in Figure 5-8:

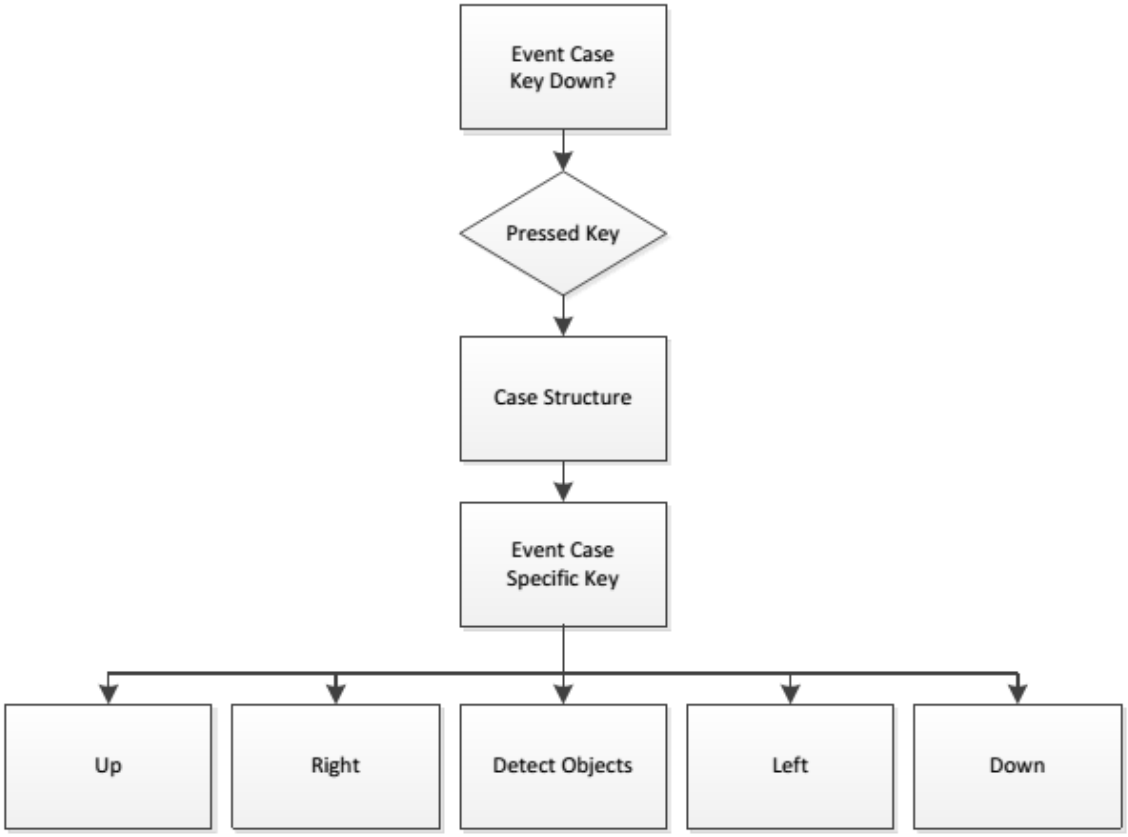


Figure 5-8 - Program Flowchart

After pressing the key, the program returns to the event structure that performs the action, by activating the proper motor (Figure 5-9).

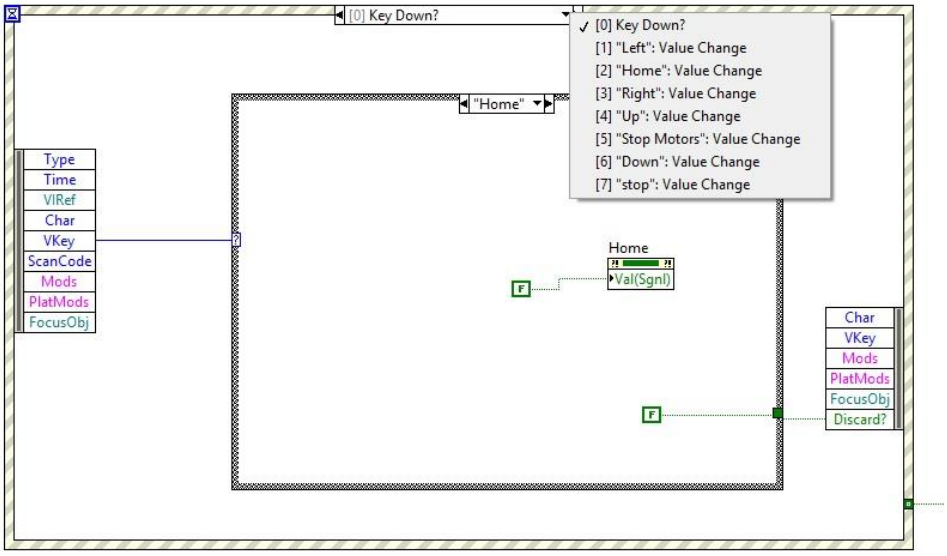


Figure 5-9 - Events used to control the robot

As illustrated, different keys are associated to different actions. These keys are linked to the event ''Key down'', which in turn triggers the appropriate action: up, down, left, right, stop. Figure 5-10 illustrates the command that actually makes the motors running and advance forward.

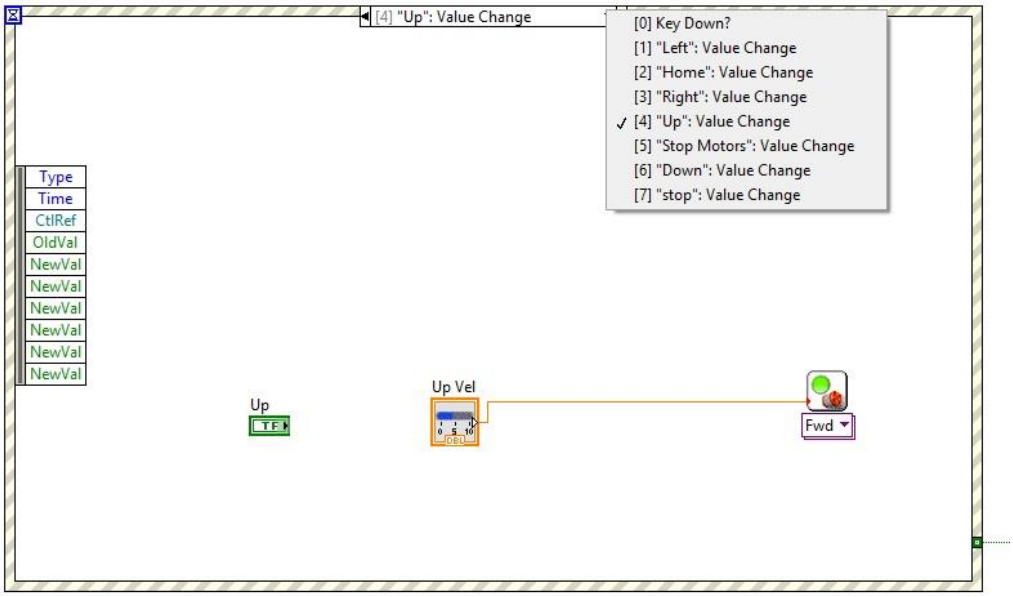


Figure 5-10 - Up action within events

The action shown in Figure 5-10 is triggered after pressing the up arrow, which in turn activates the event "UP". This event connects the motor and provides speed. The speed can also be adjusted from zero to one hundred, being null at zero and maximum at a hundred. In this implementation only the movements forward and backward can have their speed regulated.

To prevent the end of the program, these events are encapsulated within a loop structure as illustrated in Figure 5-11:

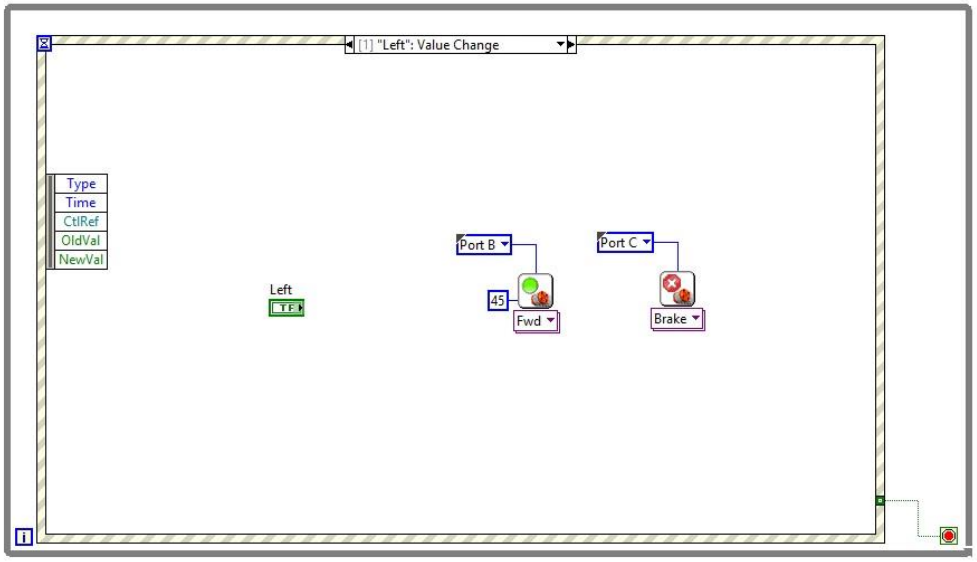


Figure 5-11 - Loop structure used to keep these events running

This structure prevents the program from closing after each action. In this way the event structure can only be finished by pressing the "panic" button.

In addition to moving, this robot can detect objects by “colliding with them”. By pressing the "Home" button on the form, the robot moves forward until the touch sensor is pressed. When pressed, the robot goes back for a second and stops. This function is shown in Figure 5-12. This example also illustrates how any other function can be programmed.

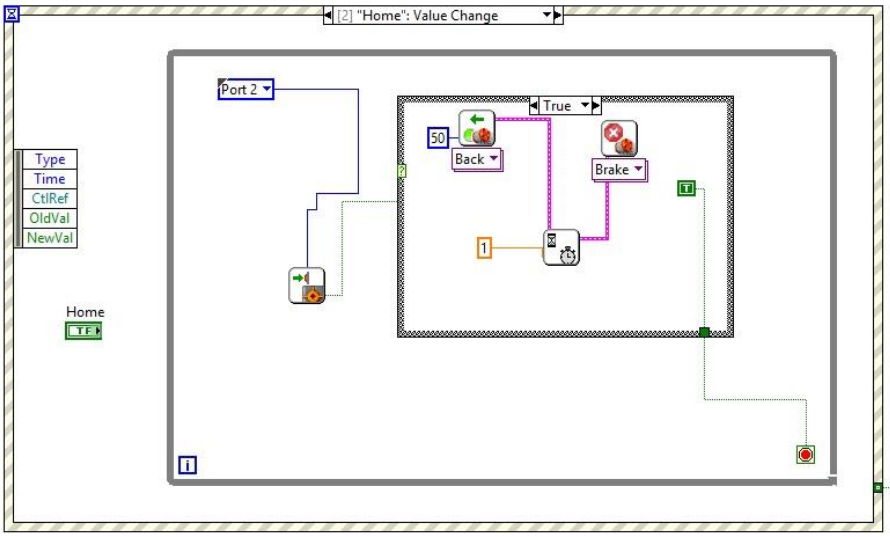


Figure 5-12 - Detecting objects function

As shown in Figure 5-12, after pressing the "Home" key, the program enters a structure "if-then", and while the condition of active sensor is false the robot continues to advance (port 2). After the sensor is active this structure returns false, which causes the robot to stop and move backward for a second and stop. When pressed, the sensor provides a Boolean as output, allowing the program to flow. Other sensors for the robot Lego may be included and programmed, such as a light sensor, a sound sensor, or

a sensor of ultrasound which provides the ability to measure the distance to objects. These sensors provide the NXT with a wide variety of applications and personalization.

(Adapted from National Instruments)

LabVIEW provides a functionality which allows users to generate remote control panels. In this way the user can create applications that can be shared and remotely controlled by other users. LabVIEW enables the creation and management of WS in a simple way, by encapsulating all the necessary variables in order to be used remotely. In Figure 5-13 we can see how LabVIEW provides the WS.

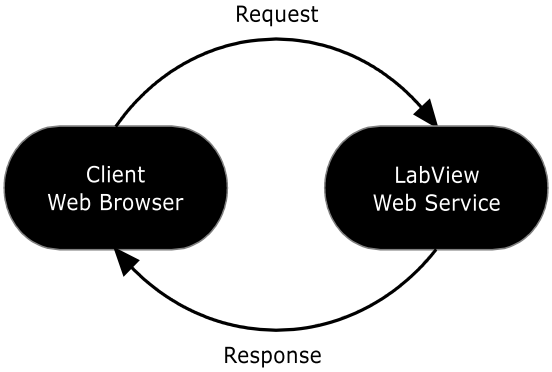


Figure 5-13 - LabVIEW Web Service example

In this implementation the basis of communication can be described as illustrated in Figure 5-14.

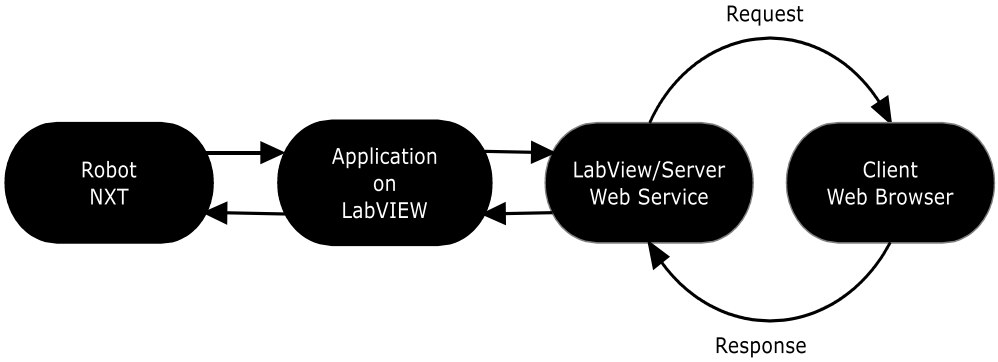


Figure 5-14 - Web Service implementation chart in LabVIEW

As illustrated in Figure 5-14, the robot receives commands from the application created in LabVIEW, which in turn is controlled by the user via a remote panel. This remote control panel has its variables and commands encapsulated by LabVIEW, allowing the panel to be available in a web browser. The client connects to the service using the URL. Through the displayed page orders are given. These orders are received by the server, which controls the robot according to the orders of the user.

In Figure 5-15 we have represented the several layers that compose Web Services:

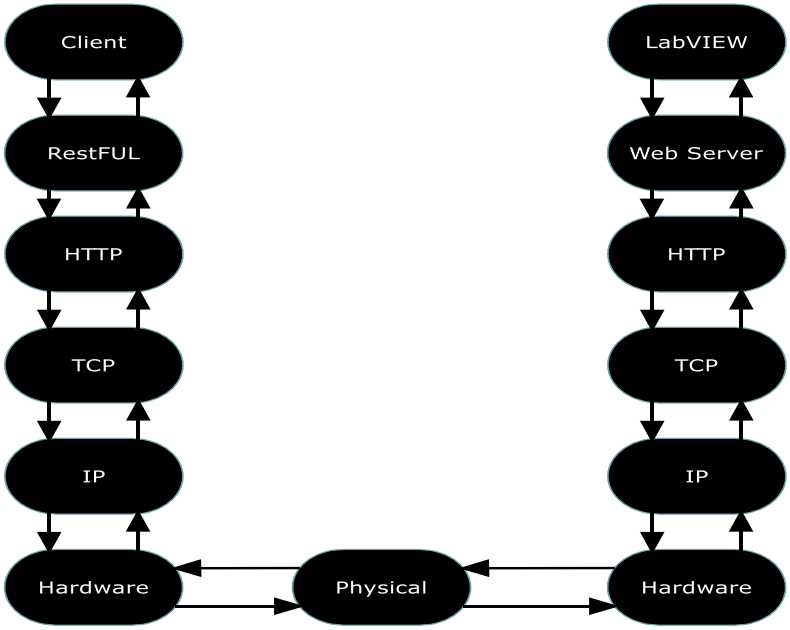


Figure 5-15 - Web Service layers on LabVIEW

Web Services in LabVIEW are designed with layers of specific protocols that provide the abstraction and all communication patterns necessary to make the services available and standard for all users. It is important to understand that this implementation only requires having a server that is running LabVIEW Web Server and the corresponding form used to control the robot. The only requirement for users to access the service is to possess the engine runtime and LabVIEW plug-in installed on the client side. To offer this service through the internet the user is required to have:

- Physical location of server;
- Port;
- Name of the Web service;
- Mapping to an application;
- Inputs.

As described in previous sections, this type of Web services, are accessible to any user, without major needs in terms of software / hardware.

After configuring the web server through LabVIEW, the form is coded allowing it to be accessed through a web page displayed in any Internet browser. This codding is automatically generated, as well as all the layers and protocols required. From this point on the user can experience the application of IoT.

## 5.5 Conclusions about the demonstration experiment

The objective of this hands-on experiment was mainly to provide the reader with a practical illustration, thus providing an insight of the IoT potential, and leaving the idea that the applications are endless, each one with their own benefits and specific characteristics.

Nowadays it is already possible to find a wide range of hardware and software components that facilitate IoT implementations.

Regarding hardware, we can use various types of components, such as Arduino or ZigBee, that provide Wifi capabilities and programmable capability in order to implement the desired functionalities. In terms of software/programming techniques it is possible to use almost all programming languages, however there are some best suited for this purpose.

In this case the chosen hardware was LegoMindstorms and the software was LabVIEW. Being the objective of this example just to demonstrate the IoT capabilities, this hardware/software provided a suitable combination. LegoMinstorms provides a small robot with the ability to be programmed and adapted. Since the objective of this example was to provide means to execute an example and let interested users to experiment the IoT, the LabVIEW was chosen to program the robot. LabVIEW provides standard mechanisms to make services available on the Internet, thus making possible the connection robot/Internet, the main characteristic of the IoT.

This experiment was very useful not only to gain experience with some IoT features, but also to acquire new knowledge in programming and connection methods.

In terms of hardware, the robot was in certain ways limited since the sensors provided could only bring limited capability to the demonstration. In an ideal case, and to be viewed as a necessary tool, a more realistic robot demonstration should be able to provide certain features such as, for instance:

-Detection and identification of humans;
-Temperature and smoke detection;
-Automatic environment adjustments;
-Demotic control;
-Emergency warnings.

However what distinguishes this simple robot prototype from others that can already be found in the market is the connection to the Internet, being the user able to control the robot from anywhere at any time, and this connection capability is why this object can be called a “thing” in the IoT. In this way, the main objective of this experiment was accomplished: the connection of a real object to the Internet.

This implementation made use of knowledge presented in several chapters of this thesis, such as: support technologies, Internet topology, representing “things” and integration. As such, even being limited, this experiment can serve to illustrate some key aspects of the IoT. This experiment can be used as a starting point to future implementations, improving not only the existing connection method, but also the hardware itself, and implementing security mechanisms from the software side.

Some other features could have been implemented in order to make the robot intelligent, however the available hardware did not support such features, being so the only intelligent ability implemented was the ‘’detect objects’’.

As mentioned above, the robot receives orders from the application, which on its turn receives orders from the remote user. The communication between the robot and the application is made by Bluetooth or cable. If the Bluetooth is chosen over cable, the security may become compromised, like mentioned in the security chapter, due to the communication type. However if we chose to communicate by cable it will restrict the robot movements. Ideally this communication would be done by Wi-Fi, which is a module that can be used by LegoMindstrom.

The communications server/user (being the server the computer that issues orders to the robot) are made by the web services and made available by the LabVIEW. Security issues in this layer can be identified: permissions, encryption, etc. Those issues could be resolved by using third party software’s (on inhouse developments), meaning that the security would have to be integrated outside of the LabVIEW, which would take us to an integration issue.
The mentioned issues, can help understand the type of research and development that is required (among others) to improve and accomplish the IoT. In this way, the robot experiment will not only serve to provide a hands-on example, but also to identify problems around the implementation, opening directions to specific future developments.

# 6 CONCLUSIONS AND FUTURE WORK

*"Humans have learned through the millennia how to benefit from their environments. Whether it was by obtaining food or shelter we learned how deferent habitats can give us fundamental elements for our survival or comfort"* (Cook, et al., 2007)

This continuous search and the need of constant evolution, gave rise to the Internet of Things, considered by all the next generation of the Internet. The main goal of this thesis was to gather, organize, and analyze the available scientific and technologic information about this subject. Besides analyzing the information, an effort was made to assess the degree of applications already existing nowadays and the future perspectives of this technology.

After analyzing the collected information, we can conclude that the Internet of Things is positioned for a very strong future in the evolution of the Internet. Due to the effort and research done in this area we can say that the IoT will go from a vision to a reality in a short period of time. IoT is expected to open the possibility for a wide range of new applications and new devices that will bring to our society an unimaginable amount of improvement.

We can consider the IoT as a network of objects at a global level. In this context the IoT can be applied in many different ways, but focusing in some areas where it is more urgent to evolve, aiming to match the most urgent needs: Industrial Internet, sensing enterprise, smart environment, smart objects, health, smart cities, security, safety, energy, agriculture, farming and automation processes. In this world that promises to connect "things" and people, a number of useful characteristics are offered: availability, both in the virtual and real world, connectivity, interactivity, full integration and adaptation among other features. These features can also provide these "things" with increasing degree of autonomy, that is especially important to meet the needs of people who use them. By combining the various technologies presented throughout this thesis, "connected things" will fulfill their purpose as smart objects and will open new and wide range of applications, both in terms of new devices, as in improved usage of the old ones. These devices have the possibility to be available, in the virtual and physical worlds. The connection to the network will allow "things" to be available anytime, anywhere and to be used by anyone with permission of access. Nowadays, we already have some examples of applications at this level. For instance, we can find applications in areas such as intelligent environments for personal spaces, intelligent machines used in advanced factories and machine-to-machine communications.

After presenting the trends, applications and future perspectives for the IoT, we also provided some data confirming the huge attention and bet on this technology, particularly through a strong commitment on the part of almost all countries in terms of the research and development of this technology. Aside from these research efforts, we can also observe specific strategic moves in market terms, which just prove that most companies believe that the IoT is increasingly becoming a reality. All these facts come from the so called ''gold rush'' to this technology.

Throughout this thesis all areas considered important for the realization of IoT were covered and analyzed in terms of technical and functional views, with the aim of providing information about the advantages and disadvantages of each important topic. Each particular area presented, such as hardware, software, regulations, forms of communication or security, can lead to new research directions exploring the advantages, and current limitations and lead to new horizons, and open several doors for the future.

One aspect that is particularly important, but that was not presented in this thesis and should be seriously discussed, is the legal side of the Internet of Things. A strong regulation framework should be created for the IoT in order to ensure protection of data and personal interests.

Although already being the object of strong research efforts and various contributions coming from different contexts, the IoT requires more multi-disciplinary cooperation. Nowadays many research groups are still working isolated from the rest of the scientific community, and this implies possible setbacks for

IoT. The IoT, without standards and without possessing a strong base for integration, simply does not make sense or will not be able to reach its maximum potential. Issues at level of individual hardware or software components can be easily solved by researchers, however, to reach an IoT able to fully integrate a plug-n-play style, a stronger interaction is necessary in the scientific community.

In terms of physical devices, the examples provided in this thesis, although not an exhaustive list, illustrate what can be used in many more application fields. The functionalities to be included in each device naturally depend on the envisaged applications. Nevertheless, some common aspects include energy efficiency and autonomy, safe and effective communications, and increasing levels of embedded computational power.

In terms of communications, after examining the information provided, it is quite safe to say that wireless communications will be the most viable for the IoT. However, not only WiFi provides good prospects, other kinds of communication can be used with the intention of supplementing communications for the IoT, for example, Bluetooth or NFC. These two types of communication, classified in this thesis as the type “connection on available”, can prove to be extremely useful for communication between “things” or between “things” and people.

In terms of network architecture, we analyzed three types: P2P, mesh and client/server. From these three architectures the most interesting is undoubtedly the client/server architecture. This architecture enables faster operations that occur in the systems since the server handles all processes. Nevertheless, new organizational structures might be needed given the fact that the number of processes, devices and requests will increase exponentially due to the constantly increasing number of devices and people to interact in the IoT.

Regarding representation of “things” three possible forms of representations in the context of the IoT were discussed and presented. Connected “things” need to “exist” in the virtual environment, and therefore it becomes necessary to characterize them in the cyber world. Of the three forms analyzed: web services, agents, and frames, it is to choose the technology that currently might adapt better, without ruling out the other two. Within this framework, Web services are the best suited. In addition to providing a service-based representation, they offer a strong layer of abstraction that allows a large degree of integration. It is not possible however to say that agents and frames will not be also options to achieve this objective in a near future.

In terms of security, much work remains to be done. The solutions used nowadays are entirely adapted to the traditional Internet which has quite different characteristics of IoT. However the existing solutions can serve as a starting point for research in order to create valid solutions to the security of IoT. We can already find some solutions today, and the one that would better adapt to the scenario of the IoT would be safety in layers. This solution provides the systems with various protection capabilities. Each layer has a specific type of protection: encryption protocols, sessions managers, passwords, firewalls, etc. This layered security is based on the OSI model, and is a type of security that must be implemented when the network is still at the design stage.

To complete this work, a small experiment based on the IoT was developed, in order to acquire hands-on-experience and provide the reader with a small taste of what the IoT can provide. Not being an example that provides major options in terms of functionality, it nevertheless allows to have an idea of the capabilities and benefits of this new technology.

To conclude, we can say that much work still needs to be done. The scientific and engineering community needs a strong approach in terms of communication and exchange of knowledge in order to accelerate progress and achieve a safe and large-scale integration. In the last few years we could already observe many conferences on IoT being organized, not only within communities of individual countries but at global scale. These conferences are very important, because they intend to establish objectives, initiate standards, open discussions on projects and exchange of information.

# 7 BIBLIOGRAPHY

**Ashton, K. 2009.** That 'Internet of Things' Thing. *RFID JOURNAL.* 1 22. http://www.rfidjournal.com/articles/view?4986

**Baltopoulos, I. G. 2005.** *Introduction to Web Services.* Department of Computer Science. London: Imperial College London. Lecture Slides. Accessed on: 02/12/2013 http://www.cl.cam.ac.uk/~ib249/teaching/Lecture1.handout.pdf

**Bandyopadhyay, S.; Sengupta, M.; Maiti, S.; Dutta, S. 2011.** *Role of Middleware For Internet of Things: A Study.* No.3, Kolkata, India: Innovation Lab, TATA Consultancy Services Ltd. Kolkata, India, International Journal of Computer Science & Engineering Survey, Vol.2, pp. 94-105. http://airccse.org/journal/ijcses/papers/0811cses07.pdf

**Berst, J. 2013.** EU and Japan to collaborate on smart city "cloud of things". *SmartCitiesCouncil.* [Online] 05 08, 2013. Access on: 02/12/2013. http://smartcitiescouncil.com/article/eu-and-japan-collaborate-smart-city-cloud-things.

**Bertoni, G.; Daemen, J.; Peeters, M.; Assche, G. 2012.** *Permutation Based Cryptography for IoT.* Antwerp: STMicroelectronics & NXP Semiconductors. CIoT 2012. p. 41. Accessed on: 12/01/2014. http://hyperelliptic.org/CIoT/slides/bertoni-ciot.pdf

**Bradley, J.; Barbier, J. and Handler, D. 2013.** *Embracing the Internet of Everything To Capture Japan's Share of $14.4 Trillion.* San Jose, CA : Cisco. p. 13, White paper. Accessed on: 02/12/2013 http://www.cisco.com/web/JP/news/pr/2013/docs/IoE_Economy_VAS_Japan_WP.pdf

**Brittenham, P. 2002.** *An overview of the Web Services Inspection Language.* developerWorks, IBM Corporation. pp. 1-13. Accessed on: 13/10/2013 http://www.ibm.com/developerworks/webservices/library/ws-wsilover/.

**Bruner, J. 2013.** *Defining the industrial Internet.*O'REILLY radar. Online Post. Access on: 15/09/2013 http://radar.oreilly.com/2013/01/defining-the-industrial-internet.html

**Camarinha-Matos, L. 2009.** *UNIDADE 4 – MODELAÇÃO EM "FRAMES".* Lisbon, 2009. p. 8. Lecture Slides available on course Web Page. Accessed on: 06/12/2013

**Camarinha-Matos, L.; Gomes, L; Goes, J; Martins, J. 2013.** *Contributing to the Internet of Things.* In: Technological Innovation for the Internet of Things, IFIP AICT. Springer, 2013. pp. 3-12.

**CASAGRAS2. 2012.** *The Internet of Things 2012 New Horizons.* [ed.] Ian G. Smith. Halifax, UK: IERC. ISBN hard cover: 978-0-9553707-9-3. http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf

**Castanier, F. 2012.** *Developing pervasive security for the IoT.* Venice, Italy : BUTLER. IoT week - June 2012. pp. 1-11. Presentation Support Slides. Accessed on: 22/10/2013 .http://www.iot-week.eu/iot-week-2012/programme-1/tuesday-1/presentations/privacy-security-workshop/BUTLER%20-%20IoT-Week%20Privacy%20and%20Security%20Workshop.pdf

**Cirani, Si.; Ferrari, G. and Veltri, L. 2013.** Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview. *Algorithms.* Algorithms. Vol. 6, 2, pp. 197-226. http://www.mdpi.com/1999-4893/6/2/197. Accessed on: 7/03/2013

**Cook, J.; Augusto, J. and Jakkula, V. 2007.** *Ambiente Intelligence: Technologies, Applications, and Opportunities.* School of Electrical Engineering and Computer Science; Washington State University, Pullman, WA, USA; School of Computing and Mathematics; University of Ulster, UK. Washington: Washington State University. pp. 1-38. Accessed on: 2/7/2013 http://www.eecs.wsu.edu/~cook/pubs/pmc10.pdf

**Dahlberg, B. 2010.** *Arrayent, Inc. Introduces the Industry's First Turnkey System to Internet-Connect Consumer Products.* London: Arrayent, Inc.,Technical information available on ompanies Web Site. Accessed on: 22/7/2013. http://www.businesswire.com/news/home/20100105006910/en/Arrayent-Introduces-Industry%E2%80%99s-Turnkey-System-Internet-Connect-Consumer.

**Dalpiaz, F. 2011.** *Agent Oriented Programming.* Information Engineering and Computer Science Department, University of Trento. Italy. pp. 1-108. Lecture on agent-oriented programming (2011). http://fabianodalpiaz.wordpress.com/teaching/. Accessed on: 15/11/2013.

**DELL SonicWALL. 2012.** *Anatomy of a cyber-attack, The strategies and tools of cyber-criminal - and how to stop them*: DELL. Online report. Accessed on: 8/12/2013. http://software.dell.com/documents/anatomy-of-a-cyber-attack-ebook-24640.pdf

**Energetics Incorporated. 2012.** *Cyber-Physical Systems: Situation Analysis of Current Trends, Technologies and Challenges.* Columbia, Maryland 21046 : National Institute of Standards and Technology, Report for the National Institute of Standards and Technology. Accessed on: 11/12/2013http://events.energetics.com/NIST-CPSWorkshop/pdfs/CPS_Situation_Analysis.pdf

**Energetics Incorporated. 2013.** *Foundations for Innovation in Cyber-Physical Systems.* National Institute of Standards and Technology . Columbia, Maryland, 2013. p. 52. Workshop report. Accessed on: 20/12/2013. http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf

**European Union. 2010.** *IOT-I.* [Online]. Accessed on: 03 19, 2013. http://www.iot-i.eu/public.

**Evans, D. 2011.** *The Internet of Things How the Next Evolution of the Internet is Changing Everything.* San Jose, CA : CISCO, pp. 1-11, White Paper. Accessed on: 10/12/2013. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL

**FIPA. 1998.** FIPA - Foundation for Intelligent Physical Agents. [Online] .Accessed on: 04 04, 2013. Online *FIPA 98 Specification*. http://www.fipa.org/specs/fipa00002/OC00002A.html.

**Fleisch, E. 2010.** *What is the Internet of Things?,An Economic Perspective.* Zurich : ETH Zurich / University of St. Gallen. Auto-ID Labs White Paper. WP-BIZAPP-053. Accessed on: 5/1/2014. http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-53.pdf

**Fleisch, E.; Mattern, F.; Sarma, S. 2008.** *Internet of Things 2008.* [ed.] University of St. Gallen and ETH Zurich. Zurich : Springer, 2008. International Conference for Industry and Academia. 0302-9743. Accessed on: 23/7/2013. http://www.the-internet-of-things.org/iot2008/

**Fabiano, N. 2012.** *Internet of Things and Privacy by Design toward a standardisation process***.**[ed.] PbD. Venice: STUDIO LEGALE. IoT Week 2012. pp. 1-11. Presentation Slides. Accessed on: 13/10/2013. http://www.iot-week.eu/iot-week-2012/programme-1/tuesday-1/presentations/privacy-security-workshop/fabiano_iotweek.pdf

**Gill, H. 2008.** *CPS: A View from the HCSS Agencies.* [ed.] NSF: NITRD High Confidence Software and Systems. CPS: A View from the HCSS Agencies. pp. 1-15. Workshop: From Embedded Systems to Cyber-Physical Systems . Accessed on: 16/5/2013. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDAQFjAA&url=http%3A%2F%2Fchess.eecs.berkeley.edu%2Fpubs%2F418%2FGill_08_CPS_CHESS_ViewFromHCSSAgencies.ppt&ei=LepJUYm6EdKB7QbTv4CwCw&usg=AFQjCNFpSUjt6xprjvJukM_wNDBM6zYCqg&sig2=nwkP8xnS

**Government of Hong Kong. 2008.** *WEB SERVICES SECURITY.* The Government of the Hong Kong Special Administrative Region . Hong Kong. Report regarding security in WS. Accessed on: 4/12/2013. http://www.infosec.gov.hk/english/technical/files/webss.pdf

**Green, S.; Hurst, L.; Nangle, Br.; Cunningham, P.; Somers, F.; Evans, R. 2007.** *Software Agents: A review.* Dublin, 2007. pp. 1-48. http://www.lsi.upc.edu/~bejar/aia/aia-web/green97software.pdf

**Guinard, D,; Ion, I. ; Mayer, S. 2012.** In Search of an Internet of Things Service Architecture: REST or WS-*? A Developers' Perspective. *Mobile and Ubiquitous Systems: Computing, Networking, and Services.* Zurich, Switzerland : Springer, Vol. 104, pp. 326-337. Study realized in WS-* vs. REST.

**Gunzer, H. 2002.** *Introduction to Web Services.* Borland. Scotts Valley, CA, 2002. pp. 1-17. White Paper. Accessed on: 4/12/2013. http://edn.embarcadero.com/article/images/28818/webservices.pdf

**Heer, T.; Garcia-Morchon, O.; Hummen, R.; Keoh, S.; Kumar, S.; Wehrle, K. 2011.** Security Challenges in the IP-based Internet of Thing. [ed.] Brian D. Woerner, Jeffrey H. Reed Theodore S. Rappaport. *Springer Journal.* 1994, Vol. 262, pp. 1-16.

**Hewlett-Packard Development Company. 2010.** *HP 360°: A PANORAMIC VIEW OF THE WORLD'S LARGEST INFORMATION.* United States : Hewlett-Packard, 2010. Technology News Report. Accessed on: 17/11/2013. http://www.hp.com/hpinfo/newsroom/hp360_ww.pdf

**Inoue, T.; Hayakawa, A.; Kamei, T. 2011.** *China's Initiative for the Internet of Things and Opportunitues for Japanese Businesses.* Corporate Communications Department, Nomura Research Institute, Ltd. NRI Papers. pp. 1-13. 165. Accessed on: 15/10/2013. http://www.nri.co.jp/english/opinion/papers/2011/pdf/np2011165.pdf

**IoT Week 2012. 2012.** http://www.iot-week.eu/. *http://www.iot-week.eu/iot-week-2012/programme-1/tuesday-1/privacy-security-workshop.* [Online] 6 18-22, 2012. Accessed on: 07 10, 2013. Workshop support slides. http://www.iot-week.eu/iot-week-2012/programme-1/tuesday-1/privacy-security-workshop.

**IoT2012. 2012.** The 3rd International Conference on the Internet of Things. [Online]. Accessed on: 14/10/2013. http://www.iot-conference.org/iot2012/.

**IOT-i. 2012.** "International Countries" ICT national contact points. *IOT-i Internet of Things Initiative.* [Online] 2012. [Cited: 03 20, 2013.] http://www.iot-i.eu/public/dissemination-1/international-countries-ict-national-contact-points.

**Janssen, C. 2011.** Internet of Things (IoT). *Technopedia.* [Online]. Accessed on: 12/5/ 2012. Technological dictionary. http://www.techopedia.com/definition/28247/internet-of-things-iot.

**Jeschke, S. 2013.** *Cyber-Physical Systems -History, Presence and Future.* Rwth Aachen University. Aachen. pp. 1-49, Presentation slides. Accessedon: 15/9/2013. http://www.ima-zlw-ifu.rwth-aachen.de/fileadmin/user_upload/INSTITUTSCLUSTER/Publikation_Medien/Vortraege/download/CPS_27Feb2013.pdf

**Jiabao, W. 2010.** Accessed on: 20/11/2013. Public speech. http://www.finnode.fi/files/43/IoT_Eric_Cheng_09062011.pdf

**Jingyue, L. 2012.** *Premier Wen Jiabao addresses CAS and CAE.* China: Chinadaily. Report on public speech. Accessed on: 19/11/2013. http://www.chinadaily.com.cn/m/beijing/zhongguancun/2012-06/20/content_15514126.htm

**Katagi, M.; Moriai, S. 2011.** *Lightweight Cryptography for the Internet of Things.* Sony Corporation, p. 4. Technical report. Accessed on: 12/1/2014. http://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf

**Kifer, M.; Lausen, G.; Wu, J. 1995.** *Logical Foundations of Object-Oriented and Frame-Based Languages.* Department of Computer Science, SUNY. New York: Journal of the Association for Computing Machinery. V.42, Nº 4 pp. 741-843.

**Koubâa, A.; Andersson, B. 2009.** *A Vision of Cyber-Physical Internet.* Portugal: HURRAY. Proceedings of the 8th International Workshop on Real-Time Networks (RTN'09), Dublin, Ireland. pp. 1-6.http://www.cister.isep.ipp.pt/docs/a+vision+of+cyber%252Dphysical+internet/475/view.pdf

**Krikorian, R.; Gershenfeld, N. 2004.** *Internet 0 — inter-device internetworking.* 4, BT Technology Journal, Vol. 22. No:4. http://black.fri.uni-lj.si/iplight/files/research/Paper28Pages278-284.pdf

**Lee, E. 2007.** *Computing Foundations and Practice for Cyber-Physical Systems: A Preliminary Report.* Department of EECS, UC Berkeley. Berkeley: National Science Foundation. pp. 1-27, Technical Report. Accessed on: 7/9/2013. http://www.eecs.berkeley.edu/Pubs/TechRpts/2007/EECS-2007-72.pdf

**Leibson, S. 2008.** www.edn.com. *EDN Network.* [Online]. Community Blog. Accessed on: 5/7/2013. http://www.edn.com/electronics-blogs/other/4306822/IPV6-How-Many-IP-Addresses-Can-Dance-on-the-Head-of-a-Pin-.

**Li, M. 2012.** *The Sensing Enterprise.* FInES Cluster Co-Chair. Warsaw. Accessed on: 12/08/2013 . https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCsQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fdigital-agenda%2Fevents%2Fcf%2Fictpd12%2Fdocument.cfm%3Fdoc_id%3D23285&ei=jBc_UpGYB9CGswbUsIHwAw&usg=AFQjCNHhQp4kPCEBp-p2tb3VkZWEulBgNg&sig2=4K90mph0bCTNwcv2UanTaw&bvm=bv.52434380,d.Yms&cad=rja

**Ma, H. 2011.** *Internet of Things: Objectives and Scientific Challenges.* Beijing Key Lab of Intelligent Telecommunications Software and Multimedia, School of Computer Science. Beijing: JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY. 26(6). http://www.cast.org.cn/n35081/n11219166/n12620949/n12621141/n13616780.files/n13617157.pdf

**Macmanus, R. 2009.** *Top 10 Internet of Things Products of 2009.* New York Times. Online Post. Accessed on: 16/10/2013. http://www.nytimes.com/external/readwriteweb/2009/12/08/08readwriteweb-top-10-internet-of-things-products-of-2009-74048.html

**Markopoulos, J. 2011.** *5 Ways The Industrial Internet Will Change Manufacturing.* Forbes, 2011, Forbes Web Site. Accessed on: 16/11/2013. http://www.forbes.com/sites/ciocentral/2012/11/29/5-ways-the-industrial-internet-will-change-manufacturing/

**Mayer, C. 2009.** *Security and Privacy Challenges in the Internet of Things.* Karlsruhe, Germany: TeleMatics. Proceedings of the KiVS Workshop on Global Sensor Networks. pp. 1-18. http://telematics.tm.kit.edu/publications/Files/322/gsn09-security-mayer.pdf

**McNamee, J.; Fiedler, K.; Humeau, M.; Maisuradze, S. 2012.** *How the Internet Works.* Brussels: EU's Fundamental Rights and Citizenship Programme. p. 25. Accessed on: 6/10/2013. http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf

**Meriwether, D. 1995.** *Vicious Fishes Web Design.* Takedown. Biography. Accessed on: 8/12/2013. http://www.takedown.com/bio/mitnick.html

**National Science Foundation. 2013.** Cyber-Physical Systems (CPS). *www.nsf.gov.* [Online]. Accessed on: 25/7/ 2013. http://www.nsf.gov/pubs/2013/nsf13502/nsf13502.pdf.

**Paolantonio, J. 2012.** The Internet of Things and Changes. *The TeleInterActive Lifestyle.* [Online] Accessed on: 18/9/2013. http://press.teleinteractive.net/tialife/2012/07/22/the-internet-of-things-and-change.

**Presson, E. 2012.** *Digi, Device Cloud.* [Online]. Information on events related to IoT. Accessed on: 14/2/2013. http://www.idigi.com/blog/events-2/upcoming-internet-of-things-cloud-data-conferences-and-events/

**Pretz, K. 2013.** The Next Evolution of the Internet. *the institute.* [Online] The IEEE news source, 1 7, 2013. [Cited: 9 18, 2013.] News Source. http://theinstitute.ieee.org/technology-focus/technology-topic/the-next-evolution-of-the-internet.

**Roman, R.; Najera, P.; Lopez, J. 2011.** Securing the Internet of Things. *IEEE Computer.* Vol. 44, 9, p. 1.

**Rotondi, D. 2012.** *Capability Based Approaches to Authentication and Authorization.* Venice: TXT e-solutions SpA. IERC AC5 IoT Security & Privacy Workshop. pp. 1-10. IoT@Work Project. Accessed on: 15/9/2013. http://www.iot-week.eu/iot-week-2012/programme-1/tuesday-

1/presentations/privacy-security-workshop/IERC%20AC5%20IoT-Sec-Priv_IoT-Work_contribution.pdf

**Sa, J. 2011.** Huawei. [Online] Huawei. Company Publication. Accessed on: 12 02, 2013. http://www.huawei.com/en/about-huawei/publications/winwin-magazine/hw-110837.htm.

**Santucci, G. 2010.** *The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects.* CORDIS. p. 40. Accessed on: 17/11/2013. http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-internet-revolution.pdf

**Savvas, A. 2013.** *Gartner: Internet of Things should not be ignored by business.* United Kingdom : COMPUTERWORLD UK, July 2013. News Source. Accessed on: 29/8/2013. http://www.computerworlduk.com/news/applications/3461686/gartner-internet-of-things-should-not-be-ignored-by-business/

**Shenkeshi, N.; Fortenberry, M.; Kawachi, Y.; Yapura, C. 2013.** Remote Panels in LabVIEW, Distributed Applications. *www.ni.com.* [Online] Feb 13, 2013. Technical Manual. Accessed on: 15/8/2013. http://www.ni.com/white-paper/4791/en/.

**Siemens Convergence Creators GmbH. 2013.** Siemens Convergence Creators Global. [Online] Siemens. Informational company product. Accessed on: 30/11/2013. https://www.cee.siemens.com/web/at/en/csb/CVC/products/Business-Support-Systems/cityWallet/Pages/cityWallet.aspx.

**Sommers, St.; Scholz, A.; Buckl, C.; Kemper, A.; Knoll, A.; Heuer, J.; Schmitt, A. 2009.** *Towards the Internet of Things: Integration of Web Services and Field Level Devices.* Proceedings of the Workshop on the Future Internet of Things and Services, 1-3 September. Accessed on: 2009, Berlin, Germany. http://www6.in.tum.de/Main/Publications/Sommer2009b.pdf

**Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. 2010.** *Vision and challenges for Realising the Internet of Things*. CERP-IoT, European Commission. p. 229. 978-92-79-15088-3. Accessed on: 20/9/2013. http://bookshop.europa.eu/en/vision-and-challenges-for-realising-the-internet-of-things-pbKK3110323/

**Telektronikk. 2002.** *XML Web Services.* Telektronikk. Vol. 98, No:4. http://www.telenor.com/wp-content/uploads/2012/05/T02_4.pdf

**Université de Montréal. 2004.** Agent communication. Jade Primer, ch.4, April 2004. Accessed on: 5/12/2013. Lecture slide. http://www.iro.umontreal.ca/~vaucher/Agents/Jade/primer4.html.

**Ursini, S. 2011.** Java tutorial, July 28, 2011. Tutorial Web Site. Accessed on: 3/12/2013. http://www.java-tutorial.ch/web-services/web-services-java-tutorial.

**Vermesan, O.; Friess, P. 2013.** *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems.* Aalborg: River Publishers.

**Vermesan, Ovidiu, et al. 2013.** *Internet of Things Strategic Research Roadmap.* IERC European Research Cluster of the Internet of Things, 2013. Accessed on: 12/12/2013. http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf

**Yu, W. 2012.** *Agent Programming with Jade.* Department of Electrical & Computer Engineering, The University of Alabama. Tuscaloosa, 2012. Lecture support slides. Accessed on: 5/12/2013. http://qh.eng.ua.edu/classes/fall2012/ece693/index_files/ECE693_Mobile_Programming_ECE_Lecture20.pdf

**Zhang, S. 2013.** *EU-China IoT Cooperation.* China: China Academy of Telecommunication Research (CATR), 2013. IoT Week 2013. p. 24. Workshop presentation slides. Accessed on: 24/11/2013. http://www.iot-week.eu/presentations/monday/international/06_EU-China%20Cooperation%20-Xueli%20Zhang-%20CATR.pdf