This is the final version of the paper accepted for publication in Ad Hoc Networks , Elsevier, 2016.
DOI: http://dx.doi.org/10.1016/j.adhoc.2016.12.004

Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm

Luigi Atzori, Antonio Iera, Giacomo Morabito

***Abstract*—The high penetration rate of new technologies in all the activities of everyday life is fostering the belief that for any new societal challenge there is always an ICT solution able to successfully deal with it. Recently, the solution that is proposed almost anytime is the "*Internet of Things*" (IoT). This apparent *panacea* of the ICT world takes different aspects on and, actually, is identified with different (often *very* different) technological solutions. As a result, many think that IoT is just RFIDs, others think that it is sensor networks, and yet others that it is machine-to-machine communications. In the meanwhile, industrial players are taking advantage of the popularity of IoT to use it as a very trendy brand for technology solutions oriented to the consumer market. The scientific literature sometimes does not help much in clarifying, as it is rich in definitions of IoT often discordant between them.**

Objective of this paper is to present the evolutionary stages, i.e., *generations*, that have characterized the development of IoT, along with the motivations of their triggering. Besides, it analyzes the role that IoT can play in addressing the main societal challenges and the set of features expected from the relevant solutions. The final objective is to give a modern definition of the phenomenon, which *de facto* shows a strong pervasive nature, and, if not well understood in its theories, technologies, methodologies, and real potentials, then runs the risk of being regarded with suspicion and, thus, rejected by users.

I. Introduction

Years have passed since the Internet of Things (IoT) has appeared on the scene becoming one of the major research and industrial subjects in the Information and Communications Technology (ICT) arena. The IoT term appears so frequently in so many contexts as rarely happened in the past to other ICT themes, so as to raise the doubt whether it is more a "trendy" name, speculatively ridden to increase the attention on studies and products around mature technologies, rather than a real element of technological discontinuity. This doubt comes also from the fact that, in spite of its huge success, what IoT really represents is not completely clear. This is mostly due to the fact that several works in the literature associate the idea of IoT to some of its building blocks only rather than to a complete combination of all the necessary elements. This is the case, for instance, of platforms that just use RFID for global traceability of goods, algorithms for new intelligence and pervasive computing solutions, network architectures based on IP protocols (especially IPV6) enhanced to support resource constrained devices, and proposals for novel application protocols to collect sensed data from wireless sensor networks. Indeed, the numerous proposals that just touch some of these disparate issues do not offer a complete picture of IoT, as it will be elaborated in Section VII. All this noise around the phenomenon has increased the confusion so that it has become necessary to shed light on it and come to a definition, shared by the whole community, of what IoT is and what is not.

Some researchers [1] [2] are inclined to think that the idea of IoT has its roots back in the late nineteenth century, when Nikolas Tesla theorized that

> "*When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, [...] and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone*"
> (Nikola Tesla, Teleautomation).

Maybe it is a little excessive to assume that the undoubted genius and visionary nature of Tesla allowed him to imagine the Internet of Things so many years ago, but certainly, from that date on, he and many others helped forming the idea of IoT by starting from a clear knowledge of current technologies and making a leap into the future. To name a few, it is the case of Mark Weiser who defined Pervasive Computing and stated that "*The most profound technologies are those that disappear. They weave themselves into the fabrics of everyday life until they are indistinguishable from it*" [3], of Bruce Sterling who coined the SPIME neologism referring to an object "*by definition, the protagonist of a documented process [...] an historical entity with an accessible, precise trajectory through space and time*" [4], of Kevin Ashton who first used the term "Internet of Things" at that time focusing mainly on the RFID technologies.

The idea of IoT has, therefore, evolved over time and has undergone succeeding transformations that will predictably still continue over the next years with the advent of new enabling technologies. For instance, the advent of the new concepts, such as cloud computing, information centric networking, big data, social networking, have already partially impacted and still are impacting the IoT idea and novel futuristic paradigms are already in the horizon (see [5], [6]).

This paper is motivated by the above considerations and aims at providing a careful analysis of the technologies that have contributed to the birth of the IoT and to its growth over the time.

The approach we follow to conduct the analysis of the Internet of Things paradigm is evolutionary in nature. Accordingly, we identify three main stages of evolution of the paradigm, each one characterized by key enabling technolo-

gies, major reference architectural solutions, and available products. The transition from one generation to the next is not only characterized by the introduction of new technologies and architectures complementary to those of the previous generation, but also by a distinctive approach to the design of the IoT. Notwithstanding, what is IoT today and what it will be in the future is, undoubtedly, the result of the convergence into the primary evolutionary path of all R&D experiences in several ICT domains, as shown in Figure 1 and described in the remainder of the paper.

To ease the reading, in Table I we summarize all the acronyms that are used throughout the paper. Additionally, in order to have a comprehensive view of all the technological fields involved in the evolution of the IoT over the three generations, in Table II we summarize the major objective for each addressed technological field, the key standards, and the representative scientific works.

The remainder of the paper is organized as follows. In Section II we describe how the IoT had the potential to play a key role in the solutions of most societal challenges. In the following Sections III, IV, and V we provide details of the major technical concepts and solutions proposed for each generation of the IoT. In Section VI we overview the technologies that will impact the evolution of the IoT in the next few years. In light of such upcoming evolutions, we elaborate on the concept of the IoT itself to reach a correct definition of the IoT paradigm in Section VII. Finally, in Section VIII we draw our final conclusions.

II. Role of IoT for Societal challenges

Our societies are facing many challenges and ICT can assume a pivotal role, with the raise of IoT systems taking a momentous responsibility in this process. An effective classification of the societal challenges is provided by the Horizon 2020 framework, which is the main program funding research and innovation activities in Europe [7]: health, demographic change and wellbeing; food security and sustainable agriculture; secure, clean and efficient energy; smart, green and integrated transport; climate action, environment, resource efficiency and raw materials; inclusive, innovative and reflective societies; secure societies.

In the following Section II-A we describe how IoT can play a key role in addressing the above societal challenges. Then, in Section II-B we describe how public authorities can support the adoption of IoT for the above purposes and discuss technical and non-technical barriers that still exist to the adoption of the IoT technologies.

A. IoT and societal challenges

The aging process of the working population puts the health and wellbeing issues among the top priorities in our society. Advancements in this area require the introduction of systems and technologies able to continuously monitor the status of the environment where people live, work, travel, and to acquire data about conditions of people themselves. The resulting information should be available everywhere to doctors, nurses, and relatives so that proper actions can be taken when needed. Automatic context-aware processes will be also activated, for instance to guide the patient in taking the right medicines. The IoT can play a key role in this context. However, this implies that its components should be ubiquitously embeddable in the environment, wearable so to constantly monitor human conditions, transparent as much as possible, and trustful in handling personal data in a secure way.

Food security and sustainable agriculture is aimed at making the best use of our biological resources. The smart farms built by exploiting the IoT paradigm represent major means to reach these goals. In a smart farm the status of the crop and terrain is always under control, many of the production procedures can be activated remotely by the farmer, sales can be synchronized with the production (as the time schedule of the crop can be shared with external systems), and the usage of resources matches the actual needs (thus, wastage are avoided). However, it is extremely important that the relevant systems are easy to deploy and use. Otherwise, the configuration and the maintenance costs may overcome the benefits.

Most countries have agreed on ambitious plans to reduce greenhouse gas emissions, increase the share of renewable energies, and improve energy efficiency. Achieving these objectives would advance our society along the path to sustainability. IoT technologies will take a major role in this context with the intent of delivering systems for automatic management of production and distribution of energy by means of sensors and actuators distributed across the whole chain, with the smart grid as one of the major application scenarios. Stringent QoS (quality of service) requirements characterize the management of power grids as immediate actions have to be taken upon failure detections. Additionally, the resulting network should be highly adaptive to match the time varying behaviour, which characterize both the renewable energy production systems and the energy consumption.

The challenge of a smart, green and integrated mobility is enabling a transportation system that is resource-efficient, environment-friendly, safe and seamless for the benefit of all citizens and of the economy. This is the area where IoT has taken its first steps, since RFID tags have been massively used to track goods and improve the efficiency of transport and logistics procedures. Indeed, real-time information processing technology based on RFID and NFC can implement real-time monitoring of almost every segment of the supply chain. By obtaining information related to products promptly, timely, and accurately, either a single enterprise or even the whole supply chain can respond to intricate and changeable markets in the shortest time. It is a matter of fact that the era of seemingly plentiful and low cost natural resources is coming to an end: sources of raw materials, water and air, as well as terrestrial, aquatic and marine ecosystems are all under pressure. As a consequence, there is a need for decoupling economic growth from resource usage. An IoT challenge in this direction is to support green economy activities. An exemplary application is the automatic management of the energy consumption in smart cities so that the waste of energy resources is limited if not completely avoided. To this end, IoT systems should be able to become aware of the environment through a sort of distributed intelligence and take appropriate local decision on

Acronym	Description
ALE	Application Level Events
API	Application Programming Interface
CCN	Content-Centric Networking
CoAP	Constrained Application Protocol Working Group
CoRe	Constrained RESTful Environment Working Group
CoT	Cloud of Things
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name Service
EPC	Electronic Product Code
EPCIS	EPC Information Service
EUI-64	64-bit Extended Unique Identifier
ETSI	European Telecommunication Standards Institute
FP7	Seventh Framework Program of the European Union
HTTP	Hypertext Transfer Protocol
ICN	Information Centric Networking
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IoE	Internet of Everything
IoT	Internet of Things
IoT-A	IoT-Architecture
IP	Internet Protocol
IPv6	Internet Protocol version 6
LLRP	Low Level Reader Protocol
LR-WPAN	Low Rate Wireless Personal Area Networks
M2M	Machine-to-Machine
NDN	Named Data Networking
NFC	Near Field Communications
ONS	Object Naming Service
PaaS	Platform as a Service
PSI	Publish-Subscribe Internet
REST	REpresentational State Transfer
RESTful	that follows REST principles
RFID	Radio-Frequency Identification
SAaas	Sensing and Actuation as a Service
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SNS	Social Networks Service
SOA	Service Oriented Architecture
SR	Super Router
SSN	Semantic Sensor Network
TaaS	Thing as a Service
TCP	Transmission Control Protocol
TEDS	Transducer Electronic Data Sheets
UDP	User Datagram Protocol
URI	Universal Resource Identifier
URL	Uniform Resource Locator
VE	Virtual Entity
WISP	Wireless Identification and Sensing Platforms
WoT	Web of Things
WSAN	Wireless Sensor and Actuator Networks
WSN	Wireless Sensor Networks
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks

TABLE I
LIST OF ACRONYMS USED THROUGH ALL THE PAPER.

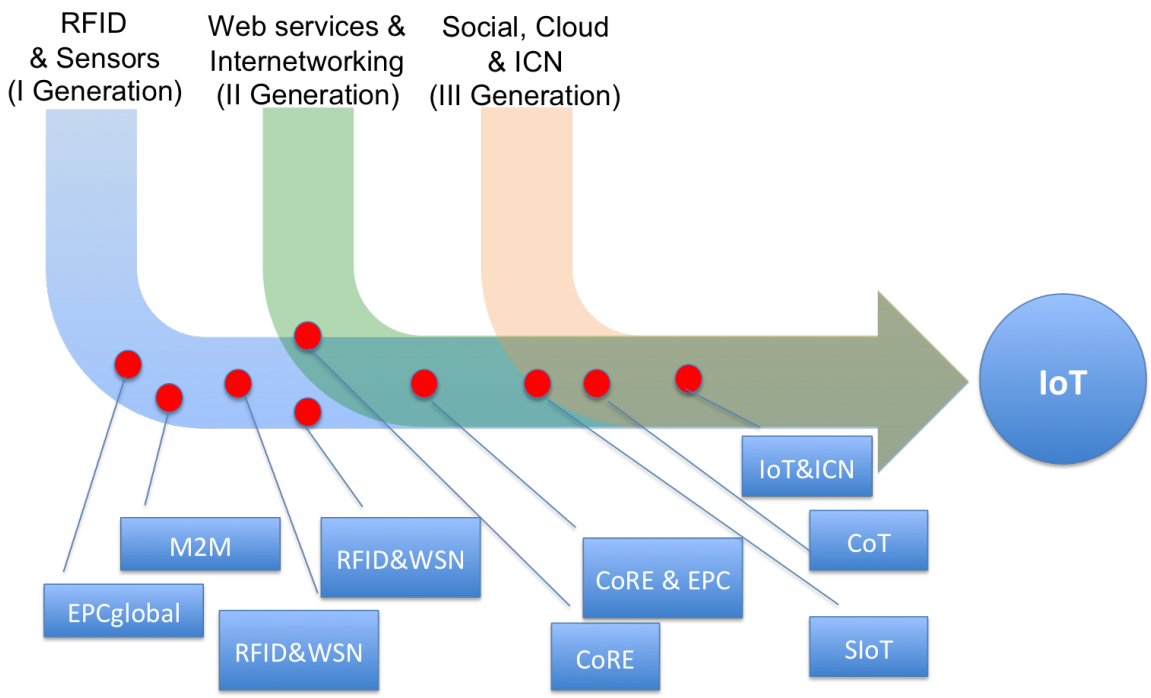

Fig. 1. Evolution of the IoT.

Generation	*Technological fields*	*Major objectives*	*Relevat standards*	*References*
I	**Tagged objects**	To uniquely identify objects through appropriate naming and architecture for the retrieval of objects' associated information	EPCglobal	[38], [42]
	Machine-to-Machine (M2M)	To define a reference architecture for machine-to-machine communications	oneM2M, ITU-T FS M2M	[44]
	Integration RFID with WSN	To seamless combine data coming from RFID tags with data generated by sensors connected through WSNs	*Missing*	[47], [16]
II	**Internetworking**	To allow constrained devices to adopt the TCP/IP protocols for a seamless integration in the Internet	IETF 6LoWPAN, ROLL RPL, IEEE 802.15.4	[54]
	Web of Things	To allow constrained devices to take part to web communications	IETF CoAP, OASIS DPWS	[26], [58], [59]
	Social network services	To allow people to share data generated by their smart objects with people they know and trust, leveraging the existing human social networks services	*Missing*	[27], [66], [67]
III	**Social Internet of Things**	To make objects able to participate in communities of objects, to create groups of interest, and to take collaborative actions with the objective to facilitate service and information discovery	*Missing*	[75], [77]
	Semantic	To describe the features of the IoT objects to foster systems interoperability	W3C SSN	[78], [79]
	Future Internet	To introduce the Information Centric Networking feature into the IoT world so as to introduce content centric-driven rather than host-driven communications	IETF ICNRG	[81], [86], [87]
	Cloud	To empower objects with storage, communications and processing capabilities coming from the cloud	*Missing*	[96], [98]
	Evolved RFID-IoT integration	To facilitate the integration of the RFIDs into the IoT applications	*Missing*	[100], [103]

TABLE II

THE THREE IOT GENERATIONS: MAJOR OBJECTIVE FOR EACH ADDRESSED TECHNOLOGICAL FIELD, KEY STANDARDS AND REPRESENTATIVE SCIENTIFIC WORKS.

Societal challenges	IoT major contribution	IoT systems desired features
Health and wellbeing	Monitoring of the people health and quality of life	Pervasivity Transparency Wear-ability Security
Food security and sustainable agriculture	Smart farms	Usability Sustainability
Secure, clean and efficient energy	Smart grids	Stringent QoS Adaptivity
Smart, green and integrated transport	Management of logistics issues	Interoperability
Climate action, environment, resource efficiency and raw materials	Smart management of energy consumption in smart cities	Distributed local awareness
Inclusive, innovative and reflective societies	Provide the opportunities to create new applications and businesses in an easy way to everybody	Available to every one Open data Open process Participation Transparency Collaboration
Secure societies	Automatic detection of malicious behaviors	Security Trustworthiness

TABLE III
EXPECTED MAJOR CONTRIBUTIONS OF THE IOT SYSTEMS IN ADDRESSING THE SOCIETAL CHALLENGES AND DESIRED FEATURES.

the energy usage.

Our society is also facing a number of important economic and political challenges posed by global interdependencies and unprecedented transformations. These strongly affect its capacity to ensure economic growth, high employment levels, and social stability. However, it suffers from sluggish growth, difficulties to effectively implement structural reforms in favour of innovation and employment, and increasing scepticism among citizens, especially young people. The revolution of having our physical world at our hands through the network, introduces huge opportunities for innovators and new entrepreneurs for the benefit of the whole society. However, the relevant technologies should be available to anybody, should be easy to understand. Thus, schools will assume a fundamental role, as they will be the places where innovations are taught to everybody. Additionally, the data generated by these systems have to be available to everybody; also the process should be open to foster the interoperability and reutilization of the services, especially those deployed by public authorities.

Security is one of the major concerns in our society, and in this respect IoT systems are involved from two different points of view. First, pervasiveness of the IoT deployments will imply that trillions of objects will be observing us in our daily activities; these must be designed so that the collected data is used in the most reliable and secure way. Second, IoT systems themselves will be used as an effective tool in support of the security of our society as the connected smart things should be able to collect data about malicious behaviours in both the digital and physical worlds. Additionally, IoT systems should be trustable, i.e., they should provide the requested services at the needed quality of service. Even more important, they should be perceived as trustable, i.e., it is necessary that people feel that IoT systems handle their data by preserving freedom and security, like it is happening with cloud services that almost everybody uses without caring about security.

Table III summarizes the described challenges and the corresponding required IoT features and possible contributions to their overcoming.

B. Role of public authorities and barriers to the adoption of IoT solutions

In the contexts we have described above, public authorities must play a key role in actively driving innovation. This may happen in different ways:

- **Forcing the diffusion of open IoT data and processes**: as already mentioned, produced data and relevant services should be available to the external world, for other public or private activities. There are already rules that obligate public authorities to provide some data in an open way. However, incentives to make available data produced by private companies should be introduced as well, at least for the data relevant to the status of public environments.
- **Fostering the utilization of the IoT infrastructure in the city management**: for instance, multiple distributed sources available in the context of the open data, the big data and the smart city activities, can be managed, analyzed and visualized to understand urban development patterns [8];
- **Introducing regulatory changes**: the way the data is exchanged must be well-regulated to prevent any abuse.

IoT has still to face several challenges to be ready to play the pivotal role we expect.

First of all, it has to gain the trust of people. In fact, the idea of a smart world all around us, which observes our habits and modifies its behavior according to what we do, what we say, and (soon maybe) what we think, may scare people for several reasons:

- What if an IoT system controlling personal health related processes makes a mistake? We are accustomed to computers and smartphones malfunctioning (due to software or hardware failures). What if the above computers or smartphones are key players in ensuring our healthy life?

In other words, the IoT, with all relevant technologies, must prove to be robust and resilient.

- What if some hackers violate IoT systems to compromise the correct functioning of the processes governing our daily life? What if they steel our private data? There are many people worldwide who avoid any form of electronic payments for this type of fear. Are we sure that those people will consciously accept the risks associated to a violation of a pervasive IoT systems? Again, IoT must prove to guarantee security and privacy.
- How can an obscure technology be trusted by people who do not have a clue about its internal operations? This is a typical problem that technology faces: to be accepted they need people to build a mental model of their operations [9]. This can be done in two ways: by educating people or by deceiving them, that is by hiding the real operations behind the interfaces people are used to. Recall: many electronic digital appliances still have a knob to control their behavior.

Only when the IoT will be much more resilient, robust, secure, and easy to understand, people will trust it.

Additionally, IoT solutions must be practical. A smart environment enriched with a large number of sensors and actuators is an attractive prospect as long as people will not be required to periodically change the batteries on each of them. A lot of work has been done in this context, however, energetically autonomous smart sensors and actuators have not reached the maturity level required to fulfil the real needs of IoT applications. In other words,

advances are required in both the domains of energy efficiency and energy harvesting.

As a last remark,

people will accept the IoT if there are **applications justifying the presence of such an intrusive system around them.**

However, applications need developers and developers need clearly defined, easily programmable, hopefully extensible, and rarely changing APIs. Here, the diffusion of the RESTful model in the Web of Things domain is helping a lot although, like we have seen, the IoT keeps evolving and nobody can safely say that the APIs typical of a RESTful model are at the end of such an evolution. In this context, public bodies can play a fundamental role by at least taking clear and shared decisions on the open APIs to be used to access those data collected by sensors deployed with the taxpayers money and, thus, belonging to the collectivity.

Furthermore, a *naming scheme* must be decided. In fact, APIs allow interactions with IoT resources (objects, services, data servers, etc.) and, to this end, it is necessary to identify these resources. A lot of work on naming is being carried within the context of *Information-Centric Networking* (ICN) and even if there are very different opinions [10], the most accepted approach is the one proposed in [11] and derived by the Universal Resource Locator [12]. As discussed in the following Section V-D, an ICN network would be able to route messages to interact with a resource by using only the name of such a resource. Nevertheless, this cannot be given for granted (at least in the short and medium term). Therefore, a function is needed which is able to locate a resource and provide information on how to reach it. This is the function of the DNS in traditional IP networks and of the ONS in the EPC platforms as we will discuss in the next section.

III. The first generation of the IoT: the tagged things

In this section we focus on the First Generation of IoT solutions. More specifically, we begin in Section III-A by providing a general overview of motivations and solutions considered within such a generation. Then we provide more details about the EPCGlobal Network (Section III-B), machine-to-machine communications (Section III-C) and the technologies provided to integrate RIFD systems and wireless sensor networks (Section III-D).

A. Overview

Unquestionably,

the Radio-Frequency IDentification (RFID) technology played the role of founding technology for the Internet of Things.

The first definition of this paradigm, given by Ashton at the end of last century, directly referred to RFID [13]. The remarkable contributions by the Auto-ID Labs [14], a world-wide network of academic research laboratories, have also put the concept of Internet of objects into strong relationship with the idea of networked RFIDs.

Consequently, the earliest steps towards the IoT have been led by efforts to create an industry-driven global standard to support the spread use of the Electronic Product Code™ (EPC) and of RFID tagging solutions at a world-wide scale [15]. The idea was to overcome the limitations of the Barcode approach and achieve a global item identification through unique worldwide identifiers, represented by the EPC codes stored in tags directly attached to objects.

The idea that RFID solutions could have been the fundaments of the IoT is recurrent in early IoT related research [16] [17] [18]. Great emphasis has been given to the potential to provide, through this technology, a cost-effective way to tag objects and give them an identity. Interesting examples of relevant applications based on RFID have been given, and new regulatory approaches to ensure privacy and security in their fruition have been suggested. Accordingly, IoT was seen as an emerging global Internet based information architecture facilitating the exchange of goods and services in global supply chain networks [18].

While the work on an RFID-based IoT was ongoing, remote sensing solutions based on Wireless Sensor Networks (WSN), Telemetry, and Supervisory Control and Data Acquisition (SCADA) [19] technologies had already reached a mature stage. It was, therefore, quite clear that these

technologies for remote sensing would have played the same key role in the IoT as RFID.

This is confirmed, for example, in [20], wherein Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) together with RFID are recognized as the

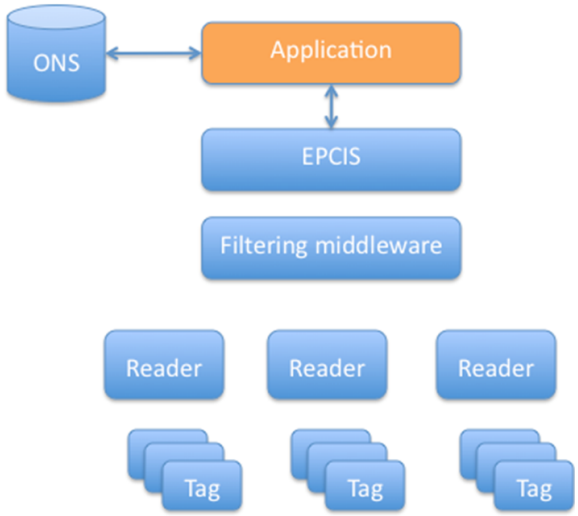

Fig. 2. The EPCglobal Network architecture.

atomic components that will link the real world with the digital world.

Within the Pervasive Computing and the RFID communities, the idea of building a global standard infrastructure for WSN and RFID, based on the framework proposed for EPC, soon began to take shape [21] [22]. However, despite the few trials performed, it was immediately evident that integrating WSNs, as they were, into the EPC framework would have been a very tough task to accomplish.

At the same time, a complementary approach was being considered by the Sensor Network community to make data generated by sensors, SCADA and other telemetry systems available in the Internet (the most relevant carried out within the context of the Machine-to-Machine Communication (M2M) group of ETSI). The great body of research carried out in this domain, summarized and commented in [23], has contributed significantly to the understanding of sensor virtualization techniques. It must be said that none of the aforementioned attempts succeeded in reaching the critical mass necessary for a real take off.

It was clear since the beginning that the proposed solutions could not incorporate the RFID technology in a simple way. Therefore, only a few research activities tried to integrate RFID systems and WSNs into a unique comprehensive picture.

B. Technologies for interconnecting RFIDs: the EPCglobal Network

Objective of the EPCglobal Network is to link information with objects, equipped with a tag identified by a unique EPC, and people. This is mainly done by defining and supporting primitives that allow applications to query specific objects about their status.

The EPCglobal Network architecture is based on a layered service oriented architecture (SOA) with an emphasis on defining the interfaces between the different components [24]. When defining the interfaces, modularity becomes a key feature with several technical and economic advantages.

As it can be seen in Figure 2, the EPCglobal Network includes six components (some physical, some logical):

- RFID tags: these represent the tags attached to the objects. They are characterized by a unique ID and may have some processing capabilities.
- RFID readers: these are responsible to query the RFID tags in their proximity and communicate the information gathered to some backend server.
- Electronic Product Code: this represents the scheme utilized to assign and interpret the unique tag identifier. [1]
- Filtering middleware: this is responsible of receiving the requests from the applications (opportunely translated by the EPC Information Service as described later), processing the data from the RFID reader(s), and returning data to the requesting element (or another system specified in the request). The data reported in the form of EPC identifier is captured by a reader, and this has happened.
- Object Name Service (ONS): this is responsible for transforming an EPC identifier into an URL and vice versa. Its function is similar to that of Domain Name Systems in the Internet.
- EPC Information Service (EPCIS): this is responsible for storing the events (as described above) and responding to the queries generated by the applications.

Interactions with the above components occur through standard interfaces as discussed below. According to EPCglobal, tags with different complexity level and functionalities can be read by RFID readers: class 1 refers to Identity-tags, which store an identifying code only; class 2 includes tags with additional memory storage and, optionally, with sensing capability, such as Wireless Identification and Sensing Platforms (WISPs) [25]; class 3 specifies battery-assisted tags which use an on-board power source to empower sensors but not to generate the communicate signal; and class 4 tags, which use batteries to also empower the communicate module. The radio communication between RFID readers and tags is regulated by the Air Interface standards, EPC Gen-2 protocol [26], and ISO 18000-63 [27]. These standards are aligned on the core functionalities and define modulations, encoding, medium access schemes, and a set of basic commands for Selection, Inventory and Access to tags.

To foster widespread adoption of these technologies, specific protocols define the message structure and the modalities for applications interacting with RFID readers. To overcome interoperability problems and to facilitate the development of applications, communications can happen at different abstraction levels. The Application Level Events (ALE) protocol [28] specifies a software interface through which client applications may interact with filtered and consolidated EPC data. Typically, the Filtering middleware implements the ALE interface, but also smart RFID readers can provide it. This

[1]In this perspective, it is worth mentioning the IEEE 1451 standard (standard for Networked Smart Transducer Interface), whose major component is the TEDS (Transducer Electronic Data Sheets). TEDS is a sort of identification card carried by a person. It stores manufacture-related information for the transducer(s), such as manufacturer identification, measurement range, accuracy, and calibration data, similar to the information contained in the transducer data sheets normally provided by the manufacturer.

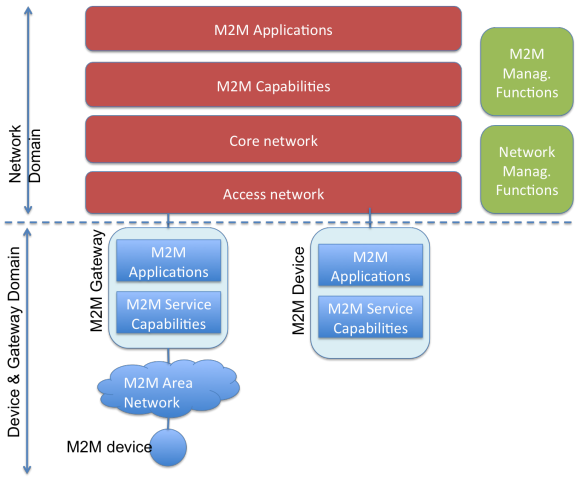

Fig. 3. High level architecture for M2M Communications according to ETSI.

interface can be used by applications or the EPCIS. By means of ALE, an application generates a high-level description of, for example, the data to be read from or to be written to tags, the period of time, and the filters to select particular tags. Alternatively, Low Level Reader Protocol (LLRP) [29] provides specific parameters and controls to set the command and timing parameters of the RFID air protocol. Obviously, the ONS and the EPCIS implement interfaces that can be used by applications to retrieve the EPC identifier associated to a logical name (a URI for example) or to query the system about some events.

An interesting project aiming at creating a microcosm for the IoT spanning applications, systems, and social issues, that are likely to emerge in a realistic day-to-day setting, has been carried out at the University of Washington. There, the involved researchers have developed a building-scale, community-oriented research infrastructure called RFID Ecosystem (http://rfid.cs.washington.edu).

C. Technologies for machine-to-machine communication

The European Telecommunication Standards Institute (ETSI) has focused on the definition of a standard for cellular M2M communications. In fact, cellular network operators see in the spreading of M2M technologies the opportunities to include machines in their user basin, so as to increase their revenues despite the continuous decrease in the per-user revenues.

The high level architecture envisioned by ETSI is depicted in Figure 3 and is based on a RESTful service approach [30]. As shown in the picture, two domains can be distinguished: the Network Domain and the Device & Gateway Domain.

Major components of the Device and Gateway Domain are the M2M Applications and the M2M Service Capabilities layers. In some cases, these layers will be executed by the M2M Device. In other cases, the M2M Devices have not enough resources to run them and therefore, the above components run in appropriate gateways (M2M Gateways) acting as a proxy between the Network Domain and a few M2M Devices. Such M2M Devices are connected to the M2M Gateway through a M2M Area Network that can be based on any LAN standard such as IEEE 802.15.4.

The M2M Service Capabilities layer has the objective to abstract the resources of the M2M Device and to establish a secure communication between the application running in the Network Domain and that running in the M2M Device. The idea is to allow different applications to run over the same M2M Device.

The M2M Application layer, instead, defines the application logic. Instances of the M2M Application layer (as well as of the M2M Service Capability layer) run in both the Device & Gateway and the Network Domains.

It is important to note that in the ETSI view, which is strongly influenced by the perspective of cellular network operators, M2M Devices or their M2M Gateway must be equipped with a cellular wireless interface.

In the Network Domain the Access Networks provide M2M Devices with access to the Core Network: these are independent, in general, from the M2M technologies, and include most of the available data access standards. The Core Network instead offers (at least) IP connectivity, service and network control functions, interconnection with other networks and roaming functionality.

D. Technologies to integrate RFIDs and WSNs in the IoT

In this context, two approaches can be considered: (i) integration at the object level, i.e., any type of objects can be integrated in the IoT; (ii) Integration at the system level, i.e., a unique abstraction of object is defined which can represent any type of device.

Integration at the object level: This integration is fostered by technological advances in miniaturization, energy harvesting, and energy efficiency that make it possible to integrate passive (in terms of energy usage) hardware platforms, like some RFID tags, with some environmental sensors and memory banks needed to store data. Relevant examples include the WISP as well as the proposals in [31] and [32].

Two families of architectures can be distinguished that support integration at the object level: some solutions consider the resulting nodes as RFID tags equipped with sensors, while others consider the resulting nodes as wireless sensor nodes with a unique ID. In the first case, the EPCglobal network architecture is the starting point and extensions are introduced to support the new formats of messages (which can accommodate the values measured by sensors). However, solutions based on such an approach cannot integrate the data generated by traditional sensor networks (already deployed in the environment) and do not support direct communications between nodes; i.e., a reader is needed in the proximity of the node to collect the measured data.

In the second case, instead, nodes can communicate with each other according to the multi-hop wireless communication paradigm supported by the WSN solutions. A remarkable example of such an approach is proposed in [33], where a Smart Object (wireless node with sensing capabilities and unique ID) is defined, which is able to directly communicate with its peers. Differently from RFID tags equipped with

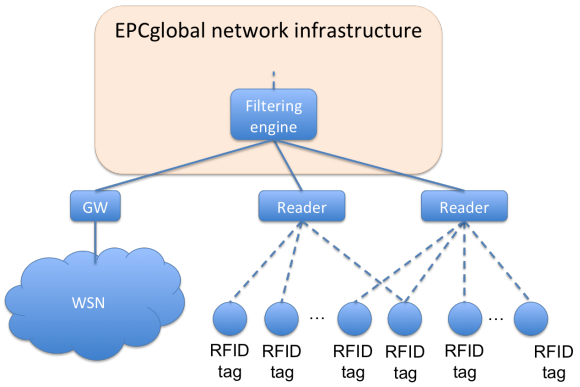

Fig. 4. Possible integration of RFID and WSN at the system level.

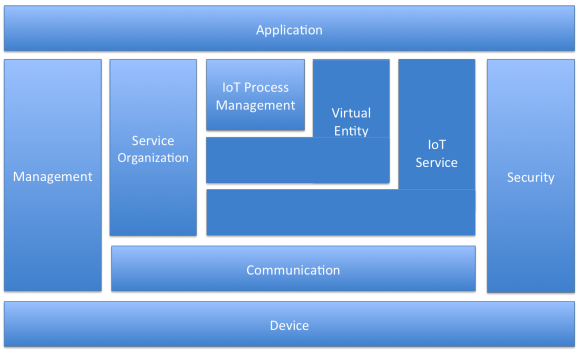

Fig. 5. IoT-A architecture.

sensors, Smart Objects are characterized by high communication and interaction capabilities as well as higher management autonomy.

Furthermore, in the solution proposed in [33] nodes are clustered and a cluster head is identified. This collects information generated by other nodes in its cluster and is responsible to transfer this information towards the network infrastructure. The use of a cluster head is common to improve efficiency in the WSN literature [34]–[36].

As a general consideration, solutions that envision the integration at the object layer are unpractical in that they cannot integrate objects already deployed in the environment.

Integration at the system level: The basic idea of the solutions envisioning the integration at the system level is to introduce a component at the edge of the network infrastructure which hides the differences and heterogeneities among nodes.

For example, as shown in Figure 4, the authors of [21] introduce a sort of gateway between wireless sensor networks and the EPCglobal network infrastructure to translate events generated by the wireless sensor network into the appropriate formats. Major advantage of such a solution is that it does not require changes in the EPCglobal network infrastructure which has strong industrial support. Nevertheless, it has two major drawbacks: it is not tailored to handle information generated by sensors and it leaves the management of the WSN external to the management of the rest of the system, which may result in inefficiencies.

A more holistic approach has been considered within the IoT-Architecture (IoT-A) project, which was funded by the European Commission to define an architecture for the IoT [37].

Central in the IoT-A architecture, shown in Figure 5, is the clear separation between the physical entities and the services associated to the IoT devices. For example, a room in a building is a physical entity whereas the temperature sensor deployed in that room provides a service associated to it. In IoT-A physical entities have representations in the digital world called Virtual Entities (VEs). Virtual Entities are associated to services offered by the IoT devices providing information about VEs. Such services are called IoT Services. Examples of IoT Services are the measure of some environmental parameter achieved through some sensor or the positioning of some object achieved thanks to RFID systems. Processes concerning a single VE are managed by the IoT Process Management component.

In the IoT-A architecture a very important role is played by the Service Organization component which is a sort of hub that orchestrates the processes triggered by the Applications to implement a meaningful business logic. Obviously, all the above components exploit the service offered by a Communication component. Finally, there will be a Management and a Security component which will span all layers of the architecture.

While the holistic approach followed by IoT-A project delivers an architecture which is able to fully integrate RFID tags and wireless sensor nodes, the implementation of relevant modules is still at the prototype stage and most solutions are still based on the EPCglobal network architecture.

In the view of the RFID and sensor integration, it is worth citing SARIF [38] and MoCoSo [39] as examples of projects that, together with the EPC Sensor Network of the Auto-ID Lab Korea, represents efforts to combine concepts of object identification, sensor data and the Internet.

IV. The second generation of the IoT: full interconnection of Things and the (social) Web of Things

In this section we focus on the Second Generation of IoT solutions. More specifically, we begin in Section III-A by providing a general overview of motivations and solutions considered within such a generation. Then we provide more details about the solutions proposed to integrate constrained devices into IP networks (Section IV-B), the Web of Things technologies (Section IV-C), and the earliest attempts to exploit social networking in the IoT (Section IV-D).

A. Overview

The second generation is characterized by a continuous reduction in the interest around tag-centric solutions. In fact, in the second stage of the IoT evolution, the major focus was on giving the simple objects the capabilities to be directly connected to the Internet like any other host.

Undoubtedly, the driving force in this direction has been the consensus gathered around the work conducted by Working Groups of the Internet Engineering Task Force (IETF) finalized to the deployment of IoT by leveraging on the IP

protocol. This latter is light, already connects a huge number of communicating devices, and can run on tiny and battery operated embedded devices. Therefore, it can support IoT through a wise adaptation of its basic functionalities and the incorporation of the reference standard for Personal Area Networks (short range networks with a radius of a few meters) into its architecture; this was exactly the task of the cited working groups. The encouraging results in this context have soon inspired several interesting attempts of integrating RFID devices into the IP-based IoT vision of the IETF [40] [41], [42], [43], [44], [45].

During the same years the new approach of designing applications in the Internet as web applications (i.e. able to run in a web browser, because created in a browser-supported programming language) was rapidly emerging. This also brought IoT into a sort of generational leap to enter the Web of Things era [46], [47]. According to this paradigm Web standards are reused to connect and integrate everyday-life objects, which contain an embedded device or computer, into the Web.

In parallel with the depicted activities, also social networking concepts began to penetrate several ICT technological domains, which span from delay-tolerant to peer-to-peer networking, from content searching to content recommendation. IoT was not immune to this phenomenon. Several research efforts appeared in the literature intended for exploiting social concepts in the IoT domain [48]. These were just the first signs of a new approach to design social IoT solutions that will emerge in its full disruptive nature during the subsequent generation of IoT.

B. Technologies for integrating constrained devices into IP networks

Towards the creation of a full IoT, Internet technologies and protocols are expected to be extended to seamlessly and efficiently integrate objects (mostly moving) into the broad internetworking community. Such extensions have been studied for more than a decade, by following two main axioms: i) Things are wirelessly connected to the rest of the world and ii) IP will continue to be the core protocol of the Internet. Accordingly, major amendments to the running Internet architectures have been proposed, which are mostly finalized to enable Things to use the IP protocol and related facilities exactly the same as it happened for other hosts.

In this framework, in 2005 the Internet Engineering Task Force (IETF) started the activities around the IPv6 over Low power Wireless Personal Area Networks (6LoWPAN [49]) working group with the major objective of an adaptation of IPv6 and the incorporation of IEEE 802.15.4, i.e. the reference standard for Low Rate Wireless Personal Area Networks (LR-WPAN, short range networks with a radius of a few meters), into the IP architecture. Accordingly, 6LoWPAN specifies a lightweight IPv6 version which can be run by resource constrained devices. One of the addressed issues is related to the size of the packet headers; indeed, appropriate strategies have been defined for their compression to the purpose of making the IP header (mostly IPv6) conveyable into low rate LR-WPANs, characterized by short frames whose payload can almost be completely filled by the combination of IPv6 and TCP headers.

Another topic addressed is related to the bootstrap phase, during which objects need to acquire their network addresses. This may happen in two ways: either statelessly by combining a EUI-64 unique identifier with an IPv6 address prefix or through a dynamic address assignment mechanism like in DHCPv6. Network discovery protocols have been also defined to support neighbour nodes to discover each other, manage the other presence, determine link-layer addresses, discover neighbour routers, and maintain information about the active neighbours.

The actual integration of 6LoWPAN networks into the Internet requires the functions of a gateway translating 6LoWPAN packets into standard IPv4 (or IPv6) packets. By deploying 6LoWPAN it is possible to consider a node of a WSN as a node of the Internet. 6LoWPAN also provides the functionality to transform each device into a web server. Additionally, sensor virtualization techniques allow for creating abstractions of sensors which could be queried without the need of knowing the specific features of the sensor node. Since its introduction, several 6LoWPAN protocol stacks have been proposed. Contiki is one of the major efforts (http://www.contiki-os.org), which is anopen sourceoperating systemfor networked, memory-constrained systems with a particular focus on low-power wirelessInternet of Things devices.

C. Web of Things technologies

Making low power sensing devices capable of communicating in an IP network is not sufficient, as explained in [50]. Integration of wireless sensor nodes into the IoT requires the support of HTTP-based services so that sensor nodes can become devices of the World Wide Web. Indeed, HTTP-based applications are the leading traffic sources of the Internet [51]. Thus, the HTTP-based interaction model is extremely popular and most software developers have developed a thorough knowhow in web technologies and programming.

It would therefore be desirable, from the point of view of software developers, to deal with all devices connected to the Internet by exploiting web services. To satisfy such a compelling request, technologies have been introduced in the market that embed Web server functionalities even in the tiniest communication devices. Examples include the ttpd (http://www.acme.com/software/thttpd/), Busybox (http://www.busybox.net), Boa (http://www.boa.org), and lighttpd (http://www.lighttpd.net).

The introduction of the Web of Things concept is a natural result of the above trend. In the Web of Things, IoT devices are considered as resources of the World Wide Web [46], [47]. Devices are modelled as web services, which are uniquely identified by a Universal Resource Identifier (URI) such as web pages in the Internet.

For example [46], the Sun SPOT platform is a Java-programmable embedded system equipped with a few sensors (light, temperature, and accelerometer) and actuators besides the internal components such as the radio transceiver and the

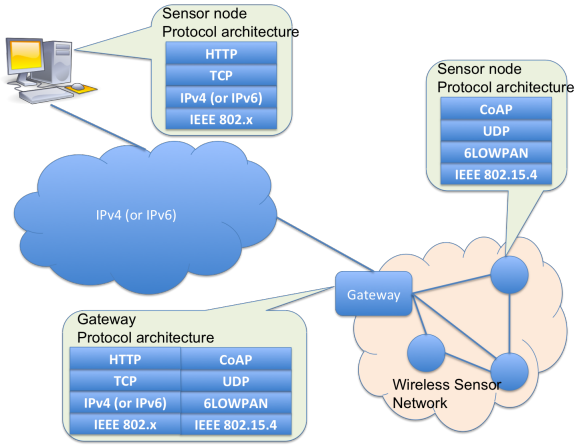

Fig. 6. Architecture envisioned by CoRE.

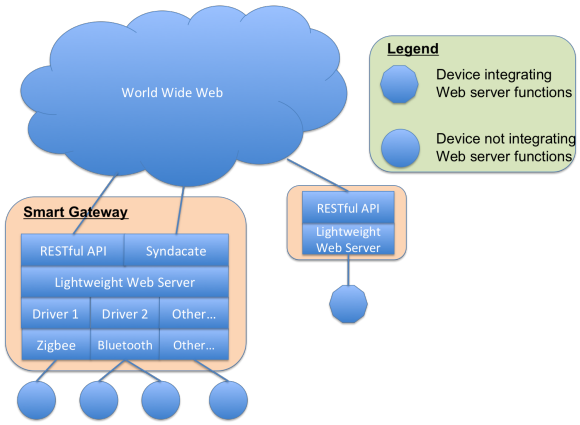

Fig. 7. Architecture of the Web of Things.

battery. Each of the above elements can be modelled as a Web resource and assigned a unique URI. Interactions with such a resource is then executed using the RESTful approach which exploits the classical HTTP methods. Therefore, the GET method is used to obtain the value measured by a given sensor or the setting of some components, whereas the SET method will be used for configuration purposes.

The format of the messages exchanged in the Web of Things must be simple and interpretable by humans. Accordingly, most solution propose to use HTML, i.e. the same language used to build web pages, or, more recently, JSON [52].

However, implementing web technologies for device communications may be inefficient in terms of both complexity and generated traffic, which are issues addressed by the Constrained RESTful Environment (CoRE) working group of the IETF [53]. The Constrained Application Protocol (CoAP) protocol is the result of the relevant standardization activities. It is designed to provide a HTTP-like application protocol that can be easily translated into HTTP and is characterized by simplicity, low overhead, and support of multicast communications; thus, it results optimal for resource-constrained devices. It provides a request/response interaction model between application endpoints, and supports built-in service and resource discovery.

In order to obtain low overhead, CoAP is usually executed over UDP (differently from HTTP that runs on top of TCP). According to CoRE, a Gateway is needed to interconnect CoAP/UDP/6LoWPAN devices with the rest of the Internet. The above Gateway is responsible for translating the message formats from the one specified in CoAP/UDP/6LoWPAN to the one used in the Internet, and vice versa, as it is shown in Figure 6.

WoT solutions have pushed also the RFID research community to approach the same issue and to propose solutions that use RESTful services in RFID platforms. As an example, the authors of [54] propose to seamlessly integrate an EPC-global network into the Web. In this way, through the HTTP protocol, tagged objects can be directly searched for, indexed, bookmarked, exchanged and feeds can be created by end-users for their future Internet/Web of Things or Mobile prototypes and products. Further relevant research activities which focus on the same issue are reported in [55] [56] [57].

A further step towards the integration of RFID technology and platforms in IoT systems is represented by the achievements of studies (still ongoing) focusing on inclusion of the RFID technology in CoAP [53]. The RESTful paradigm implemented by CoAP could ensure the seamless and effective integration of RFID resources in the Web, by using specific proxy functionalities, like in [58]. The approach proposed in [40] is a major breakthrough towards RFID applications no longer considered as stand-alone solutions. In fact, the proposal is the access to a common set of RFID resources through standardized IETF IoT protocols, similarly to the way resources of other smart things are accessed. The ultimate aim is to facilitate and foster the deployment of interoperable RFID applications in the IoT domain.

Devices which do not offer web server functionalities can be connected to the Web of Things by exploiting appropriate proxies, as shown in Figure 7. In this case, the communication between such proxies, called Smart Gateways in [46], and the devices can be based on ZigBee, Bluetooth or any standard (as well as proprietary) technology. The Smart Gateway offers a RESTful API for the sake of devices energy usage. Another feature of the Smart Gateway is represented by the Syndicate module which offers an API for interacting with a collection of devices (instead of single devices). This is useful in several application scenarios and can be used to support object localization [59].

D. Social Networking technologies

Significant efforts have been put to exploit social networking concepts in the IoT domain [48]to facilitate the integration of objects in the existing IoT services. The major motivation is the improvement of the potentialities of the owners to share data generated by their smart objects with people they know and trust (e.g., relatives, friends, colleagues, and fellow researchers), leveraging the existing human Social Networks Services (SNS) platforms.

Table IV lists the different possible objectives in using social technologies in the IoT arena during the second generation. As previously said, the major value, in general, is represented by

Objective	Use of human SNS	Type of communication	Papers
Personal data available to the owner	Yes	Object to humans	[49]
Personal data available to the owner friends	Yes	Object to humans comunities	[50], Nike+, [51]
Activities and performance benchmarking	Yes	Object to humans comunities	[49]
Objects management	Yes	Human to objects	[52][53]
IoT-enabled social media marketing	Yes	Human to human	[54], Nike+, Toyota Friend
Customer relationship management	Yes	Customers to objects to vendors	Toyota Friend
Object establishing a connection (data and service exchange)	No	Object to object	[55]
Facilitating human social communications	No	Mediator in human communicastions	[56][57]
Understand and analyse object related data	No	N/A	[58]
Improving devices' usability and interaction	No	Human to human	[66]

TABLE IV
POSSIBLE SCENARIOS OF INTEGRATING OBJECTS DATA INTO SOCIAL NETWORKS WITH RELEVANT TYPE OF COMMUNICATION AND PAPERS.

the fact that data sensed by things is made available to the humans through their major social communication platforms. However, this major objective can be further classified according to the specific intended use of the data produced by the objects.

Some implementations are aimed at enabling the owners to have an easy way to access her own objects data though the object capability of posting messages on the owner social board with limited visibility. In this way, users are continuously connected to and updated about their social things while also connected to their friends. This is the case of the socialFarm experimented in [60], in which farmers check the status of the animals, crops and greenhouses by making relevant sensors capable of publishing their data on Facebook.

Other implementations are instead specifically focused on making this information available to the community of either current friends or potential friends, i.e. unknown people but with high level of homophily discovered though the social things. One of the first proposals along this line is in [61]. The main idea proposed in that article is that a user who wishes to share data sensed by her own objects can do this by posting such data on Facebook and allowing selected people to view them. A similar approach is proposed in the CenceMe application [62], which focuses on combining information on the presence of individuals obtained through off-the-shelf sensor-enabled mobile phones, with the user profile in social networking platforms such as Facebook and MySpace.

Slightly different from the previous scenario are those of benchmarking and crowdsourcing. According to the former, data gathered from the IoT systems is used to benchmark the activity of humans in a given domain with respect to the average behaviour of communities of interest. This is the case, for instance, of the SocialElectricity prototype, which is a Facebook application that allows people to compare their electricity footprint with their friends in a wide-scale. [60].

Some works have proposed the use of the human social networking platforms to manage things. This is the case of the Paraimpu project, where the humans can connect sensing devices to either actuating devices or web services by accessing her own social networking account [63]. A more complete framework in this sense is the one presented in [64], where the authors design a social networking service as the converging point for people, web services, and devices and the SN is considered as a meaningful opportunity to finally bring the Semantic Web and the IoT to users. Another interesting solution is the Toyota Friend Network, which has been conceived as one of the earliest platforms in which data generated by objects, in this case automobiles, are made available in a social network of humans for marketing purposes.

In all the mentioned scenarios, objects interact with humans through their SNS. In parallel there have been studies that augmented the objects with social capabilities to improve their aptitude in exchanging data with the external world without the use of human SNS. Indeed, one of the first ideas of pseudo-socialization between objects can be found in [65], which proposes the Smart-Its Friends procedure that allows users to have a very easy-to-use interface to impose temporary relationships / connections among smart wireless on the basis of the devices context. Other approaches had the objective of facilitating human social communications. Finally, some researchers focused on tools for the analysis of IoT data [66].

The tools to compose and build personalized and social applications that process data from different sources are in continuous evolution. Among these tools are: Ninja Blocks [67], IFTTT [68] and the already mentioned Paraimpu [63]. Ninja Blocks controls devices that can sense their environment and can act by controlling lights, power sockets, and other actuators. The system provides a tool to drive the composition of actions and sensing tasks with common social web sites such as Twitter, Facebook, Instagram. IFTTT is aweb-based service that allows users to create chains of simple conditional statements involving any type of objects and through many social network sites. Accordingly, when some events monitored by objects make some statements becoming true, other objects are triggered to perform specific actions.

A further remarkable project to mention is under development at the Ericsson Research laboratories, where researchers of the Usability Laboratory are implementing their vision of Social Web of Things [9]. Accordingly, objects become capable of more autonomy and the interactions between objects of the IoT are presented in analogy to the interactions people usually experience in Facebook or Twitter or other social networks. This helps people to master the complexity introduced by the IoT networking paradigm.

V. THE THIRD GENERATION OF THE IOT: AGE OF SOCIAL OBJECTS, CLOUD COMPUTING, AND FUTURE INTERNET

In this section we focus on the Third Generation of IoT solutions. More specifically, in Section V-A we provide an overview of the motivation and solutions considered within

this generation. In the following sections we then present the major characteristics of Social Internet of Things solutions (Section V-B), the use of semantic technologies and ICN paradigm in the IoT domain (Sections V-C and V-D), the integration of IoT and cloud computing solutions (Section V-E), and the evolved RFID solutions in the IoT (Section V-F).

A. Overview

The Internet world is rapidly evolving under the pressure of a new wave, which is changing the way of building Internet services and enabling ubiquitous, convenient, on-demand access to them: cloud computing. At the same time, a new generation of social objects is raising and is pushing towards new disruptive paradigms for social networks of things. Last, the Internet, as we have been knowing it, is about to undergo profound transformations which put content and services at the very center of the network operations.

All these aspects are causing a further generational leap which is taking the IoT in what is often referred to as the *Future Internet* which will exploit cloud computing technologies and will be people-, content-, and service-centric.

The reasons for an extension of cloud computing technologies and solutions to the IoT domain are various. Things generate great amounts of data that need to be stored. Being local device memory usually limited and costly, the best solution is to send data to the cloud, where functionalities such as encryption, authentication, duplication, annotation [69] can be implemented easily. Also the things need for on-demand use of IT resources (e. g., computer, storage, and network) in a scalable and cost efficient way matches the cloud computing paradigm very well. Besides, IoT devices are highly heterogeneous in terms of interfaces, achievable performance, and capabilities. The cloud may help in managing this heterogeneity by providing a common IoT application development layer wherein the different hardware devices are virtualized. At the same time, services from different providers can be merged (mashup process) in the cloud to provide complex services [70].

As already mentioned, during the third stage disruptive novel approaches to exploiting social networking concepts and technologies in the IoT domain are fast arising. The driving idea is to allow objects to *autonomously* establish social relationships and create their own social network separated from the one of the humans. The motivation is that a social-oriented approach is expected to boost the deployment of effective solutions to discover, select, and compose services and data provided by distributed objects. It allows objects to create a network, which manifests interesting properties in terms of navigability, trustworthiness in data exchange and, scalability in a community of billions of devices.

At the network layer, the *Information Centric Networking* (ICN) paradigm, recently proposed to replace the host-centric networking paradigm of the Internet with a solution centred around the exchanged data units, is gaining ground [71]. It represents a solution to the difficulties in matching the stringent performance requirements of IoT systems (scalability, robustness, energy efficiency, to mention some) by relying on IP-based solutions. ICN features such as the effective content naming schemes, the associated data retrieval and data sharing approaches, the native mobility support, the in-network caching, and the content-based security are very appealing to IoT designers. Therefore, the strong commitment of several research groups towards the application of ICN principles in IoT contexts opens new opportunities [72].

As a further point, it is worth highlighting the central role played by knowledge representation solutions in this stage of the IoT evolution. Currently, IoT systems and applications cannot be effective without a complete knowledge about their components, characteristics and features, which must be, somehow, formalized and disseminated. To this end, ontology can be used to introduce a formal, explicit specification of a shared conceptualization so as to represent knowledge within a domain as a set of concepts related to each other. Ontology is then used by semantic engines for different purposes, such as: search, composition, and translation.

To conclude the description of this new era of the IoT, it is also worth pointing out what happened to its funding technology, i.e. RFID. Actually the interest on it has not completely disappeared, but surely its centrality in third generation IoT solutions is severely reduced.

B. Social Internet of Things

A keen attention to the social potential of the IoT building blocks characterizes this generation. In fact, one finds papers, such as [73], which describe architectures where objects are clearly identified as potentially able to participate in communities of objects, create groups of interest, and take collaborative actions. This kind of researches, however, theorize the Social Internet of Things but do not indicate how to build the envisioned social network of objects and how to implement the needed architecture and protocols. This is provided by [74], where the authors propose mechanisms that can be used by objects to build friendship relationships. Besides, they suggest an architectural model for the resulting social IoT with the major building blocks to create and manage the objects social network. By relying on this architecture, [75] analyses the problem of evaluating the trustworthiness of each node in the network and propose a method to allow objects mimicking the behavior of the humans when evaluating the trustworthiness of friends. Motivated by the considerable amount of work in this field, a recent review of related researches appeared in the literature [76]. Herein, the use of the social networking technologies are seen as means to increase the pervasiveness and ubiquity of the computing systems as (social) interactions among objects in our living places are necessary to improve the ICT system performance.

C. Semantic in the Internet of Things

One of the most notable efforts in this area is the Semantic Sensor Network Ontology (SSN) [77], which is not application-dependent and is frequently adopted in different IoT domains to describe the sensor and context properties. SSN is natively able to model the most common context

properties and the set of properties can also be extended unlimitedly. An important characteristic of SSN is that sensors are not constrained to physical sensing devices; rather a sensor is anything that can estimate or calculate the value of a phenomenon. Therefore, either a device or a computational process or combination of these can play the role of a sensor, while a sensing device is a device that implements sensing and belongs to the sensor class [78].

The main drawback of SSN lies in the limitations of the adopted semantic web approach, which is unable to describe and perform reasoning over the system dynamics. In the IoT, this precludes any object representation that can evolve over time (e.g., having their access policy, availability, geo-location, etc. changing over time). The highlighted issue is clearly identified in the recent literature. Proposals are appearing, which propose to combine semantic web technologies with temporal and spatial reasoning in order to accurately reflect the behavior of the considered IoT systems. The contribution in [79] is noteworthy in that it also demonstrate that the effectiveness of proposed solutions can be increased by adopting distributed models.

D. The Information Centric Networking paradigm in the IoT

The "prehistory" of ICN approaches for the IoT is probably represented by the ideas proposed by Ivan Stojmenovic and Stephan Olariu in their work [80], which dates back to 2005, when the idea of IoT had not received yet the attention it is receiving now. Although the authors actually review a number of emerging topics pertaining to a data-centric view of wireless sensor networks (such as data-driven routing for example), their work already includes some interesting ideas that have been later recovered to handle data in ICN-based solutions for the IoT. Scenarios for information centric wireless sensor and actuator networks are also the subject of later works, such as [81], [82], [83], and [84].

More recently, several research activities have been devoted to the integration of the ICN concepts specifically into the IoT. Research in this area is still at an early stage, although the advantages and opportunities that ICN offers and the related challenges in a perspective of ICN-IoT integration have already emerged. Also, solutions to the problems of service discovery and naming for IoT have already been proposed as part of the main platforms of ICN developed.

Recent IETF Drafts [85], [86] address the issue of building a unified IoT platform based on the Information Centric Network architecture. The authors clearly highlight the limitations of IP in serving as an internetworking layer for the different intranets of things developed without any form of coordination. They also illustrate the potential of the main features of ICN to achieve seamless mobility support, scalability, and efficient content and service delivery in an Internet of Things.

Most of the work concerning the integration of ICN in the IoT has the *Content-Centric Networking* (CCN) [11] architectures at its very basis. CCN provides a core network for the future Internet characterized by in-network memory and composed of Super Routers (SRs) with large content stores, high computing capabilities, and relatively reliable communication performance. Devices with constrained resources, typical of the IoT, greatly differ from the SRs in the core networks. Therefore, a content-centric internetworking scheme and relevant specific strategies to adapt to the needs of weak devices, playing the role of producers and consumers of IoT data and applications, are studied in [87]. Similarly, the work in [88] combines CCN with the concept of IoT and investigates different ways to make use of the hierarchical CCN content naming, in-network caching, and other information-centric networking characteristics in a sensor environment.

Differently, with reference to the *Named Data Networking* (NDN) architecture, a high-level architecture for IoT systems has been described in [89]. On top of the Thing layer, that accounts for the multitude of devices of the IoT ecosystem, NDN acts as a networking layer, which hides to applications the complexity and diversity of the underlying things by adapting its modules to their features. Besides, in [90], the authors propose an NDN-based framework for the support of multi-source data retrieval (e.g., environmental monitoring), which is a typical IoT traffic pattern not natively supported by NDN.

An overview of possible naming schemes for the IoT is also described in [91] as part of a study conducted by referring to the MobilityFirst architecture [2]. This report is interesting in that it lists the different naming scheme applicable to IoT and compares them with naming schemes available in ICN solutions.

Differently, in [92] the authors propose a service discovery architecture for IoT which enables multi-ownership and flexible management of information that is associated with an object during its entire supply chain (clearly they refer to objects tagged by RFID technology). The authors claim that a prototype will be implemented, based on the information centric Publish-Subscribe Internet (PSI) architectures, originally created by the FP7 project PSIRP[3].

E. The IoT moves to the Cloud

The need to migrate to the cloud typical features of IoT is rooted in the specific nature of the objects that populate it. Due to the energy-constrained nature of wireless sensor devices, several solutions in the relevant literature envision the alternation of duty-periods [93] and periods in which the RF interface of these devices is switched off. Similarly, RFID tags spend most of their time outside the radio coverage of an RFID reader. It can be concluded that IoT things are unreachable during most of their lifetime. Oppositely, IoT applications usually require things to be always reachable.

Hence, the need has been identified for a digital counterpart of any IoT devices always on and running in some Internet servers [94] and to design solutions in which applications interact with such digital representatives of physical entities. According to the current technological trends in the ICT community, the straightforward next step is to move these entities into the cloud. Therefore, solutions have been proposed that envision a Cloud of Things [95], [96], [97].

[2]http://mobilityfirst.winlab.rutgers.edu/

[3]http://www.psirp.org/

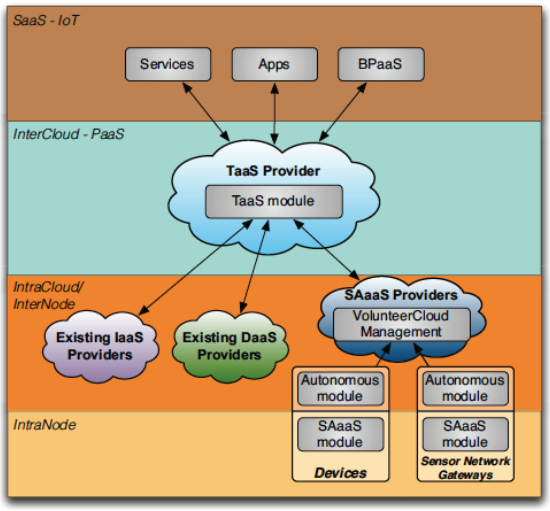

Fig. 8. Architecture for the Cloud of Things (taken from [95]).

The reference architecture for a Cloud of Things is shown in Figure 8 [95]. IntraNode is the bottom layer of the protocol stack, which deals with the virtualization of the resources provided by devices. At this layer, the Sensing and Actuation as a Service (SAaaS) module runs all functions to virtualize the services offered by a sensor or an actuator node.

The IntraCloud/InterNode layer is responsible for the interactions between the virtualizations of different nodes run by the same cloud. At this layer, a key role is played by the SAaaS Provider which offers the APIs to manage and use the services offered by the virtualizations of the nodes running in the same cloud.

The InterCloud/Platform as a Service (PaaS) layer handles the interactions between entities running in different clouds and executes the Thing as a Service (TaaS) module, which supports the meshup between heterogeneous resources in different clouds. Through the APIs offered by this layer it is possible to virtualize the resources of physical objects running in different clouds.

Finally, the Software as a Service (SaaS) gives the potentiality to run instances of IoT software used by different applications.

The great interest in the development of cloud based IoT solutions is also witnessed by the worldwide funded researches for this purpose. Among the others, the EU is currently funding ClouT (http://clout-project.eu), a major project aimed at defining APIs and reference infrastructures for Cloud IoT and at developing relevant tools. This is an EU-Japan collaboration project leveraging the Cloud Computing as an enabler to bridge the Internet of Things with Internet of People via Internet of Services, to establish an efficient communication and collaboration platform exploiting all possible information sources to make the cities smarter.

Interestingly, several real IoT platforms are already developed on the cloud.This is the case of Xively (xively.com), which makes use of the LogMeIn cloud platform. Similarly, Oracle is taking a significant position in providing IoT PaaS (Platform as a Service) services from its leading market position in database management. Nimbits (www.nimbits.com) is already providing cloud services to record and process time and geo stamped sensor data on the cloud. All the used software is open source and can be freely used to develop the desired applications. The access to the cloud services relies on RESTful API web interfaces.

F. Evolved RFID-based solutions in IoT

Still, in this generation, the process of integration between IoT concepts and solutions based on RFID technology continued still following two parallel paths of integration at the system- and device level. A sample solution of system level integration is available in [98], where the authors focus on the EPC Network and explain how a wider adoption of its standards and tools will go through the inclusion of virtualization, cloud computing, and Web related concepts. The continuous momentum towards a tighter integration of RFID into IoT platforms is also testified by the researches in [99], [100] and [101]. Authors of [99] propose a system architecture based on EPC-RFID technologies for what they call smart awareness system. It can be seen as a specific application of a smart IoT, whose architecture foresees intelligent agent, awareness servers, and a middleware system. Instead, the objective of [100] is to develop cognitive robots based on RFID technology within the Internet of Things and giving a social perspective to the interactions of things. Last, the work in [101] presents a software framework architecture for mobile devices that aims at facilitating the development process of embedded RFID applications and the integration process of business applications and EPC Network instances.

At the same time, we are witnessing the design of novel devices and HW platforms integrating the RFID technology to cope with the needs of IoT applications in several everyday-life scenarios. [102] and [103] address the mentioned design challenge in environments where e-health application are made available. In [102] a personal device called Movital, i.e. mobile solution for vital sign monitoring is introduced. It combines reference technologies for the IoT, such as a module for contactless identification (RFID and NFC) with a module for 6LoWPAN networking. [103], instead, gives a survey on the state-of-the-art of RFID for application to body centric systems and for environmental sensing. Passive sensors based on RFID are introduced for environmental sensing, as well as wearable and implantable RFID tags with capabilities of monitoring vital signs.

VI. Enabling Technologies for Next Generation IoT

The current generation of IoT is definitely not the culmination of the evolutionary process depicted, thanks to emerging technological trends that will keep on shaping the IoT of the future. In fact, in several technological areas, solutions are being specifically designed to fit the peculiarities of IoT devices and applications. These solutions, in our opinion, will boost the IoT diffusion and provide new impetus to the IoT evolution.

What is happening in the *Cloud Computing area* is a remarkable example. Cyber counterparts of objects virtualized in the Cloud offers to IoT important advantages that many research and industrial players are currently trying to exploit: supporting the discovery and the mash up of services involving etherogeneous devices, fostering the creation of complex applications, improving the objects energy management efficiency, as well as addressing heterogeneity and scalability issues. Notwithstanding, it is manifest that cyber counterparts of physical things running in remote servers can cause long delays, due to the distance between physical objects and their virtual counterparts, and large consumption of communication resources. This problem has to be quickly addressed by bringing closer the IoT objects (sensors, actuators, etc.) to the cyber counterpart devoted to its management. Next generation solutions shall thus move the cyber counterparts of the things to the extreme edge of the network.

At the same time, what is needed is to implement a kind of personal networks interconnecting all (physical and virtual) IoT devices belonging to a given user in the same broadcast domain. This is an unavoidable way to simplify the discovery of relevant nodes/services, and to isolate personal IoT devices from the rest of the world, which will allow for achieving a high degree of privacy and security.

The mentioned activities are witnessing a great interest from big actors, such as Cisco, actively promoting the Fog Computing paradigm [104], mainly with a focus on latency as required to support interactive and locally-relevant IoT applications. Similarly, across Europe, several funded projects are paving the way to this further evolution in the IoT platforms for things and data management.

Software Defined Networking (SDN) [105] is a further technology originally conceived to foster network programmability, by decoupling the control and data planes, which can play a relevant role in facing the main hurdle to the take-off of IoT networks represented by the poor flexibility and adaptability of the network infrastructure. Early efforts to bring SDN in IoT can be found in [106], where the usage of heterogeneous wireless networks are orchestrated by the centralized control plane. The next challenge is to include in this picture IoT nodes inherently able to sense the real world, take actions but also to store, manipulate and forward data, through in-network processing, cross-layering, security and privacy issues covered by design through SDN.

Recently, also *cellular networks* are being considered as enabling internetworking solutions for IoT devices, as witnessed by the novel features introduced by the Third Generation Partnership Project (3GPP) [107] to support IoT (also named machine-type communications MTC in this context) characterized by intrinsic battery-constrained capabilities and challenging traffic patterns.

Still, a significant amount of research is necessary to improve the access procedures of LTE/LTE-A systems to prevent IoT traffic load from adversely affecting Human-to-Human (H2H) traffic. The research community is hardly working on this issue, as witnessed by the research achievements and standardized solutions [108], [109]. Besides, it is our view, widely shared by the scientific community [110], [111], that the next-to-come fifth generation (5G) wireless systems will play a key role in fulfilling the IoT requirements. In fact, these represent a revolution in the wireless ICT scenario thanks to the innovative network features they will provide [112], among which are: native support of MTC, small-cell deployments, interoperability, optimized access/core segments also through network virtualization techniques.

In this evolutionary scenario, the *device-to-device (D2D) paradigm*, according to which devices communicate directly with each other without routing the data paths through a network infrastructure, will contribute to the IoT evolution in future 5G scenarios [113]. Nonetheless, when considering the possibility of D2D-based interconnection of IoT devices in cellular environment, severe challenges still need to be faced, such as efficient device discovery in heterogeneous environment, optimized link selection for highly dynamic multi-tenant networks, security issues, and so on [113].

VII. Defining the Internet of things of year 2020!

From the picture given in previous sections, it clearly appears that the term Internet of Things (or IoT) has been associated to very different concepts, technologies, and solutions during its first appearance in the scientific community. The oddity of a term so abused and associated to many different meanings in such a short timeframe suggests that, maybe, there is a basic misunderstanding in its use. Such misunderstanding has been amplified by the fact that there are significant overlappings between the IoT and other important research areas such as smart objects, cyber physical systems, and ambient intelligence, for example.

Then, we believe it is worth trying to shed light on what IoT actually is. The approach we choose is to start from highlighting the substantial differences between IoT and terms and technologies often confused with it, rather than merely proposing a further definition that might add further chaos.

The task is not simple, because at first glance it is clearly evident that each definition of IoT is a result of two biasing elements:

1) *The historical period, with all the relevant evolutionary history of ICT technologies adopted by IoT, in which the definition is conceived*. The rapid evolution of ICT technologies observed in these last few years has inevitably influenced the definition of a term that aspires to identify something related both to connectivity (as the word Internet implies) and to computing devices of various kind (hence the presence of the word Things).
2) *The different points of view of the IoT stakeholders which have proposed the definition* [114]. Differences, sometimes substantial, in the IoT visions raised from the fact that stakeholders, business alliances, research and standardization bodies started approaching the issue from either an Internet oriented or a Things oriented perspective, depending on their specific interests, finalities and backgrounds. Besides, the attention to the representation and storing of the exchanged information became brought directly to a third, Semantic oriented, perspective.

The definitions available from the literature or originated by the main research projects [115] are wide-ranging and vary from some that are more minimalist, i.e., expressed by simple formulas (such as Services + Data + Networks + Sensors = Internet of Things, given by Nick Wainwright, HP Labs and Chair of the UK Future Internet Strategy Group) or simple concepts, to those so complex to make an excess of technology converge into the IoT. The problem with the former kind of definitions is twofold. These either oversimplify the meaning of IoT, by reducing the scope to a few technologies and solutions, or just represent mere repetitions, in more structured ways, of nothing than the concept of "generic network that connects generic objects to provide generic services," which could be true (we are talking about an Internet of Things), but does not contribute to the understanding of the phenomenon.

The latter approach suffers from a main drawback: if one brings into the Internet of Things many concepts derived from different architectures and technologies, such as ubiquitous/pervasive computing, Internet Protocol (IP), Machine-to-Machine and embedded devices, Internet of People, then eventually this makes IoT synonymous with everything and, therefore, denies to IoT the specific connotation it deserves.

Fortunately, there are common features that occur in many of the definitions given for IoT:

- A widely accepted feature is the presence of a global network infrastructure or network connectivity, which allows the interoperability of the elements of an IoT, their seamless integration and a unique addressing scheme. This infrastructure shall be a whatever global infrastructure (not necessarily IP-based) allowing to overcome the idea of separate Intranet of Things [116].
- Everyday objects, not only ICT devices, are the main players of the IoT. These have to be readable, recognizable, locatable, addressable, and/or controllable. As a consequence, it is widely accepted that there is a need for solutions that allow for linking physical and virtual objects. The meaning is that sensors and actuators shall be embedded into physical objects to enable them to operate through their virtual representations within a digital overlay information system that is built over the physical world. The interesting definition[4] of IoT as an "intersection of people (meatspace), systems (cyberspace) and physical world (atomspace)" goes in this direction as well.
- Autonomy and autonomicity are two recurrent features which are claimed to characterize the objects that populate the IoT. This has not to surprise, as it clearly emerges from the literature [117] that system complexity can be controlled through the achievement of self-governance (autonomy) and self-management (autonomicity).
- Particular attention has to be paid to the design of effective (better if "intelligent") interfaces both between humans and things and between things.
- Heterogeneity of the technologies involved is another feature often emphasized. This also requires the design of appropriate solutions that enable the coexistence of these technologies within the interconnection platform chosen for the implementation of IoT (via ad-hoc gateways or other solutions).
- Services need to be associated to the objects. These services may be complex or elementary and are built upon the information (sensing, identification, multimedia, etc.) associated to each object [118].

Reasonably, if we assume that all these elements must be present in a platform so that it can be classified as an Internet of Things, then, paradoxically, very few of the solutions available from various experiences focusing on IoT can be considered true IoT solutions. To support the above claim in Table V we provide which IoT features can be found and which cannot be found in relevant technological frameworks that are currently presented as IoT solutions.

Accordingly, there is the clear impression that, often, technological solutions, which have been already available in the scientific community and in the market for years, are enhanced with some minor features and re-proposed under the IoT hat; this would make IoT a mere rebranding for marketing purposes of already existing technologies.

It is our convincement that IoT deserves a higher dignity than this. It can rather be seen as a conceptual framework with a disruptive potential, which is fast gaining ground and is carrying along with it a new enthusiasm and a wider attention on the enhancement of already pre-existing enabling technologies and systems. We can analyse this framework from three different perspectives.

From a technological point of view, definitely IoT is not a new technology that has recently appeared on the ICT scenario and promises to get rid of all the competing technologies by 2020 when the target of billions (the collective imagination is constantly pushing up on a monthly basis this number, as if all had been hit by a sort of "IoT rush") of interconnected objects will participate to the IoT world. Contrarily, it is inclusive in the sense that it encompasses existing technologies (and those to come) with their own peculiarities, compliantly with the basic features listed above.

From the point of view of the approach to service design, IoT integrates several technologies to convey information from sources that are not only people (through their traditional devices: laptop, desktop, cell-phones, and similar) but also real and virtualized objects that are part of the environment in which the service is delivered to users. A further aspect is that such data should not only be available to a particular application, but should become a sort of common informative base, so that different applications can share freely and on a global scale the sources of that information (i.e. the Things, in the IoT acronym) properly organized in the form of a generic network (i.e., the Internet, in the IoT acronym). In this view, IoT becomes the potential service-oriented architectural model of the Future Internet.

From the point of view of its finalization, IoT is a new way of addressing issues with remarkable social impact, relevant to new ways of educating (IoT for education), new ways of conceiving homes and cities on a human scale and responsive to the human needs (IoT for smart home and smart city),

[4]The definition has been given by Rick Bullotta in a Linkedin IoT group discussion in April 2010.

Technology	IoT features	Missing features
RFID platforms	Pervasiveness; often integrated with sensors/actuators	Effective object virtualization; autonomy and autonomicity; interaction between objects
Pervasive computing platforms	Pervasiveness, autonomy and autonomicity; heterogeneity of technologies; association of services with objects	Global network infrastructure; interfaces for thing to thing interactions
Cyber-physical systems	Pervasiveness; autonomy and autonomicity; interfaces between humans and things as well as between things; heterogeneity of technologies; association of services with objects	Global network infrastructure
Sensor networks	Autonomy and autonomicity; association between services and physical resources	Global network infrastructure; pervasiveness; heterogeneity of the technologies;
M2M systems	Connectivity and global network infrastructure; Interfaces between humans and things as well as between things; heterogeneity of the technologies	Pervasiveness; autonomy and autonomicity

TABLE V
CURRENT TECHNOLOGICAL FRAMEWORKS: EXISTING AND MISSING IOT FEATURES.

new ways of addressing energy management issues (IoT for energy), new approaches to handling people health and well-being (IoT for e-health). The novelty is that not only human beings, using objects enhanced by pervasive technologies in innovative way, are involved in the process. Rather people and objects interact with each-other, as peers. Such an inclusion of everyday objects (or better their virtual representations) in the process allows to create applications with a higher penetration rate into everyday life.

If one does not accept the definition of IoT as a new "conceptual framework" that includes these three points of views, which might seem a little too inclusive, then, for intellectual honesty, the risk is having to define IoT a "big hoax" because the greatest part of the self-styled IoT technological solutions, which nowadays are inflating the ICT market, would discover to be nothing more than solutions belonging to the old domains of pervasive computing, wireless sensor networks, M2M, RFID based tracking, and social sharing of devices.

It is indisputable that today the attention on the use of these technologies under the new name of IoT has grown at an incredible pace, never observed before, and has brought great results. In this view, "the Internet of Things panacea" is welcome; but unfortunately, at least for now, it is hardly possible to speak about any new real emerging IoT technology in the current ICT scene. Rather, we are persuaded that the best definition that can be given, in our humble opinion, for the Internet of Things as it appears today and is sketched in Figure 9 is:

a conceptual framework that leverages on the availability of heterogeneous devices and interconnection solutions, as well as augmented physical objects providing a shared information base on global scale, to support the design of applications involving at the same virtual level both people and representations of objects.

In accordance with the above definition, we envision that in the next future IoT platforms will evolve towards the architecture shown in Figure 10, as explained in the following. Appropriate software drivers will create abstractions of the IoT physical resources. Note that drivers can run either in the IoT devices or in some server. Such abstractions will hide the specific hardware/software features of the IoT resources. The abstractions of the IoT resources will be used by the IoT Operating System which is organized in three layers:

- *Southbound API*: This is a common layer of modern Network Operating Systems, e.g., [119], and is responsible of creating internal representations of the IoT resources and their services which are used by the Core layer. One of the most important operations executed by the Southbound API layers are the mapping between a unique, platform-independent identifier of a specific IoT resource and the platform-dependent address of such a resource. Another fundamental operation of the Southbound API layer is the implementation of the specific communication/interoperation protocol of the physical resource.
- *Core layer*: This is responsible of the most critical operations executed by the IoT Operating System. In the Core layer the Social IoT will play a key role as it allows to create an overlay network spanning different and even heterogeneous IoT platforms [74]. Other important operations performed by the Core layer are related to the management of the resources and include Scheduling, the management of Security and Trust, and the Resource/Service Discovery. Note that Security and Trust Management as well as Resource/Service Discovery will strongly rely on-the SIoT.
- *Northbound API*: Finally, we have the Northbound API, which is responsible of creating an abstraction of the services offered by the physical resources. A good starting point for the Northbound API is the work carried out within the Open Connectivity Foundation

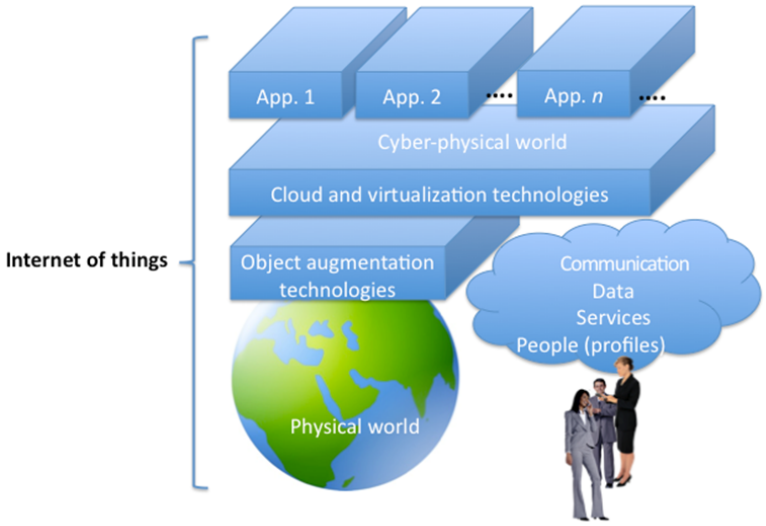

Fig. 9. A high level representation of the IoT conceptual framework.

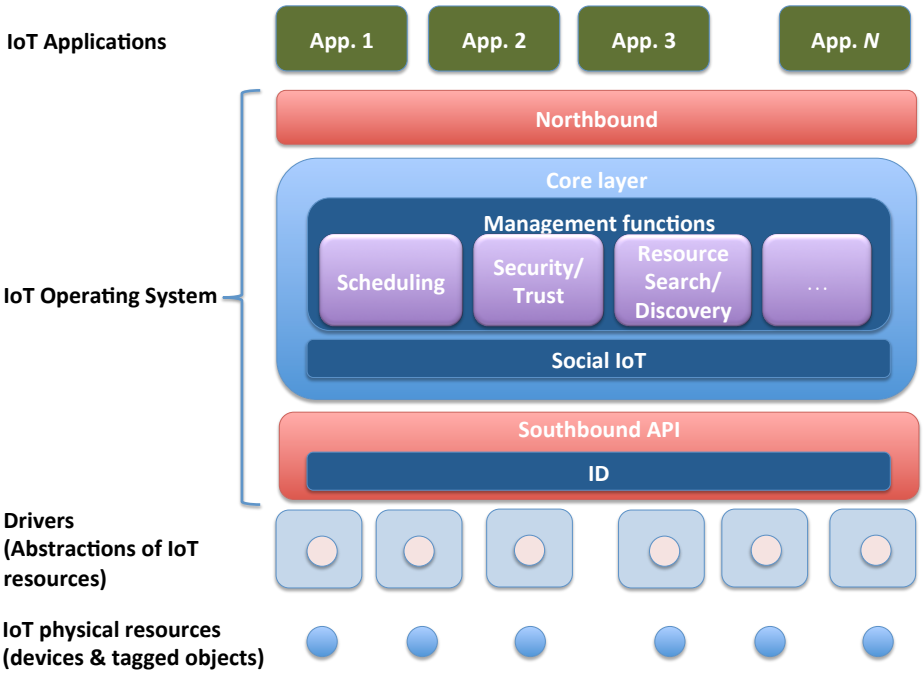

Fig. 10. A general architecture for the upcoming Internet of Things.

(https://openconnectivity.org). By leveraging the Northbound API, it will be possible to implement applications according to the SAaaS as presented in Section V-E.

VIII. Conclusions

This article has analyzed the Internet of Things phenomenon from an evolutionary point of view, by emphasizing that the IoT has undergone several transformations in its characterizing technologies and principles since its introduction. As a result of this analysis, three generations of IoT have been identified: the first one of tagged objects; the second one of things interconnection through web technologies; the third one of social objects, semantic data representation, and cloud of things.

It is obvious that the IoT will continue to evolve as new computing and communication paradigm will arrive at a mature stage, consider the seminal work in [5], [6] on the Internet of Nano Things, for example, and therefore we have provided a definition of the IoT as conceptual framework which is independent of the specific technologies involved. Indeed, we believe that at the present time finding an answer to the question "what IoT is and what it is not" avoids confusions

that could lead to the rejection of such a paradigm, which instead has the potentials to impact significantly on most of our current societal challenges.

REFERENCES

[1] S. Jeschke, "The internet of things in production technology: Heterogeneous agent systems for decentralized production paradigms," in *6. Expertenforum. Agenten im Umfeld von Industrie 4.0*, May 2014.

[2] [Online]. Available: http://postscapes.com/internet-of-things-history

[3] M. Weiser, "The computer for the twenty-first century," *Scientific American*, pp. 66–75, 1991.

[4] B. Sterling, *Shaping Things*. MIT Press, 2005.

[5] I. F. Akyildiz and J. M. Jornet, "The internet of nano-things," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 58–63, December 2010.

[6] J. M. Jornet and I. F. Akyildiz, "The internet of multimedia nano-things," *Nano Communication Networks*, vol. 3, no. 4, pp. 242–251, 2012.

[7] European Commission, "Horizon 2020 work programme 2014 2015, european commission decision c," July 2013.

[8] Policy Modelling and Governance Tools for Sustainable Urban Development, "State-of-the-art and future challenges," October 2013.

[9] J. Formo, A. Fasbender, M. Grdman, and T. Matsumura, "Social web of objects," Patent US 20 110 161 478 A1, 2011.

[10] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker, "Naming in content-oriented architectures," in *In Proc. of ACM SIGCOMM - ICN Workshop*, August 2011.

[11] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proc. of ACM CoNEXT*, December 2009.

[12] T. Berners-Lee, R. Fielding, and L. Masinter, "Uniform resource identifier (uri): Generic syntax," *IETF RFC 3986*, January 2005.

[13] K. Ashton, "presentation at procter & gamble in 1999, reported in internet of things thing. in the real world things matter more than ideas," *RFID Journal*, June 2009.

[14] "Auto-id labs." [Online]. Available: http://www.autoidlabs.org/

[15] *The EPCglobal Architecture Framework, EPCglobal Final Version 1.3*, March 2009.

[16] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using rfid: the rfid ecosystem experience," *IEEE Internet Computing*, vol. 13, no. 3, pp. 48–55, march 2009.

[17] A. Belpaire, "Internet of things "already a reality today", interview in eurescom mess@ge," *The Magazine for Telecom Insiders*, vol. 2, 2009.

[18] R. H. Weber, "Internet of things - new security and privacy challenges," *Computer law & security review*, vol. 26, pp. 23–30, 2010.

[19] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 860–880, May 2013.

[20] M. Presser and A. Gluhak, "The internet of things: Connecting the real world with the digital world, eurescom mess@ge," *The Magazine for Telecom Insiders*, vol. 2, 2009.

[21] J. Sung, T. Sanchez-Lopez, and D. Kim, "The epc sensor network for rfid and wsn integration infrastructure," in *Proc. of Fifth IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2007)*, March 2007.

[22] W. Wang, J. Sung, and D. Kim, "Complex event processing in epc sensor network middleware for both rfid and wsn," in *Proc. of the 11-th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*, May 2008.

[23] H. Liu, M. Bolic, A. Nayak, and I. Stojmenovic, "Taxonomy and challenges of the integration of rfid and wireless sensor networks," *IEEE Network*, vol. 22, no. 6, pp. 26–32, December 2008.

[24] "Epcglobal inc., network frame architecture." [Online]. Available: http://www.epcglobalinc.org/standards

[25] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev, "A wirelessly-powered platform for sensing and computation," in *Proc. of UbiComp 2006*, September 2006.

[26] "EPC radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz - 960 mhz, version 2.0.0," *Specification for RFID Air Interface*, November 2013.

[27] "ISO/IEC 18000-63 - Information technology - Radio frequency identification for item management - Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C," 2013.

[28] "Application level events (ale), version 1.1.1, epcglobal specification," March 2009.

[29] "Low level reader protocol (LLRP), Version 1.0.1, EPCglobal specification," August 2007.

[30] "ETSI. machine-to-machine communications (M2M): Functional architecture. etsi ts 102 690," 2013.

[31] A. N. Parks, A. P. Sample, Y. Zhao, and J. R. Smith, "A wireless sensing platform utilizing ambient rf energy," in *Proc. of IEEE Topical Meeting on Wireless Sensors and Sensor Networks*, January 2013.

[32] B. Kellog, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, "Wi-fi backscatter: Internet connectivity for rf-powered devices," in *Proc. of ACM SigComm*, August 2014.

[33] T. S. Lopez, D. Ranasinghe, M. Harrison, and D. McFarlane, "Adding sense to the internet of things: An architecture framework for smart object systems," *Personal and Ubiquitous Computing*, vol. 16, no. 3, pp. 291–308, March 2012.

[34] W. Heinzelman, A. Chandrakasan, , and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," in *Proc. of HICSS 2000*, January 2000.

[35] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," in *In Proc. of IEEE Infocom 2003*, March-April 2003.

[36] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14-15, pp. 2826–2841, October 2007.

[37] F. Carrez and et al., "Deliverable d1.5 final architectural reference model for the iot v3.0," IoT-A, Tech. Rep., 2013. [Online]. Available: http://www.iot-a.eu

[38] Y. Shim, T. Kwon, and Y. Choi, "Sarif: A novel framework for integrating wireless sensors and rfid networks," *IEEE Wireless Communications*, vol. 14, pp. 50–56, 2007.

[39] T. S. Lpez, D. Kim, G. H. Canepa, and K. Koumadi, "Integrating wireless sensors and rfid tags into energy-efficient and dynamic context networks," *Computer Journal*, vol. 52, pp. 240–267, 2009.

[40] I. Farris, A. Iera, A. Molinaro, and S. Pizzi, "A coap-compliant solution for efficient inclusion of rfid in the internet of things," in *In Proc. of IEEE Globecom*, December 2014.

[41] S. Lee, M. K. Shin, and H. J. Kim, "EPC vs. IPv6 mapping mechanism," in *Proc. of the The 9th International Conference on Advanced Communication Technology*, February 2007.

[42] S. Dominikus, M. Aigner, and S. Kraxberger, "Passive rfid technology for the internet of things," in *Proc. of ICITST 2010*, November 2010.

[43] S. E. H. Jensen and R. H. Jacobsen, "Integrating rfid with ip host identities," *in Book: Radio Frequency Identification from System to Applications*, 2013.

[44] A. J. Jara, S. Varakliotis, A. F. Skarmeta, and P. Kirstein, "Extending the internet of things to the future internet through ipv6 support," *Mobile Information Systems*, vol. 10, no. 1, pp. 3–17, January 2014.

[45] M.-C. Chung, G. M. Lee, N. Crespi, and C.-C. Tseng, "Rfid object tracking with ip compatibility for the internet of things," in *Proc. of IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing*, November 2012.

[46] D. Guinard, V. Trifa, and E. Wilde, "Architecting a mashable open world wide web of things," ETH, Tech. Rep., 2010.

[47] D. Guinard, V. Trifa, F. Mattern, and E. Wilde, *From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practice*. in D. Uckelmann, M. Harrison, F. Michahelles, "Architecting the Internet of Things", 2011.

[48] L. Atzori, A. Iera, and G. Morabito, "From "smart objects" to "social objects": The next evolutionary step of the internet of things," *IEEE Communications Magazine*, vol. 52, no. 1, pp. 97–105, January 2014.

[49] N. Kushalnagar, G. Montenegro, and C. Schumacher, "Ipv6 over low-power wireless personal area networks (6lowpans): Overview, assumptions, problem statement, and goals," *IETF RFC 4919*, August 2007.

[50] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebeke, F. V. den Abeele, E. D. Poorter, I. Moerman, and P. Demeester, "Ietf standardization in the field of the internet of things," *Journal of Sensor and Actuator Networks*, vol. 2, no. 2, pp. 235–287, June 2013.

[51] Sandvine Intelligent Broadband Networks, "Global internet phenomena report," 2013.

[52] D. Crockford, "The application/json media type fro javascript object notation (json)," *IETF RFC 4627*, July 2006.

[53] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "The constrained application protocol (coap)," *RFC 7252*, June 2014.

[54] D.Guinard, M. Mueller, and J.Pasquier-Rocha, "Giving rfid a rest: Building a web-enabled epcis," in *Proc. of Internet of Things Conference*, November-December 2010.

[55] F. Paganelli, S. Turchi, L. Bianchi, L. Ciofi, M. C. Pettenati, F. Pirri, and D. Giuli, "An information-centric and rest-based approach for epc information services," *Journal of Communications Software and Systems*, vol. 9, no. 1, March 2013.

[56] A. J. Jara, P. Moreno-Sanchez, A. F. Skarmeta, S. Varakliotis, and P. Kirstein, "Ipv6 addressing proxy: Mapping native addressing from legacy technologies and devices to the internet of things (ipv6)," *Sensors*, vol. 13, no. 5, pp. 6687–6712, May 2013.

[57] M. Mller, "RESTful EPCIS: Design and Implementation of a Web-enabled Electronic Product Code Information Service (EPCIS)," Master's thesis, University of Fribourg, 2009.

[58] A. Castellani, S. Loreto, A. Rahman, T. Fossati, and E. Dijk, "Best practices for http-coap mapping implementation," 2013. [Online]. Available: draft-castellanicore-http-mapping-07

[59] S. D'Oro, L. Galluccio, G. Morabito, and S. Palazzo, "Exploiting object group localization in the internet of things: a performance analysis," *To appear in IEEE Transactions on Vehicular Technology*, 2014.

[60] A. Kamilaris, D. Papadiomidous, and A. Pitsillides, "Lessons learned from online social networking of physical things," in *International Conference on Broadband and Wireless Computing, Communication and Applications*, October 2011.

[61] T. Schmid and M. B. Srivastava, "Exploiting social networks for sensor data sharing with senseshare," *CENS 5th Annual Research Review*, November 2007.

[62] E. Miluzzo, N. D. Lane, K. Fodor, R. A. Peterson, H. Lu, M. Musolesi, Shane, B. Eisenman, X. Zheng, and A. T. Campbell, "Sensing meets mobile social networks: The design, implementation and evaluation of the cenceme application," in *Proc. of 6th ACM Conference on Embedded Networked Sensor Systems*, April 2008.

[63] A. Pintus, D. Carboni, and A. Piras, "Paraimpu: a platform for a social web of things," in *Proc. of the 21st international conference companion on World Wide Web*, April 2012.

[64] V. Beltran, A. M. Ortiz, D. Hussein, and N. Crespi, "A semantic service creation platform for social iot," in *In Proc. of IEEE World Forum on Internet of Things (WF-IoT)*, March 2014.

[65] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahutha, M. Beigl, and H. Gallersen, "Smart-its friends: A technique for users to easily establish connections between smart artefacts," in *Proc. of ACM UbiComp*, September-October 2001.

[66] A. Zelenkauskaite, N. Bessis, S. Sotiriadis, and E. Asimakopoulou, "Interconnectedness of complex systems of internet of things through social network analysis for disaster management," in *Proc. of the 4th International Conference on Social networking*, September 2012.

[67] "Ninja blocks - the api for atoms," 2012.

[68] "Ifttt / put the internet to work for you."

[69] J. Zhou, T. Leppnen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, H. Jin, and L. T. Yang, "Cloudthings: a common architecture for integrating the internet of things with cloud computing," in *Proc. of IEEE International Conference on Computer Supported Cooperative Work in Design*, June 2013.

[70] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, p. 16451660, September 2013.

[71] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, p. 2636, July 2012.

[72] M. Amedeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. Aguiar, and A. Vasilakos, "Information-centric networking for the internet of things: Challenges and opportunities," *IEEE Network*, vol. in press, 2015.

[73] A. C. Boucouvalas, E. A. Kosmatos, and N. D. Tselikas, "Integrating rfids and smart objects into a unified internet of things architecture," *Advances in Internet of Things*, vol. 1, no. 1, pp. 5–12, April 2011.

[74] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot): when social networks meet the internet of things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, November 2012.

[75] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253 – 1266, May 2014.

[76] A. Ortiz, D. Hussein, S. Park, S. Han, and N. Crespi, "The cluster between internet of things and social networks: Review and research challenges," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 206–215, June 2014.

[77] Semantic Sensor Network XG, "Final report: W3c incubator group report," 2011. [Online]. Available: http://www.w3.org/2005/Incubator/ssn/XGR-ssn-20110628/

[78] C. Perera, A. Zaslavsky, C. H. Liu, M. Compton, P. Christen, and D. Georgakopoulos, "Sensor search techniques for sensing as a service architecture for the internet of things," *IEEE Sensors Journal*, vol. 14, no. 2, February 2014.

[79] S. De, B. Christophe, and K. Moessner, "Semantic enablers for dynamic digital-physical object associations in a federated node architecture for the internet of things," *Elsevier Ad Hoc Networks*, vol. 18, pp. 102–120, 2014.

[80] I. Stojimenovic and S. Olariu, "Data-centric protocols for wireless sensor networks," *in Handbook of Sensor Networks: Algorithms and Architectures*, 2005.

[81] N. Dinh and Y. Kim, "Icn wireless sensor and actor network baseline scenarios," *ICNRG Internet Draft*, January 2013.

[82] ——, "Potential of information-centric wireless sensor and actor networking," in *Proc. of COMMANTEL 2013*, January 2013.

[83] T.-X. Do and Y. Kim, "Information-centric wireless sensor and actor network in the industrial network," in *Proc. of ICTC*, October 2013.

[84] D. Kutscher and S. Farrell, "Towards an information-centric internet with more things," *IETF Internet Draft*, February 2011.

[85] Y. Zhang, D. Raychadhuri, L. Grieco, R. Ravindran, and G. Wang, "Icn based architecture for iot," *ICNRG Internet-Draft*, July 2014.

[86] Y. Zhang, D. Raychadhuri, L. Grieco, E. Baccelli, J. Burke, R. Ravindran, and G. Wang, "Icn based architecture for iot requirements and challenges," *ICNRG Internet-Draft*, July 2014.

[87] Y. Song, H. Ma, and L. Liu, "Content-centric internetworking for resource-constrained devices in the internet of things," in *Proc. of IEEE International Conference on Communications*, June 2013.

[88] O. Waltari, "Content-Centric Networking in the Internet of Things," Master's thesis, University of Helsinki, 2013.

[89] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro, "Named data networking for iot: an architectural perspective," in *In Proc. of European Conference on Networks and Communications*, June 2014.

[90] M. Amadeo, C. Campolo, and A. Molinaro, "Multi-source data retrieval in iot via named data networking," in *In Proc. of ACM Information-Centric Networking Conference*, September 2014.

[91] Y. Li, "Naming in the internet of things," 2013. [Online]. Available: http://www.cse.wustl.edu/ jain/cse570-13/index.html

[92] G. Marias, N. Fotiou, and G. C. Polyzos, "Efficient information lookup for the internet of things," in *Proc. of IEEE WoWMoM*, June 2012.

[93] P. Santi and J. Simon, "Silence is golden with high probability: maintaining a connected backbone in wireless sensor networks," *Wireless Sensor Networks*, vol. 2920, pp. 106–121, 2004.

[94] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From todays INTRAnet of things to a future INTERnet of things: a wireless- and mobility-based view," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 44–51, December 2010.

[95] S. Distefano, G. Merlino, and A. Puliafito, "Enabling the cloud of things," in *Proc. of IMIS 2012*, July 2012.

[96] S. Karnouskos, "Smart houses in the smart grid and the search for value-added services in the cloud of things era," in *Proc. of IEEE ICIT 2013*, February 2013.

[97] K. Tei and L. Gurgen, "Clout: Cloud of things for empowering the citizen cloud in smart cities," in *Proc. of IEEE WF-IoT*, March 2014.

[98] D. Guinard, C. Floerkemeier, and S. Sarma, "Cloud computing, rest and mashups to simplify rfid application development and deployment," in *Proc. of ACM WoT 2011*, June 2011.

[99] X. Shang, R. Zhang, D. Chen, and Y. Chen, "Agent-based epc-rfid network for smart awareness system," *Advances in Information Sciences and Service Sciences*, vol. 3, no. 6, July 2011.

[100] C. Turcu and C. Turcu, "The social internet of things and the rfid-based robots," in *Proc. of ICUMT 2012*, October 2012.

[101] L. A. Amaral, F. P. Hessel, E. A. Bezerra, J. C. Corra, O. B. Longhi, and T. F. Dias, "ecloudrfid a mobile software framework architecture for pervasive rfid-based applications," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 972–979, May 2011.

[102] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "Drug identification and interaction checker based on iot to minimize adverse drug reactions and improve drug compliance," *Personal Ubiquitous Computing*, vol. 18, no. 1, pp. 5–17, January 2014.

[103] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "Rfid technology for iot-based personal healthcare in smart spaces," *IEEE Internet of Things Journal*, vol. 1, no. 2, April 2014.

[104] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *In Proc. of the First Workshop on Mobile Computing*, August 2012.
[105] D. Kreutz, F. M. V. Ramos, P. E. Verssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of IEEE*, vol. 103, no. 1, pp. 14–76, January 2015.
[106] A. C. Anadiotis, L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "Towards a network operating system for the internet of things," in *Proc. of IEEE World Forum on Internet of Things (WF-IoT)*, December 2015.
[107] G. T. 22.368, "Service requirements for machine-type communications (mtc), v13.11.0," December 2014.
[108] ——, "Evolved universal terrestrial radio access (e-utra): Radio resource control (rrc) v10.5.0," March 2012.
[109] Z. 3GPP TSG RAN WG2 71, "Mtc simulation results with specific solutions, document r2-104662," 2010.
[110] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: a comprehensive survey," *IEEE Communication Survey and Tutorials*, vol. 18, no. 3, 2016.
[111] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," *IEEE Access*, 2015.
[112] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Next generation 5g wireless networks: a comprehensive survey," *IEEE Communication Magazine*, vol. 52, no. 2, pp. 74–80, February 2014.
[113] L. Militano, G. Araniti, M. Condoluci, I. Farris, and A. Iera, "Device-to-device communications for 5g internet of things," *EAI Endorsed Transactions on Internet of Things*, vol. 1, no. 1, 2015.
[114] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, October 2010.
[115] "Internet of things definitions." [Online]. Available: http://postscapes.com/internet-of-things-definition
[116] G. Venkat, "NoT IoT," June 2014. [Online]. Available: https://www.linkedin.com/today/post/article/20140620064438-52931539-not-iot
[117] R. R. Sterritt and M. Hinchey, "Autonomicity - an antidote for complexity?" in *Proc. of IEEE Computational Systems Bioinformatics Conference*, August 2005.
[118] P. Buxmann, T. Hess, and R. Ruggaber, "Internet of services," *Business & Information Systems Engineering*, vol. 1, no. 5, pp. 341–342, September 2009.
[119] ON.Lab, "Open network operating system (onos)," April 2016. [Online]. Available: http://onosproject.org