Towards Multi-layer Interoperability of Heterogeneous IoT Platforms: The INTER-IoT Approach

Giancarlo Fortino, Claudio Savaglio, Carlos E. Palau, Jara Suarez de Puga, Maria Ghanza, Marcin Paprzycki, Miguel Montesinos, Antonio Liotta and Miguel Llop

Abstract Open interoperability delivers on the promise of enabling vendors and developers to interact and interoperate, without interfering with anyone's ability to compete by delivering a superior product and experience. In the absence of global IoT standards, the INTER-IoT voluntary approach will support and make it easy for any IoT stakeholder to design open IoT devices, smart objects, services, and complex systems and get them to be operative and interconnected quickly, thus creating new IoT interoperable ecosystems by using a bottom-up approach. In particular, INTER-IoT

G. Fortino (✉) · C. Savaglio
DIMES - University of Calabria, Via P. Bucci, 87036 Rende (CS), Italy
e-mail: g.fortino@unical.it

C. Savaglio
e-mail: csavaglio@dimes.unical.it

C.E. Palau · J.S. de Puga
DCOM – Universitat Politecnica de Valencia, Camino de Vera S/N,
46022 Valencia, Spain
e-mail: cpalau@dcom.upv.es

J.S. de Puga
e-mail: jasuade@dcom.upv.es

M. Ghanza · M. Paprzycki
Systems Research Institute, Polish Academy of Sciences, ul. Newelska 6,
01-447 Warsaw, Poland
e-mail: mganzha@dcom.upv.es

M. Paprzycki
e-mail: marcin@dcom.upv.es

M. Montesinos
PRODEVELOP, PlaÇa de Joan de Vilarasa, 14-5, 46001 Valencia, Spain
e-mail: mmontesinos@prodevelop.es

A. Liotta
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven,
The Netherlands
e-mail: aliotta@tue.nl

M. Llop
Avinguda Moll del Turia s/n, 46024 Valencia, Spain
e-mail: MLlop@fundacion.valenciaport.com

R. Gravina et al. (eds.), *Integration, Interconnection, and Interoperability of IoT Systems*, Internet of Things, DOI 10.1007/978-3-319-61300-0_10

is based on hardware/software tools (INTER-Layer) granting multi-layer interoperability among IoT system layers (i.e. device, networking, middleware, application service, data and semantics), on frameworks for open IoT application and system programming and deployment (INTER-FW), and on a full-fledged CASE tool-supported engineering methodology for IoT systems integration (INTER-Meth). The INTER-IoT approach is notably exemplified through two use cases: INTER-LogP, involving interoperability of port logistics ecosystems, and INTER-Health, encompassing integration between e-Health at home and in mobility infrastructures.

Keywords Internet of things · Interoperability · Platforms · Device · Networking · Middleware · Application services · Data · Semantics · e-Health · Smart port logistics

1 Introduction

In recent years, due to a great interest of both Industry and Academy in researching and developing Internet of Things (IoT) technology [23, 44], many solutions at different levels (from the IoT device-level to full-fledged IoT platforms) have been implemented. However, there is no well-established reference standard for IoT platform technology and we do not foresee one in the near future. Hence, IoT scenarios will be characterized by a high-degree of heterogeneity at all levels (device, networking, middleware, application service, data/semantics), preventing interoperability of IoT solutions [10, 28].

Lack of interoperability causes major technological and business issues such as impossibility to plug non-interoperable IoT devices into heterogeneous IoT platforms, impossibility to develop IoT applications exploiting multiple platforms in homogeneous and/or cross domains, slowness of IoT technology introduction at a large-scale, discouragement in adopting IoT technology, increase of costs, scarce reusability of technical solutions, and user dissatisfaction [22, 40].

A multi-layered approach to integrate heterogeneous IoT devices, networks, platforms, services and data will allow heterogeneous elements to cooperate seamlessly to share information, infrastructures and services as in a homogenous scenario [1, 49]. Thus, the main goal of the INTER-IoT approach being developed in the EU-funded H2020 INTER-IoT project is to comprehensively address the lack of interoperability in the IoT realm by proposing a full-fledged approach facilitating "voluntary interoperability" at any level of IoT platforms and across any IoT application domain, thus guaranteeing a seamless integration of heterogeneous IoT technology.[1] The proposed approach will allow effective and efficient development of adaptive, smart IoT applications and services atop different heterogeneous IoT platforms, spanning single and/or multiple application domains. INTER-IoT focuses in two application domains.

[1] INTER-IoT project website: http://www.inter-iot.eu.

The INTER-IoT approach thus aims to provide open interoperability, which delivers on the capability of enabling vendors and developers to interact and interoperate, without interfering with anyone's ability to compete by delivering a superior product and experience. In the absence of global IoT standards, the INTER-IoT project is supporting and making it easy for any company to design IoT devices, smart objects, and/or services and get them to the market quickly, thus creating new IoT interoperable ecosystems.

This chapter is organized as follows. In Sect. 2, a state-of-the-art analysis on IoT platform interoperability approaches is presented. Section 3 describes the INTER-IoT approach, specifically detailing the technical solutions defined for IoT interoperability. In Sect. 4, we introduce the two main use cases that will be developed in the project. Finally, conclusions are drawn and future work is delineated.

2 Related Work

Interoperability among heterogeneous systems can be understood and involves [27]:

- *Technical Interoperability*, which is associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centered on (communication) protocols and the infrastructure needed for those protocols to operate.
- *Syntactical Interoperability*, which is associated with data formats.
- *Semantic Interoperability*, which is associated with the meaning of content and concerns the human rather than machine interpretation of the content.
- *Organizational Interoperability*, which is the ability of organizations to effectively communicate and transfer (meaningful) data (information) across different information systems over widely different infrastructures. Organizational interoperability depends on the former three.

In the following subsections, we briefly overview platforms and projects (Sects. 2.1 and 2.2) and standardization efforts (Sect. 2.3) strongly correlated to IoT systems interoperability and also highlight their links to INTER-IoT.

2.1 Projects Related with IoT and IoT Platforms

Several projects funded in previous years by the European Commission and other international organizations worldwide have been focusing on domain-specific and/or open IoT platforms. In Table 1, the most known and diffused ones are reported. In particular, a short description is provided along with similarities and differences with respect to our INTER-IoT approach. Considering that INTER-IoT is not presenting a new IoT platform but an interoperability framework.

Table 1 Representative projects proposing general-purpose and domain-specific IoT architectures/platforms

International/European R & D & I activities	Link to INTER-IoT
IOT-A[a] Creation of an architectural reference model together with the definition of an initial set of key building blocks for enabling the emerging IoT	*Similarities*: Reference architecture for IoT platforms. *Differences*: No development of a concrete platform for interoperability among other IoT platforms. No integration methodology is provided
COMPOSE[b] Creation of an ecosystem transforming the IoT into an Internet of Services, through an open marketplace	*Similarities*: Promotion of a bottom-up approach for IoT ecosystems development. *Differences*: Not specifically addressing interoperability issues. No integration methodology is provided
Web of Objects[c] Development of a network and services infrastructure for autonomic cooperating smart objects	*Similarities*: Reference architecture and virtualization as means for integration. *Differences*: Not focused on granting interoperability through integration. No methodology is provided
iCore[d] Development of a cognitive management framework for the reliable mash-up of smart objects and smart services	*Similarities*: Interoperability between IoT devices and IoT services through virtualization. *Differences*: Global and layer-oriented interoperability is not addressed. No integration methodology is provided
Butler[e] Integration of current IoT technology and development of new technologies to form a "bundle" of applications, platform features and services, emphasising pervasiveness, context-awareness and security for IoT	*Similarities*: Interoperability at device-level through Smart Gateway. *Differences*: No global and layer-based interoperability is provided and neither an integration methodology
IoTLaB[f] Creation of a crowdsourcing infrastructure together with the supporting mechanisms that will enable multidisciplinary experimentation platform in the general domain of IoT	*Similarities*: Resource virtualization for virtual interconnection of networks and devices. *Differences*: No global and layer-based interoperability is provided and neither an integration methodology
IoT@Work[g] Development of an IoT-based plug and work concept centered on industrial automation, specifically enabling IoT applications in automation domains	*Similarities*: Network-oriented interoperability among industrial IoT devices. *Differences*: Special-purpose domain (industrial plants). No global and layer-based interoperability (apart from the network-layer) is provided and neither an integration methodology
OpenIoT[h] Development of an open source middleware for collecting information from sensor clouds of heterogeneous domains and offering utility-based IoT services	*Similarities*: Interoperability at device level through Global Sensor Network. *Differences*: No platform integration infrastructures and methodology available. Data-level integration of heterogeneous IoT sources

(continued)

Table 1 (continued)

International/European R & D & I activities	Link to INTER-IoT
CASAGRAS/CASAGRAS2[i] Provision of a framework of foundation studies concerning radio frequency identification (RFID) with particular reference to the emerging IoT	*Similarities*: Interoperability between RFID-oriented devices through an Interrogator-Gateway Layer. *Differences*: Strongly RFID oriented. No applicability in more general IoT contexts. No platform integration infrastructures and methodology available
Smart Santander[j] Development of city-scale experimental research facility to support typical applications and services for smart cities, exploiting existing frameworks as WISEBED, SENSEI and USN	*Similarities*: Integration approach of exploiting other framework/platform strengths. *Differences*: Heterogeneity across three specific frameworks but not across layers; no methodology or reference architectures provided; very focused on the Smart City domain
TRESCIMO[k] Aims at developing a M2M platform that links Smart Applications to Sensor Networks and low level devices w.r.t. smart energy management and smart grid	*Similarities*: M2M-based reference architecture. *Differences*: Single domain (Smart Cities) and specific focus on M2M and energy. Thus, global and layer-based interoperability is not provided; no integration methodology is proposed
SunRise[l] Creation of a federation of experimental facilities covering the diverse marine environments allowing researchers to experiment with novel paradigms for the Internet of Underwater Things	*Similarities*: Efforts in defining standard interoperable methods and architectures. *Differences*: Focus on underwater IoT and its peculiar communication issues. No methodology for IoT platform interoperability
Webinos[m] Development of an Open Source Platform and software components for the FI to enable web applications and services to be used and shared consistently and securely over converged and connected devices	*Similarities*: Provision of interoperability and interconnectivity by means of gateway and open Web standards. *Differences*: No full-fledged layer-oriented interoperability. Focus is on software concepts based on web-based services
SANDS[n] Development of a physical and computational networked infrastructure for household appliances, forming an IoT ecosystem, to meet the needs of their owners	*Similarities*: Open (social-oriented) IoT architecture. *Differences*: Specific focus on domotic. Not addressing platform interoperability and integration methodology
VITAL[o]: Development of a Cloud-of-Things-based platform integrating and interacting with a multitude of different IoT data sources and systems within the Smart City domain	*Similarities*: Lightweight open meta-architecture for IoT frameworks integration based on voluntary interoperability. *Differences*: The integration meta-architecture provides global integration and not layered-oriented integration that would allow higher performance and reduce reliability and security issues. Not providing any systematic methodology for IoT platforms integration

(continued)

Table 1 (continued)

International/European R & D & I activities	Link to INTER-IoT
FIWARE[p] development of a middleware for the Future Internet based on Generic and Specific enablers, it includes several components to integrate IoT and services	*Similarities*: Approach based on the deployment of enablers and integration of services. *Differences*: Device and network layers are transparent to the framework of IoT

[a]Internet Of Things – Architecture, available at http://www.iot-a.eu
[b]Collaborative Open Market to Place Objects at your Service, available at http://www.compose-project.eu
[c]Web of Objects, available at http://www.web-of-objects.com/
[d]Internet Connected Objects for Reconfigurable Eco-systems, available at http://www.iot-icore.eu/
[e]uBiquitous, secUre inTernet-of-things with Location and contEx-awaReness, available at http://www.iot-butler.eu/
[f]Internet-of-Things Laboratory, available at http://www.iotlab.eu
[g]Internet-of-Things at Work, available at http://www.iot-at-work.eu/
[h]Open Internet-of-Things, available at http://www.openiot.eu
[i]Coordination and Support Action for Global RFID-related Activities and Standardisation, available at http://www.iot-casagras.org
[j]Smart Santander Project, available at http://www.smartsantander.eu/
[k]Testbeds for Reliable Smart City Machine to Machine Communication, available at http://trescimo.eu/
[l]Sensing, monitoring and actuating on the UNderwater world through a federated Research InfraStructure Extending the Future Internet, available at http://fp7-sunrise.eu
[m]Secure WebOS Application Delivery Environment, available at http://webinos.org
[n]Social AND Smart, available at http://www.sands-project.eu/
[o]Virtualized programmable InTerfAces for smart, secure and cost-effective IoT depLoyments in smart cities, available at http://vital-iot.eu
[p]FI-PPP Future Internet Core Platform, available at http://www.fiware.org

2.2 IoT-EPI

IoT-EPI is a European Initiative addressing the new EU-funded H2020 programs about IoT platform and interoperability development. At the core of IoT-EPI are the following seven research and innovation projects: INTER-IoT (i.e., the subject of this chapter), BIG IoT, AGILE, symbIoTe, TagItSmart!, VICINITY and bIoTope. The European Platforms Initiative is coordinated by two Collaborative Support Actions (CSAs): Unify-IoT and Be-IoT. In Table 2 a brief description of the projects along with similarities and differences with respect to INTER-IoT is reported.

2.3 IoT Standardization

Currently several standardization efforts are underway to define architectural standards for IoT systems interoperability. The most important ones are reported in Table 3 along with a comparison with the INTER-IoT approach. It worth noting that the main difference is that INTER-IoT aims at voluntary (i.e., non standards-oriented) interoperability.

Table 2 IoT-EPI projects

Project	Link to INTER-IoT
BIG IoT[a] aims at establish interoperability by defining a unified Web API for IoT platforms: the BIG IoT API. This Web API is aligned with the standards currently developed by the W3C Web of Things group. An IoT platform or service implements the API to register and access the BIG IoT Marketplace so as to interoperate with services/applications available in the marketplace. BIG IoT pilots involve Smart City applications	*Similarities*: it is not developing yet another IoT platform but the aim is higher-level interoperability of already existing heterogeneous IoT services and applications. It is worth noting that the BIG IoT API has a similar role of the INTER-FW API. *Differences*: the approach only offers a high-level API to grant application and/or service interoperability and does not provide methods and methodology to integrate IoT platforms at the different finer-grain layers identified by INTER-IoT. Moreover, the use cases are in a different application domain
AGILE[b] (An Adaptive and Modular Gateway for the IoT) builds a modular and adaptive gateway for IoT devices. Modularity at the hardware level provides support for various wireless and wired IoT networking technologies (KNX, ZWave, ZigBee, BLE, etc.). At the software level, different components enable new features: data collection and management on the gateway, intuitive interface for device management, visual workflow editor for creating IoT apps, and an IoT marketplace for installing IoT apps locally. AGILE pilots involve open field and animal monitoring, enhanced retail services, people monitoring based on wearables	*Similarities*: the device layer provides interoperability among heterogeneous devices based on different communication protocols. The use case based on wearables is similar somehow to the INTER-Health use case. *Differences*: the approach only offers device layer interoperability and does not provide methods and methodology to integrate IoT platforms at the different finer-grain layers identified by INTER-IoT. Moreover, the other use cases are in a different application domain
symbIoTe[c] (symbiosis of smart objects across IoT environments) will enable the discovery and sharing of resources for rapid cross-platform application development and will facilitate the blending of next generation of smart objects with surrounding environments. symbIoTe will achieve all of the above by designing and implementing an Open Source mediation prototype. Its pilots encompass several smart environments and smart mobility	*Similarities*: it steps into the IoT landscape to devise an interoperability framework across existing and future IoT platforms. Specifically, like INTER-IoT it chooses the challenging task to implement IoT platform federations so that they can securely interoperate, collaborate and share resources for the mutual benefit, also supporting the migration of smart objects between various IoT domains and platforms. *Differences*: the approach is basically based on a mediation prototype to support interoperability and does not provide methods and methodology to integrate IoT platforms at the different finer-grain layers identified by INTER-IoT. Moreover, the use cases are in different application domains

(continued)

Table 2 (continued)

Project	Link to INTER-IoT
TagItSmart![d] (Smart Tags driven service platform for enabling ecosystems of connected objects) has the objective of creating a set of tools and enabling technologies integrated into a platform with open interfaces enabling users across the value chain to fully exploit the power of condition-dependent FunCodes to connect mass-market products with the digital world across multiple application sectors. Its pilots are related to from preproduction to recycling smart chains	*Similarities*: the aim to define open interface for easing interconnection, even though interoperability is not a main issue to deal with. The project proposes the creation of a developers community which will be providing new services in a market place directly using the API and the funny tags developed in the project. *Differences*: the approach is not aimed at interoperability of heterogeneous IoT systems based on integration/interconnection methods and methodologies. Moreover, the use cases are in different application domains
VICINITY[e] (Open virtual neighbourhood network to connect IoT infrastructures and smart objects) aims to provide the owners of connected IoT infrastructures with a decentralized interoperability. It connects different smart objects into a "social network" called virtual neighbourhood where infrastructure owners keep under control their shared devices and data thanks to web based operator console called VICINITY neighbourhood manager (VNM). Guest IoT infrastructures, VICINITY enabled services as well as the VICINITY auto-discovery space are connected to a VICINITY interoperability gateway using the same VICINITY gateway API. Use cases are in the energy, building, e-Health, and mobility application domains	*Similarities*: it grants decentralized interoperability through interconnection of heterogeneous systems through gateways and data concentrators. The project proposes the definition and development of an ontology to allow semantic interoperability between IoT platforms (cloud and gateway level) related with the associated use cases. *Differences*: the approach is basically (standard or proprietary) based on infrastructure gateways to support interoperability but does not provide methods and methodology to integrate IoT platforms at the different finer-grain layers identified by INTER-IoT. Moreover, the use cases are in different application domains apart from the e-Health use case
bIoTope[f] (Building an IoT OPen innovation Ecosystem for connected smart objects) provides the necessary standardised Open APIs to enable the publication, consumption and composition of heterogeneous information sources and services from across various platforms, including FI-WARE, OpenIoT, city dashboards, etc. Pilots are in the area of Smart Cities	*Similarities*: interconnection of heterogeneous IoT platforms and systems through common API, the project looks for specific standards to achieve interoperability. *Differences*: the approach only offers a high-level API to grant systems of systems interconnection and does not provide methods and methodology to integrate IoT platforms at the different finer-grain layers identified by INTER-IoT. Moreover, the use cases are in a different application domain

[a]BIG IoT - Bridging the Interoperability gap of the Internet of Things, http://big-iot.eu/
[b]AGILE - An Adaptive and Modular Gateway for the IoT, http://agile.eu/
[c]symbIoTe - symbiosis of smart objects across IoT environments, https://www.symbiote-h2020.eu/
[d]TagItSmart! - Smart Tags driven service platform for enabling ecosystems of connected objects, http://www.tagitsmart.eu/
[e]VICINITY - Open virtual neigh-bourhood network to connect IoT infra-structures and smart objects, http://vicinity2020.eu/vicinity/
[f]bIoTope - Building an IoT OPen innovation Ecosystem for connected smart objects, http://biotope.cs.hut.fi/

Table 3 IoT Standardization Initiatives

Standardization initiative	Link to INTER-IoT
AIOTI[a] was initiated by the European Commission in 2015, with the aim to strengthen the dialogue and interaction among IoT players in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the take up of IoT	*Similarities*: AIOTI uses the same architecture reference model (ARM) for IoT exploited by INTER-IoT. Such ARM derives from the IoT-A project. *Differences*: the aim of INTER-IoT is not to propose a standard but to interconnect heterogeneous systems based on even different standards or proprietary solutions
IEEE P2413[b] is a standard that defines an architectural framework for the IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements. It also provides a blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety	*Similarities*: IEEE P2413 is based on an ARM that is similar to the IOT-A ARM on which INTER-IoT is based. Moreover, both reference models share several commonalities that are used to extend INTER-IoT Interoperability Reference Model. *Differences*: the aim of INTER-IoT is not to propose a standard but to interconnect heterogeneous systems based on even different standards or proprietary solutions. The reference model provided by INTER-IoT does not have the aim to be used as a reference for developing new open platforms, but for allow interoperability of existing platforms
oneM2M[c] has the purpose and goal of developing technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M and IoT application servers worldwide	*Similarities*: a Service Layer granting access to heterogeneous machines and subsystems. Additionally, INTER-IoT considers gateway nodes in order to allow device to device and network interoperability. *Differences*: INTER-IoT does not aim at defining standard specifications but is based on voluntary interoperability concept. However, the use of standards may allow a broader connectivity with other nodes

[a]The Alliance for Internet of Things Innovation (AIOTI), http://www.aioti.org/
[b]P2413 - Standard for an Architectural Framework for the Internet of Things (IoT), https://standards.ieee.org/develop/project/2413.html
[c]OneM2M - Standards for M2M and the Internet of Things, http://www.onem2m.org/

3 The INTER-IoT Approach

The solution adopted by INTER-IoT includes three main solutions to grant voluntary interoperability (see Fig. 1):

- *INTER-LAYER*: methods and tools for providing interoperability among and across each layer (virtual gateways/devices, network, middleware, application services, data and semantics) of IoT platforms. Specifically, we will explore real/virtual

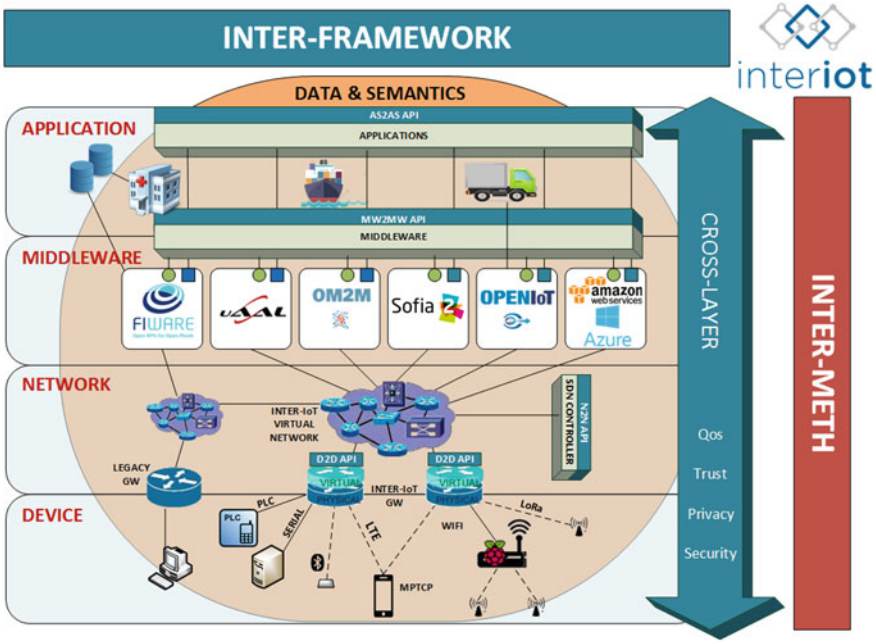

Fig. 1 The INTER-IoT abstract architecture highlighting INTER-IoT multi-layer solutions (device, networking, middleware, application, data and semantics), their interconnection (cross-layer), and their tools (INTER-FrameWork and INTER-METH)

gateways [2, 36] for device-to-device communication, virtual switches based on SDN for network-to-network interconnection, super middleware for middleware-to-middleware integration, service broker for the orchestration of the service layer and a semantics mediator for data and semantics interoperability [1, 20, 21].

- *INTER-FW*: a global framework (based on an interoperable meta-architecture and meta-data model) for programming and managing interoperable IoT platforms, including an API to access INTER-LAYER components and allow the creation of an ecosystem of IoT applications and services. INTER-FW will provide management functions specifically devoted to the interconnection between layers. The provided API includes security and privacy features and will support the creation of a community of users and developers.
- *INTER-METH*: an engineering methodology based on CASE (Computer Aided Software Engineering) tool for systematically driving the integration/interconnection of heterogeneous non-interoperable IoT platforms.

3.1 INTER-LAYER

Differently from current interoperability approaches (see Tables 1 and 2), INTER-IoT uses a layer-oriented approach to fully exploit specific functionalities of each

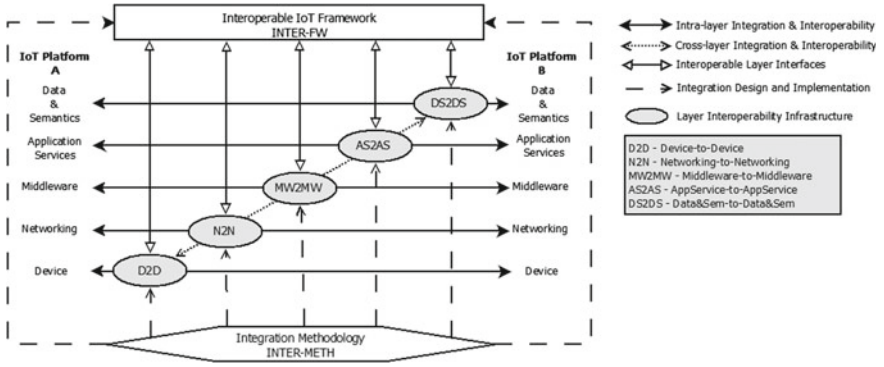

Fig. 2 Abstract schema of INTER-LAYER

layer (device, networking, middleware, application services, data and semantics). Although the development of a layer-oriented approach is a research challenge, as compared to an application-level approach, it has a higher potential to deliver tight bidirectional integration among heterogeneous IoT platforms, notably guaranteeing independence, thus providing higher performance, modularity, adaptability, flexibility, reliability, security, privacy and trust. Furthermore, what is extremely important, INTER-IoT will give more control on functional and non-functional requirements.

As highlighted in Fig. 2, INTER-IoT approach is based on the following real/virtual layer interoperability infrastructures among peer layers guaranteeing interoperability/integration: Device-to-Device (D2D); Networking-to-Networking (N2N); Middleware-to-Middleware (MW2MW); Application Services-to-Application Services (AS2AS); Data and Semantics-to-Data and Semantics (DS2DS). We will investigate two main types of D2Ds: smart device gateways and device virtualization wrappers. N2N will be based on Network Functions Virtualization components, representing the gateways adapted to different protocols; also the virtual gateways will be connected using Software Defined Network enabled switches. The use of NFV and SDN through a software controller provides extra flexibility and adequate management of data flows priorities and QoS. MW2MW will rely on smart brokers coordinating between heterogeneous middleware manager components. Virtualization will be exploited to develop AS2AS due to the effectiveness and flexibility that service virtualization can provide at application level. Finally, DS2DS will be designed around smart data and semantics management concepts. Every interoperability mechanism will be accesses through INTER-API of INTER-FW, see Sect. 3.2.

Each layer interoperability infrastructure (implementable in hardware, software, or both) not only provides strong coupling between peer layers but also exposes an interface, which can be programmed to control/interact with the component. Interfaces will be controlled by a meta-level framework to provide global interoperability (see Fig. 3). Moreover, the layer interoperability infrastructures can communicate with each other to provide cross-layering that aims at strengthening integration among layers so providing more efficiency and reliability, while still supporting flexibility

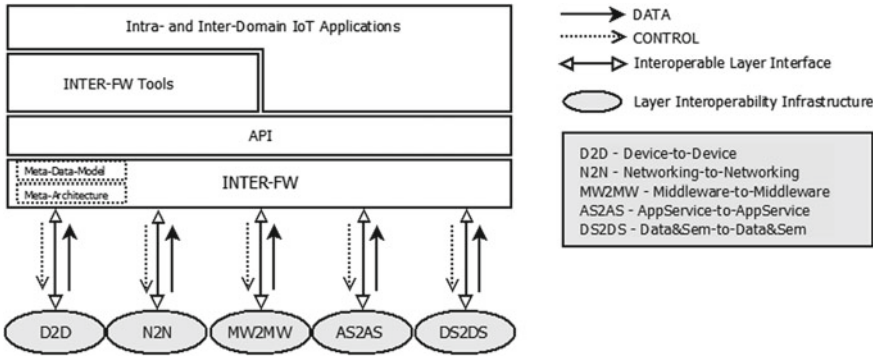

Fig. 3 Abstract schema of INTER-FW

and adaptability. Cross-layer component is fully devoted to the support and coordination of security and privacy mechanisms and services for the whole INTER-Layer.

3.1.1 Device

As sensors, actuators and smart devices become smaller, more versatile, lower cost and more power efficient, they are being deployed in greater numbers, either as special-purpose devices or embedded into other products. The unification and convergence of the vast number of platforms already deployed, the accessibility (API and interfaces) of the platform to app developers, requires interoperability. Smart-phones are key components in Device-to-Device (D2D) communication and interoperability, however there are many other types of devices that are currently deployed, both independently (e.g., smart watches and other wearables) and as part of other devices and platforms (e.g., consumer electronics or Cyber-Physical Systems).

Different communication protocols are used at device level. Here, Cellular and WiFi that are ubiquitous; they are evolving to support higher bandwidths and lower cost. Bluetooth is also becoming lower cost. New communication technologies like Bluetooth low energy (Bluetooth LE) and NFC are opening new possibilities for IoT. However, also traditional communication protocols and mechanisms for sensors, actuators and smart objects have to be considered (e.g., ZigBee, ISA100, WirelessHart, LoRa or SigFox), in addition to other non-standard proprietary protocols developed by individual vendors.

Different classes of IoT objects need different communication supports: e.g. ‘deterministic’ communication protocols (MAC and Routing layers) are not possible using current Internet protocols, but may be needed by some application. Standardization on these topics is just starting (e.g., detnet working group in IETF). Yet, deterministic communications will hardly meet the interoperability requirements of all IoT objects. Typically, device-level interconnection of IoT architectures has been performed using gateway-based solutions. FP7 Butler project (Table 2) proposed a

device-centric architecture where a SmartGateway allows interconnection between smart objects (sensors, actuators, gateways) using IPv6 as communication protocol. Different approaches have been developed to integrate and interoperate devices in IoT architectures. Basic devices (e.g., sensors, tags, actuators) are virtualized and can be composed in more complex smart systems [4]. The idea has been to create virtual objects, allowing object composition, considering a virtual object as a counterpart of existing smart objects [7].

INTER-IoT will provide fundamental benefits and competitiveness improvements in the way IoT devices will communicate with each other and will interface with different IoT platforms and subsystems. One of the proposed progresses regarding D2D interaction is to complement standardized communication protocols (which are mostly deterministic and reactive) with an ability for objects to make sense of their surroundings in order to understand how to best interplay with their neighbours. This requires new 'proactive' and 'predictive' communications capabilities, whereby a node can determine its communication requirements and those of its neighbours well before communication is required [29]. It has recently been proven that machine learning capabilities can run even on small sensors (with as little as 20 Kbytes of RAM) [6]. **INTER-IoT** is developing an interoperable communication layer that accommodate for opportunistic communications among heterogeneous nodes/devices, based on prediction mechanisms.

In particular, interoperability at device level implies that (i) heterogeneous IoT devices are able to interact with each other; (ii) heterogeneous IoT devices can be accessed through a unifying interface although they use different communication protocols; heterogeneous IoT devices can be integrated into any IoT platform. Regarding interoperability, we are exploring two different approaches: gateway-based and virtualization. In the former, a gateway-based approach are defined to adapt different communication protocols/languages on which heterogeneous devices are based. In the latter, virtualization techniques are defined to create virtual IoT devices that can be accessed through a unified service-oriented interface and interact through application-level interaction protocols.

With regards to integration, we are reusing the approaches for interoperability and further exploit wrapping methods to integrate IoT devices into non-interoperable IoT platform. We also consider fully reconfigurable devices supporting the emerging SDR (Software Defined Radio) paradigm. In particular, these specific devices can be used to implement communication interoperability by acting as "transparent bridges or gateways" between different radio technologies. This approach could be very effective when different smart objects, placed in a specific environment and equipped with different low range radio technologies such as Bluetooth, ZigBee, Wi-Fi, would communicate with each other. The deployment of novel SDR hardware and software architectures can effectively help in solving many internetworking issues at lower levels of the architecture. Coupling heterogeneous devices and/or integrating them into heterogeneous IoT platforms could bring to reliability (in broad sense), security and trust issues that need to be addressed to have fully interoperability at functional and non-functional level. INTER-IoT is analyzing in depth such issues to provide techniques with the required level of reliability, security and trust, and to be

compliant with the different recommendations and guidelines from security experts and standardization organizations.

3.1.2 Networking

IoT products will encompass different data communication scenarios. Some may involve sensors that send small data packets infrequently and do not prioritize timely delivery. Others may involve storage in order to sustain periods when the communication link is down (e.g., Delay Tolerant Networks). Others may need high bandwidth but be able to accept high latency. And others may need high quality, high bandwidth, and low latency. Large amounts of traffic with relatively short packet sizes will require sophisticated traffic management and traffic engineering procedures. More efficient protocols and management mechanisms will help reducing overheads but may present challenges to system integrity, reliability and scalability. Interface standardization is desirable so that IoT objects can communicate quickly and efficiently, and allow mobility between interoperable IoT platforms. IoT objects will need a way to quickly and easily discover each other and learn their neighbour's capabilities.

At networking layer different protocols can be used like 6LowPAN, TCP/HTTP, UDP/CoAP. Communication between real objects and the gateway can be based on universal plug and play (UPnP) or DLNA. Use of buses based on MQTT protocol can also be used to implement asynchronous communications between entities. The most promoted networking protocol in IoT environments is IPv6 and its version for constrained devices 6LoWPAN, even though its adoption is slow, and without global adoption it will be impossible for IoT to proliferate. IPv6 provides the following benefits to IoT configurations: (i) IPv6 auto-configuration; (ii) Scalable address space (sufficiently large for the enormous numbers of IoT objects envisioned); (iii) Redefined headers that enable header compression formats; (iv) Easy control of the system of things; (v) Open/Standard communications; (vi) IPv6 to IPv4 transition methods; (vii) IPv6 over constrained node networks (6LO, 6LoWPAN).

IoT platforms have usually mechanisms for integrating with external systems, but they are all based on specific point-to-point connections, usually with legacy systems in the area of interest of the IoT platform (e.g. city, neighbourhood, factory, hospital, port, house, etc.). The integration between IoT platforms will allow tracking the behaviour of these objects when they move outside the intrinsic area of interest and get into the area of interest of another IoT platform. The pub/sub mechanism usually available in the communication buses at the core of these IoT platforms and the possible object context sharing allow a powerful and easy way to track the behaviour of these objects among different IoTs scope areas.

INTER-IoT will provide support for as many networks as possible. Main contributions of the project are focused on multi-homing capabilities among the different IoT objects in order to provide network offloading connectivity and seamless mobility between different IoT platforms of moving objects. **INTER-IoT** is using SDN components to configure interconnection at network level(including an OpenFlow

software controller) as support for interoperability and roaming of smart objects between different platforms of the same ecosystem while keeping secure connectivity and also guaranteed quality of service. Resource management and scalability so as reliability, trust, privacy and security are non-functional requirements that will be addressed.

In particular, **INTER-IoT** is defining and analysing methods to integrate and allow interoperability of IoT components at network layer. It will specifically address: (i) pervasiveness and ubiquity network aspects including seamless mobility of smart objects between different IoT architectures in both use cases; (ii) the highly constrained environment in terms of physical size, available memory, CPU power and battery life in addition to communicating over wireless low power lossy networks in which operate Smart Objects; (iii) research in routing mechanisms to overcome traditional routing protocols drawbacks, specially route of information over IPv6, in particular, carrying IPv6 over low power networks (6LowPAN) and RPL (Routing Protocol for Low Power and Lossy Networks). Another key issue to be developed in the task will be IoT device mobility within different IoT architectures, including (i) network offloading with connectivity to different access networks; (ii) multihoming and (iii) secure seamless mobility.

3.1.3 Middleware

Middleware, widely used in conventional distributed systems [5], is a fundamental tool for the design and implementation of both IoT devices and IoT systems [23]. They provide general and specific abstractions (e.g., object computation model, inter-object communication, sensory/actuation interfaces, discovery service, knowledge management), as well as development and deployment tools, through which IoT devices, IoT systems and their related applications can be easily built up. Indeed, middleware (i) enable connectivity for huge numbers of diverse components comprised at Device Layer, (ii) realize their seamless interoperability at Networking Layer, and (iii) ensure operational transparency at Application Service Layer. In such a way, heterogeneous, often complex and already existing IoT devices and IoT systems, belonging to different application domains and not originally designed to be connected, can be easily integrated, effectively managed and jointly exploited. It follows that the role of middleware within the cyberphysical, heterogeneous, large scale and interconnected IoT scenario is even more crucial than within conventional distributed systems.

Over the years, many IoT middleware have been proposed, so much so that only in [3, 14, 37] more than 70 contributions have been surveyed and compared. The best way to analyse such plethora of middleware, regardless of the specific detail or technology, is to build up comparison frameworks around well-defined criteria to effectively highlight their salient differences and similarities. In such direction, middleware have been compared:

- in [14], according to their requirements at device or system levels;

- in [37], according to their functional, not functional and architectural requirements, as well as to their design approaches (application-specific, service oriented, agent-based, etc.);
- in [3], according to their functional requirements and supported low-level interface protocols.

Taking into account these three contributes and their related comparison frameworks, in Table 4 we identified eight recurrent criteria, which can be hence considered as IoT middleware main features, and the four IoT middleware that better fulfil them. In very few words, LinkSmart [8] is service-based middleware for ambient intelligence (AmI) systems, supporting devices communication, virtualization, dynamic reconfiguration, self-configuration, energy optimization and security by means of WebService-based mechanisms enriched by semantic resolution. UbiROAD [42] is sematic, context-aware, self-adaptive agent-based middleware for smart road environments, aiming at collecting, analysing and mining real time data from in-car and roadside heterogeneous devices. ACOSO [11, 12, 40] is an agent-oriented middleware with a related methodology [13] fully supporting the development (from the modelling to the implementation phase [18, 19]), management and deployment of smart objects and IoT systems, as well as their integration with the Cloud [15, 17]. IMPReSS [26], finally, is a middleware conceived for the rapid development of context-aware, adaptive and real-time monitoring applications to control and optimize energy usage in smart cities. Table 4 shows how these four middleware (Totally, Partially or Not) fulfil the eight IoT middleware main features.

In particular, **INTER-IoT** will focus on defining component-based methods for middleware interoperability/integration; in particular, we focus on discovery, management and high-level communication of IoT devices in heterogeneous IoT platforms. We will define two main approaches: (i) definition of overlay middleware components able to couple the middleware components of the heterogeneous IoT platforms; (ii) virtualization of the heterogeneous middleware components. In the first approach, we will design overlay middle components such as mediators and brokers.

In the second approach, the middleware components will be virtualized into a virtual layer which will be the integration point providing management and unified access to the three main middleware services (discovery, management and communication) for IoT devices. Both approaches will be experimentally evaluated to determine their suitability and effectiveness in the different scenarios in which the integrated heterogeneous IoT platforms usually operate. At this level, reliability, real-time requirements and security (and trust) need to be guaranteed by defining suitable policies and algorithms, and incorporating them into the overlay middle components (mediator and broker) or into the virtualization layer.

Table 4 IoT middleware main features

IoT middleware feature	Source	IMPReSS	ACOSO	UBIROAD	HYDRA
Device abstraction - Heterogeneous devices need to be abstracted in virtualized, homogeneous entities in order to couple them or make them interact	Rl, R2, R3	T	T	T	T
Hardware/software interface abstraction - Interfaces need to be made generic and standardized through higher level mechanisms so that their use will be straightforward	Rl, R2, R3	T	T	T	T
Heterogeneous data source and type management - Data generated according to different modalities, formats and types require shared representation to be exchanged and exploited	Rl, R2, R3	T	T	T	T
Device Management - Device need to be efficiently and autonomously discovered, used and composed, trying to minimize the human intervention	Rl, R2, R3	P	T	T	T
Context-awareness - Implicit and explicit information about users, devices, and the environment need to be considerate for enhance the service provision	Rl, R2, R3	T	T	T	T
Security and privacy - Efficient and scalable mechanisms are needed to ensure global connectivity and accessibility but, at same time, security and privacy	R2, R3	T	N	T	T
Development process support - Suitable methods and tools need to be defined to effectively and systematically support the development process	Rl, R2	P	T	N	N
Reliability and Timeliness - Specific methods need to be defined for guaranteeing the reliable and on-time delivery of information	Rl, R2	P	T	P	T

3.1.4 Application Services

There are currently very different paradigms for Cloud-based services supporting the IoT. They range from Virtual Objects [51], which mirror a sensor or 'thing' in the network with its abstract representation in the cloud, to smarter yet more complex multi-agent [31] and event-based architectures [45]. These approaches allow the definition of logical paths for the data, based on internal and external information including aggregation. Additionally, there are a number of meta-services, such as service discovery, management, and live-updates, which facilitate the deployment and functioning of a heterogeneous IoT system [25].

State-of-the-art communication network architectures and solutions for the real-time information exchange are characterized by the adoption of virtualization technologies, SDN in data centres and cloud virtualization, respectively, and service architectures developed in the M2M domain clearly separate functional entities and service layers in the device and network domains. While standardization (e.g., by oneM2M.org) is still on its way toward stable and widely accepted specifications, commercially available service platforms - offered as licensed software on customer infrastructure or software as-a-service – already drive down cost of solution development, through powerful horizontal services, and enable cost-efficient scalability in the service delivery [34].

Regardless of the abstraction level, what they all have in common, is that they all run in a network designed for high bandwidth and short delays, which is foreign to the IoT network that is designed for efficiency and low consumption, and where intermittent communication failures are expected. Cloud services for IoT have a wide spectrum including data storage, information synchronization, data analysis, and M2M communication, as well as others that are more specific, such as geolocation or streaming. Often, they are not IoT specific, and can greatly benefit from a layer that manages the interaction between the two, making it easier for both parties to operate in an efficient way. For example, a very simple low-power sensor can make use of a very high level cloud-based service without degrading its battery life by means of interoperability at network, middleware, and some additional caching app services. That is a very powerful mechanism that allows us to connect existing IoT networks with existing Cloud Services without the need of modifying either.

INTER-IoT framework aims to be generic, allowing for different approaches to coexist on the platform like cloud services that make use of an IaaS layer to scale its functioning as needed. Nevertheless, the platform will provide the necessary components to support different approaches and meta-services, such as a de-coupling middleware system that will effectively separate the different networks in order to present an appropriate behaviour to the different elements on each side of the communication. Despite the work done in the integration and homogenization of IoT systems, most efforts aim to connect different standards and services within a single virtual environment and at a single level of abstraction. **INTER-IoT**, on the other hand, will provide with a cross-level integration schema, which allows

for diverse elements to interact without the need of additional intermediaries, using NodeRed[2] as an example of such integration.

In particular, **INTER-IoT** aims to make interoperable and/or integrate application services furnished by heterogeneous IoT platforms. To fulfil it, we are defining methods based on service-oriented computing and virtualization. Specifically, application services will be first virtualized and then managed through a well-defined virtual service management component that also aims to provide automated service composition. Moreover, service composition needs to be reliable and secure.

3.1.5 Data and Semantics

Semantic interoperability can be conceptualized as an approach to facilitate "combining" multiple IoT platforms. The simplest case, of combining two IoT platforms, could be addressed by developing a one-to-one translator (a "gateway") to allow "semantic understanding" between them [33]. However, this approach does not scale, as for every subsequent entity joining an assembly of N platforms. Thus, N translators would have to be created. The two main approaches to avoid this problem, and deal with semantic interoperability are: (i) common communication standards; (ii) ontology and semantic data processing.

Developing a common communication standard was tried in the travel domain[3] with the OTA message specification a standard consisting on a set of (XML-demarcated) messages; or in the healthcare domain (and thus related to the INTER-Health use case) with OpenEHR,[4] which is an open domain-driven platform for developing flexible e-health systems. Here, multiple projects strive to establish interoperability between already known standards and the OpenEHR, e.g., establishing semantic interoperability of the ISO EN 13606 and the OpenEHR archetypes [32]. Similarly, the Think!EHR Platform (health data platform based on vendor-neutral open data standards designed for real-time, transactional health data storage, query, retrieve and exchange)[5]; aims at establishing interoperability of the OpenEHR and the HL7 standard (a framework for the exchange, integration, sharing, and retrieval of electronic health information).[6] Interestingly, development of the Think!EHR Platform had to deal with the data standards problem caused by existence of HL7 RIMv3, ISO13606, and OpenEHR standards.[7] While it is possible to envision an approach similar to this, applied to individual domains, it is not likely to be easily generalizable

[2] http://nodered.org.

[3] Open Travel Alliance available at http://www.opentravel.org/.

[4] OpenEHR available at http://www.openehr.org/what_is_openehr.

[5] Think!EHR platform, available at http://www.marand-think.com/.

[6] http://www.hl7.org/implement/standards/.

[7] Borut Fabian, "Interoperability with Think!EHR", available at http://www.hl7.org/documentcenter.

to support interactions between domains. Therefore, approaches based on ontologies and semantic data processing will be used in the project.[8]

INTER-IoT approach is developing a generic ontology of IoT Platforms (GOIoTP). The GOIoTP is used as the centrepiece for establishing platform interoperability (allowing for, among others, data interoperability, message translation, etc.). It should be stressed that, state-of-the-art ontologies of the IoT,[9] will constitute the starting point for construction of the GOIoTP, needed in our project. The proposed approach will require, (i) ontology matching [41], (ii) merging, noting that ontology merging is often reduced to ontology matching,[10] as well as (iii) techniques for establishing semantic distance (needed for ontology matching) [38]. Observing that this approach allows "understanding" and adaptability (handled through ontology adaptation) of heterogeneous data.

The creation of GOIoTP in **INTER-IoT**, combined with the state-of-the-art approaches to ontology matching/merging, allows the development of a comprehensive support for facilitation of semantic interoperability between IoT platforms, in the form of a IoT Platform Semantic Mediator (IPSM). The resulting approach, based on conducted research, will consist both of the methods and supporting tools and will include, among others, methods for:

- Combining two (or more) IoT platforms with explicitly defined ontologies. Here, among others, the following issues will be researched: (i) bringing multiple ontologies to a common format/language (for example, transforming XML into RDF and further transforming it into OWL-demarcated ontology using XLST), (ii) ontology matching, to allow for (iii) ontology merging into the extended GOIoTP (as the top-level ontology).
- Joining an "incoming" IoT platform (with an explicitly defined ontology) to an existing federation of IoT platforms (with an already defined common ontology). Here the process would be somewhat a simplified version of the previous method as only two ontologies will be integrated.
- Dealing with IoT platforms without an explicitly defined ontology/taxonomy/etc. Here, appropriate set of tools will be adapted to help instantiate an ontology for the multi-IoT-platform under construction. Specifically, the ontology will be built on the basis of information contained in one, or more: (i) definition of used data; (ii) structure of the database(s); (iii) queries issued on the database(s); and (iv) exchanged messages.

In particular, **INTER-IoT** defines methods for data and semantics interoperability. The key method for data semantics and interoperability is the development of GOIoTP (see above). Next a complete method, and a set of tools, to support development of platform semantic interoperability layer will be created. The method, resulting from research activities undertaken within the task, will include, among others, issues involved in (i) combining two (or more) IoT platforms with explicitly

[8] http://www.semantic-web-journal.net/sites/default/files/swj247_0.pdf.

[9] https://hal.inria.fr/hal-00642193/document.

[10] http://www.jfsowa.com/ontology/ontoshar.htm#s5.

defined ontologies (in any format). Here, the method will take into consideration: (a) bringing ontologies to a common format/language, (b) ontology matching, and (c) ontology merging within the GOIoTP. (ii) Joining an incoming IoT platform (with an explicitly defined ontology) to an existing federation of IoT platforms (with an already defined common ontology). (iii) Dealing with IoT platforms without an explicitly defined ontology/taxonomy/etc. Here, appropriate set of tools will be developed to help instantiating an ontology for the multi-IoT-platform under construction. Main achievements: (a) experimentally-tested methodology for IoT platform semantic integration for all possible cases of onto-semantic inputs from platforms to be integrated and (b) experimentally-tested tools for IoT platform semantic integration for all possible cases of onto-semantic inputs originating from platforms to be integrated.

3.1.6 Cross Layering

INTER-IoT specifically aims at creating cross-layer interoperability and integration between heterogeneous IoT platforms. Cross-layer approaches are fundamental to made interoperable/integrate the whole layer stack (device, networking, middleware, application service, data and semantics) of IoT platforms. Cross layering will be therefore based on the outcomes of the previous points (see Sects. 3.1.1–3.1.5).

Moreover, important requirements and features such as Quality of Service (QoS), Quality of Experience (QoE), Security, Privacy, Trust and Reliability, require to be addressed at each layer with different mechanisms. Such transversal approach allows retaining the benefits of a layered architecture (e.g., modularity, interoperability, etc.) but adding, at the same time, flexibility (e.g., optimization, tunable design, etc.) to those components that require it. Considering the heterogeneity and spread of IoT devices and IoT applications, it is straightforward that such design choice is more than suitable to properly support (i) dynamic QoS and QoE (the former, basically aiming at splitting traffic up into priority classes and trying to guarantee a particular performance metric, the latter at combining more subjective aspects related to user perception into evaluating a service) [9]; (ii) novel security and privacy techniques (that consider the cyber-physical nature of IoT devices as well as of the IoT application contexts) [39]; extended trust models (in which unconventional actors, like social networks, play an important role) [50] and (iv) enhanced reliability mechanisms (to deal with failure of resource-limited IoT device, lack of coverage from access networks in some region, rapid application context switches, etc.) [30].

3.2 INTER-FW

The Interoperable IoT Framework (INTER-FW) aims at providing global and open platform-level interoperability among heterogeneous IoT platforms coupled through specifically developed LIIs. INTER-FW will rely on an *architectural meta-model* for

IoT interoperable platforms and on a *metadata-model* for IoT interoperable semantics. Figure 3 shows the abstract schema of the INTER-FW. It provides a programming library (i.e., INTER-API) that will be used both by the INTER-FW tools, providing global-level management of the integrated IoT platforms, and by new, possibly cross-domain, IoT applications developed atop INTER-FW and that will be developed in WP4, in full compliance with the designed INTER-IoT meta architecture and meta data model.

Thus, INTER-FW advances the state-of-the-art by providing a general and effective method for inter-platform interoperability, addressing at a global level: real-timeliness, reliability, security, privacy, trust. In particular, INTER-FW will be designed and implemented considering the need to respect, where applicable, user data privacy (e.g., anonymization, hidden ID, use of separate databases for identification and data content with controlled access) and secure access to data (only authorized devices, ensure authentication and non-repudiation). Furthermore, access to data by non-authorized parties should be prevented (especially malevolent ones). Every other functional and non-functional requirement (e.g., reliability or user-friendliness) will be incorporated to the specification and implementation of INTER-FW, including the tools, INTER-API and an interoperability flexible engine. INTER-FW includes also a management mechanism and API used to access and coordinate the different layers of INTER-IoT. This aspect of INTER-FW is mainly needed for aspects like discovery, registration of devices and smart objects and also for security and privacy management.

3.3 INTER-METH

The engineering methodology INTER-METH aims at supporting the integration process of heterogeneous IoT platforms to obtain interoperability among them and allow implementation and deployment of IoT applications on top of them. To date, no proposals provide a systematic methodology driving the integration implementation (see Tables 1 and 2). It is widely recognized that using an engineering methodology is fundamental in any engineering application domain (e.g., software engineering, hardware/software codesign, civil engineering, etc.). The manual and non-systematic application of complex techniques, methods and frameworks would very likely lead to an increase of the degree of errors during integration [13]. The process of INTER-METH is shown in Fig. 4. It is envisioned as iterative, including the following six phases: Analysis, Design, Implementation, Deployment, Testing and Maintenance. Each phase produces work-products that are inputs for the successive phase/s. Iteration could involve single phases, set of successive phases or the whole process, thus assuring adaptability to new elements.

In particular:

- The Analysis phase defines the integration requirements, both functional and non-functional (e.g., real-timeliness, reliability, security, privacy, trust).

- The Design phase produces the design of the integration in terms of diagrams of (i) layer interoperability infrastructures and related interfaces, and (ii) INTER-FW programming and management patterns, to fulfill the elicited requirements.
- The Implementation phase focuses on the implementation of the design work-product to obtain the full-working (hardware and/or software implemented) system.
- The Deployment phase involves the operating set-up and the configuration of the integrated IoT platform.
- The Testing phase allows performing tests to validate the integrated platform according to the functional and non-functional requirements.
- The Maintenance phase manages the upgrade and evolution of the system.

A Computer Aided Software Engineering (CASE) tool, named INTER-CASE, for integration is under development to provide full support to the automated application of INTER-METH, covering all aforementioned integration phases.

4 Use Cases

The INTER-IoT approach is use case-driven, implemented and tested in three realistic large-scale pilots:

- **INTER-LogP**: it has been designed and built to specifically accommodate the communication and processing needs of moving vehicles and cargo items (being conceived as moving things according to the IoT paradigm), e.g., by seamless and secure integration of various vehicle telematics solutions as well as mobile devices serving as retrofitting equipment. It will work over smart containers (i.e., reefers and IMOs), trucks and different infrastructures, allowing exchange of information associated with the operations and movements of containers inside the terminal.

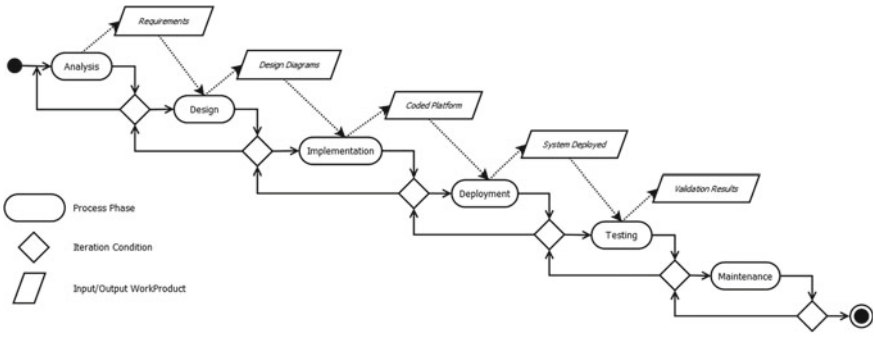

Fig. 4 Abstract schema of the INTER-METH process

- **INTER-Health**: aims at developing an innovative, open integrated m-Health IoT platform for humans monitoring in a decentralized way and in mobility. The integrated platform, derived from existing platforms (i.e., UniversAAL [24], and BodyCloud [16]), will be open to be further enhanced by integrating new subsystems by using the INTER-IoT approach.
- **INTER-Domain**: a cross-domain pilot involving IoT platforms from different application domains, including transport and logistics and e-Health, but extendable to other domains (e.g. smart cities or smart mobility).

In the following subsections, INTER-Health and INTER-LogP will be described in more detail.

4.1 INTER-LogP

4.1.1 Smart Port Transportation for Containers and Goods

In the ports of the future, port users, equipment and infrastructures will achieve a zero distance interaction offering more sustainable transport solutions. The use of IoT platforms will enable locating, monitoring, and handling different transport and cargo equipment and storage areas. The requirements for a better management of equipment and resources and the huge complexity of interactions involving large quantity of simultaneous transport movements around big logistics nodes (e.g., container terminals, ports, warehouses and dry ports) originates the need to introduce IoT platforms with multiple sensors in all logistics elements to control and monitor the several operations like energy consumption, gas emissions, or machine status. With these platforms, logistics service providers will be able to monitor and control in real time all the operations and movements of freight, equipment, vehicles and drivers on logistics nodes.

The Port of Valencia premises extend for several square kilometres. It is the largest Mediterranean port in terms of container handling. The port contains five container terminals (e.g., NOATUM and MSC), and several other facilities (e.g., train freight station, warehouses, and parking spaces). The port includes several kilometres of road within the premises.[11] The Port Authority has several deployed IoT platforms connected to different HMI and SCADA with different goals (e.g., traffic management, security, safety and environmental protection, or vessels identification). Some of these platforms provide selected data to the Port Community System (PCS) like tamper proof RFID tags and e-seals that are installed on trucks and semi-trailers. In particular, A Port Community System is an electronic platform that connects the multiple systems operated by a variety of organisations that make up a seaport, airport or inland port community. It is shared in the sense that it is set up, organised and used by firms in the same sector – in this case, a port community. There is an

[11] http://www.valenciaport.com/BoletinEstadistico/2013/December%202013.pdf.

increasing need that trucks, vehicles and drivers seamlessly interoperate with the port infrastructures and vice versa. All deployed IoT platforms do not interoperate as they are based on different standards, and remain isolated with a clear lack of interoperability at all layers.

NOATUM Container Terminal is one of the biggest container terminals in the Mediterranean located at the port of Valencia. It is the fifth largest European port in container handling, i.e. it deals with more than 50,000 movements per day, produced by more than 200 container handling units (e.g., cranes, forklifts, RTGs, internally owned tractors and trailers, etc.); more than 4,000 trucks and other vehicles visit terminal premises; with more than 10,000 containers involved in these movements. These values show the complexity of this environment and the opportunities that the information compiled by the sensors installed on the equipment, trucks and containers; and the IoT interconnected architectures can bring to the terminal (e.g., in terms of optimization in the operations, safety, security or cost and energy savings). Container terminals like the one managed by the NOATUM have a huge number of sensors, CPS (Cyber Physical Systems) and smart objects; fixed and mobile deployed and exchanging information within one or between several platforms deployed in their premises. The sensors from the internal equipment (i.e., container terminal IoT ecosystem), constitute 5% of total vehicles moving daily within terminal premises, and they generate more than 8,000 data units per second. The other 95% of the vehicles are external trucks and other vehicles, with sensors belonging to other IoT ecosystems, currently unable to interact with the terminal IoT solution. Additionally, containers (mainly used to transport controlled temperature cargoes) have their own IoT architecture, which cannot be accessed by the terminal, when the container is stored in the yard or moved across it. This lack of interoperability of outdoor ambulatory IoT things based on heterogeneous architectures represents a big barrier that **INTER-IoT** aims at removing.

This use case illustrates the need to seamlessly IoT platforms interoperation within port premises, e.g., container terminal, transportation companies, warehouses, road hauliers, port authorities, customs, border protection agencies, and outside the port. Port IoT ecosystems used to be operated by a large number of stakeholders, and typically require high security and trust, due to mobility and seamless connectivity requirements, that currently are not available with the exception of proprietary and isolated solutions. Introduction of interoperability mechanisms and tools will therefore bring about new solutions and services leading to developments of the ports of the future.

4.1.2 The INTER-LogP Pilot

INTER-LogP will be an **INTER-IoT** outcome to facilitate interoperability of heterogeneous Port Transport and Logistics-oriented IoT platforms already in place, i.e., VPF and NOATUM and other components that will be brought to the use case in order to achieve the **INTER-IoT** proposed goals, e.g., I3WSN from UPV and other IoT platforms from companies operating in the Port managed premises.

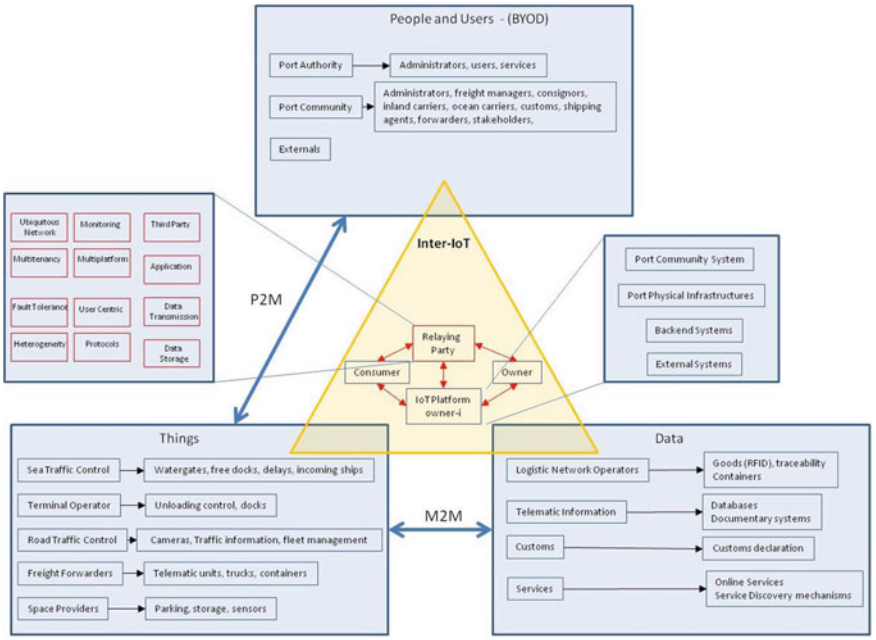

Fig. 5 **INTER-IoT** interconnection for transport and logistics (INTER-LogP)

The Port Authority of Valencia will provide its own IoT platform ecosystem to the project, including (i) the climate and weather forecast infrastructures, which monitor the environmental conditions in real-time and maintain historical data; (ii) beacon data acquisition system, which monitors and controls whenever necessary all the buoys distributed on the sea side; (iii) PCS-IoT platform, developed to cover different transportation and logistics components throughout the port premises, integrates an internal communication network and connects (more than 400) operating companies in the port (see Fig. 5).

NOATUM provides the SEAMS platform to be included in the INTER-LogP use case. SEAMS is an outcome from the Sea Terminals action (Smart, Energy Efficient and Adaptive Port Terminals) co-funded by the Trans-European Transport Network (TEN-T). It is an operational tool based on the reception of real-time energy and operative data coming from the whole machinery and vehicle fleets of NOATUM Container Terminal Valencia (NCTV). SEAMS integrates the whole set of machines (including Rubber Tyre Gantry cranes (RTG), Ship-To-Shore cranes (STS), Terminal Tractors (TT), Reach Stackers (RS) and Empty Container Handlers (ECH)) and vehicles deployed and available in the terminal premises.

INTER-IoT will help to expand the possibilities offered by not only SEAMS and the sensors installed on its own container terminal vehicles and container handling equipment units, but also sensors available on third party equipment (i.e., reefer con-

tainers)[12] and vehicles (i.e., external trucks picking up and delivering containers). Finally, it will allow installation of sensors on legacy equipment that does not have them available. Moreover, **INTER-IoT** will allow to seamlessly connecting the container terminal IoT ecosystem with other ecosystems owned by other parties, e.g., the port authority, road hauliers, the individual trucks, vehicles, containers and vessels through intelligent objects offered by different vendors, some of them managed by the PCS.

On the other hand, UPV will provide I3WSN [22], semantic IoT methodology and platform deployed in application domains like factories, automotive and defence. This generic architecture was developed within a large Spanish National project FASyS[13] and has been extended to be used in different areas like port transportation and m-health. The framework provides interoperability at different layers and includes reliability, privacy and security by design. Additionally, devices from the partners will be added to the trialsand devices from the users (e.g., truck drivers or terminal operators) like smart phones will be added to the system following BYOD (Bring Your Own Device) philosophy, allowing the integration of COTS devices in the large scale trials.

Although the different platforms that the transport and logistics use case integrates (in particular, IoT-PCS from VPF, NOATUM TOS, I3WSN UPV and the IoT platforms from other stakeholders) share some characteristics, they have different aims (i.e., focused on the particular benefits of the administrator/operator and use different technologies). All of them gather data, using different M2M and P2M protocols; some of them are cloud-based and others will be, but the most important thing is that they lack interoperability in terms of the five identified layers. There is a potential integration using one of the platforms (i.e., IoT-PCS) as a matrix architecture; however interoperability and integration will not profit the power of the proposed approach neither the capabilities of interoperable architectures rather than interconnected architectures. The use case, mainly focused in the transportation of containers, as it is the most sensorized in port transportation (especially reefer and International Maritime Organization – IMO safe containers), may improve efficiency, security and benefits to the whole transport chain. Additionally, **INTER-IoT** will provide the possibility to interact with other IoT platforms available in the port surroundings like Valencia City FIWARE infrastructure (i.e., VLCi) that is an open platform that will provide contextual information for different services and interactions at data and services layers.

[12] http://en.wikipedia.org/wiki/Refrigerated_container, last visited 13th April 2015.

[13] http://www.fasys.es/en/index.php, last visited 13th April 2015.

4.2 INTER-HEALTH

4.2.1 Decentralized and Mobile Monitoring of Assisted Livings' Lifestyle

The Decentralized and Mobile Monitoring of Assisted Livings' Lifestyle use case [35], aims at developing an integrated IoT system for monitoring humans' lifestyle in a decentralized way and in mobility, to prevent health issues mainly resulting from food and physical activity disorders. Users that attend nutritional outpatient care centres are healthy subjects with different risk degrees (normal weight, overweight, obese) that could develop chronic diseases. Only the obese (in case of second and third level obesity) need, at times, hospital care and get into a clinical and therapeutic route. The medical environment in which the pilot will be developed and deployed is the Dept. of Prevention/Hygiene Nutrition Unit at ASLTO5.

The use case will focus in the fact that in main chronic diseases, such as cardiovascular diseases, stroke, cancer, chronic respiratory diseases and diabetes, there are common and modifiable risk factors that are the cause of the majority of deaths (and of new diseases). Between the common and modifiable risk factors there are wrong lifestyles such as improper and hyper caloric diet and, in particular, the lack of physical activity. Every year in the world [48]: 2.8 million people die for obesity or overweight; 2.6 million people die for high cholesterol levels; 7.5 million people die for hypertension; 3.2 million people die for physical inactivity. These wrong lifestyles are expressed through the intermediate risk factors of raised blood pressure, raised glucose levels, abnormal blood lipids, particularly Low Density Lipoprotein (LDL cholesterol) and obesity (body mass index $\geq 30\,kg/m^2$) [43].

According to the reference standard medical protocol for the global prevention and management of obesity [46, 47], written by the World Health Organization, in order to assess the health status (underweight, normal weight, overweight, obesity) of the subject (of a given age) during the visit at the healthcare center, objective and subjective measurements should be collected (and/or computed) by a health-care team (doctor, biologist nutritionist, dietician, etc.). The objective measurements are: weight, height, body mass index (enabling diagnosis of overweight and obesity), blood pressure or waist circumference. The subjective measurements reported by the subject, are collected through computerized questionnaires, and concern the eating habits: quality and quantity of food consumed daily and weekly, daily consumption of main meals (breakfast, lunch, dinner and snacks) and the practice of physical activity (quality and quantity of physical activity daily and weekly). The physical activity degree is detected subjectively during the first visit and could be objectively monitored through wearable monitoring devices. On the basis of these measurements, the caloric needs are automatically calculated, and the diet of the subject is defined. From this point forward, the subject must be monitored periodically (for example, every three months) for a period of at least one year. Usually monitoring is carried out at the health-care center, where the objective and subjective measurements are cyclically repeated. Based on the results, and depending on the health status reached

by the subject (improved or worsened), the possibility of redefining his diet and his physical activity is analyzed.

By exploiting an integrated IoT environment, the aforementioned monitoring process can be decentralized from the healthcare center to the monitored subjects' homes, and supported in mobility by using on-body physical activity monitors. Specifically, the system will be created by using a new IoT platform, named INTER-Health [35], obtained by integrating two already-existing heterogeneous, non-interoperable IoT platforms for e-Health according to the approach proposed in the **INTER-IoT** project, based on the INTER-FW and its associated methodology INTER-METH: (i) UniversAAL, developed by UPV [24], and (ii) BodyCloud [16], developed by UNICAL.

4.2.2 The INBTER-Health Pilot

There is a need of integrating different IoT platforms as proposed in the INTER-Health use case. The effective and efficient integration of heterogeneous e-Health IoT Platforms will provide an appropriate answer to the challenges described in **INTER-IoT** proposal. The two platforms considered are UniversAAL and BodyCloud, and the result of the integration will allow developing a novel IoT m-Health system for Lifestyle Monitoring.

This flexibility allows deploying universAAL-based solutions in multiple configurations, such as local-only nodes, mobile nodes connected to server instances, or non-universAAL nodes connecting to a multi-tenant server. Communication between applications and/or sensors happens through three different buses. Messages and members are always described semantically using the domain ontologies at hand: (i) Context bus - An event-based bus for sharing contextual information from context publishers to context subscribers; (ii) Service bus - A request-based bus for on-demand execution and information retrieval from service callers to service providers and (iii) User Interface bus - A centrally-managed bus that allows applications to define abstract interfaces to be rendered by different User Interface (UI) modalities. In each bus, semantic reasoning is used to match the transferred messages to the appropriate destination. This way, applications and sensors only need to describe what they provide and what they require from others. There is no need to specify recipients, connections nor addresses explicitly [24].

BodyCloud [16] is a SaaS architecture that supports the storage and management of body sensor data streams and the processing (online and offline analysis) of the stored data using software services hosted in the Cloud. In particular, BodyCloud endeavours to support several cross-disciplinary applications and specialized processing tasks. It enables large-scale data sharing and collaborations among users and applications in the Cloud, and delivers Cloud services via sensor-rich mobile devices. BodyCloud also offers decision support services to take further actions based on the analyzed BSN data.

The BodyCloud approach is centered around four main decentralized components (or sides), namely Body, Cloud, Viewer, Analyst: (i) Body-side is the component,

currently based on the SPINE Android, that monitors an assisted living through wearable sensors and stores the collected data in the Cloud by means of a mobile device; (ii) Cloud-side is the component, based on SaaS paradigm, being the first general-purpose software engineering approach for Cloud-assisted community BSNs; (iii) Viewer-side is the Web browser-enabled component able to visualize data analysis through advanced graphical reporting; and (iv) e Analyst–side is the component that supports the development of BodyCloud applications.

The two platforms, UniversAAL and BodyCloud, share some high-level characteristics while differ in objectives and technology. Specifically, they are both e-Health platforms, based on Bluetooth technology to interact with measurement devices, and based on Cloud infrastructures to enable data storing, off-line analysis, and data visualization. However, they have different specific objectives and are not interoperable from a technological point of view (at each layer and at the global level). Their specific objectives are complementary: UniversAAL is focused mainly on non-mobile remote monitoring based on non-wearable measurement devices, whereas BodyCloud provides monitoring of mobile subjects through wearable devices organized as body sensor networks. Thus, their integration will produce a full-fledged m-Health integrated platform (Fig. 6) on top of which multitudes of m-Health services could be developed and furnished. The use case of Sect. 4.2.1 will be fully deployable atop the integration of UniversAAL and BodyCloud: (i) the automated monitoring at the health-care center and the decentralization of the monitoring at the patients' homes will be supported by UniversAAL remote services; (ii) the monitoring of mobile assisted livings would be enabled by the BodyCloud mobile services; (iii) new cross-platform services will be developed for enabling complete analysis of the measurement streams coming from assisted livings.

5 Conclusions and Future Work

In this chapter we have presented the INTER-IoT systemic approach, which is being created within the INTER-IoT project together with necessary software tools and end-user applications. It will provide ways of overcoming interoperability problems between heterogeneous IoT systems across the communication/software stack, including: devices, networks, middleware, application services, data/semantics. Henceforth, reuse and integration of existing and future (even standard) IoT systems will be facilitated and made possible to obtain interoperable ecosystems of IoT platforms.

As the ecosystem of interoperable devices and services expands, so will increase the value of building new devices for and applications working within this ecosystem. This emerging ecosystem is not owned by any business or entity, but rather it exists to enable many entities to pool their resources together to create larger opportunities for all. Open interoperability delivers on the promise of open source software, enabling vendors and developers to interact and interoperate, without interfering with anyone's ability to compete by delivering a superior product and experience. In the absence

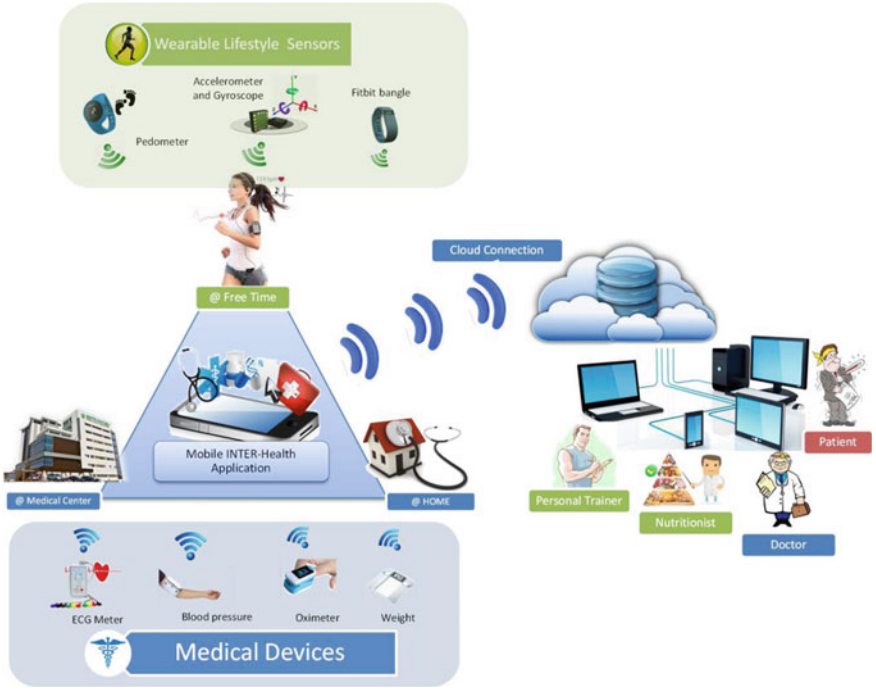

Fig. 6 **INTER-IoT** interconnection for m-Health (INTER-Health)

of global IoT standards, the INTER-IoT project and results will support and make it easy for any company to design IoT devices, smart object, or services and get them to market quickly, to a wider client-base, and to create new IoT interoperable ecosystems. In the long term, ability for multiple applications to connect to and interact with heterogeneous sensors, actuators, and controllers, thus making them interoperable, will become a huge enabler for new products and services.

Acknowledgements This work has been carried out under the framework of INTER-IoT, Research and Innovation action - Horizon 2020 European Project, Grant Agreement #687283, financed by the European Union.

References

1. Alaya, M.B., Medjiah, S., Monteil, T., Drira, K.: Toward semantic interoperability in oneM2M architecture. IEEE Commun. Mag. **53**, 35–41 (2015)
2. Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W., Savaglio, C.: A mobile multi-technology gateway to enable IoT interoperability. In: 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 259–264. IEEE (2016)

3. Bandyopadhyay, S., Sengupta, M., Maiti, S., Dutta, S.: Role of middleware for internet of things: a study. Int. J. Comput. Sci. Eng. Surv. **2**, 94–105 (2011)
4. Bassi, A., Bauer, M., Fiedler, M., Kramp, T., Van Kranenburg, R., Lange, S., Meissner, S.: Enabling things to talk. Des. IoT Solut. IoT Archit. Ref. Model, 163–211 (2013)
5. Bernstein, P.A.: Middleware: a model for distributed system services. Commun. ACM **39**, 86–98 (1996)
6. Bosman, H.H., Iacca, G., Wörtche, H.J., Liotta, A.: Online fusion of incremental learning for wireless sensor networks. In: 2014 IEEE International Conference on Data Mining Workshop (ICDMW), pp. 525–532. IEEE (2014)
7. Doukas, C., Antonelli, F.: COMPOSE: Building smart & context-aware mobile applications utilizing IoT technologies. In: 2013 Global Information Infrastructure Symposium, pp. 1–6. IEEE (2013)
8. Eisenhauer, M., Rosengren, P., Antolin, P.: A Development platform for integrating wireless devices and sensors into ambient intelligence systems. In: 2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops. Presented at the 2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, pp. 1–3 (2009). doi:10.1109/SAHCNW.2009.5172913
9. Ernst, J.B., Kremer, S.C., Rodrigues, J.J.: A survey of QoS/QoE mechanisms in heterogeneous wireless networks. Phys. Commun. **13**, 61–72 (2014)
10. Fortino, G., Di Fatta, G., Ochoa, S.F., Palau, C.E.: Engineering Future Interoperable and Open IoT Systems. Elsevier, Amsterdam (2017)
11. Fortino, G., Guerrieri, A., Lacopo, M., Lucia, M., Russo, W.: An agent-based middleware for cooperating smart objects. International Conference on Practical Applications of Agents and Multi-Agent Systems, pp. 387–398. Springer, Berlin (2013)
12. Fortino, G., Guerrieri, A., Russo, W.: Agent-oriented smart objects development, In: 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 907–912. IEEE (2012)
13. Fortino, G., Guerrieri, A., Russo, W., Savaglio, C.: Towards a development methodology for smart object-oriented IoT systems: a metamodel approach. In: 2015 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1297–1302. IEEE (2015)
14. Fortino, G., Guerrieri, A., Russo, W., Savaglio, C.: Middlewares for smart objects and smart environments: overview and comparison. In: Internet of Things Based on Smart Objects, pp. 1–27. Springer International Publishing (2014)
15. Fortino, G., Guerrieri, A., Russo, W., Savaglio, C.: Integration of agent-based and cloud computing for the smart objects-oriented IoT. In: Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 493–498. IEEE (2014)
16. Fortino, G., Parisi, D., Pirrone, V., Di Fatta, G.: BodyCloud: A SaaS approach for community body sensor networks. Future Gener. Comput. Syst. **35**, 62–79 (2014c)
17. Fortino, G., Russo, W.: Towards a cloud-assisted and agent-oriented architecture for the internet of things. In: Baldoni, M., Baroglio, C., Bergenti, F., Garro, A. (eds.) CEUR Workshop Proceedings WOA@AI*IA, pp. 60–65. http://CEUR-WS.org (2013)
18. Fortino, G., Russo, W., Savaglio, C.: Simulation of agent-oriented internet of things systems. In: Proceedings of 17th Workshop From Objects to Agents. pp. 8–13 (2016)
19. Fortino, G., Russo, W., Savaglio, C.: Agent-oriented modeling and simulation of IoT networks. In: 2016 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 1449–1452. IEEE (2016)
20. Ganzha, M., Paprzycki, M., Pawlowski, W., Szmeja, P., Wasielewska, K.: Semantic interoperability in the internet of things: an overview from the INTER-IoT perspective. J. Netw. Comput. Appl. **81**, 111–124 (2016)
21. Ganzha, M., Paprzycki, M., Pawlowski, W., Szmeja, P., Wasielewska, K., Fortino, G.: Tools for ontology matching—practical considerations from INTER-IoT perspective. In: International Conference on Internet and Distributed Computing Systems, pp. 296–307. Springer (2016)

22. Giménez, P., Molina, B., Calvo-Gallego, J., Esteve, M., Palau, C.E.: I3WSN: industrial intelligent wireless sensor networks for indoor environments. Comput. Ind. **65**, 187–199 (2014)
23. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**, 1645–1660 (2013)
24. Hanke, S., Mayer, C., Hoeftberger, O., Boos, H., Wichert, R., Tazari, M.-R., Wolf, P., Furfari, F.: universAAL–an open and consolidated AAL platform. In: Ambient Assisted Living, pp. 127–140. Springer (2011)
25. Iftikhar, S., Khan, W.A., Ahmad, F., Fatima, K.: Semantic Interoperability in E-Health for Improved Healthcare. Semant, ACTION-APPLICATIONS Scenar, vol. 107 (2012)
26. Kamienski, C., Jentsch, M., Eisenhauer, M., Kiljander, J., Ferrera, E., Rosengren, P., Thestrup, J., Souto, E., Andrade, W.S., Sadok, D.: Application development for the Internet of Things: A context-aware mixed criticality systems development platform. Comput. Commun. (2016)
27. Kubicek, H., Cimander, R., Scholl, H.J.: Layers of Interoperability. In: Organizational Interoperability in E-Government, pp. 85–96. Springer, Berlin, Heidelberg (2011). doi:10.1007/978-3-642-22502-4_7
28. Li, S., Xu, L.D., Zhao, S.: The internet of things: a survey. Inf. Syst. Front. **17**, 243–259 (2015). doi:10.1007/s10796-014-9492-7
29. Liotta, A.: The cognitive NET is coming. IEEE Spectr. **50**, 26–31 (2013)
30. Madsen, H., Burtschy, B., Albeanu, G., Popentiu-Vladicescu, F.: Reliability in the utility computing era: towards reliable fog computing. In: 2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP), pp. 43–46. IEEE (2013)
31. Manate, B., Munteanu, V.I., Fortis, T.-F.: Towards a scalable multi-agent architecture for managing iot data. In: 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pp. 270–275. IEEE (2013)
32. Martínez-Costa, C., Menárguez-Tortosa, M., Fernández-Breis, J.T.: An approach for the semantic interoperability of ISO EN 13606 and OpenEHR archetypes. J. Biomed. Inform. **43**, 736–746 (2010)
33. Mesjasz, M., Cimadoro, D., Galzarano, S., Ganzha, M., Fortino, G., Paprzycki, M.: Integrating Jade and MAPS for the development of Agent-based WSN applications. In: Intelligent Distributed Computing VI, pp. 211–220. Springer (2013)
34. Meyer, S., Ruppen, A., Magerkurth, C.: Internet of things-aware process modeling: integrating IoT devices as business process resources. In: International Conference on Advanced Information Systems Engineering, pp. 84–98. Springer (2013)
35. Pace, P., Aloi, G., Gravina, R., Fortino, G., Larini, G., Gulino, M.: Towards interoperability of IoT-based health care platforms: the INTER-health use case. In: Proceedings of the 11th EAI International Conference on Body Area Networks (BodyNets 2016). Presented at the The 11th EAI International Conference on Body Area Networks (BodyNets 2016). Turin, Italy (2016)
36. Pradilla, J., Palau, C., Esteve, M.: SOSLITE: Lightweight sensor observation service (SOS) for the internet of things (IOT). In: 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015). Presented at the 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), pp. 1–7. (2015). doi:10.1109/Kaleidoscope.2015.7383625
37. Razzaque, M.A., Milojevic-Jevric, M., Palade, A., Clarke, S.: Middleware for internet of things: a survey. IEEE Internet Things J. **3**, 70–95 (2016). doi:10.1109/JIOT.2015.2498900
38. Rhee, S.K., Lee, J., Park, M.-W., Szymczak, M., Ganzha, M., Paprzycki, M., others: Measuring semantic closeness of ontologically demarcated resources. Fundam. Informaticae **96**, 395–418 (2009)
39. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**, 2266–2279 (2013)
40. Savaglio, C., Fortino, G., Zhou, M.: Towards interoperable, cognitive and autonomic IoT systems: an agent-based approach. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 58–63, IEEE (2016)
41. Shvaiko, P., Euzenat, J.: Ontology matching: state of the art and future challenges. IEEE Trans. Knowl. Data Eng. **25**, 158–176 (2013)

42. Terziyan, V., Kaykova, O., Zhovtobryukh, D.: UbiRoad: Semantic middleware for context-aware smart road environments. In: 2010 Fifth International Conference on Internet and Web Applications and Services. Presented at the 2010 Fifth International Conference on Internet and Web Applications and Services, pp. 295–302 (2010). doi:10.1109/ICIW.2010.50
43. Tunstall-Pedoe, H.: Preventing Chronic Diseases. A Vital Investment: WHO Global Report. Geneva: World Health Organization, 2005. pp 200. CHF 30.00. ISBN 92 4 1563001. http://www.who.int/chp/chronic_disease_report/en.IEA (2006)
44. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I.S., Mazura, M., Harrison, M., Eisenhauer, M., others: Internet of things strategic research roadmap. Internet Things-Glob. Technol. Soc. Trends **1**, 9–52 (2011)
45. Wan, J., Li, D., Zou, C., Zhou, K.: M2m communications for smart city: an event-based architecture. In: 2012 IEEE 12th International Conference on Computer and Information Technology (CIT), pp. 895–900. IEEE (2012)
46. World Health Organization. Obesity: preventing and managing the global epidemic. World Health Organization (2000)
47. World Health Organization. Physical status: The use of and interpretation of anthropometry, Report of a WHO Expert Committee (1995)
48. World Health Organization, others, 2013. Global status report on noncommunicable diseases 2010. Geneva: World Health Organization. Google Sch (2011)
49. Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., Du, H.-Y.: Research on the architecture of Internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp. V5–484. IEEE (2010)
50. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for internet of things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
51. Yuriyama, M., Kushida, T.: Sensor-cloud infrastructure - physical sensor management with virtualized sensors on cloud computing. In: 2010 13th International Conference on Network-Based Information Systems. Presented at the 2010 13th International Conference on Network-Based Information Systems, pp. 1–8 (2010). doi:10.1109/NBiS.2010.32