APPROACHES TO THE INTERNET OF THINGS

[1]**Sorin BURLACU,** *PhD*
e-mail: sburlacu@amp.ase.ro
[2]**Corneliu GUȚU,** *PhD*
[3]**Răzvan Cătălin DOBREA,** *PhD*
*e-mail:*svegombos@yahoo.com.sg
[4]**Dumitru-Alexandru BODISLAV,** *PhD*
e-mail: alexandru.bodislav@gmail.com
[5]**Svetlana PLATAGEA GOMBOS ,** *PhD Student*
e-mail: cgutu@mail.com
[1, 3, 4,5] *Bucharest University of Economic Studies*
6 Piata Romana, 1st district, Bucharest, 010374 Romania
[2]*Academy of Economic Studies of Moldova, Republic of Moldova*

Abstract. *Today, the Internet provides access to information and content by connecting multiple devices, such as PCs, smartphones, or TVs, to Internet sites. The next evolution will make it possible to access information related to the environment using connected objects, able to understand the environment using sensors and to communicate with each other with or without human intervention. The evolutions registered at the level of the whole society, generated by the continuous progress of the field of information and communication technology, as well as by the success of the superior exploitation of resources, of the realization of new products and of the efficiency of daily activities, occur through IoT implementation. Undoubtedly, IoT creates a number of advantages such as: increased efficiency, reduced energy consumption, simplification of processes and activities, easy and simultaneous access to multiple resources, increased reliability. Through this article we intend to present a series of aspects regarding the Internet of Things with direct implications in the business environment but also in public administration.*
Keywords: *internet of things, management*

JEL CLASSIFICATION*: F63, L86*

INTRODUCTION

We live in a world of "connected" objects capable of communicating with each other or with us, collecting, analyzing, transmitting a lot of information, sometimes so much that we wonder if there are not too many. From the creation of Internet-based applications to the present day, they have undergone a series of transformations until the phenomenon known as the Internet of Things. It is essential to understand the differences between applications that traditionally use Internet resources and the collection of tools that make up the IoT to understand the phenomenon studied, its main applications and those that are already used.

During the first 40 years of use of the Internet, it has been used mainly to connect people by exchanging emails, discussion forums and growing lately, through the sites of social networks that collect and distribute information and data. It should be noted that today the Internet is used to connect devices, machines and other things through wireless and wired networks, thus creating a new position called the Internet of Things [Dutton, 2005].

THE STAGE OF KNOWLEDGE IN THE FIELD

The term "Internet of Things - Internet of Things" was first used in 1999 by Ashton, one of the pioneers of British technology has helped develop the concept. It is pertinent to mention that the applicability and sophistication of these technologies are enough to see it as an innovation in the field of ICT and in the use of the Internet [Gubbi, Marusic & Palaniswami, 2013].

The Internet of Things aims to extend to the physical world the constant ability to connect and distribute data and remote control among other capabilities [Peoples, 2013]. To achieve this performance, the Internet of Things captures many permutations of detecting, marking or identifying things, such as by *identifying radio frequencies* - RFID, barcodes, fast response codes - QR, sensors, through the Internet for purposes such as identifying, monitoring, detecting or operating other devices that are *online*. These technologies allow products or other objects to store, send, and receive information in a way that can transform the way people do things and justify the Internet of Things as a new technological concept [Dutton, 2014].

Due to the rapid growth of technologies towards IoT, several definitions are presented in the current literature, presenting some difficulties in defining what this set of tools really means to understand its central ideas, the social, economic and technical implications that may arise through its implementation and use [Zorzi, Gluhak, Lange & Bassi, 2010; Vasseur, Agarwal, Hui, Shelby, Bertrand & Chauvenet, 2011; Dutton, 2014; Saxby, 2015].

The reason for these difficulties is present in the syntactic interpretation of the term Internet of Things, which deals with two concepts capable of leading to different interpretations in which the first term, the Internet, leads to a vision of the network that the Internet of Things is able to generate. while the second term, objects, leads to a vision aimed at something generic that can be integrated into a more familiar landscape [Atzori, Iera & Morabito, 2010].

Given the context developed so far, it is assumed that the union of terms and their presentation as the Internet of Things, creates a meaning that breaks down the barriers of innovation in modern communication. Thus, the Internet of Things translates into a global network of unique interconnected things, based on standard communication protocols [Li, Da Xu & Zhao, 2014].

Such a reality is built around an indefinite number of objects involved in the process, resulting in the collection, exchange, storage and interpretation of information from multiple sources that come from the activities of humans and machines, leading directly to a new way of looking at these technologies. -an perspective oriented towards the Internet of Things [Ashraf & Habaebi, 2015].

Atzori et al. [2010] emphasize that IoT is represented by the paradigm given by the convergence points of these three visions, as shown in Figure 1.

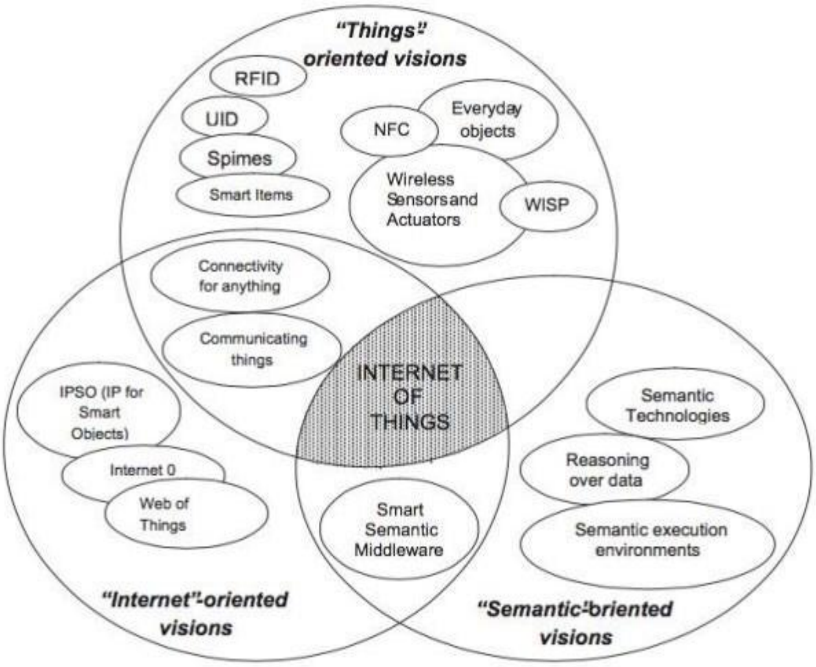

Figure 1.Visions on the Internet of Things
Source: Atzori, et al., [2010].

The first vision presents a things-oriented perspective. It is a vision seen by the authors as a more simplistic, since it is concerned with initial elements that can be considered basic, such as RFID - Radio Frequency Identification [identification by radio frequency] wireless sensor, NFC - Near Field Communication, making them, key elements for the full implementation of the IoT vision. However, IoT has a larger and more complex condition than the idea of a simple identifier of things. According to Presser, Barnaghi, Eurich and Villalonga [2009] RFID technology is seen as one of the core technologies of IoT. This perception is attributed to the low cost of technology and its stability, factors that make technology suitable in industry and business. However, there is a wide range of devices, networks and services, technologies that build IoT.

In this sense, a perspective oriented towards things that go beyond RFID, presented by the United Nations - UN that predicts the emergence of IoT as a reality based on ambiguity, in which people can become the minority compared to devices on traffic generators and receivers' network. Such changes are made possible by the advent of IoT and the network of smart devices in everyday life that it will be able to support [Botterman, 2009]. Similarly, other relevant institutions have emphasized the concept that the Internet of Things tends to be mainly focused on objects and that the solution to full implementation must start with the growth of smart devices. In favor of this concept, in the IoT study appears the term *spime*, defined as an object that can be traced through time and space throughout its existence, with a model of self-support and can be uniquely identified in the network [Atzori et al., 2010].

Although its definition is presented in a generic way and in a theoretical way, *spime* will be implemented in the real world with its extended functionalities, in which devices are popularly called smart objects that are not limited to location, wireless communication and can be pursued as described in the initial concept, but acquiring memory and training capacity, the ability to sustain themselves autonomously, proactivity, environmental and context awareness, collaborative communication, among other skills that vary depending on the applicability of the intelligent object [Atzori et al., 2010; Vasseur, Agarwal, Hui., Shelby, Bertrand & Chauvenet, 2011].

Constant innovations in these technologies have paved the way for a new vision of the IoT, in which connectivity that is available to anyone will also be available to any object [Strategy & Unit, 2005]. Such a vision of the Internet of Things is similar to the vision presented by the European Commission in which objects with virtual identity and personality operate in intelligent spaces, using intelligent interfaces to connect and communicate with the user's social, environmental context [Li et al., 2014].

In a second, Internet-oriented vision, the IoT effort is geared toward creating smart environments, where things can automatically communicate with each other or with others, improving existing products and services and providing new ones to brings benefits to society.

Vasseur and Dunkels [2010] propose a concept of intelligent environment based on a vision of the Internet of Things as a global infrastructure to which objects are physically and virtually connected, which may include existing networks, new developments that the Internet will go through.

In this sense, IoT becomes a generator of an environment called intelligent environment, with the natural ability to implement services and applications characterized by a high level of data and information management in an autonomous and uninterrupted way. Such features appear as the link that connects the first, thing-oriented vision to the second vision that centralizes the Internet in the IoT concept. As regards the third version, the oriented semantics is concerned with issues of how to collect, store, access, search and organization of information generated by the Internet of Things, arguing that the challenges listed in these actions to be included in discussions primary in relation to IoT, due to the complexity and challenges associated with it. In this context, semantic technologies could play a key role, becoming crucial elements in the construction of solutions capable of searching and modeling data and information generated by IoT, building and activating the interpretation and communication structure of the Internet of Things [Atzori et al., 2010].

Confronted with different visions of a whole that constitutes the Internet of Things, this paper adopts the definition of Li et al., [2014] which defines IoT as a set of applications developed for the Internet, based on physical objects and the environment integrated into the information network. The Internet of Things consists of protocols and related technologies that allow different elements to communicate through electronic communication channels, wired or wireless, through a data network and exchange of information composed of things and people [Valéry, 2012].

Therefore, as Dutton [2014] pointed out, IoT stands out because it allows electronic information to be transmitted by objects, as if it were moving through space, in a manner similar to wireless networks that transmit electronic signals, creating a new dimension for internet design and utility.

FEATURES OF THE INTERNET OF THINGS

Abdmeziem, Tandjaoui, Romdhani [2016] argue that the most important features of the Internet of Things are the following:

• *Distributivity:* The Internet of Things will evolve in a highly distributed environment. Data will be able to be collected from different sources and processed by several entities in a distributed way;

• *Interoperability*: devices from different vendors will need to cooperate to achieve common goals. Systems and protocols will need to be designed in a way that allows objects [devices] from different manufacturers to exchange data and work in an interoperable way;

• *Scalability:* Billions of objects are expected to be part of the network in the Internet of Things. Thus, systems and applications running at the top of the network will have to manage an unprecedented volume of data;

• *Deficit of resources:* both energy power and computing resources will be extremely limited;

• *Security*: the existence of an unknown external control will generate frustration among users, which would be a serious impediment to the implementation of the Internet of Things.

INTERNET OF THINGS APPLICATIONS

For the general public, today, the Internet of Things appears as a mixture of home applications and smart industrial elements [Bassi & Horn, 2008]. But in fact, it has the potential to have a much wider applicability. Only when the connected world becomes a reality will the Internet of Things transform almost all-important segments - from homes to hospitals and from cars to cities. Most of these points are called "smart", such as Smart Home or "connected" such as Connected Health. Currently, the main applications in the field of the Internet of Things include:

• *Smart Home / Home automation*: the concept of smart home presents the connectivity inside homes. This includes thermostats, smoke detectors, light bulbs, appliances, entertainment systems, windows, doors, locks and more. Among the best known organizations involved in the field are Nest, Apple, Philips and Belkin;

• *Wearables*: whether it's Jawbone Up, Flex Fitbit or Apple SmartWatch, easy-to-wear devices represent the majority of devices in the field of consumer Internet applications;

• *Smart City*: The smart city covers a lot of use cases, from traffic management to water distribution, environmental monitoring, waste management and urban security. Smart City solutions promise to come to offer help in solving the problems faced by city dwellers. These issues include: traffic congestion, reducing noise and environmental pollution and supporting urban safety;

• *Smart grid*: the smart grid promises to use information about the behavior of electricity suppliers and consumers in an automatic way to raise the level of efficiency, reliability and economy of electricity;

• *Industrial Internet:* Market research, such as Gartner or Cisco, considers the industrial Internet to be the concept with the highest potential in the field of the Internet of Things.

Applications include, but are not limited to, smart factories or connected industrial equipment;

• *Connected cars:* there is real competition for the car of the future. Whether it's self-driving or simply an assisted driver, connecting to other cars, mapping or traffic control services will play a key role. The next generation of in-vehicle multimedia systems and remote monitoring are also interesting concepts to consider. A number of major manufacturers, which play an important role such as: Google, Microsoft and Apple, have developed platforms dedicated to connected cars;

• *Connected health [Digital Health / Telehealth / Telemedicine]:* the concepts of smart medical devices and connected health system have a huge potential, not only for organizations but also for the well-being of beneficiaries in general. New types of tools for real-time health monitoring and improvement of medical decisions based on large amounts of patient data are some of the expected benefits;

• *Smart Retail:* Proximity-based advertising, in-store shopping behavior, or smart payment solutions are just a few of the concepts of the Smart Retail Internet of Things;

• *Smart supply chain*: supply chains are becoming much smarter. Solutions for tracking goods in real time or for exchanging information between suppliers are some of the applications in the supply chain, which are part of the Internet of Things;

• *Smart agriculture*: Carrying out agricultural activities remotely and the ability to monitor as many animals as possible make agriculture an interesting field for the application of the Internet of Things.

CHALLENGES OF THE INTERNET OF THINGS

The evolving nature of the IoT in terms of technologies and features, as well as new ways of interacting with the Internet of Things, have given rise to certain threats and challenges. The Internet of Things faces the technological challenges [Friedmann, Floerkemeier, 2010] highlighted below:

Scalability: The Internet of Things has a much wider potential global scope than the conventional Internet. But things are mainly cooperating in a local environment. So, key functionalities such as communication and service discovery must work just as well and efficiently in both environments, both large-scale and small-scale.

Acceptance and operation: Smart objects used on a daily basis should not be perceived as computers requiring their users to configure and adapt them to certain situations. Mobile objects, which are often used only sporadically, need to design connections at random and organize and configure to suit their specific environment.

Interoperability: just as the world of physical objects is very diverse, in the Internet of Things each type of smart device has different capabilities for processing and communicating data. Smart objects can be subjected to very different conditions, such as available energy and the bandwidth required to communicate information. However, in order to facilitate cooperation and communication, common standards and practices are needed. This is especially important for device addresses. These devices should follow a standard scheme, if possible, in line with the lines of the IP standard used in the field of conventional Internet.

Discovery: in dynamic environments, services for things must be automatically identified, which requires appropriate semantic means to describe their functionality. Users may want to receive product-related information and use search engines that can find things or provide information about the status of an object.

Software complexity: Although smart object software systems operate with few resources, smart network management and background servers are required for smart object management and support services, as are conventional integrated systems.

Data volumes: While some scenarios involve short, low-frequency communication, others, such as sensor networks, logistics, and large-scale "real-world awareness" scenarios require impressive volumes of data on central nodes or servers. network.

Interpretation of data: Supporting users of intelligent objects involves interpreting as accurately as possible the context determined by local sensors. In order for service providers to take advantage of the disparate data that will be generated, it must be possible to draw some conclusions from the interpreted data from the sensors. However, generating useful information from raw data from sensors that can trigger an action accordingly is by no means an easy action.

Security and privacy of personal data: In addition to the security and protection of the Internet, familiar to most users [such as the confidentiality of communications, the authenticity and credibility of communication partners, and the integrity of messages], there are other requirements that are important in the Internet of Things. For example, a user may allow things to have selective access to certain information or services or may prevent them from communicating with other things at certain times or in an uncontrolled manner; commercial transactions involving smart objects would need protection against unauthorized access by competitors to the market.

Error tolerance: the world of objects is much more dynamic and mobile than the world of computers, there are situations that change quickly and in unexpected ways. However, users want to rely on objects that work properly. Structuring the Internet of Things in the most complete and reliable way possible requires multi-layered redundancy and the ability to automatically adapt to change.

Power supply: things are usually not powered by the grid, so their intelligence must be powered by a self-sufficient energy source. Although passive RFID transponders do not need their own power source, their functionality and range of communications are very limited. In many cases, mains batteries and power supplies are problematic because of their size and weight, and especially because of maintenance requirements. Unfortunately, battery technology is progressing relatively slowly, and power supply, ie the generation of electricity from the environment [using differences in temperature, vibration, air currents, light, etc.], is not yet well enough developed to meet energy requirements. of current electronic systems in most application scenarios. Energy saving is an important factor not only in hardware architecture, but also in software. There are already wireless sensors without batteries that can transmit their data from a distance of a few meters. Like RFID systems, they obtain the necessary energy, either remotely or from the measurement process itself, for example by using piezoelectric or pyroelectric materials to measure pressure and temperature.

Interaction and short-range communications: Wireless communications a few centimeters apart are sufficient, for example, if one object is touched by another object. If such short distances are involved, very little energy is required, the approach is simplified [often there is only one possible destination] and there is usually no risk of interception. NFC is an example of this type of communication. Like RFID, it uses inductive coupling. During communication, one partner is in active mode and the other can be in passive mode. Active NFC units are small enough to be used in mobile phones; Passive units are similar to RFID transponders and are much smaller, cheaper and do not need their own power source.

Wireless / wireless communications: from an energy point of view, wireless technologies such as GSM, UMTS, Wi-Fi and Bluetooth are much less appropriate; Newer WPAN standards such as ZigBee and others still under development may have narrower bandwidth, but they use significantly less power.

CONCLUSIONS

Although the Internet of Things is by far the most popular term used to describe the phenomenon of a connected world, there are other similar concepts [Aijaz & Aghvami, 2015]. Most of these concepts are similar in meaning, but have slightly different definitions. These concepts are presented below:

- *Machine to Machine (M2M):* The term has been used for over a decade and is well known in the telecommunications industry. Initially, M2M communication was a one-to-one connection that connects one machine to another. But now, the explosion of mobile connectivity has the effect that data can be more easily transmitted over an IP network to a much wider range of devices.
- *Industrial Internet*: The term industrial Internet of Things goes beyond M2M because it not only focuses on connections between machines, but also includes human interfaces.
- *Internet of Things (IoT):* The term IoT has extensive coverage, as it includes links beyond the industrial context, such as devices that are easy for people to wear.
- *Internet*: Connections are made only between people.
- *Web of Things*: The web of things has a much narrower scope compared to other concepts because it focuses exclusively on software architecture.
- *Internet to any (Internet of Everything – IOE):* The term Internet anything is still a vague concept. IoE aims to include all imaginable connections.
- *Industry 4.0*: The term Industry 4.0 is strongly supported by the German government, but is as limited as the industrial Internet because it focuses only on industrial

environments. However, this term has the widest scope of all concepts because it describes a set of concepts that underlie the next industrial revolution. The term Industry 4.0 includes all kinds of connectivity concepts, but goes even further to include real changes in the physical world such as 3D printing technologies, new augmented hardware reality, robotics and advanced materials.

REFERENCES

1. Ashraf, Q. M., & Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things. Journal of Network and Computer Applications, 49, 112-127.
2. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.
3. Bassi, A.; Horn, G. (2008): Internet of Things in 2020: A Roadmap for the Future. European Commission: Information Society and Media.
4. Botterman, M. (2009, May). for the European Commission Information Society and Media Directorate General. In Networked Enterprise & RFID Unit–D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic.
5. Chelcea, S. (2001) „Metodologia cercetării sociologice. Metode cantitative și calitative", București, Editura Economică, p. 70.
6. Friedemann, M., Floerkemeier, C.(2010) From the Internet of Computers to the Internet of Things. In Sachs, K., Petrov, I., Guerrero, P. (Eds): From Active Data Management to Event-Based Systems and More, Springer Berlin Heidelberg, 2010, pp. 242—259.
7. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.
8. Dutton, W. H. (2005). The Internet and social transformation: reconfiguring access. Transforming enterprise: The economic and social implications of information technology, 375397.
9. Dutton, W. H. (2014). Putting things to work: social and policy challenges for the Internet of things. info, 16(3), 1-21.
10. Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.
11. Peoples, C., Parr, G., McClean, S., Scotney, B., & Morrow, P. (2013). Performance evaluation of green data centre management supporting sustainable growth of the internet of things. Simulation Modelling Practice and Theory, 34, 221-242.
12. Presser, M., Barnaghi, P. M., Eurich, M., & Villalonga, C. (2009). The SENSEI project: Integrating the physical world with the digital world of the network of the future. IEEE Communications Magazine, 47(4), 1-4.
13. Saxby, S. (2015). The 2014 CLSR-LSPI Lisbon seminar on 'the digital citizen'–Presented at the 9th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) 15– 17 October 2014, Vieira De Almeida & Associados, Lisbon, Portugal. Computer Law & Security Review, 31(2), 163-180.
14. Vasseur, J., Agarwal, N., Hui, J., Shelby, Z., Bertrand, P., & Chauvenet, C. (2011). RPL: The IP routing protocol designed for low power and lossy networks. Internet Protocol for Smart Objects (IPSO) Alliance, 36.
15. Vasseur, J. P., & Dunkels, A. (2010). Interconnecting smart objects with ip: The next internet. Morgan Kaufmann.
16. Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's intranet of things to a future internet of things: a wireless-and mobility-related view. IEEE Wireless Communications, 17(6).