20

Building Blocks of the Internet of Things: State of the Art and Beyond

Alexandru Serbanati, Carlo Maria Medaglia and Ugo Biader Ceipidor
CATTID- "Sapienza" University of Rome
Italy

1. Introduction

ICT has simplified and automated many tasks in the industry and services sector. Computers can monitor and control physical devices from very small to very large scales: they are needed in order to produce semiconductor wafers and can help operating ships, airplanes or manufacturing devices. Until some years ago though, these solutions were monolithic and thus application specific.

In the field of monitoring and control, the wide adoption of modular design patterns and standardization, together with the improvements in communication technologies, paved the way to the diffusion of single component products that could be integrated as building blocks for ever more complex applications. An array of embedded devices and autoID technologies are now available as well as off-the-shelf platforms (ref Oracle, IBM, Arduino, Arch Rock, Sensinode) which can be used and customized for addressing specific purposes.

One of the biggest paradigms behind this trend is the Internet of Things (IoT) which foresees a world permeated with embedded smart devices, often called "smart objects", inter-connected through the Internet[1]. These devices should help blending together the digital and the physical world by providing Things with "identities and virtual personalities" (European Technology Platform on Smart Systems Integration [EPoSS], 2008) and by providing pervasive sensing and actuation features.

This scenario is very challenging as not all the building blocks of the IoT are yet in place. Standardization efforts are essential and have only recently been made and a reference architecture is still missing. Other researches on this topic nowadays focus on hardware and software issues such as energy harvesting, efficient cryptography, interoperability, communication protocols and semantics. The advent of IoT will also raise social, governance, privacy and security issues.

This work provides a historical and conceptual introduction to the IoT topic. In the second part of the chapter, a wide perspective on the aforementioned issues is provided. The work also outlines key aspects in the process of moving from the current state of the art of IoT, where objects have digital identities, towards a network of objects having digital personalities and being able to interact with each other and with the environment. In the last part, a selection of the possible impacts of the IoT is analyzed.

[1] A better definition of the phrase "Internet of Things" will be provided in the next Section.

2. Evolution of a vision

The concept of Internet of Things was originally coined by Kevin Ashton of the MIT Auto-ID Center to describe the possibility of using RFID tags in supply chains as pointers to Internet databases which contained information about the objects to which the tags were attached. The concepts heralded in the presentation made by Ashton in 1998, were soon realized in practice with the birth of the EPCglobal, a joint venture aiming to produce standards from the Auto-ID Center, which eventually created the EPC suite of standards and the homonymous architecture framework (Armenio et al., 2007).
The phrase maintained this meaning (Meloan, 2003), untill 2004, when, for the first time a world where "everyday objects [had] the ability to connect to a data network" was conceived (Gershenfeld et al., 2004). Innovative concepts such as the extreme device heterogeneity and IP-based, narrow-waist protocol stack were for the first time introduced for what was also called Internet0.
In the last years the hype surrounding the IoT grew in proportions. In the last years, quite a few definitions have been given and we will analyse them briefly in order to provide a better definition of the Internet of Things phrase.
In the final report of the Coordination and Support Action (CSA) for Global RFID-related Activities and Standardisation [CASAGRAS] project (CASAGRAS, 2009) the reader can find a compiled list of definitions which capture different aspects of and meanings given to the concept of Internet of Things:

Initial CASAGRAS definition: "*A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability*", Anthony Furness, European Centre of Excellence for AIDC

The CASAGRAS definition was given in the first part of year 2009, and was then confirmed in the final report of the project. In this definition the IoT is first and foremost a network infrastructure. This is coherent with the semantic meaning of the phrase which assumes that the IoT builds upon the existing Internet communication infrastructure. The definition is also focused on connection and automatic identification and data collection technologies that will be leveraged for integrating the objects in the IoT.

SAP definition: "*A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.*" Stephan Haller, SAP AG

We would like to note here the focus on the physical objects which are in the center of the attention as main participants of the IoT. They are described as active participants in the business processes. Besides, the IoT here is more a vision than a global network, as the word "world" would suggest. Also the idea of using services as communication interfaces for IoT is explicited. Services will soon become one of the most popular tools to broaden the basis of communication interoperability in the IoT vision. Security and privacy, though not related to the definition of IoT, are also highlighted as critical issues (see Section 5.3).

Future Internet Assembly/Real World Internet definition: *The IoT concept was initially based around enabling technologies such as Radio Frequency Identification (RFID) or wireless sensor and actuator networks (WSAN), but nowadays spawns a wide variety of devices with different computing and communication capabilities – generically termed networked embedded devices (NED). […] More recent ideas have driven the IoT towards an all encompassing vision to integrate the real world into the Internet […].*

More recent definitions seem to emphasize communication capabilities, and to assign a certain degree of intelligence to the objects (EPoSS, 2008; cited in Botterman, 2009).

"a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols."

"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts."

In conclusion, we can thus identify two different meanings (and thus definitions) of the phrase: the IoT network and the IoT paradigm. First and foremost, the Internet of Things is a global network, an extension of the current Internet to new types of devices – mainly constrained devices for WSANs and auto-ID readers –, aiming at providing the communication infrastructure for the implementation of the Internet of Things paradigm. The Internet of Things paradigm, on the other hand, refers to the vision of connecting the digital and the physical world in a new worldwide augmented continuum where users, either humans or physical objects (the things of the Internet of Things), could cooperate to fulfill their respective goals.

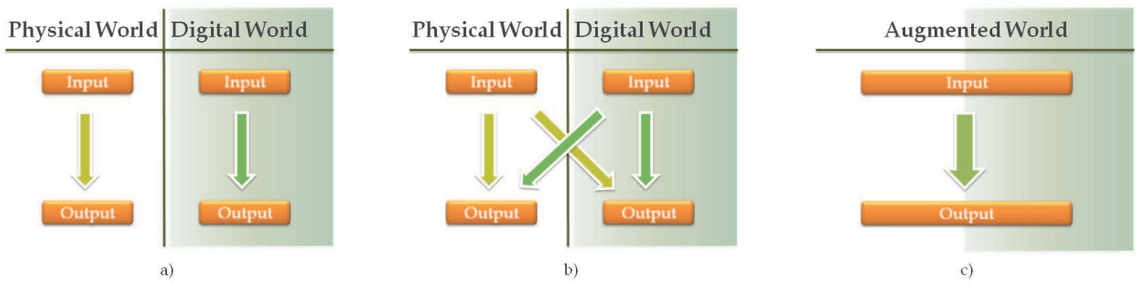


Fig. 1. The paradigm of IoT: from the current situation where digital and physical environments are uncoupled (a), to one where physical and digital world can interact (b) and finally to one where physical and digital worlds are merged sinergically in an augmented world (c).

In order to realize the IoT paradigm, the following features will be gradually developed and integrated in or on top of the Internet of Things network infrastructure, slowly transforming it into an infrastructure for providing global services for interacting with the physical world:

- object identification and presence detection
- autonomous data capture
- autoID-to-resource association
- interoperability between different communication technologies
- event transfer
- service-based interaction between objects
- semantic based communication between objects
- cooperation between autonomous objects.

3. A model for the Internet of Things

The aim of this section is to provide insight on the actors and components of the Internet of Things and how they will interact. We will provide our definition on the concepts we deem essential in the Internet of Things as previously defined in Section 2 .What is expressed in the following paragraphs has been heavily influenced by the fruitful interaction with our partners in the IoT-A project.

The generic IoT scenario can be identified with that of a generic *User* that needs to interact with a (possibly remote) *Physical Entity* of the physical world. In this short description we have already introduced the two key actors of the IoT. The *User* is a human person or a software agent[2] that has a goal, for the completion of which the interaction with the physical environment has to be performed through the mediation of the IoT. The *Physical Entity* is a discrete, identifiable part of the physical environment that can be of interest to the User for the completion of his goal. *Physical Entities* can be almost any object or environment, from humans or animals to cars, from store or logistic chain items to computers, from electronic appliances to closed or open environments.

Fig. 2. Basic abstraction of the IoT interaction

In the digital world *Digital Entities* are software entities which can be agents that have autonomous goals, can be services or wimple coherent data entries. Some *Digital Entities* can also interact with other *Digital Entities* or with *Users* in order to fulfill their goal. Indeed, *Digital Entities* can be viewed as *Users* in the IoT context. A *Physical Entity* can be represented in the digital world by a *Digital Entity* which is in fact its *Digital Proxy*. There are many kinds of digital representations of *Physical Entities* that we can imagine: 3D models, avatars, objects (or instances of a class in an object-oriented programming language) and even a social network account could be viewed as such. However, in the IoT context, *Digital Proxies* have two fundamental properties:

- they are *Digital Entities* that are bi-univocally associated to the *Physical Entity* they represent. Each *Digital Proxy* must have one and only one ID that identifies the represented object. The association between the *Digital Proxy* and the *Physical Entity* must be established automatically
- they are a synchronized representation of a given set of aspects (or properties) of the *Physical Entity*. This means that relevant digital parameters representing the characteristics of the *Physical Entity* can be updated upon any change of the former. In the same way, changes that affect the *Digital Proxy* could manifest on the *Physical Entity* in the physical world.

While there are different definitions of smart objects in literature (Kortuem et al., 2009), we define a *Smart Object* as the extension of a *Physical Entity* with its associated *Digital Proxy*. We have chosen this definition as, in our opinion, what is important in our opinion is the

[2] We prefer, wherever it is possible, not to introduce a distinction between the world of constrained devices and the one of full function devices. Some authors refer to the IoT as a concept related only to constrained devices. We prefer to stick to the previously provided definition, where the IoT is conceived as an extension of the Internet, thus including it and all the related concepts and components.
In this case for example, the 'software agent' can equally be one residing on a server, on an autonomous constrained device or running on the mobile phone.

synergy between the *Physical Entity* and the *Digital Proxy*, and not the specific technologies which enable it. Moreover, while the concept of "interest" is relevant in the IoT context (you only interact with what you are interested in) the term "Entity of Interest" (Haller, 2010) focuses too much attention on this concept and doesn't provide any insight on its role in the IoT domain. This term was an alternative to Entity in (Sensei, 2008), which in turn we view as an unnecessary abstraction that can also be misleading. For these reasons we have preferred the term *Smart Object*, which, even if not perfect (a person might be a *Smart Object*), is widely used in literature.

Indeed, what we deem essential in our vision of IoT though, is that any changes in the properties of a *Smart Object* have to be represented in both the physical and digital world. This is what actually enables everyday objects to become part of the digital processes.

This is usually obtained by embedding into, attaching to or simply placing in close vicinity of the *Physical Entity* one or more ICT devices which provide the technological interface for interacting with or gaining information about the *Physical Entity*, actually enhancing it and allowing it to be part of the digital world. These devices can be homogeneous as in the case of Body Area Network nodes or heterogeneous as in the case of RFID *Tag* and *Reader*. A *Device* thus mediates the interactions between *Physical Entities* (that have no projections in the digital world) and *Digital Proxies* (which have no projections in the physical world) extending both.

From a functional point of view, Device has three subtypes:

- *Sensors* can provide information about the *Physical Entity* they monitor. Information in this context ranges from the identity to measures of the physical state of the *Physical Entity*. The identity can be inherently bound to that of the device, as in the case of embedded devices, or it can be derived from observation of the object's features or attached *Tags*. Embedded *Sensors* are attached or otherwise embedded in the physical structure of the *Physical Entity* in order to enhance and provide direct connection to other *Smart Objects* or to the network. . Thus they also identify the Physical Entity. *Sensors* can also be external devices with onboard sensors and complex software which usually observe a specific environment in which they can identify and monitor *Physical Entities*, through the use of complex algorithms and software training techniques. The most common example of this category are face recognition systems which use the optical spectrum. *Sensors* can also be readers (see *Tags* below).
- *Tags* are used by specialized *Sensor* devices usually called readers in order to support the identification process. This process can be optical as in the case of barcodes and QRcode, or it can be RF-based as in the case of microwave car plate recognition systems and RFID.
- *Actuators* can modify the physical state of the *Physical Entity*. *Actuators* can move (translate, rotate, ...) simple *Physical Entities* or activate/deactivate functionalities of more complex ones.

It is also interesting to note that, as everyday objects can be logically grouped together to form a composite object and as complex objects can be divided in components, the same is also true for the *Digital Entities* and *Smart Objects* which can be logically grouped in a structured , often hierarchical way. As previously said, *Smart Objects* have projections in both the digital and physical world plane. Users that need to interact with them must do so through the use of *Resources*. *Resources*[3] are digital, identifiable components that implement different capabilities, and are associated to *Digital Entities*, specifically to *Digital Proxies* in the case of IoT. More than one *Resource* may be associated to one *Digital Proxy* and thus to one *Smart Object*. Five general classes of capabilities can be identified and provided through *Resources*:

[3] In this work we depart from the original and abstract meaning of the term (Berners-Lee, 1998) which we consider closer to the definition of *Entity of Interest*.

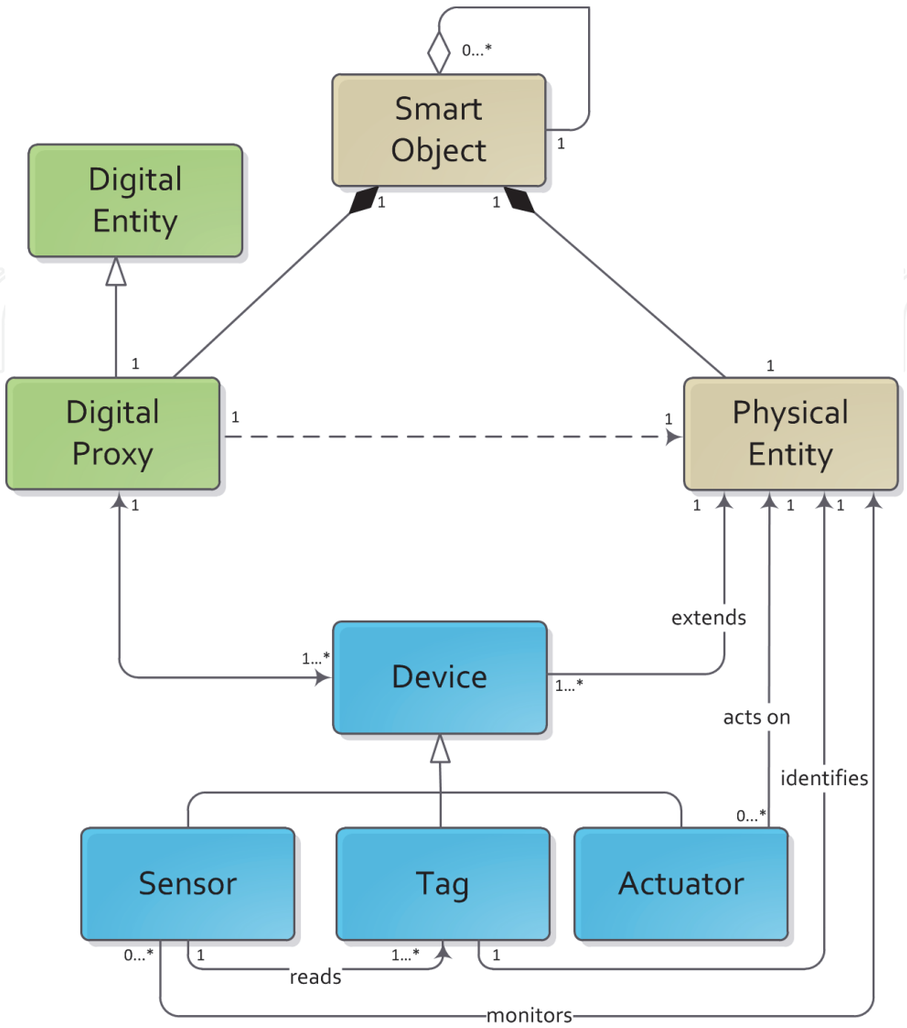


Fig. 3. Conceptual model of a Smart Object

- retrieval of physical properties of the associated *Physical Entity* captured through *Sensors;*
- modification of physical properties of associated *Physical Entity* through the use of *Actuators;*
- retrieval of digital properties of the associated *Digital Proxy;*
- modification of digital properties of the associated *Digital Proxy;*
- usage of complex hardware or software services provided by the associated *Smart Object*[4].

In order to provide interoperability, as they can be heterogeneous and implementations can be highly dependent on the underlying hardware of the *Device*, actual access to *Resources* is provided as *Services*.

[4] The use of remote processing capabilities for computation intensive operations (e.g. the resolution and lookup processes) or the usage of specific hardware (e.g. printers or projectors) are good examples of this kind of *Resources*.

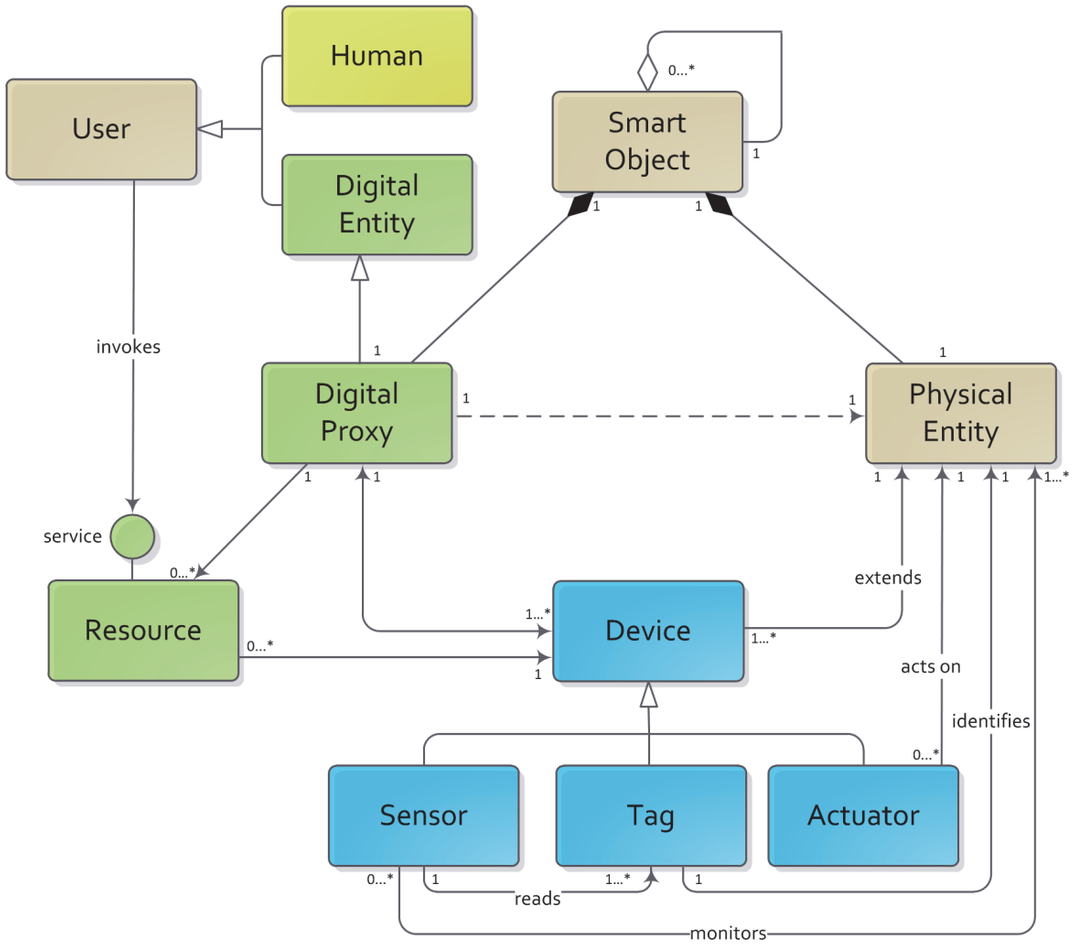


Fig. 4. Proposed Internet of Things reference model

The associations between *Smart Objects* and *Resources* (i.e. their identity) and the locations (i.e. network addresses) of the relative *Services* is either recorded in the *Smart Object* itself or can be stored (along with a small amount of auxiliary information) in what we call *Resolution Service*, an infrastructural component of the Internet of Things. The *Resolution Service* is conceived as a registry-based provider of the essential resolution service. Its task is very similar to that of current DNS or ONS service: it takes as input the ID of a *Smart Object* or *Resource* and provides as output the network addresses of the *Services* associated to it.
In the same way, a semantic description of the *Resources* and the ID of the associated *Virtual Proxy* is recorded in what we define the *Lookup Service*. This is similar to nowadays semantic search engines in that it accepts an input query and provides a relevance-ordered set of IDs, identifying *Resources* that might be useful to the *User*, according to the semantic query provided by the *User*.
Both the resolution and the lookup services can be provided as *Services*.

4. Identification, data collection and communication

The IoT vision had its base in the automatic identification (autoID). For the first time, ICT systems could assign an identity to common objects and soon these were able to become –

passive – part of automated, computer-managed processes. Such processes initially aimed at shadowing physical processes by monitoring them through the use of autoID.

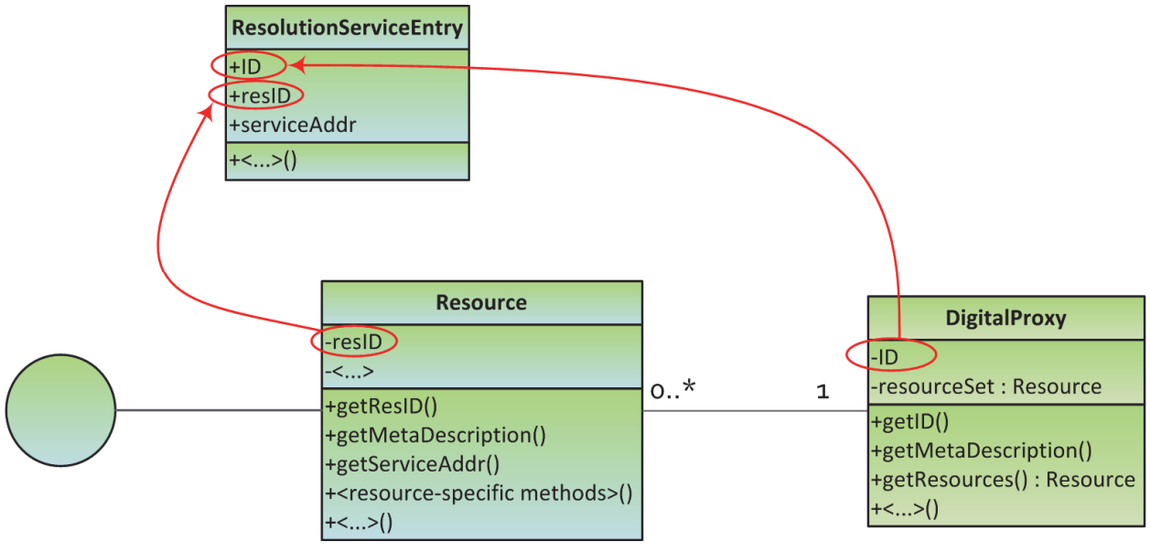


Fig. 5. Representation of the resolution registry

In the beginning, barcodes provided the first means of identifying items through optical labels. Barcodes eventually evolved, also thanks to the spread of camera-integrating mobile phones, to bi-dimensional optical codes such as QRcode (Denso Wave, n.d.). In the meanwhile, the well known RFID technology allowed for the first time real-world objects to be efficiently integrated in the digital processes, making in this way the first step towards the convergence and integration of digital and real world as the IoT paradigm proclaims. A relative small form-factor and low price together with the limited need of maintenance made this technology a good solution for specific supply chain and asset management solutions (Bose & Pal, 2005).
Unfortunately though, the RFID technology has its limits. Designed for identification, it can only provide information about presence and it also brings along a set of privacy and security issues. Semi-passive RFID tags can provide readings from battery powered sensors, but communication is still one-way and objects are not connected.
Sometimes passive RFID is also erroneously thought of as an authentication technology. This is a misconception, albeit common. The option of using RFID for authentication purposes should be thoroughly investigated prior to adoption and could prove even dangerous if system designers believe that RFID could provide a secure way of identifying things (Lehtonem et al., 2009).
When it comes to data collection, networks provide the most powerful solution. Bidirectional communication, enabling constant monitoring as well as command actuation, an always-available connection and higher data-rates sound definitely appealing. Wireless networks on the other hand prove to be a good solution because they need no physical infrastructure for operating and the deployment process is easier. And so, Wireless Sensor Networks (WSN) were born and provided new performance levels that were needed in some fields of data collection.
WSNs are made of a number of network (usually WPAN or LR-WPAN) nodes that often have automatically (re-)configuration capabilities and provide a wireless communication

channel for the data gathered by onboard sensors. A user or a central business logic can get the collected data through a special node, usually the coordinator of the network, that acts as gateway. A good knowledge base on WSNs can be found in (Akyldiz & Vuran, 2010). Bidirectional communication is also useful for requesting real-time data and commanding actuators. Hence the phrase Wireless Sensor and Actuator Network[5] thereafter WSAN) was coined. Bidirectional communication is also useful for reprogramming devices directly on the field (Karlof et al., 2004).

These technologies paved the way to a whole new set of applications thanks to their ease of deployment. With almost no need for a physical network infrastructure, WSANs attracted a lot of interest from application designers aiming to employ them in fields ranging from home and industrial automation (Sleman & Moeller, 2008), smart metering (Kistler et al., 2008), to precision agriculture (Xuemei et al., 2008), environmental monitoring and healthcare (Yang & Yacoub, 2006).

These applications though are just the top of a submerged iceberg when it comes to the possibilities provided by embedding sensor and actuators in the environment. The real revolution will take place when embedded devices will be able to provide and access resources through the Internet. This, together with the use of semantics will also uncover the untapped potential of context-awareness and autonomous decision making.

The first steps towards this vision have already been taken. As the IP protocol is the cornerstone of the Internet and, as the IoT will be an extension of the current Internet, many have proposed to use IP, and in particular IPv6, as the shared narrow-waist of IoT-capable protocol stacks (Vasseur, & Dunkels, 2010). Indeed, the perspective of having 50 to 100 billion devices by 2020 (Sundmaeker et al., 2009) can be even viewed as one of the drivers of the adoption of the IPv6.

In this context, the work of the 6LoWPAN group in providing an adaptation layer between IPv6 NWK layer and the MAC layer of IEEE 802.15.4 is worth mentioning (Bormann et al., 2009). The adaptation was needed because of the different purposes of the IPv6 and of the IEEE 802.15.4 standard for Low Rate WPANs (LR-WPANs). The former was based on the existing features of IPv4, and was designed for the Internet while, at design time, LR-WPANs were required to optimize energy consumption. Thus the work had to deal with the typical limitations of constrained devices.

One of the greatest issues was that the LR-WPAN PHY layer packet length of 127 bytes. This forced the workgroup to rely on the compression for the 40 bytes IPv6 header in order to achieve larger application-level payloads and thus greater efficiency in communication, which lead to RFC4944 (Montenegro et al., 2007). The reasons behind this choice can be understood considering that the MAC header has a maximum length of 25-bytes, that the possible overhead due to the MAC layer security can take up to 21 bytes and that fragmentation support in upper layers can reduce even more the actual application payload.

The potential of having small – though constrained devices – to the Internet has been readily perceived by the actors of the embedded devices market. For example, alongside the interest focused from the academic environment, it is relevant that all embedded platforms previously cited already provide support to 6LoWPAN. Contiki and Tiny OS, two of the major operating systems for embedded devices, also provide modules for 6LoWPAN.

[5] While in literature the term 'WSN' is much more used, we prefer to use 'WSAN' because, limiting the functional definition of such network to sensing doesn't fit with the IoT scenario, where the interaction with the real world is bidirectional

Communication capabilities are essential for achieving other features that have been associated to the Internet of Things. Cooperation among *Smart Objects* and the auspicated context-awareness are the most relevant. In order for devices to exchange meaningful data a proper support at service and application layer level is essential.

5. The missing building blocks

The IoT paradigm is a visionary one. Currently there are more questions than answers and many challenges need to be taken into account. Some building blocks, such as autoID technologies, WSANs and basic IP-based communication are (almost) available, yet others are still needed and obstacles pave the path to the advent of IoT. Nonetheless, this vision, unlike many others, is in the realm of possibility and the sheer momentum of the effort it focuses might lead to its success.

This section lists and analyzes the most relevant technological and scientific missing building blocks. Many of these topics have been discussed in the frame of the Internet of Things Architecture [IoT-A] project (IoT-A, 2010)[6], which aims at bridging many of these gaps.

A governance framework is also considered to be necessary, yet missing, and the relative issues will be depicted in the relative sub-section.

5.1 Interoperability

The paramount challenge at the moment seems to be interoperability. This issue has many facets, some of which are tightly intertwined to technical aspects. Even though there are many other challenges for the IoT, one of the most important requirement to keep in mind when addressing them is that they need to be solved in a common way for interoperability's sake. We have identified the following topics on which efforts from the research and stakeholder community in creating inter-operable solutions and towards standardization are most needed:

- reference architecture and protocol suites
- identification schemes
- routing and addressing
- resource resolution and lookup
- semantics

Though not strictly related to standardization, governance and intellectual property management also have to be addressed jointly and in an international frame. In this case though, it's not the research or stakeholder community that has to make efforts and take decisions, but the international entities that will be responsible of the management of the infrastructure of the IoT.

5.2 An architecture and a reference conceptual framework

Despite the interest in the topic and the huge amount of scientific papers, books and workshops about the Internet of Things, there is a manifested lack of consensus on some concepts and definitions related to the IoT.

As seen in Section 2, there is a certain degree of misalignment even in the definition of the Internet of Things and this also extends to other concepts used in this context. This

[6] See http://www.iot-a.eu

misalignment translates in the fact that the set of expected capabilities of the IoT is not the same throughout the scientific community. For example, it is not clear whether the ability of co-located objects to interact must be necessarily mediated by the central infrastructure services or could be realized by local service discovery processes.
Also, there's much uncertainty on the functional components of the IoT. Depending on the required features of the IoT, new infrastructure services will be needed. In Section 2, we have proposed the definition of *Lookup* and *Resolution Services*, but many other may be needed to cope with security and privacy issues for example. Such services also raise the problem of scalability from three perspectives:

- number of devices requesting a service from the IoT infrastructure.
- number of *Resource* entries in the registry of an infrastructure service on which to perform the search
- client device resources (bandwidth, battery, processing power, which decrease going towards the periphery of the IoT network)

In this context, the fact that there is no reference architecture for the IoT is almost a consequence. To our best knowledge, there is very limited literature on the topic yet (Tsiatsis et al., 2010; Vazquez et al., 2010). The IoT-A project (IoT-A, 2010), as the name suggests, will address thoroughly this issue in its three years' course.

5.3 Privacy and security

Privacy and security, or the lack of, also pose a significant challenge for the correct deployment of the IoT concept. Clearly, the peripheral part of the IoT is the most vulnerable one. Here, networks of constrained devices and data-collection systems, generally characterized by very limited resources, aim to collect and transport sensible and sometimes critical data.
More and more often, such systems rely on wireless communication, which has greatly improved the ease of deployment of data-collection systems, overcoming physical limitations related to the weaving of cables needed for the communication infrastructure. From a security point of view though, wireless systems (such as today's WNANs or RFID systems) have an intrinsic downside: they use a shared physical medium for communication. To share the air as physical medium means that attackers can easily and anonymously obtain access to packets sent over the air from far away and with minimum costs. Access to data is then a simple matter if this is not encrypted. Moreover, as there is no physical authentication, malicious users can inject forged packets at Link Layer level, disrupting the network and possibly compromising any functionality of the upper layers.
Though many solutions for improving passive RFID security have been proposed in the scientific community, very few standards actually implement relevant security features (Oertel et al., 2005). The general problem is that passive RFID tags provide a very limited and vulnerable memory storage as well as minimal processing capabilities. These aspects limit in turn the flexibility of the security features, so that, at the best of our searches to date, it is impossible to secure (provide at least authentication, confidentiality and freshness) the typical IoT scenarios where RFID tags can move around and interact with different readers, pertaining to different security domains.
For what concerns peripheral networks, in order to provide confidentiality, integrity and authentication features, security frameworks (Casado et al., 2009; Karlof et al., 2004; Luk et al., 2007) can be used. These frameworks work at Link Layer level in order to protect the functionalities of the higher layers. On the downside though, they introduce a relatively consistent communication and processing overhead to achieve their goal. Authentication in particular is essential in order to deny packet forging and avoid replay attacks.

Even for these systems, there is another common issue: in such systems there is no trusted actor (i.e. device) by default. The process of defining a trusted actor and sharing the "secret", or key, subsequently used for authentication or encryption, is a critical and vulnerable one. Because of its utter importance, it also has to be done in a safe environment which generally means connecting to the devices physically (by cable) or wirelessly in a safe environment. Moreover, in such systems, keys are usually network-wide because of memory constraints, which means that compromising one node, might compromise the whole network/system. Also, such keys cannot be as long as the standard length for unconstrained devices because of the limited computational power.

As pointed out in (Vazquez et al., 2010), smart objects with communication capabilities usually use a gateway in order to connect to the Internet. This gateway usually is at the edge between the domain of constrained and unconstrained devices and usually having less constraints than peripheral devices. It is interesting to note that these devices are also on the border of two domains characterized by different security capabilities. It is thus reasonable to delegate to these devices the task of providing the needed security scalability for providing end-to-end security features. In Figure 5 we describe three possible scenarios for what concerns authentication scalability. We consider that gateways can authenticate all traffic incoming from the Internet side with a standard length key and that, in the most demanding scenario, they, at the same time authenticate all the outgoing from the WSAN. These scenarios can be easily adapted for the confidentiality and integrity features.

A more complex scenario though configures in the case of nomadic nodes that use unfamiliar networks to connect to the Internet and thus were not pre-configured. In this case, there is also the issue of having nodes that do not trust the gateway by default. A Certification Authority (thereafter CA) could be used to provide mutual trust between the gateway and he mobile node, but this might prove risky as the access to the CA is provided by the (un-trusted) gateway.

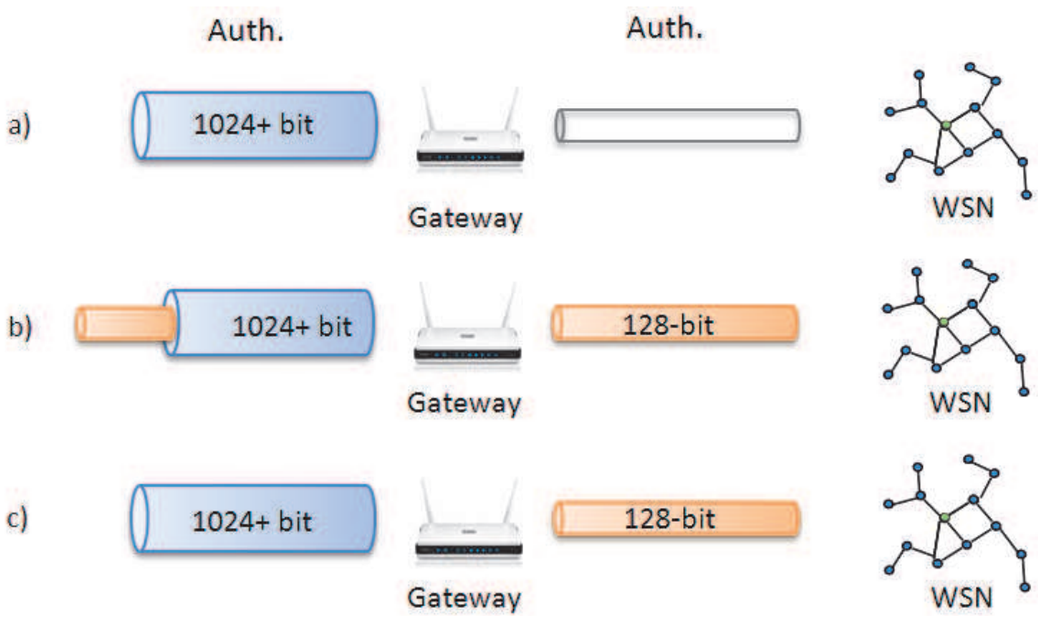


Fig. 6. Security scalability scenarios: only the gateway (and thus the source network) can be authenticated, b) tunnelling and c) active scaling of features

In conclusion, in current WSAN-based IoT-like systems a) an Internet-wide security framework implementation for granting Link Layer security features is not feasible, b) long keys cannot be used for cryptography/signing on embedded devices, c) security of mobile constrained devices is even more problematic and d) we suggest the use of gateways as tools for scaling the security features between the core area of the IoT network and the peripheral part.

5.4 Governance

A specific regulatory frame that takes into account private, business and public needs for the IoT is needed. Also, governing bodies have to adopt a shared strategy for managing, maintaining a global, international and possibly critical infrastructure such as the Internet of Things.

Defining and enforcing policies for such a network is also an important and delicate issue due to its characteristics (physical pervasiveness, trans-national reach, transport of sensitive data, ...) and the criticality of the potential implications.

If today's Internet has stretched the previous definitions of intellectual property, the IoT scenario will likely challenge the old definitions. For example, imagine a future environment, a private ground that is publicly accessible, such as a supermarket. Many people move through this space and the devices they wear continuously collect data in the open environment. This data might be made accessible to users all over the world through the IoT. But whose property is this data? Does it belong to the environment's owner, to the sensor's owner, or to the collector of the data? And in the case that the sensor simply traces other devices? How will the user be informed that some data regarding him has been acquired? Actually will he be informed? How will privacy rules be enforced in such an environment?

Many questions, but few answers. It is certain though that the Internet of Things will introduce a whole new set of security and privacy issues and that users shall be able to understand and manage the security and privacy features of their devices in order to benefit from the deployment of IoT. This is of the utmost importance and we believe that it is one of the main priorities of the governance to design and supervise this process.

6. Implications

6.1 Social implications

Pervasive technologies might have a consistent and positive impact on society but they also have the power to be very disruptive. For these reasons, the design and adoption of the Internet of Things shall be performed taking into account the implications on society that we can foresee and limiting, where it can be done, the consequences we cannot predict.

For example, the digital divide is one of the issues which we can foretell that will be accentuated by the adoption of the IoT, if not correctly designed. In first stance, the digital culture is not homogeneously distributed across the territory: people living in densely populated areas usually are more used to technology and adapt easier to new IT developments. IoT will be a great challenge for all users because the interaction paradigm will be completely new to them. In order just to realize how difficult it will be, one could think of how the users will manage the privacy and security features of the 3 to 8, display-less devices which have been forecasted belong to their personal space.

In second stance, while deploying stand-alone WSAN solutions in remote areas is relatively easy, taking the Internet of Things to rural areas will be very difficult due to the fact that a proper infrastructure and maintenance will be needed. The advent of IoT without a properly

established and pervasive infrastructure for connecting to the Internet could accentuate the division between less and more urbanized areas.
Another underestimated impact of the IoT in on education. The acceleration of the information flow and the handily availability of information in what will be an augmented reality will drastically change the way people learn things. If young people manage to master the new interaction paradigms that will characterize IoT, their relation to the physical world will also be drastically changed and we do not know how these changes will manifest later on.

6.2 Economic implications

The IoT will doubtlessly have an impact on economy. While in the first phase we expect only a limited, vertical impact, with the wider adoption of IoT-enabled solutions, the benefit derived from adopting the IoT paradigm will increase in a typically exponential way.
The first impact we foresee is the improvement of process efficiency in all economic sectors thanks to the adoption of large-scale automation. In second stance, brand new services for private, public and business users will be designed and developed.
There are though many open questions related to the economic implications of large-scale adoption of IoT. Such questions involve all scales from enterprise-level to an international level:

- what will the underlying business models look like? When will the ROI rate be high enough to sustain the spontaneous adoption of the IoT paradigm by mainstream enterprises in industry and agriculture?
- will excessive automation change the economic model of countries? Will it have a negative impact on society?
- as the time of adoption of the IoT by developed countries will come sooner than in in-development countries, will this accentuate the gap between them? Or could this even help the economy of such countries?

While we strongly believe that it's important to keep these questions in mind while designing the Internet of Things, we also believe that, due the expected highly-accelerated rate of development and adoption, having accurate long-term forecasts in the IoT scenario is very difficult.

6.3 Environmental impact

Having such a large amount of "things" integrating electronic circuitry and components might have a significant impact on the environment. First of all, the shear amount of hardly recyclable or even hazardous materials that will be introduced in the environment could represent a serious pollution danger. Moreover objects integrating electronic devices that are disposed of at the end of their life cycle will be difficult to treat, let alone to recycle, which again can increase pollution. Thus, new materials and recycling techniques for objects incorporating electronic devices should be developed.

7. Conclusions

From a technical point of view, the Internet of Things is an interesting evolutionary path in the Age of Information, likely making the newborn smart objects replace humans as the main consumers of Internet-transported data in a 10 years' time span. It also has the potential to radically change our life and the relationship with the environment. We have provided a reference model for the Internet of Things and highlighted some of the most

critical missing building blocks needed for its advent. We also looked into some impacts of this advent that apparently have been neglected till now.
One important concept we would like to disseminate through this article is that designing the IoT in all its aspects is very important. The results of this design phase will affect human life in almost all aspects and at all territorial scopes.

8. Acknowledgment

The authors would like to thank the European Commission for their timely commitment to the research on the Internet of Things topic and, in particular, for the sponsorship of the IoT-A project in the frame of FP7. We would also like to acknowledge the fruitful discussions with the partners in the IoT-A frame, which were the seeds of many of the ideas presented herein.

9. References

Akyldiz, I., Vuran, M.C. (2010), *Wireless Sensor Networks*, John Wiley & Sons Inc., 978-0-470-03601-3 (H/B), New York, NY, USA.

Arch Rock, (2009) Available from: http://www.archrock.com Note: as Arch Rock has been acquired by Cisco as of Sept. 20, 2010, some resources on the site might not be accessible.

Arduino, Available from: http://www.arduino.cc

Armenio, F., et al. (2007) EPCglobal Architecture Framework v1.2, available http://www.gs1.org/sites/default/files/docs/architecture/architecture_1_2-framework-20070910.pdf

Berners-Lee, T., Fielding, R., Irvine, U. C., Masinter, L., (1998) RFC2396: Uniform Resource Identifier (URI): General Syntax, last accessed A 2011, available from http://tools.ietf.org/html/rfc2396

Bormann, C., Mulligan, G., Arkko, J., Townsley, M., (2009) IPv6 over Low power WPAN (6LoWPAN), last accessed March 2011, available from http://www.ietf.org/html.charters/6lowpan-charter.html

Bose, I., Pal, R., (2005) Auto-ID: managing anything, anywhere, anytime in the supply chain, *Communications of the ACM*, 48(8), pp.100-106.

Botterman, M., (2009) Internet of Things: an early reality of the Future Internet. Workshop Report, European Commission Information Society and Media.

Casado, L., Tsigas P. (2009) ContikiSec: A Secure Network Layer for Wireless Sensor Networks under the Contiki Operating System, *Lecture Notes in Computer Science*, vol. 5838, pp. 133-147, Springer Berlin / Heidelberg.

Coordination and Support Action (CSA) for Global RFID-related Activities and Standardisation [CASAGRAS] (2009) Final report, Available from http://www.rfidglobal.eu

European Technology Platform on Smart Systems Integration, [EPoSS], (2008) Internet of things in 2020, report of *Beyond RFID - the Internet of Things*, joint EU-EPoSS workshop, Brussels (BE), February 2008, last accessed March 2011, available from http://www.smart-systems-integration.org/public/internet-of-things

Gershenfeld N., Krikorian R., Cohen D., (2004) The Internet of Things, *in Scientific American*, October 2004, pp 76-81.

Haller, S., The Things in the Internet of Things, *Proceedings of Internet of Things Conference 2010*, Tokyo, 2010

IBM, IBM Mote Runner, last accessed March 2011, available from: http://www.sensinode.com/

Internet of Things Architecture [IoT-A], 2010, available from http://www.iot-a.eu

Karlof, C., Sastry, N., Wagner, D. (2004) TinySec: a link layer security architecture for wireless sensor networks. *Proceedings of 2nd International Conference on Embedded Networked Sensor Systems*, SenSys 2004, Baltimore, MD, USA, November 3-5, 2004, pp. 162–175, ACM.

Kistler, R., Knauth, S., Klapproth, A., (2008) EnerBee – An Example of an Advanced Metering Infrastructure Based on ZigBee, EuZDC.

Kortuem, G., Kawsar, F., Fitton, D., Sundramoorthy, V. (2009) Smart objects as building blocks for the Internet of things, Internet Computing, IEEE Journal of, Vol.14, pp44–51.

Lehtonen, M., Ruhanen, A., Michahelles, F. and Fleisch, E., Serialized TID numbers - A headache or a blessing for RFID crackers?, *Proceedings of RFID, IEEE International Conference on*, Orlando (FL), April 2009.

Luk, M., Mezzour, G., Perrig, A., Gligor, V., (2007) MiniSec: a secure sensor network communication architecture. *Proceedings of 6th International Conference on Information processing in Sensor Networks*.

Meloan, S., (2003) Toward a Global "Internet of Things", Available from http://java.sun.com/developer/technicalArticles/Ecommerce/rfid/.

Montenegro, G., Kushalnagar, N., Hui, J., Culler, D. (2007) IPv6 over IEEE 802.15.4", RFC 4944.

Oertel, B., Wölk, M., Hilty, L., (2005) Security Aspects and Prospective Applications of RFID Systems, Federal Office for Information Security, last accessed March 2011, available from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/RFID/RIKCHA_englisch_pdf.pdf .

Oracle, Oracle Sun SPOT, Available from: http://www.sunspotworld.com/.

SENSEI, (2008) SENSEI Reference Architecture, Retrieved from: http://www.ict-sensei.org/index.php?option=com_docman&task=doc_download&gid=44&Itemid=49

Sleman, A., Moeller, R., (2008) Integration of Wireless Sensor Network Services into other Home and Industrial networks; using Device Profile for Web Services (DPWS), *Information and Communication Technologies: From Theory to Applications 2008*, pp. 1-5.

Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S., (2009) Vision and Challenges for Realising the Internet of Things, last accessed March 2011, available from http://docbox.etsi.org/tispan/open/IoT/CERP-IOT_Clusterbook_2009.pdf.

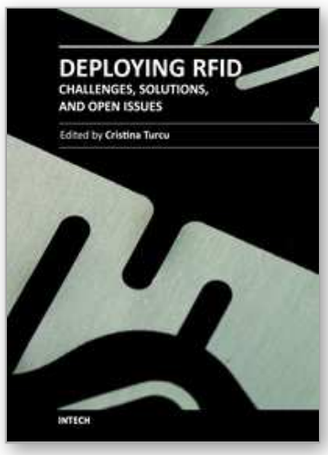
Tsiatsis, V., Gluhak, A., Bauge, T., Montagut, F., Bernat, J., Bauer, M., Villalonga, C., Barnaghi, P., Krco, S., (2010), The SENSEI Real World Internet Architecture, *in Towards the Future Internet - Emerging Trends from European Research*, pp 247-256, 2010, IOS Press, 978-1-60750-538-9

Vasseur, J.P., Dunkels, A. (2010) *Interconnecting Smart Objects with IP: The Next Internet*, Morgan Kaufmann, 978-0-12375-165-2.

Vazquez, J. I., Ruiz-de-Garibay, J, Eguiluz, X. , Doamo, I., Rentería, S., Ayerbe, A., (2010) Communication Architectures and Experiences for Web-Connected Physical Smart Object, *in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on*, 978-1-4244-6605-4 , Mannheim, March 29 - April 2 2010.

Xuemei, L., Yuyan, D., Lixing, D. (2008) Study on Precision Agriculture Monitoring Framework Based on WSN, International Conference on Anti-counterfeiting Security and Identification, pp. 182-185.

Yang, G.Z., Yacoub, M., (2006) *Body Sensor Networks*, Springler Berlin / Heidelberg, 978-1-84628-272-0, London, UK.



Deploying RFID - Challenges, Solutions, and Open Issues
Edited by Dr. Cristina Turcu

ISBN 978-953-307-380-4
Hard cover, 382 pages
Publisher InTech
Published online 17, August, 2011
Published in print edition August, 2011

Radio frequency identification (RFID) is a technology that is rapidly gaining popularity due to its several benefits in a wide area of applications like inventory tracking, supply chain management, automated manufacturing, healthcare, etc. The benefits of implementing RFID technologies can be seen in terms of efficiency (increased speed in production, reduced shrinkage, lower error rates, improved asset tracking etc.) or effectiveness (services that companies provide to the customers). Leading to considerable operational and strategic benefits, RFID technology continues to bring new levels of intelligence and information, strengthening the experience of all participants in this research domain, and serving as a valuable authentication technology. We hope this book will be useful for engineers, researchers and industry personnel, and provide them with some new ideas to address current and future issues they might be facing.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen