Architecting the Internet of Things: State of the Art

Architecting the Internet of Things: State of the Art

Mohammed Riyadh Abdmeziem[1], Djamel Tandjaoui[2], and Imed Romdhani[3]

[1] LSI, USTHB: University of Sciences and Technology Houari Boumedienne
BP 32, El Alia Bab Ezzouar, Algiers, Algeria.
rabdmeziem@usthb.dz
[2] CERIST: Center for Research on Scientific and Technical Information
03, Rue des freres Aissou, Ben Aknoun, Algiers, Algeria.
dtandjaoui@mail.cerist.dz
[3] School of Computing, Edinburgh Napier University
10, Colinton Road, EH10 5DT, Edinburgh, UK.
I.Romdhani@napier.ac.uk

Keywords: Internet of Things, Architecture, Middleware, RFID, WSN, Sensor Cloud, Robotic Cloud

Abstract. Internet of things (IoT) constitutes one of the most important technological development in the last decade. It has the potential to deeply affect our life style. However, its success relies greatly on a well-defined architecture that will provide scalable, dynamic, and secure basement to its deployment. In fact, several challenges stand between the conceptual idea of IoT, and the full deployement of its applications into our daily life. IoT deployment is closely related to the establishment of a standard architecture. This architecture should support future extensions, and covers IoT characteristics such as distributivity, interoperability, and scalability. A well defined, scalable, backward compatible, and secure architecture is required to bring the IoT concept closer to reality. In the literature, several architectures have been proposed. Nevertheless, each architecture brings a share of drawbacks, and fails covering all IoT characterisitcs. In this chapter, we review the main proposed architectures for the Internet of Things, highlighting their adequacy with respect to IoT requirements. Firstly, we present IoT building blocks. Then, we introduce the high level architecture of IoT before diving into the details of each proposed architecture. In addition, we introduce a classification of the reviewed architectures based on their technical aspects, and their ability to match IoT characteristics. Finally, based on the main shortcomings of the proposed architectures, we conclude with some design ideas for shaping the future IoT.

1 Introduction

Internet of Things (IoT) is one of the main communication development in recent years. It makes our everyday objects (e.g. health sensors, industrial equipements, vehicules, clothes, etc.) connected to each other and to the Internet. According to [1], the basic concept behind IoT is the pervasive presence around us of various wireless technologies such as Radio-Frequency IDentification (RFID) tags, sensors, actuators and mobile phones, in which computing and communication systems are seamlessly embedded. Through unique adressing schemes, these objects interact with each other, and cooperate to reach common goals. In fact, this interconnection allows the objects surrounding us to share data, to interact, and to act autonomously on behalf of their users. This prospect opens new doors toward a future, where the real and virtual world merge seamlessly through the massive deployment of embedded devices. These latter enhance dumb objects with computational, communication and storage capabilities. By enabling interactions with and among smart objects, IoT has the potential to add a new dimension in the communication sector. In addition, technology advances coupled with users need will encourage the wide spread deployement of IoT's applications. These applications would deeply affect our corporations, communities, and personal lives. In fact, enabling the objects in our everyday environment to possibly communicate with each other, and process the gathered information will open wide horizons for unpredicted applications [2].

From the perspective of a private use, e-health is one of the most interesting applications. In fact, it provides medical monitoring to millions of elderly and disabled patients while preserving their autonomy and comfort anywhere. For instance, using sensors planted in or around a patient, physiological data is gathered and transmitted to qualified medical staff that can intervene in case of an emergency. At home, energy management could be improved through the control of home equipments such as air conditioners, refrigerators, washing machines, etc. An other illustration of IoT applications in the personal sphere relies on social networking paradigm. Indeed, an interesting development would be using a Twitter like concept. In this concept, various objects in the house can periodically tweet the readings, which can be easily followed from anywhere [3]. From the perspective of business use, environmental monitoring can be achieved by keeping track of the number of occupants, and by managing the utilities within a building. Supply chains could also benifits from the introduction of RFID and NFC (Near Field Communication) devices. As a result, real-time and precise data on the inventory of finished goods could be gathered. In addition, from the perspective of utility services, smart grids are one of the most interesting applications. Using these applications, efficient energy consumption can be achieved through continuous monitoring of electric consumption. Furthermore, gathered data is used to maintain the load balance within the grid ensuring high quality of service [4].

Several challenges stand between the conceptual idea of IoT and the full deployement of its applications into our daily life. In fact, IoT successful deployment is closely related to the establishment of a standard architecture. This latter should cover IoT characteristics and support future extensions, the same way current Internet architecture achieved during the past forty years. A well defined, scalable, backward compatible, and secure architecture is required to bring the IoT concept closer to reality. In the literature, several architectures have been proposed [5][6][7][8][9][10] [11]. Nevertheless, each architecture brings a share of drawbacks, and fails covering all IoT characterisitcs. These characteristics can be summarized as follows:

- **Distributivity:** IoT will likely evolve in a highly distributed environement. In fact, data might be gathered from different sources and processed by several entities in a distributed manner.
- **Interoperability:** Devices from different vendors will have to cooperate in order to achieve common goals. In addition, systems and protocols will have to be designed in a way that allows objects (devices) from different manufacturers to exchange data and work in an interoperable way.
- **Scalability:** in IoT, billions of objects are expected to be part of the network. Thus, systems and applications that run on top of them will have to manage this unprecedent amount of generated data.
- **Resources scarcity:** both power and computation ressources will be highly scarce.
- **Security:** users feelings of helplessness and being under some unknown external control could seriously hinder IoT's deployment.

In this chapter, we review the main proposed architectures for the Internet of Things, highlighting their adequacy with respect to IoT requirements. We introduce the enabling technologies that are expected to form the building blocks of the IoT in section 2. In section 3, we discuss in detail and classify the different proposed architecture for the IoT gathered into two categories, clean slate architectures and tailored acrchitectures. In section 4, we provide an in-depth analysis of the proposed architectures based on their technical aspect and their ability to match IoT characteristics. Section 5 concludes the chapter.

2 IoT building blocks

Instead of emerging as a completely new category of systems, the Internet of Things is likely to rise through an incremental development approach. In fact, in order to reach the physical realm, IoT building blocks will be progressively integrated to the existing Internet. In this section, we focus on the enabling technologies that are expected to form the IoT building blocks. Each technology is briefly introduced, along with its future impact on IoT. The different technologies are classified into three categories.

- The sensing technologies through which the required data is gathered.
- The middleware layer that is in charge of processing and managing the obtained raw data. In fact, it provides an abstraction level to users and developers.
- The actuating technologies that represent the physical extension of IoT applications.

As a result, IoT would not only provide a digital support but also a physical one that can directly affect our real world. In the following, we briefly introduce the building blocks of each category.

2.1 Sensing

In the IoT, wireless technologies will play a central role in data harvesting and data communication. In fact, the major part of data traffic between objects will be carried through wireless media. Wireless Sensor Networks (WSN) and radio-frequency identification (RFID) are considered as the two main building blocks of sensing and communication technologies for IoT [2]. Indeed, their ability of sensing the environment and self-organizing into ad hoc networks represent an important feature from the IoT perspective. Nevertheless, these technologies suffer from different constraints (e.g. energy limitation, realiability of wireless medium, security and privacy, etc). In particular, the scarcity of energy resources available in the embedded devices is a sensitive issue. Consequently, to increase energy efficiency, a number of solutions have been introduced in the literature. For instance, lightweight MAC protocols [12], energy efficient routing protocols [13], and tailored security protocols [14] have been proposed to mitigate the impact of resources scarcity on sensing technologies. Still, their limited autonomy remains a considerable obstacle to their widespread deployment into our daily lives. Besides, the future objects, enhanced with sensing capabilities, are expected to share a set of common characteristics and functionnalities. Indeed, these objects will have to properly manage heterogeneity in order to move towards an incremental deployment. In the following, we provide a broad presentation of RFID, WSN, and their integration into the IoT.

RFID technology is considered as an important development in the embedded devices field. In fact, RFID allows the design of tiny microchips (called tags), which can be appended to an object of our daily life. As a result, stored data in these tags can automatically be used to identify and extract useful information from the object. Thus, the tag acts as an electronic barcode.

From a hardware perspective (Figure 1) an RFID tag is a tiny microchip (e.g. 0.4 mm x 0.4 mm x 0.15 mm) attached to an antenna, which is used for both receiving the reader signal and transmitting the tag identity. The tag is manufactured in a package that can be used as an adhesive sticker [15].

Generally, RFID devices are classified into two categories: passive and active. The passive RFID tags are not battery powered. In fact, they use the power of the readers interrogation signal to communicate their data. A lot of applications from several fields use this kind of tags. Particularly, in retail, supply chain management, and transportation. They are also used in bank cards and road toll tags as an access control mean. However, the active RFID readers possess their own battery energy, and are able to trigger a communication. Although the radio coverage is more important compared to passive tags, this is obtained

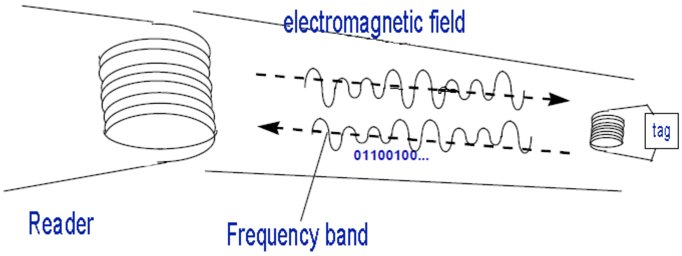

Fig. 1. RFID tag and reader

at the expense of higher production costs. In fact, one of the most interesting advantge in the use of RFID technology is the limited cost, which would allow a widespread adoption. Among other applications, active RFID tags can be used in port containers for monitoring cargo, robotics in a smart home context, and in hotels to provide automated check-in for customers[16].

Sensor networks on their side will also play a crucial role in the future deployment of IoT. In fact, they can cooperate with RFID systems to better track the status of things (e.g. their location, temperature, movements, etc). Doing so, WSN are able to augment their awareness of the environment. Hence, they act as a further bridge between the physical and the digital world.

Sensor networks consist of a certain number, which can be very high, of sensing nodes communicating in a wireless multi-hop fashion (Figure 2). In general, nodes report their sensing results to a small number of special nodes called sinks (or base stations). A lot of effort has been undertaken by the scientific community on sensor networks. Indeed, many work have addressed several problems at the different layers of the protocol stack. In these works, the main issues concern energy efficiency (which is a limited resource in WSN), scalability (the number of nodes can rise significantly), reliability (the system might be involved in critical applications), and robustness (nodes might be subject to failure) [17].

Integration of sensing technologies into passive RFID tags would bring completely new applications into the IoT context. In fact, sensing RFID systems will allow to build RFID sensor networks, which consist of small RFID-based sensing and computing devices. RFID readers would constitute the sinks of data generated by sensing RFID tags. Moreover, they would provide the power for the different network operations. Efficiently networking tag readers with RFID sensors would allow real-time queries on the physical world. This could lead to

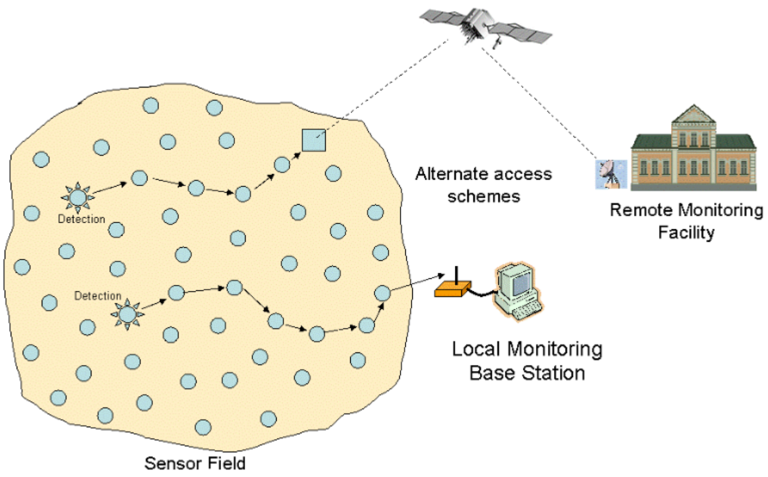

Fig. 2. Wireless Sensor Network

better forecasts, new business models, and improved management techniques [18].

2.2 Middleware

The middleware is a software interface between the physical layer (i.e. hardware) and the application one. It provides the required abstraction to hide the heterogeneity and the complexity of the underlying technologies involved in the lower layers. In fact, the middleware is essential to spare both users and developers from the exact knowledge of the heterogeneous set of technologies adopted by the lower layers. It allows the developpers to primarily focus on issues related to the designed applications. Hence, it spares these developpers losing time and efforts on issues in relation with the management and the utilization of the underlying IoT physical technologies.

The approaches based on service-oriented computing (SOC) could be in charge of playing the middleware role in the context of IoT. A service-oriented architecture (SOA) is a set of communicating services based on standardized interaction models [19]. SOC can be used to manage web services and to make them act like a virtual network. Thus, it adapts the applications to the specific users needs. Besides, Cloud computing [20] is based on a distributed architecture, in which entities are treated in a uniform way and accessed via standard interfaces. Thus, providing a common set of services and an environment for service composition. Actually, combining cloud computing with SOA could provide an efficient middleware for IoT supporting a high level of heterogeneity and flexibility.

The service based approaches lying on a cloud infrastructure open the door toward highly flexible and adaptive middleware for the IoT. For instance, Sensor-Cloud is one of the most interesting design idea to handle the huge amount of sensing devices (see section 2.1), and the unprecedented amount of generated data. In fact, a Sensor-Could infrastructure provides to the end user service instances based on virtual sensors in a automatic way. Actually, the platform offers a virtual feeling to the user as if these sensors are part of its classical IT resources (e.g. disk storage, CPU, memory, etc.) [10]. The end users do not have to bother with their actual physical location or their actual state. In addition, they do not even have to own the physical sensors. Instead, it is possible to create a set of sensor services to be exploited in different applications for different users through the cloud [21]. Moreover, decoupling the application logic from the embedded devices, and moving it to the cloud will allow developers to provide applications for the heterogeneous devices that will compose the future IoT environment [22].

2.3 Actuating

Internet of Things enhances the dumb objects around us with processing and communication capabilities. Hence, the resulted pervasive applications have the potential to deeply impact our way of life. In fact, the range of domains that might be concerned is impressive. In these domains, solutions might be deployed in both public and private areas. However, bringing to reality the future vision of our societies under the umbrella of IoT can not be achieved by limiting the scope of technology enhancement to cyberspace. In fact, physical support (i.e. actuating) in the real world is definitely required [11].

As an illustration, let us consider an e-health scenario. Indeed, e-health applications are highly promising solutions intending to provide unobtrusive support to frail and elderly people. In particular, these applications might be highly critical in case of a medical emergency. In the following, we present an e-health scenario that highlights the importance of actuating capabilities, in addition to emphasizing the involved IoT building blocks, along with their specific functionalities. Firstly, specialized sensing nodes planted in, or on a patient body are used to collect health-related data (e.g. blood glucose level), plus contextual sensors that gather data such as room temperature and humidity level. Then, gathered data is transmitted to a middleware back-end infrastructure through wireless connexion (e.g. Bluetooth, ZigBee, Wifi). Upon adequate processing, decisions can be made such as alerting medical staff, or family members. To understand the role of actuating devices, we consider the case where a hypoglycemia is detected. If the influence of the system is limited to the digital world, the application would only trigger an alarm. Actually, an hypoglycemia could rapidly engender disastrous consequences to the brain [23]. Thus, a rapid intervention is required. In fact, waiting for emergency teams to arrive might be too late. Consequently, e-health applications have to be enhanced with actuating capabilities through which a decision to provide the patient with sugar (e.g. using an injection) can be executed immediately, probably, saving his life.

Could-Robotics could constitute an ideal candidate to fulfill the role of physical support to IoT applications. In fact, Could-Robotics abstracts robotic functionalities and provides a means for utilizing them. Various equipments and devices that can measure the world or interact with people in both the physical and digital worlds are treated uniformly. Such devices include individual robots, sensors, and smartphones. These robots are logically gathered to form a cloud of robots by networking. Hence, they realize an integrated system that provides seamless support for daily activities using the available resources on demand [24].

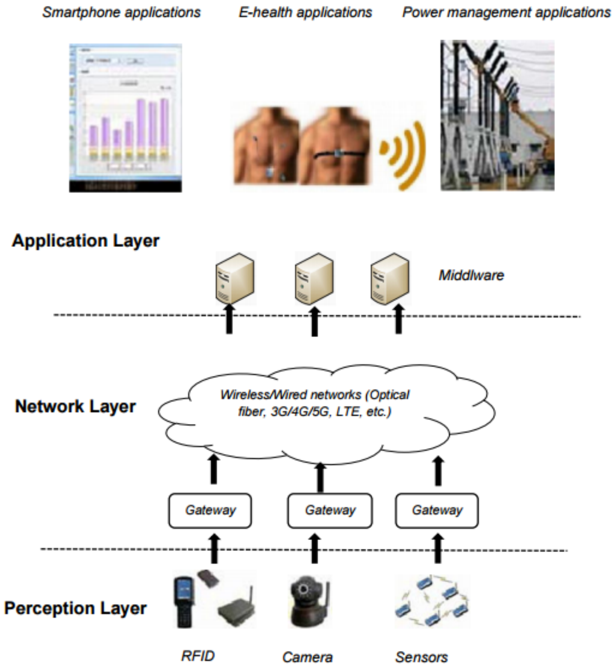

Fig. 3. The three-layer IoT architecture

3 The proposed IoT architectures and classification

In this part, we review the proposed architectures in the literature. We start by introducing a high level architecure that is commonly accepted to constitue the basement of the future IoT architecture. Then, we introduce our classification that gathers the approaches into two classes. The first class of approaches is based on existing architectures tailored to the context of IoT. The second one is based on clean slate approaches that propose novel architectures from scratch.

3.1 High level architecture

A well defined IoT architecture is still not established. However, a three-layer high level architecture is commonly accepted [25]. This architecture consists of three layers: Perception Layer, Network Layer, and Application layer (Figure 3). A brief description of each layer is given:

Perception Layer: the main task of the perception layer is to perceive the physical properties of things around us that are part of the IoT. This process of perception is based on several sensing technologies (e.g. RFID, WSN, GPS, NFC, etc.). In addition, this layer is in charge of converting the information to digital signals, which are more convenient for network transmission. However, some objects might not be perceived directly. Thus, microships will be appended to these objects to enhance them with sensing and even processing capabilities. Indeed, nanotechnologies and embedded intelligence will play a key role in the perception layer. The first one will make chips small enough to be implanted into the objects used in our every day life. The second one will enhance them with processing capabilities that are required by any future applications.

Network Layer: the network layer is responsible for processing the received data from the Perception Layer. In addition, it is in charge of transmitting data to the application layer through various network technologies, such as wireless/wired networks and Local Area Networks (LAN). The main media for transmission include FTTx, 3G/4G, Wifi, bluetooth, Zigbee, UMB, infrared technology, and so on. Huge quantities of data will be carried by the network. Hence, it is crucial to provide a sound middleware to store and process this massive amount of data. To reach this goal, cloud computing is the primary technology in this layer. This technology offers a reliable and dynamic interface through which data could be stored and processed. Indeed, research and development on the processing part is significant for the future development of IoT.

Application Layer: the application layer uses the processed data by the previous Layer. In fact, this layer constitutes the front end of the whole IoT architecture through which IoT potential will be exploited. Moreover, this layer provides the required tools (e.g. actuating devices) for developpers to realize the IoT vision. In this vision, the range of possible applications is impressive (e.g. Intelligent transportation, logistics management, identity authentication, location based services, safety, etc.).

To suit IoT specificities, the three-layer architecture provides a high level framework through which different approaches might be implemented. In the following, we present and classify the IoT architectures proposed in the literature, either resulting from public projects, or academic research.

3.2 Tailored architectures

IETF protocol suite: given that the protocol suite TCP/IP is recognized as the cornerstone of the current Internet, it is understandable to consider the same protocol stack to be used for IoT deployment [26]. Nevertheless, IoT specificities such as resources scarcitiy, instable wireless links, and heterogeneity of both traffic and devices, will seriously hinder IP-based protocols deployment in IoT environments. To the end of tailoring the existing TCP/IP architecture to IoT, the Internet Engineering Task Force (IETF) is working on standardizing the corresponding communication protocols for each layer of the communication stack. Namely, IEEE 802.15.4 [27] for the data link layer, IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [28] as a lightweight addressing scheme, Routing Protocol for Low Power and Lossy Networks (RPL) [29] as a routing protocol, and Constrained Application Protocol (CoAP) [30] to be adopted in the application layer. In the following, we briefly introduce each protocol.

- *IEEE 802.15.4* is a standard developed by the IEEE 802.15 Personal Area Network (PAN) Working Group. It specifies both physical layer and media access control for wireless constrained devices. Due to its provided features, which aim to be as less resource consuming as possible, several protocols such as WirelessHART [31] and ZigBee are based on the IEEE 802.15.4. In addition, more and more IoT devices are built as IEEE 802.15.4-compliant devices.
- *6LoWPAN* is a standard that aims to transfer IPv6 packets to IEEE 802.15.4 based networks. 6LoWPAN uses IPV6 header compression mechanisms of IPv6 datagrams. Compression mechanisms are motivated by the limited space available in 802.15.4 frames to encapsulate IPv6 packets. 6LoWPAN defines encoding formats for compression based on shared state within contexts. In other words, it takes advantage of the fields that are implicitly known to all nodes in the network or can be deduced from the MAC layer.
- *RPL* is a a standardized distance-vector routing protocol designed for constrained IP-based environments. It takes into consideration limitations either in energy power or in computational capabilities of such networks. The protocol organizes a logical representation of the network topology as a Directed Acyclic Graph (DAG). This graph is composed of one or more Destination Oriented DAGs (DODAGs) with one root per DODAG. Each root is typically a border router (BR). This latter establishes an optimum path based on defined routing metrics, which it receives thourgh broadcast messages.
- *CoAP* is an application layer protocol devloped by the IETF CoRE Working Group. It is designed for contrained environements. Based on a REST style architecture, the protocol considers the various objects in the network as resources. A Unique Universal Resource Identifier (URI) is assigned to each resource. The protocol uses the corresponding URI to operate the different resources.

SENSEI project: future networks will be enhanced with ambient intelligence capabilities enabling IoT applications to spread in our environment. To realize this future vision of our communications patterns, heterogeneous wireless sensor and actuator networks have to be integrated into a common framework of global scale. In addition, they have to be made available to services and applications via universal interfaces. The SENSEI project [32] solves the inaccessibility of low-resource end devices by collecting all data from the end devices, and making them available in a centrally accessible database. In fact, it provides necessary network and information management services to enable reliable and accurate context information retrieval and interaction with the physical environment.

The main results of the SENSEI project can be summarized as follows [33]:

- A highly scalable architectural framework with corresponding protocol solutions. These solutions enable easy plug and play integration of a large number of globally distributed devices (i.e. things) into a global system. Doing so, it provides support for network and information management, security, privacy and trust, and accounting.
- An open service interface and corresponding semantic specifications to unify the access to context information and actuation services offered by the system.
- Efficient WSN and actuators solutions consisting of a set of cross-optimised and energy aware protocol stacks.
- Pan European test platform. This platform enables enabling large-scale experimental evaluation of SENSEI results. In addition, it provides a tool for long term evaluation of WSN and actuators integration into IoT.

By adding mechanisms for accounting, security, privacy and trust, SENSEI will enable an open and secure market space for contextawarness and real world interactions.

CASAGRAS project: CASAGRAS is considered as the first view on relevant topics of the IoT (e.g. architecture, features, governance, etc.), which is the result of an international analysis and discussion [33]. CASAGRAS project [5] aims to collect, review and analyze current and emerging proposals and solutions in the IoT. Although CASAGRAS's reference architecture provides the basis for implementing a distributed IoT, the processing is not pushed to the edge of the network, which is in charge of data gathering only. In fact, the logic is located in the Information Management System Layer. The CASAGRAS model includes three layers:

- **Physical Layer:** this layer identifies physical objects, and delivers the sensed data. In order to provide interoperability, objects are organized in networks through the specific Automatic Identification and Capture (AIDC) technology. In fact, an Universal Data Capture Appliance Protocol (UDCAP) is envisioned, whereby each AIDC technology will use its own implementation of UDCAP.

- **Interrogator-Gateway Layer:** it connects object-devices with information management systems.
- **Information Management Systems:** this layer provides the functional platform for supporting applications and services.

Server based approach: in [8], the authors introduce a Server-Based Internet of Things Architecture (SBIOTA). The main idea is to develop protocols, algorithms and services, based on a gateway server. This latter allows networked devices with extremely limited computation and communication capabilities to be part of the IoT in an effective, efficient, and secure way. In the following, we provide a broad overview of the main features of this approach:

- **Physical and link layer connectivity:** it is assumed that each small device is directly connected to a single server, which provides an intelligent gateway function between the device and the Internet.
- **Network layer connectivity:** IP connectivity will be based on IPv6 networking. Any necessary IPv4 to IPv6 translations or tunnelling will be handled by the gateway. Each device will have a dynamically assigned IP address. Because a full IPv6 implementation is costly for small devices, the 6lowPAN [28] protocol for communication on the links between the server and the device will be prefered. The server will also act as a firewall for each device.
- **Transport layer functions:** the two major IP-based transport layer protocols are UDP and TCP. The server will act as an endpoint for these protocols. Since UDP is more lighweight, and hence more adapted to the IoT context, the server will communicate with the devices using UDP over 6lowPAN.
- **Application layer functions:** the Internet is moving away from providing access to data and hosts, towards providing access to services [34]. In this context, it is assumed that every device will offer a HTTP web-server interface to its functionalities for authorized users. Each of these web-servers will be hosted on the gateway server.

Network virtualization a solution based on virtual networks is introduced in [35]. According to the authors, current solutions that integrate smart resource-constrained objects into the Internet are mostly gateway-based. Their approach focuses on the objects, both resource-constrained and non-constrained, that need to cooperate by integrating them into a secured virtual network, named an Internet of Things Virtual Network or IoT- VN.

The authors have categorized the different approaches to expose services offered by resource-constrained devices to the internet into two main categories. The first one is based on the use of gateways that are in charge of translating between protocols used in the Internet and protocols used in the sensor networks. The second one is based on integrating sensors into the IP-world. This approach allows direct end to end communication between the end sensors.

Both approaches have their advantages and disadvantages, characterized by the degree of openness in accessing the services on the resource-constrained devices. In fact, the use of gateways has certainly many advantages (e.g. high degree of access control, offload heavy computational operations, etc.) at the expense of a reduced flexibility of usage. Besides, IP-enabled sensors allows the overcome of some drawbacks of the previous approach such as providing the possibility of having gateways and sensors from different vendors. However, allowing direct communication between resource-constrained devices, new challenges related to connectivity, scalability and security are introduced. In this context the authors propose a novel, complementary approach.

Based on the fact that in several cases there is no need to expose the data generated by resource-constrained devices to the whole network. Only a limited number of devices are involved. The proposed complementary approach aims to realize a secured and confined environment in which all objects that need to cooperate can communicate in an end-to-end manner. This is achieved by creating a virtual network of all involved devices, including resource-constrained devices.

Inside this virtual network, communication can take place between the networked objects regardless whether they are resource-constrained or not. This is achieved through the use of protocols that take into account the limitations of the most resource-constrained device. The authors described how this concept can constitute a valid alternative approach for realizing certain real-life scenarios by providing some several generic use cases such as partitioning, aggregating multiple sensor networks or extending a sensor network with non-constrained devices.

3.3 Clean slate architectures

BRIDGE project: the EPC Information Services (EPCIS) are used for storage and retrieval of processed information regarding supply-chain events. EPCIS provides a complete decentralized architecture. In fact, they include two separate interfaces, one for query requests and the other one for capture operations. A secure lookup service for locating the different providers of the distributed shares of information is required. Indeed, objects full information in relation with its life-cycle history or its complete supply-chain is spread through the different entities.

To enable RFID and EPCglobal standard solutions in practice, technical, social and educational constraints, particularly in the area of security must be overcome. BRIDGE (Building Radio frequency IDentification solutions for the Global Environment) [6] extends the EPC network architecture and focuses on the following aspects [33]:

Network:

- Serial-level lookup service to enable unique item level product information storage and retrieval

- Identification and authentication of tags and readers
- Data management of large amounts of real-time data

Application Software:

- Serial-level inventory management
- Management of large networks of EPC readers
- Models to exploit environmental data (e.g. temperature, humidity, etc)

Security:

- Security and privacy to prevent illicit use of EPC
- Prevention of cloning and emulation of tags in EPC
- Secure transmission of data between readers and tags

In a nutshell, BRIDGE aims to enable the deployment of EPC global applications in Europe. Its main axis are focused on developing security mechanisms in hardware, software and business practises.

IDRA approach, direct connectivity: in the future IoT, a tremendous amount of heterogeneous devices (i.e. things) using vendor-specific proprietary network solutions will be connected. As a result, communication will only be possible through the use of gateway nodes, resulting in inefficient use of the wireless medium. In fact, there is no existing architecture yet that:

- Enables optimized communication at a network and link level between co-located heterogeneous networks without the use of complex translation gateways
- Has been implemented and evaluated as a prototype in a large scale experimental setting
- Is compact enough to fit even on low-resource embedded devices
- Is fully clean slate, but is also backward compatible with legacy networks.

In order to enable an end to end communication and overcome the use of gateways, the authors in [36] have tailored the IDRA architecture [37] to the context of IoT. This latter was designed specifically to enable connectivity between heterogeneous resource constrained objects. Its main advantages can be summurized as follows:

- IDRA can connect co-located objects directly, without the need for complex translation gateways;
- The architecture is clean slate, but supports backward compatibility with existing deployments;
- Due to its low memory footprint, the architecture can be used in resource-constrained objects.

Based on its characteristics, IDRA architecture is believed to provide an approach that fills the gap between the current architectures and the future IoT requirements.

EPC based approach: in [38], the authors present an EPC (Electronic Product Code) based Internet of Things (IoT) architecture. The key concept of the architecture is deploying EPC over heterogeneous networks. The architecture focuses on a ZigBee network as it can collect information about things. In fact, the EPC Network provides certain static information such as names and manufacturers of the 'things'.

According to the authors, an EPC based IoT requires a minimum set of features, such as uniquely identifying a 'thing', automatic registration of the objects into the network, and providing Standard Application Programing Interfaces (APIs) to search, register, observe and control objects made by different companies. In order to deal with the precedent requirements, the proposed architecture provides two functions, one is how to register new things or devices to a home area network. The other is how to make things communicate through the Internet with generic protocols. The proposed EPC architecture is based on the combination of sensor networks and EPC networks which provide product information through web services from the manufacturers. UPnP protocol is used to automatically collect the EPC of a new connected object. ZigBee network system is applied for communication, and XML based web services are used for the application protocol. Genuine HTTP is a heavy protocol particularly for low bandwidth network such as ZigBee and IEEE 802.15.4. Therefore, CoAP (Constrained Application Protocol) is adopted to support web services over ZigBee network. End to end communication is thus established regardless of the type of the network.

Cloud based approach: in the IoT paradigm, information and communication systems are invisibly embedded in the environment around us. This will result in the generation of huge amount of data which have to be stored, processed and presented in a seamless, efficient and easily interpretable way. According to [3], cloud computing is the most recent paradigm to emerge promising high reliability, scalability and autonomy. In fact, it provides ubiquitous access, dynamic resource discovery and composability required for future IoT applications. This platform acts as a receiver of data from the ubiquitous sensors, as a computer to analyze and interpret data, as well as a provider of easy to understand web based visualizations.

The Cloud not only reduces costs of deploying ubiquitous applications, but is also highly scalable. Indeed, sensing service providers can join the network and offer their data using a storage cloud, analytic tool developers can provide their software tools, artificial intelligence experts can provide their data mining and machine learning tools, and finally computer graphics designer can offer a variety of visualization tools. The cloud computing can offer these services to the IoT as infrastructures, platforms, or softwares where the full potential of human creativity can be exploited. The generated data, used tools, and the process of generating complex visualizations are hidden in the background.

Social network approach: the Social Internet of Things (SIoT) architecture is introduced in [9]. The approach establishes a link between social networks and IoT. The main idea is that a large number of individuals tied in a social network can provide far more accurate answers to complex problems than a single individual (even knowledgeable one). Indeed, the idea has emerged from the fact that in the future, things will be associated to the services they can deliver. Thus, within a given social network of objects, a key objective will be to publish information/services, find them, and discover novel resources to better implement the services. This can be achieved by navigating a social network of 'friend' objects instead of relying on typical Internet discovery tools that cannot scale to the trillions of future devices.

Authors in [9], claim that social relationships among humans might be applicable to certain kinds of behaviors of typical objects that implement pervasive applications. There is no doubt that many applications and services should in the future be associated with groups of objects, which will cooperate in order to reach the overall interest of providing services to users (e.g. the same idea is behind the approaches involving the use of swarm intelligence and swarm robotics).

The social architecture relies upon basic kinds of relationships such as the **Parental object relationship (POR)** that is established among objects belonging to the same production batch or the **Ownership object relationship (OOR)** that is established among heterogeneous objects which belong to the same user (e.g. mobile phones, game consoles, etc.). The authors draw attention about the fact that the establishment and management of such relationships should occur without human intervention. This is not in contrast with a future vision of a fully networked human. This latter is only responsible for setting the rules of the objects, and their social interactions. This is a clear paradigm shift from other proposals, according to which the objects just participate in the human social network built by their owners.

4 Critics and Analysis

The proposed architectures, either the public projects or those introduced by the research community aim to reduce the gap between the concept of IoT and its real deployment into our daily lives. We have proposed a classification that gathers the different architectures into two categories. The first one, called the tailored architectures contains the approaches that propose an evolution of the current Internet to a more suitable network for the IoT such as network virtualization, and server based approach. This category will certainly provide the advantage of backward compatibility with existing architectures. However, several issues remain such as security and resources limitations. The second category includes clean slate architectures such as the IDRA approach and the social network approach. These approaches claim a novel vision of the future IoT that inherently copes with next-generation network challenges. In fact, this provides

Architectures	Description	Drawbacks	Potential improvements
IETF protocol suite	Focuses on proposing and adapting standard-based communication protocols for the IoT.	Resources limitations, QoS support for heterogeneous traffic, and security issues.	Introducing QoS management by handling differently the various classes of traffic. Designing, and integrating built-in standard-based security protocols.
SENSEI [32]	EU project designing an architecture for the connectivity of global and heterogeneous sensor and actuator networks via the specification of open service interfaces.	The use of centrallly accessible data base results in significant network overhead. No ID standards. The SENSEI project is still under development.	Adoption of ID standards. The project need to reach a mature state before its results can be evaluated.
BRIDGE [6]	The bridge project aims at supporting ambient sensors and sensor enabled RFID tags in the EPC global networks for supply chain monitoring.	No extension of the EPC Network standard to deal with sensor data is provided.	Extend EPC Network standard with sensor data.
CASAGRAS [5]	Focuses on global standards regulatory and other issues concerning RFID and its role in the Internet of Things.	Any interaction must pass through an Information Management System at the service or application layer which constitutes the narrow-waist of the architecture. CASAGRAS's focus is too much on RFID only.	
IDRA approach [36]	Enabling direct connectivity between heterogeneous objects through a network-service-oriented architecture.	Additionnal processing delay is caused by the different computations in the system.	Taking into account the QoS requirements of the packet, additional delay will only be introduced for low-priority traffic.

Server based approach [8]	Communication between networks from different vendors, or between devices that use different network protocols is achieved by connecting each network to a vendor-specific translation gateway.	This approach breaks the end to end communication paradigm. Results in an inefficient use of the wireless medium. Presents a single point of failure.	
EPC based approach [38]	Emerging industrial RFID standards architecture based on unique item identification via the Electronic Product Code (EPC).	Does not yet handle sensor data.	Extend current standards with sensor data.
Cloud approach [3]	Offload resource intensive tasks to more capable nodes.	This approach could be implemented in the network layer to handle processing tasks, it does not solve connectivity challenges.	
Social network approach [9]	A parallel is made between the current social networks and a futur network of objects.	Could only be implemented in the application layer, does not deal with lower layers issues.	
Virtual networks approach [35]	Network virtualization is used to present underlying network layers in a uniform way toward a high-level application.	Scalability has not been proven yet and complexity might be an issue on resource-constrained embedded devices.	Reduce the complexity of the used techniques and provide tests on huge and scalable networks comparable to the future IoT network scale.

Table 1. Summary of the proposed architectures

the benefit of a design, completely dedicated to be tailored to IoT characteristics. Nevertheless, backward compatibility with existing approaches remains a challenge.

Each presented architecture in this paper is summarized in table 1, along with a brief description and the main shortcomings. Some eventual improvements are also provided. In the following, we propose an analysis of each architecture highlighting the matching of its characteristics with IoT requirements.

The IETF is focusing its efforts on adapting existing protocols, which have been developed for the classical Internet to the constrained environment of IoT. To this end, the IETF proposes an equivalent the existing protocols for each layer of the TCP/IP stack such as 6LoWPAN for IPV6, and CoAP for HTTP. However, although the precedent solutions constitute a sound basement on which further efforts can be made, several challenges remain. For instance, the limited channel capacity of the IEEE 802.15.4 can hinder the scalability and the traffic load of future IoT applications. Moreover, Quality of Service (QoS) support for networks with heterogeneous traffic is still problematic in IEEE 802.15.4 [39]. In addition, several studies such as [40] highlight security breaches in the IETF protocol suite. Thus, the IETF protocol suite has to be strengthen regarding the security aspect, which is considered as a primary concern in IoT.

SENSEI [32] focuses on equipping the objects with a certain kind of intelligence by embedding processing capabilities into them. The project provides the architecture for connecting heterogeneous objects via the specification of open service interfaces. However, the use of centrally accessible database results in a significant network overhead and could constitute a single point of failure. Additionally, the SENSEI project is still under development, it needs to reach a mature state before an effective evaluation. CASAGRAS [5] also proposes a vision of IoT whereby both virtual and physical generic objects are connected through a global infrastructure. The project focuses too much on RFID as the main building block of IoT while it is likely to have a multitude of integrated technologies forming the future IoT. Like SENSEI, CASAGRAS presents a narrow-waist. Any interaction has to pass through the Management System at the service or application layer. BRIDGE [6] aims to research, develop and implement tools to enable the deployment of Radio Frequency Identification (RFID) and EPC-global Network applications. The core of BRIDGE is communication centric, it addresses the problem of handling queries between distributed entities. Nevertheless, the work with sensors does not extend the EPC network standards.

The IDRA [36] architecture proposes a clean slate approach that challenges the layered vision of the current internet architecture. IDRA aims to enable a direct connectivity between heterogeneous objects through a network-service-oriented architecture. However, additional processing might impede an efficient deployment in a resource-constrained environment. The virtualization approach

[35] also aims to establish an end-to-end communication between the devices that need to cooperate by integrating them into a secured virtual network regardless whether the resources are constrained or not. Yet, the scalability has not been proven and the complexity of the protocols used might be an issue. Another promising architecture to provide an end to end communication regardless of the type of the access network was presented in the EPC based approach [38]. The main idea is to combine sensor networks with EPC networks which provide product information through web services from manufacturers. Server based approach [8] proposes a different solution to connect networks from different vendors, or devices that use different protocols. The idea is to use a translation gateway. Nevertheless, this solution breaks the end to end communication principle. In addition, the gateway could represent a single point of failure.

The social network approach [9] introduces an interesting idea by making the parallel between the current social networks and a future network of objects. The goal is to publish, find information and discover novel resources to better implement the services. Nevertheless, this approach does not deal with the issues of lower layers of the network. Besides, the cloud approach [3] proposes to offload resource intensive tasks to more capable nodes in order to take into account the scarcity of resources in the future IoT. In fact, the cloud offers both flexibility and a high scalability level. However, the cloud architecture does not deal with the connectivity challenges at lower levels of the network.

In a nutshell, we do believe that a well-defined architecture is required instead of letting the current Internet raise to IoT in an uncontrolled way. Issues like security need to be addressed during design time. In addition, we consider that the different proposed architectures are not contradictory, an hybrid architecture including several approaches might be an efficient way to address IoT's specificities. Based on the commonly accepted three-layer architecture, each approach might be implemented in the appropriate layer. For instance, the cloud approach affects the application layer whereby the future applications will need to be ubiquitously accessible while the IDRA approach could be implemented in the network layer to secure a dynamic adaptation of the network.

5 Conclusions

Internet Of Things brings the possibility to connect billions of every-day's objects to the Internet, allowing them to interact and to share data. This prospect open new doors toward a future where the real and virtual world merge seamlessly through the massive deployment of embedded devices. The IoT has the potential to add a new dimension to the ICT sector by enabling communications with and among smart objects, leading to the vision of anytime, anywhere, any media and anything communication paradigm. Though, a lot still to be done in order to fulfill the IoT vision. A scalable, backward compatible and secure architecture is required to bring the IoT concept closer to reality. In this chapter, we have provided an overview of the main proposed architectures, along with the building blocks technologies that are considered well-adapted to suit IoTs requirements. We have also introduced a classification highlighting the suitability of the proposed architectures regarding IoT characteristics. In addition, we have underlined the main shortcomings of the current approaches and proposed our vision regarding IoT's future architecture based on the current state of the art, and IoT's requirements. As a future research direction, we plan to design a suitable approach that deals with the different challenges of IoT at each layer of the network.

References

1. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer Networks (May 2010) 2787–2805
2. Miorandi, D., Sicari, S., Pellegrini, F.D., Chlamtac, I.: Internet of things: Vision, applications and research challenges. Ad Hoc Networks (April 2012) 1497–1516
3. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, Volume 29, Issue 7 (2007) 24
4. Yun, M., Yuxin, B.: Research on the architecture and key technology of internet of things (iot) applied on smart grid. Advances in Energy Engineering (ICAEE) (2010) 6972
5. CASAGRAS: Casagras project. (2009) http://www.rfidglobal.eu.
6. BRIDGE: Bridge: Building radio frequency identification solutions for the global environment. (2009) http://www.bridge-project.eu.
7. Dunkels, A., Vasseur, J.: Internet protocol for smart objects. IPSO Alliance, White Paper 1 (september 2008) http://www.ipso-alliance.org.
8. Bergmann, N.W., Robinson, P.: Server-based internet of things architecture. The 9th Annual IEEE Consumer Communications and Networking Conference (2012)
9. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The social internet of things (siot) when social networks meet the internet of things: Concept, architecture and network characterization. Computer Networks, Volume 56, Issue 16 (November 2012) 3594–3608
10. Hassan, M.M., Song, B., Huh, E.N.: A framework of sensor-cloud integration opportunities and challenges. ACM, ICUIMC 09 (January 2009)
11. Hu, G., Tay, W.P., Wen, Y.: Cloud robotics: Architecture, challenges and applications. IEEE Network (June 2012)
12. Ye, W., Heidemann, J., Estrin, D.: An energy-efficient mac protocol for wireless sensor networks. INFOCOM. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies (2002) 1567–1576
13. Curt, S., Srivastava, M.: Energy efficient routing in wireless sensor networks. IEEE Military Communications Conference MILCOM. Communications for Network-Centric Operations: Creating the Information Force **1** (2001) 357–361
14. Abdmeziem, M., Tandjaoui, D.: Tailoring mikey-ticket to e-health applications in the context of internet of things. In: International Conference on Advanced Networking, Distributed Systems and Applications (Short Papers). (June 2014) 72–77
15. Want, R.: An introduction to rfid technology. Pervasive Computing, IEEE **5**(1) (2006) 25–33

16. Nath, B., Reynolds, F., Want, R.: Rfid technology and applications. IEEE Pervasive Computing **5**(1) (2006) 22–24
17. Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks **38**(4) (March 2002) 393–422
18. Zhang, L., Wang, Z.: Integration of rfid into wireless sensor networks: Architectures, opportunities and challenging problems. In: Grid and Cooperative Computing Workshops. GCCW'06., IEEE (2006) 463–469
19. Papazoglou, P., Georgakopoulos, D.: Service oriented computing. Communications of the ACM **46**(10) (October 2003)
20. Wei, Y., Blake, B.: Service-oriented computing and cloud computing. IEEE INTERNET COMPUTING (2010)
21. Zhou, J., Leppanen, T., Harjula, E., Ylianttila, M., Ojala, T., Yu, C., Jin, H., Yang, L.: Cloudthings: A common architecture for integrating the internet of things with cloud computing. In: 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE (2013) 651–657
22. Kovatsch, M., Mayer, S., Ostermaier, B.: Moving application logic from the firmware to the cloud: Towards the thin server architecture for the internet of things. In: Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), IEEE (2012) 751–756
23. Won, S.S., Hamby, A.M., Swanson, R.A.: Hypoglycemia, brain energetics, and hypoglycemic neuronal death. Glia **55**(12) (2007) 1280–1286
24. Kamei, K., Nishio, S., Hagita, N.: Cloud networked robotics. IEEE Network (may/june 2012)
25. Wu, M., Lu, T., Ling, F., Sun, J., Du, H.: Research on the architecture of internet of things. In: 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE (2010)
26. J.Vasseur, Dunkels, A.: Interconnecting smart objects with ip: The next internet. Morgan Kaufmann (2010)
27.
28. Shelby, Z., Bormann, C.: 6LoWPAN: The wireless embedded Internet. Volume 43. John Wiley & Sons (2011)
29.
30. Shelby, Z., Hartke, K., Bormann, C.: The constrained application protocol (coap). RFC 7252 (June 2014)
31. Song, J., Han, S., Mok, K., Chen, D., Lucas, M., Nixon, M.: Wirelesshart: Applying wireless technology in real-time industrial process control. In: Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS'08. IEEE, IEEE (2008) 377–386
32. : Sensei project (2010) http://www.ict-sensei.org/.
33. Bui, N.: Internet of things architecture. Technical report, Project co-funded by the European Commission within the Seventh Framework Program (2011)
34. Schroth, C.: The internet of services: Global industrialization of information intensive services. In: In Proceedings of 2nd IEEE International Conference on Digital Information Management, ICDIM '07
35. Ishaq, I., Hoebeke, J., Moerman, I., Demeester, P.: Internet of things virtual networks. IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing (2012) 293–300
36. Poorter, E., Moerman, I., Demeester, P.: Enabling direct connectivity between heterogeneous objects in the internet of things through a network-service-oriented

architecture. Journal on Wireless Communications and Networking, volume 2011, Issue 1 (August 2011)

37. overview of the currently available network services in the IDRA architecture, A.: http://idraproject.net/protocols-and-applications
38. Hada, H., Mitsugi, J.: Epc based internet of things architecture. IEEE International Conference on RFID-Technologies and Applications (2011) 527–532
39. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., Leung, K.: A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. Wireless Communications, IEEE **20**(6) (2013) 91–98
40. Medjek, F., Tandjaoui, D., Abdmeziem, M., Djedjig, N.: Analytical evaluation of the impacts of sybil attacks against rpl under mobility. In: International Symposium on Programming and Systems, IEEE (April 2015)