Internet of Things New Challenges in Distributed Artificial Intelligence

Maroua Ahmid¹, Okba Kazar¹, Souraya Hamida¹, Laid Kahloul¹ and Parisa Ghoudous²

Abstract—The Internet of Things as global information architecture emerges on the Internet by facilitating the exchange of services is gradually developing. At that time, the technology of Internet of Things is still under discussion. Internet-of-Things envisions a future in which digital and physical entities can be linked, through information technology and appropriate communication. In this paper, we present a study of technologies, applications and research challenges for the Internet of Things.

Keywords— Web, Internet of Things, web service research, security.

I. INTRODUCTION

The combination of technologies and Internet, such as near-field communications, location in real time and embedded sensors allows us to transform everyday objects into intelligent objects that can understand and respond to their environment. These objects are building blocks for Internet of Things. This last is a concept in which the virtual world of information technology integrates seamlessly with the real world of objects.

The rest of the paper is organized as follows. In Section 2, we introduce the different definition of Internet of Things. The main Internet of Things technologies are the subject of Section 3, while the descriptions of the main applications are addressed in Section 4. Section 5 gives a look at the outstanding issues on which research should focus, emphasizing on topics such as authentication, security, and privacy. Conclusion is given in Section 6.

II. DEFINITION

Haller / Karnouskos / Schroth define the Internet of Things as "a world in which physical objects are perfectly integrated into information network, and where physical objects can become active participants in the business process. Services are available to interact with these smart objects on the Internet, query their state and any information associated with them, taking security and privacy issues into account."[1] [4]

The CERP-IoT “Cluster European research projects on the Internet of things” defines the Internet of things like: “a dynamic infrastructure of a global network. This global network has ability of auto-configuration based on standards and communication protocols interoperable. In this network, physical and virtual objects have identities, physical attributes, virtual personalities and intelligent interfaces, and they are integrated into the network in a transparent manner "[3] [9]

III. THE REQUIRED TECHNOLOGIES

The update of IoT concept in the real world is possible through the integration of several enabling technologies. In this section, we discuss the most relevant. Note that it is not our goal to provide a comprehensive study of each technology. Our main objective is to provide a picture of the role they likely play in the IoT. [6].

3.1 Identification and Technologies of Detection and Communication

- Radio Frequency Identification RFID: RFID is a generic term for technologies that use radio waves to automatically identify people or objects. [1] [2]. There are several methods of identification, the most common is to associate the unique identifier of the RFID label with an object or a person. An RFID system typically includes the following elements:
  - An RFID device (label);
  - a reader of label with an antenna and transmitter-receiver;
  - a host system or the connection to an enterprise system [ 2]
- Near Field Communication (NFC): is a technology that allows a device to communicate with another at a maximum distance of approximately 20 cm or less [7]. Near Field Communication (NFC) is a specification for communication between two devices without contact. NFC is based on the technology used for RFID. NFC is intended to make it easier and more practical to make transactions, exchange of digital content, and connect electronic devices with a key [ 10]
- Sensor Network: a network of sensors is composed of a large number of sensor nodes, which are deployed at high density on the inside of the phenomenon to monitor or very near to him. Take advantage of the idea of sensors networks based on collaborative effort of a large number of nodes. The sensor networks represent a significant improvement over traditional sensors, which are deployed in the two following ways:
  - Sensors can be placed far from the genuine phenomenon, that is, a thing known by the sensory perception. In this approach, large sensors that use some complex techniques to distinguish the targets of noise in the environment are needed.

¹LINFI, Mohamed Khaid University, Biskra, Algeria
²LIRIS, National Institute of Applied Science of Lyon, Lyon, France.
Several sensors that perform only can be deployed for detection. The positions of sensors and communication topology are carefully designed. They transmit the time series of the phenomenon detected to the central nodes where the calculations are performed and the data are merged. [8]

3.2 Middleware

The middleware is a software layer or a set of sub-layers interposed between the technologies and application. Its functionality to hide the details of different technologies is fundamental to exempt the programmer from issues that are not directly related to his point of view, which is the development of the specific application enabled by IoT infrastructure [6]

- The applications are on the top of the architecture, the export all the functionality of the system to the end user. [6]
- Service composition: This is a layer provides the functionality for the composition of the services offered by simple objects in network to create specific applications. On this layer there is no concept of devices and the only assets are visible services. [6]
- Services management: This layer provides the main functions which should be available for each object and who allow their management in the scenario of the IoT. A set of basic services includes: the dynamic object, status monitoring, discovery and configuration of the service. [6]
- Object abstraction: the IoT is based on a broad and heterogeneous set of objects, each of them providing specific functions accessible via its own dialect. There is therefore the need for a layer of abstraction capable of harmonizing access to various devices with a common language and of the procedure. [6]

IV. APPLICATIONS

Potential offered by the IoT make possible the development of a large number of applications, of which only a very small part is currently available for our society. Many are the domains and the environments in which new applications would be likely to improve the quality of our lives: at home, traveling, when sick, to work, these can be grouped in the following domains: [6]

4.1. Transportation and Logistics Domain

Advanced cars, trains, buses as well as bicycles along with roads and/or rails are becoming more instrumented with sensors, actuators, and processing power. Roads themselves and transported goods are also equipped with tags and sensors that send important information to traffic control sites and transportation vehicles to better route the traffic, help in the management of the depots, provide the tourist with appropriate transportation information, and monitor the status of the transported goods. [6]

In this area the IoT will support the current efforts around the intelligent vehicles in the service of the road safety and the driving assistance. This will focus on the communication inter-vehicle and between vehicles and road infrastructure.

The IoT will provide a natural extension of "intelligent transportation systems" and their inputs in terms of road safety, comfort, effectiveness of the management of traffic and economy of the time and energy. [3]

4.2. Healthcare Domain

Many are the advantages provided by the IoT technologies for this domain and the applications that will result can be grouped mainly in: the tracking of objects and persons (staff and patients), the identification and authentication of persons, and automatic data collection and sensing. [6] the IoT will enable the deployment of personal networks for the control and monitoring of clinical signs, particularly for the elderly. This will allow as well to facilitate remote monitoring of patients in homes, and to provide solutions for the autonomy of persons with reduced mobility. [3][5]

4.3. Smart Environments Domain

The intelligent environment is that make his "employment" easy and comfortable thanks to the intelligence of the contained objects, whether it is an office, a home, a factory, or a environment of leisure. [6] the IoT will enable better management of the various networks that feed our cities (water, electricity, gas, etc.) by allowing a continuous monitoring in real time and precise [3][5]

The technology of the IoT can be properly applied to the monitoring of the application environment. In this case a key role is played by the detection capability, in a distributed model and the self-management of the mode, the natural phenomena and processes (e.g., temperature, wind, precipitation, the height of the river). [5]

4.4. Personal and Social Domain

The applications falling within in this area are those that allow the user to interact with other people to maintain and strengthen the social relations. In effect, things can automatically trigger the transmission of messages to friends to allow them to know what we are doing or what we have done in the past, such as moving from/to our house/office, travelling, meeting some common mates or playing soccer [6]

V. THE CHALLENGES AND PROBLEMS

5.1. Authentication

Identification each object must be identifiable. Depending on the specific scenarios, the objects may need to be uniquely identified, or to be identified as belonging to a given class (f., ex., this object is a pen, whatever the pen is). [5] authentication is difficult in the IoT because it requires authentication infrastructures appropriate which will not be available in the scenarios of the IoT. In addition, the objects have limited resources in relation to the communication devices and current computing. [6]

5.2. Security and Confidentiality

In the case of the IoT, the security and privacy becomes even more crucial that their support becomes more difficult. The reasons for these difficulties came from for both the
quantity and the sensitivity of the data that will be generated and flows through the network, and the limits of computing and communication devices that will be included in the IoT and who are therefore much more vulnerable to all kinds of attacks of security and confidentiality. [11].

3.5. Cloud Computing

Integrated IoT and the cloud computing applications allowing for the creation of intelligent environments must be able to combine the services offered by multiple stakeholders and evolve to support a large number of users in a reliable system and decentralized manner. They must be able work in the two environments of wired and wireless network and deal with the constraints, such as the access devices or data sources with limited power and unreliable connectivity. The cloud application platform need to be improved in order to support the rapid creation of applications by providing the tools for programming specific to the field and environments and seamless execution of applications exploiting the capacity of several of dynamic resources and heterogeneous to meet the requirements of quality of service of different users. [12].

VI. Conclusion

The Internet has radically changed the way we live, the IoT has the potential to add a new dimension to this process by enabling communications with and between the intelligent objects, thereby leading to the vision of (at any time, anywhere, any media, any things) communications.

In this paper, we have studied the most important aspects of the IoT by putting the emphasis on what is fact and what are the issues that require a more thorough search.

REFERENCES

http://dx.doi.org/10.1007/978-3-642-11710-7

http://dx.doi.org/10.1016/j.cose.2005.12.003


http://dx.doi.org/10.1016/j.adhoc.2012.02.016

http://dx.doi.org/10.1016/j.comnet.2010.05.010


http://dx.doi.org/10.1016/S1389-1286(01)00302-4