People-Centric Internet of Things—Challenges, Approach, and Enabling Technologies

Fernando Boavida, Andreas Kliem, Thomas Renner, Jukka Riekki, Christophe Jouvray, Michal Jacovi, Stepan Ivanov, Fiorella Guadagni, Paulo Gil and Alicia Triviño

Abstract Technology now offers the possibility of delivering a vast range of low-cost people-centric services to citizens. Internet of Things (IoT) supporting technologies are becoming robust, viable and cheaper. Mobile phones are increasingly more powerful and disseminated. On the other hand, social networks and virtual worlds are experiencing an exploding popularity and have millions of users. These low-cost technologies can now be used to create an Internet of People (IoP), a dynamically configurable integration platform of connected smart objects that allows enhanced, people-centric applications. As opposed to things-centric ones, IoP combines the real, sensory world with the virtual world for the benefit of people while it also enables the development of sensing applications in contexts

This is an invited paper.

F. Boavida (✉)
CISUC, DEI, Universidade de Coimbra, Coimbra, Portugal
e-mail: boavida@uc.pt

A. Kliem · T. Renner
Technische Universitaet Berlin, Berlin, Germany
e-mail: andreas.kliem@tu-berlin.de

T. Renner
e-mail: thomas.renner@tu-berlin.de

J. Riekki
University of Oulu, Oulu, Finland
e-mail: jpr@ee.oulu.fi

C. Jouvray
Trialog, Paris, France
e-mail: christophe.jouvray@trialog.com

M. Jacovi
IBM Israel Science and Technology, Haifa, Israel
e-mail: JACOVI@il.ibm.com

S. Ivanov
Waterford Institute of Technology, TSSG, Waterford, Ireland
e-mail: sivanov@tssg.org

P. Novais et al. (eds.), *Intelligent Distributed Computing IX*,
Studies in Computational Intelligence 616,
DOI 10.1007/978-3-319-25017-5_44

such as e-health, sustainable mobility, social networks enhancement or fulfilling people's special needs. This paper identifies the main challenges, a possible approach, and key enabling technologies for a people-centric society based on the Internet of Things.

Keywords Internet of people · People-centric IoT · Smart systems integration

1 Introduction

Although considerable work has been done in the recent past regarding the Internet of Things (IoT) [4], most technologies and solutions for accessing real-world information are vertical, i.e., they are either closed, platform-specific, or application-specific. Recent efforts to define IoT reference architectures, such as IoT-A [7], OpenIoT [8], SENSEI [9], or FIWARE [10], are important steps in the right direction, but still they lack adaptability, intuitiveness, and integration features that are crucial for people-centric applications. So, on one hand, there is need to define an IoT architecture that goes beyond vertical solutions by integrating all required technologies and components into a common, open and multi-application platform. On the other hand, there is need to develop a set of common building blocks, middleware and services that can be used to construct people-oriented applications in an open, dynamic and more effective way into smart environments including but not restricted to smart cities, businesses, education and e-health. We call it an Internet of People (IoP) [5].

One important, overall challenge for IoP is to define a generic version of an architecture that can be used for supporting specific solutions for each particular people-centric application domain. Naturally, this will require identifying specific challenges regarding several key aspects, such as interoperability, reliable communications, self-management and adaptability, human-machine interaction, security and privacy, ontologies, and big data analytics.

Subsequently, in addition to the IoP architecture definition, it is important to develop and make generally available several easy-to-use tools, namely middleware

F. Guadagni
San Raffaele S.p.A, Milan, Italy
e-mail: guadagnifiorella@gmail.com

P. Gil
UNINOVA—Instituto de Desenvolvimento de Novas Tecnologias, Setúbal, Portugal
e-mail: psg@fct.unl.pt

A. Triviño
Universidad de Málaga, Málaga, Spain
e-mail: atc@uma.es

and services, on which people-centric applications can be built. These will build on technological solutions such as wireless sensor networks, wireless mesh networks, mobility, and ubiquity. Moreover, these tools must be context-aware, so they can be used to build applications in a variety of contexts, such as smart cities, e-learning, and e-health contexts, thus enhancing the autonomy and quality of life of citizens.

Following this general identification of motivations and overall approach, the remainder of this paper is organised as follows. Section 2 identifies the main challenges for developing people-centric Internet of Things solutions. Section 3 details a possible approach, by addressing the vision, infrastructural needs and design principles. Section 4 identifies enabling technologies, including relevant related work. Section 5 provides the conclusions and identifies guidelines for further work.

2 Challenges

Several challenges can be identified in what concerns developing people-centric Internet of Things platforms and applications. This section identifies two overall challenges and several related and/or complementary challenges. All of them are key to the success of the IoP paradigm that will be presented in Sect. 3.

Open, Smart Platform The IoP concept requires an open, smart platform that will support People2People and People2Thing interactions and can be used to develop a variety of people-centric applications. Moreover, IoP does not limit itself to a technology-oriented approach nor to an application-oriented view. IoP provides a comprehensive approach that brings together actors along the value chain, from suppliers of components and customized computing systems to system integrators and end users, going from reference architectures to applications, from application-specific approaches to an open application-development framework, from an individual devices view to resource virtualization, and from the Internet of Things to the Internet of People.

Sharing in IoT Environments Sharing physical devices leads to a paradigm shift in how IoT-related applications can be designed. Paradigms like Infrastructure as a Service (IaaS), On-Demand Resource Provisioning or Pay-As-You-Go (PAYG) pricing models became very popular along with the proliferation of cloud computing and its applications. However, looking at IoT-related applications, a completely different picture of how these applications work and are designed can be observed. IoT applications are often built upon a gateway-based approach. This can be briefly described as a single system (e.g. a router or a smart phone), that integrates available sensors, collects data from them and forwards the resulting data streams to application layer components (e.g. a computer centre hosting data analysis applications). The IoP approach aims at broadening our understanding of the term cloud. By introducing concepts for provisioning of sensors and embedded devices on a PAYG basis, the cloud turns from an endless remote resource to an overall resource surrounding us constantly.

Connectivity, Mobility and Ubiquity As we witness an unprecedented increase in the deployment and use of wireless technologies (mobility management, pervasive sensing, automated object-to-object and object-to-person communications, the Internet of Things, etc.), it is becoming important to guarantee universal connectivity, using a variety of communication technologies, including 4 G, 5 G, IEEE 802.11ad, wireless mesh networks (WMN), mobile and vehicular ad hoc networks (MANET/VANET), and devise new and more efficient ways for their operation. WMNs and MANET/VANET may play an important role in generalised use of IoT. Nevertheless, despite considerable work done in the past in the area of routing in WMNs [1], the fact is that several challenges persist and there is need to go beyond traditional proactive or reactive routing algorithms and protocols.

Adaptive, Dynamic and Mobile Configuration Capabilities There is need for tools and methods to cope with moving or disappearing nodes while keeping the transparency constraint. Device integration platforms should enable integrating sensors into any smart devices capable of doing so. This properly reflects the mobility of devices and users, because devices with limited communication range may need to be integrated at different locations (e.g. medical sensors moving with a patient in case of an emergency). In addition, service might have to be migrated or the data routing probably has to be adapted, which may have significant impact on the overall network structure. New nodes can introduce new features, which again may require adapting significant parts of the service deployment, routing and network structure.

Effective Device Integration Novel device integration and management platforms able to handle large amounts of devices (proprietary and standard based) are needed, assuring device integration and platform adaptation at runtime (online-reconfiguration), and providing device abstraction to expose uniform interfaces of heterogeneous devices to applications. For this purpose, platforms will need to understand the devices (e.g. capabilities, data structures they produce, device configurations) or at least need to be able to gather integration knowledge if required (e.g., when a new device joins the platform). This may demand for sensor markup languages (SensorML) and sensor ontologies.

Scalability and Expandability There is need for dynamic expandability of network components (things), services, applications and users. These capabilities are fundamental for an effective device integration and adaptive, dynamic and mobile configuration capabilities. Scalable and expandable systems for a large amount of heterogeneous devices and data streams, as well as ability to establish billions of different IoT connections between devices and objects, are an important challenge.

High Availability, Dependability and Fault Tolerance Adaptive and dynamic functionalities are needed for monitoring and managing the infrastructure in a self-manageable mode at runtime. This will allow platforms to be permanently available and have the ability to quickly recover from faults, as well as dynamic access and network management for a large number of robust and dynamic connections. There is also the need for integrating online adjustment technologies from

other domains, like Software-Defined Networking (SDN) and Data-Centric infrastructures.

Quality of Service and Non-Functional Requirements There is the need for functionalities to manage and differentiate between critical (e.g. e-Health) and non-critical (e.g. entertainment) applications and their data streams from different domains on the same commodity transport and infrastructure. Therefore, platforms should consider and allow for quality-of-service and non-functional requirements such as reliability, determinism, or performance to transmit and deliver data in real-time.

Interoperability, Data-Models and Nomenclatures One important challenge is the ability for independent devices to cooperate and exchange information with each other. Therefore, there is need to efficiently provide knowledge repositories, which allow handling heterogeneous (probably unknown) incoming data streams in a protocol agnostic fashion. This will be a key enabler to provide technologies like context-awareness, content-based routing or quality of service, and integrate different IoT domains with each other.

User-Centred Requirements Analysis Nowadays, IoT systems are mainly focused on the technical level, like performance, interoperability, integration, etc. However, whenever use-cases are targeting human users the focus must not be solely on these aspects, as the human factor must be also considered. It is thus essential to apply a user-centred approach based on the use of the repertory grid method as well as the application of personalized and interactive e-assessment technology. This will allow identifying application-specific user features and understanding the users' needs, motivations and beliefs.

Big Data (Graph) Analysis People-centric IoT architectures must be used for modelling the Internet of People and the things they interact with, i.e., the relationships of people-to-people and people-to-things. In this respect, there is clear need for research and progress beyond state-of-the-art in at least the following three areas: efficiently and scalably streaming data into the graph; real-time discovery of effected patterns; and discovering trends based on social and temporal proximity.

Security and Privacy Secure granting and withdrawal of device access tokens is required to allow for device sharing. Issues related to trusted nodes, authentication, security and, privacy are crucial for the implementation, deployment and success of any people-centric application platform. Final users must be able to define privacy preferences in order customize policies according to their demand. Legal aspects and regulations must be completely met.

3 Approach

This section presents an overall IoP vision, a possible supporting infrastructure, and some design principles.

3.1 Vision

The emerging Internet of Things (IoT) concept and the availability of a multitude of sensors, smart devices and applications for use by individuals and communities point to the need for defining a people-centric IoT architecture—which we name Internet of People, IoP (Boavida 2013)—that can go beyond devices, technologies, services and passive entities and can be used in people-oriented IoT applications. The IoP paradigm can be considered as a specialization of the IoT paradigm, in which humans and their interactions can simultaneously be viewed as data sources and sinks, in a network of connected embedded devices, bridging the gap between IoT and the beneficiaries of technologies.

The basic IoT assumption is that people are no longer supported by a single monolithic computing system, such as a PC, but rather use all the small embedded systems (smart devices/objects) surrounding them to fulfill their needs. Currently, most of these smart devices act like closed "boxes" and barely interconnect or collaborate with each other. Moreover, usually an application domain oriented segmentation of IoT related solutions can be observed (i.e. one box for entertainment, one box for smart home control, one box for e-health services). Hence, in order to allow for both efficient resource utilization and smarter applications, an application domain independent solution serving multiple applications within an openly designed and integrated IoP infrastructure is required. The infrastructure needs to open and connect so far isolated heterogeneous devices with each other, provide sufficient enablers for spontaneous interoperability, and offer open APIs that allow people and services to utilize the infrastructure in an application domain independent and technology agnostic manner.

3.2 Infrastructure

As shown in Fig. 1, several basic components can be identified as elements of a possible IoP infrastructure, on which services and applications can be built. The complexity introduced by the IoP vision and its infrastructure design requires establishing a uniform notion of abstraction throughout the whole architecture. Neither sensors or devices nor applications or users should have to care about the heterogeneity of the corresponding spaces (i.e. which nodes integrate or execute them). To hide the complexity of the IoP infrastructure, it is separated into three spaces, namely Physical Space, IoP Runtime Space and Social Space.

The Physical Space includes all physical devices, systems and networks collaborating in the IoP domain. In order to allow for seamless integration of all available nodes in the physical space, the following segmentation is defined: (i) Device Nodes (DN) refer to data resources (i.e. sensors); techniques such as sensor virtualization or on-demand provisioning of the physical device itself can be used to enable them for IoP operation; (ii) Aggregation Nodes (AN) refer to smart

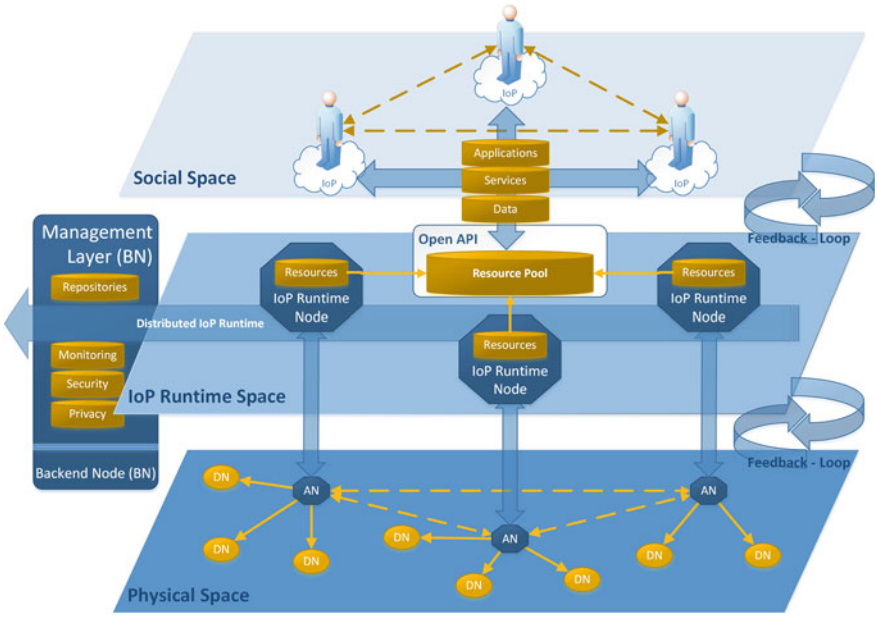

Fig. 1 IoP infrastructure components

devices that additionally provide computational or storage resources and allow hosting the IoP Runtime Nodes (i.e. a software node of the distributed IoP runtime middleware corresponding to the IoP Runtime Space); (iii) Backend Nodes (BN) refer to regular servers (e.g. IaaS Cloud) and provide management and monitoring components used for the IoP runtime.

The IoP Runtime Space will provide capabilities to uniformly access the different types of nodes. Its distributed runtime environment abstracts from the technical details of the underlying physical space and therefore hides the complexity of the physical infrastructure from the application layer. The following components are defined: (i) IoP Runtime Nodes (IRN) refer to software nodes that constitute the distributed IoP Runtime Middleware; (ii) Distributed IoP Runtime is the core middleware solution composed out of the connected IRNs; it is used by the IoP to integrate physical resources and expose them to applications and services; (iii) Management Layer, which provides repositories, like a device directory, offering knowledge about devices and data streams (e.g. nomenclatures, data-models) and therefore allowing IRNs to reconfigure themselves at runtime in order to properly handle unknown devices and incoming data streams in an application domain independent manner; (iv) the Resource Pool abstracts from all individual resources of the underlying physical space and centralizes all resources of the platform in federated and virtual resource pool.

The Social Space models the people and their things as nodes in a Big Graph along with their applications collaborating in the IoP domain. These people have access to the shared resource pool and can use the data sensed by different DNs and the computational resources of all ANs for their applications and services.

3.3 Design Principles

A possible IoP platform addressing the identified challenges and implementing the presented vision and infrastructure will benefit from several design principles identified in the following paragraphs.

Technology and Protocol Agnostic The IoP infrastructure shall be designed in a technology and protocol independent manner. Based on modularity features, knowledge required to integrate and operate newly developed devices and communication protocols shall be addable at runtime without the requirement to manually change or adapt core components of the infrastructure.

Platform Independence The IoP Runtime has to ensure platform independence. Each software module provided by the knowledge base needs to be compliant with the IRN specifications and is therefore executable on each instance, regardless of the underlying platform.

Adaptability and Openness The infrastructure, in particular the IoP Runtime, should run in a highly dynamic environment, in which changes occur very frequently, creating the need for adaptation support for changes in environment and changes that are imposed by the users themselves. The IoP Runtime shall be able to autonomously adapt itself to the requirements of the current environment, (e.g., changes in device, network, service, application, and user requirements). This means that the distributed IoP middleware should act as a general device integrator and service executor, not statically related to any pre-defined set of devices, application domains or vendors.

Peer to Peer Collaboration Because of the federated shape of the resource pool and the possibly huge amount of participating actors that can contribute and consume resources, a peer-to-peer style of interaction is required. This interaction happens both locally with nearby people and resources, and system-wide.

Abstraction and Spontaneous Interoperability The IoP infrastructure must be highly dynamic regarding the resources available in the pool and the communication links established between the participants or between the spaces (i.e. between applications and devices). A related requirement is providing appropriate measures for abstraction that allow hiding functional details like device control or protocol logic from applications.

Cloud Computing Paradigms As mentioned in Sect. 2, one of the main technical requirements for the IoP runtime is to map resource virtualization and provisioning concepts into the IoT world. This goes along with several upcoming approaches like sensor virtualization or cyber physical cloud computing. From the

perspective of a user, the platform that serves his/her needs is no longer a set of statically bound physical devices and sensors.

Context Awareness The IoP architecture needs to provide dynamic and adaptive capabilities to support a great variety of smart environments, services, business and persons. Context awareness can be a key driver to enable these capabilities, because it allows applications to adapt its behaviour automatically to the current user context.

Quality of Service Given the huge amount of sensors and smart devices, the rapidly increasing amount of data, and the dynamic IoP infrastructure, efficiently applying and monitoring Quality of Service will become a major issue in IoP. Services can only be delivered efficiently if the required data are available at the required location at the required time.

Security and Privacy The IoP infrastructure shall provide necessary security and privacy features. This can include code signing mechanisms to ensure the integrity of software modules, mechanisms to ensure integrity and confidentiality for exchanged data, authentication and authorization mechanisms, or anonymization techniques. Users shall have the possibility to define different levels of confidentiality or integrity.

4 Enabling Technologies

IoP in particular and IoT in general have a strong relationship to and partially rely on other technologies and paradigms known from the distributed systems and computing domain. Some of these technologies and paradigms, which contribute foundations necessary to set up the IoP approach, will be introduced and put into a contextual relationship.

Machine-to-Machine Communication M2M describes the exchange of information between devices like machines, cars, sensors or, actuators usually performed in an automated manner and without human interaction [16]. Thus, M2M is often referred to as the building block of IoT, because the virtual representations of things made available by IoT can also be described as the service endpoints to an M2M system. M2M has a high relevance to the IoP approach, since it deals with similar challenges like heterogeneity of devices and communication networks, device manageability or scalability in general that altogether lead to the overall problem of device integration.

Mobile Grid and Mobile Cloud Computing Mobile computing evolved out of the dissemination of small, mobile and wirelessly connected devices like smart phones that offer computing capabilities. The term mobile grid covers both, the demand for users with mobile devices to access resources offered by the grid and the utilization and integration of the resources offered by the mobile devices themselves. Thus, the mobile grid can be defined as an extension to the regular grid providing capabilities to support mobile users and resources in a seamless, transparent, secure and efficient way [13].

Sensor Networks and Cloud Integration Wireless Sensor Networks (WSN) may consist of several up to thousands of resource-constrained nodes, and are often designed towards the specific requirements of the application domain. In contrast to cloud computing, data consumers usually have to be aware of the actual location, the resource constraints and the infrastructure management requirements of the sensor nodes in order to properly access and utilize them. This often limits the set of consumers being able to access the WSN. As a remedy, concepts like sensor-cloud integration [3] or sensor virtualization [2] were introduced. These approaches basically aim at overcoming the resource constraints of traditional WSNs by integrating cloud resources and providing access of multiple users to physical sensors.

Cognitive Services A number of models of selective attention have been proposed in Cognitive Science (e.g., [11]). Particularly related with these models is the issue of measuring the value of information. Most of those measures rely on assessing the utility or the informativeness of information (e.g., [14]). However, little attention has been given to the surprising and motive congruence value of information, given the beliefs and desires/goals of a user or of an agent acting on his/her behalf. Cognitive models for ordinary or creative reasoning are of high importance in the IoP architecture.

Big Graph Technologies In the era of Big Data, Big Graphs have a special place, by modelling not only the objects, but the relationships between them. The proliferation of social networks is the main driver behind the evolution of Big Graph technologies, as the interactions of people over social network map naturally into a graph. Social networks often model not only people (as nodes), but also objects that they interact with (e.g., online documents, posts, comments).

In the following paragraphs, some architectures/frameworks, resulting mostly from R&D activities under public funding (EU-FP7), are also mentioned, as they are related to and can be used in the development of the IoP vision.

Future Internet Architectures Future Internet Architectures is a generic term for several research projects and initiatives, like FI-PPP [12], FIWARE [10] or, FI-STAR [15], that investigate in the improvement or redesign of the aging IP-based infrastructure in order to cope with challenges like ubiquitous network access, mobility, or integrated security. It is assumed, that the increasing amount of users and the demand for future applications require a paradigm shift from machine-centered and packet delivery based infrastructures towards data, content and, user-centered ones.

SOCIETIES [6] Open scalable service architecture and platform for pervasive computing was developed during a European funded research project. The project expands the concept of pervasive computing from the scope of an individual user to a community. Relevance, similarity of contextual information and social networking history are used to connect users and organize them into communities. The communities are formed in an intelligent manner to ensure their ability for self-organization, self-orchestration, self-healing. The communities are further used for information exchange and resource sharing between users and their devices.

SENSEI In the SENSEI project [9] the focus has been drawn on the realization of ambient intelligence in a future network and service environment. In this environment, heterogeneous wireless sensor and actuator networks (WSAN) are integrated into a common framework of global scale and make it available to services and applications via universal service interfaces. In this pursuit, SENSEI intended to create an open business driven architecture that fundamentally could address inherent scalability problems for a large number of globally distributed wireless sensor and actuator nodes.

IoT-A IoT-A [7] technical objective was to create the architectural foundations of the Future Internet of Things, allowing seamless integration of heterogeneous IoT technologies into a coherent architecture and their federation with other systems of the Future Internet. In this context an architectural reference model for the interoperability of IoT systems was introduced. The project also focused on other technological issues, such as scalability, mobility, management, reliability, security and privacy.

5 Conclusion

Current low-cost sensing technologies and IoT-related developments make it now possible to go from simple sensing and actuating applications to people-centric applications. Nevertheless, despite considerable advancement of the state of the art, most emerging systems and applications are still platform-specific and/or application-specific. In the current paper we identified the main challenges, a possible approach and the key enabling technologies for open, platform- and application-independent, people-centric systems.

The main overall challenges are the development of an open, smart platform able to support people-to-people and people-to-thing interactions, and the virtualisation and sharing of physical and logical devices. Complementary challenges include connectivity, mobility and ubiquity, dynamic configuration and provisioning, device integration, scalability and expandability, dependability and fault tolerance, quality of service, data models and nomenclatures, user-centred analysis big data analysis and, last but not least, security and privacy.

A possible approach to the implementation of the IoP vision was briefly presented, by identifying the infrastructure components and main design principles. Lastly, several enabling and supporting technologies were identified in order to provide the reader with relevant information on related work.

Acknowledgments The authors would like to thank the participants in the IoP consortium for their insights and contributions.

References

1. Akyildiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: a survey. Comput. Netw. J. **47** (4), 445–487 (2005)
2. Alam, S., Chowdhury, M.M., Noll, J.: (2010) Senaas: an event-driven sensor virtualization approach for internet of things cloud. In: Paper presented at NESEA 2010—IEEE International Conference on Networked Embedded Systems for Enterprise Applications, Xi'an Jiaotong-Liverpool University International Conference Center, Suzhou, China, 25–26 Nov 2010
3. Alamri, A., Ansari, W.S., Hassan, M.M., Hossain, M.S., Alelaiwi, A., Hossain, M.A.: (2013) A survey on sensor-cloud: architecture, applications, and approaches. Int. J. Distrib. Sensor Netw. 2013: Article ID 917923, http://dx.doi.org/10.1155/2013/917923
4. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. J. **54**(15), 2787–2805 (2010)
5. Boavida, F., Silva, J.S.: IoP—Internet of People. Future Internet Networking Session. ICT 2013, Vilnius, Lithuania. http://ec.europa.eu/digital-agenda/events/cf/ict2013/item-display.cfm?id=10400 (2013). Accessed 1 June 2015
6. Doolin, K.: SOCIETIES—Self Orchestrating Community Ambient Intelligence Spaces. http://www.ict-societies.eu/ (2014). Accessed 1 June 2015
7. Günter, K.: IoT-A—Internet of Things Architecture. http://www.iot-a.eu/public (2013). Accessed 1 June 2015
8. Hauswirth, M.: OpenIoT—Open Source cloud solution for the Internet of Things. http://openiot.eu/ (2014). Accessed 1 June 2015
9. Hérault, L.: SENSEI—Integrating the Physical with the Digital World of the Network of the Future—http://www.sensei-project.eu/ (2010). Accessed 1 June 2015
10. Hierro, J.: FIWARE—Core platform of the Future Internet. http://www.fiware.org/ (2014). Accessed 1 June 2015
11. Horvitz, E., Jacobs, A., Hovel, D.: (1999) Attention-sensitive alerting. In: Paper Presented at the Fifteenth Conference on Uncertainty and Artificial Intelligence. Morgan Kaufmann, p. 305–313, Stockholm Sweden, 30 July—1 August (1999)
12. Lakaniemi, I.: FI-PPP—Future Internet Public-Private Partnership. Internet-Enabled Innovation in Europe. http://www.fi-ppp.eu/ (2013). Accessed 1 June 2015
13. Litke, A., Skoutas, D., Varvarigou, T.: Mobile grid computing: changes and challenges of resource management in a mobile grid environment. In: Paper presented at the 5th International Conference on Practical Aspects of Knowledge Management (PAKM 2004), Vienna, Austria, 2–3 Dec 2004
14. MacKay, D.: (1992) Information-based objective functions for active data selection. J Neural Comput. **4**(4), 590–604 (1992)
15. Usländer, T., Berre, A.J., Granell, C., Havlik, D., Lorenzo, J., Sabeur, Z., Modafferi, S.: The future internet enablement of the environment information space. Environmental Software Systems, Fostering Information Sharing, pp. 109–120. Springer, Berlin Heidelberg (2013)
16. Wu, G., Talwar, S., Johnsson, K., Himayat, N., Johnson, K.D.: M2M: From mobile to embedded internet. Commun. Mag. IEEE **49**(4), 36–43 (2011)