Legal and Regulative Aspects of IoT Cloud Systems

E. E. Kalmar, A. Kertesz, Sz. Varadi
Software Engineering Dept., University of Szeged
H-6720 Szeged, Dugonics ter 13, Hungary
Email: kalmar.edua.eszter@stud.u-szeged.hu

R. Garg, B. Stiller
Communication Systems Group, IfI, University of Zurich
CH-8050 Zurich, Binzmuehlestrasse 14, Switzerland
Email: garg@ifi.uzh.ch

Abstract—**Organizations envisioning adopting cloud computing have to consider numerous factors, including technical, organizational, economical and relational ones. Legal and regulative constraints increase the complexity and can vary with different deployment models and service levels. Nowadays a growing number of powerful devices are joining the Internet. Data users produce with these devices are continuously posted to online services, which require the use of cloud providers to efficiently handle these data. In our former work we have derived a general federation architecture for clouds from definitions of international organizations, and used it to define common cloud computing usage patterns. The aim of this paper is to revise purely cloud usage patterns and identify scenarios with cases involving Internet of Things (IoT) utilization based on corresponding European projects. These cases are also examined against legal and regulative constraints, in order to help users to better understand IoT ecosystems and companies to design better applications for IoT cloud environments.**

1. Introduction

The concept of cloud computing has been pioneered by commercial companies like Amazon, IBM and Microsoft, with the promise to allow elastic construction of virtual infrastructures. Services offered by clouds range from the infrastructure to the application-level, and they have already opened new market opportunities by allowing organizations to focus on their core competencies. The Cluster of European Research Projects on the Internet of Things [1] defined the Internet of Things (IoT) as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols. Things in this network interact and communicate among themselves and with the environment by exchanging data and information sensed, and react autonomously to events and influence them by triggering actions with or without direct human intervention. Recent trends and estimations call for an ecosystem that provides means to interconnect and control these devices. With the help of cloud solutions, user data can be stored in a remote location, and can be accessed from anywhere. There are more and more PaaS cloud providers offering IoT specific services (e.g. Amazon AWS IoT Platform, Azure IoT Suite). Some of these IoT features are unique, but every PaaS provider addressing IoT has the basic capability to connect to and store data from devices.

Organizations envisioning adopting IoT and cloud technologies have to consider a multitude of factors. These factors can be assigned to different fields, such as technical, organizational, economical and relational [2]. The application of these technologies also moves functions and responsibilities away from local ownership and management to third-party provided services, which in turn raises legal issues, such as data protection. Legal and regulative constraints increase the complexity further and vary depending on the location of different stakeholders. Different deployment models and service levels can lead to a high variety of important considerations. All these factors including regulative constraints cannot be considered by themselves, since they are interconnected and influence each other. In the supply of any goods and services, the law gives certain rights that protect the consumer and provider, which also applies for IoT cloud systems: it is subject to legal requirements and constraints to ensure cloud services are accurately described and provided to customers with guarantees on quality and fitness-for-purpose.

Data that users produce with mobile devices are continuously posted to online services, which require the use of cloud providers to efficiently handle these data. In our previous work we have derived a general federation architecture for clouds from definitions of international organizations, and used it to define common cloud computing usage patterns [3]. The goal of this work is to revise these purely cloud usage patterns and to extend them with cases involving IoT utilization by examining corresponding European projects. These cases are also examined against legal and regulative constraints, in order to help users to better understand the ecosystem and companies to design better applications for IoT cloud systems.

The remainder of this paper is as follows: Section 2 summarizes earlier identified cloud use cases and their legal aspects. Section 3 introduces IoT application areas and highlights four relevant IoT use cases by surveying recent European projects. Section 4 discusses recent advances in European legislation and their implied regulative constraints related to the presented cases. Finally, we conclude the paper in Section 5.

2. Legal Constraints of Cloud Use Cases

As a result of the pace of technical and economic progress in clouds, it was important to determine the compliance of common cloud computing usage patterns with legal constraints and requirements. To protect the consumer against the provider misusing their data, data processing legislation has been developed to ensure that the fundamental right to privacy is maintained [4]. Data protection covers the dynamic provisioning and processing of data in cloud environments including the majority of currently available cloud characteristics and functions (e.g., shared data storages, multi-jurisdictional servers and establishments). The distributed nature of cloud computing (i.e. cloud services being available from anywhere in the world) makes is difficult to analyze every country's data protection laws for common cloud usage evaluation criteria. Therefore it is important to know how the corresponding legislation affects the behavior of cloud providers.

In a former work [3] we provided a method for and the results of an evaluation of commonly-observed cloud federation use cases against the law applied to cloud computing. To clarify and exemplify legal compliance in the identified usage patterns, we considered the Data Protection Directive (DPD) of the European Union (EU) [4], which is a commonly accepted and influential directive in the field of data processing legislation. We discussed six cases where legal issues may arise due to private data processing at multiple jurisdictions resulting from utilizing cloud data center establishments at different geographical locations. Considering European cloud federations, the Article 4 of the current DPD states that the location of the data controller's establishment determines the national law applicable for data processing. In cases where an establishment is outside the EU, an adequate level of data protection should be provided according to the DPD. We also found that new developments in legislation regulation applying to clouds were still needed.

3. IoT Application Areas and Use Cases

IoT application areas and scenarios have been categorized, such as by Want et al. [6], who set up three categories: (i) Composable systems – ad-hoc systems can be built from a variety of nearby things by making connections among these possibly different kinds of devices. As these devices can discover each other over local wireless connections, they can be combined to provide higher-level capabilities. (ii) Smart cities – utilities of modern cities could be managed more efficiently with IoT technologies, e.g. traffic-light systems can be capable of sensing the location and density of cars in the area, and optimizing red and green lights to offer the best possible service for drivers and pedestrians. (iii) Resource conservation – with the extensive use of Internet-connected, networked sensors major improvements can be made in the monitoring and optimization of resources such as electricity and water.

Atzori et al. [7] examined IoT systems in a survey. They identified many application scenarios, and classified them to five application domains: transportation and logistics, healthcare, smart environments (home, office, plant), personal and social, finally futuristic domains. They described these domain in detail, and defined open issues and challenges to all of them. Concerning privacy they stated that a lot of information about a person can be collected without the person being aware, and control on all such information is impossible with current techniques. Escribano [8] discussed the first opinion [9] of the Article 29 Data Protection Working Party (WP29) on IoT. According to these reports four categories can be differentiated: (i) wearable computing, which means the application of everyday objects and clothes, such as watches and glasses, in which sensors were included to extend their functionalities. (ii) Quantified Self things can also be regularly carried by individuals to record information about their own habits. With such things we can examine physical activities (e.g. sleep patterns, burned calories), track movements, and measure weight, pulse or other health indicators. (iii) Home automation covers applications using devices placed in offices or homes such as connected light bulbs, thermostats, or smoke alarms that can be controlled remotely over the internet. They also mention smart cities as the fourth category, but they do not define them explicitly. They argue that sharing and combining data through clouds will increase locations and jurisdictions, where personal data resides. Therefore it is crucial to identify and realize which stakeholder is responsible for data protection. WP29 named the following challenges concerning privacy and data protection: lack of user control, low quality of user consent, secondary uses of data, intrusive user profiling, limitations for anonymous service usage, and communication- and infrastructure-related security risks.

From these related works four IoT cloud cases (see Figure 1) can be derived: (1) local, ad-hoc IoT systems can be formed from near-by things (e.g. smart watch, thermometer, smartphome and TV) to perform a certain task. In this case no data is moved to the cloud. (2) a mobile device is working with an application running in the cloud. The smartphone can be used to produce, store and process data, thus it acts as an application component (or a VM) in a local private cloud. (3) a mobile phone can act as a bridge or gateway to move sensor data to the cloud. In this way data can be stored and processed both locally at the smartphone, and in a remote location in the cloud. Visualization of the processed data can usually be done in a browser. Finally, (4) is a group for IoT applications, where things (such as smart TVs) communicate with the cloud directly. In this case data is both stored and processed in the cloud.

3.1. European projects addressing IoT clouds

In this subsection we examine recent European projects addressing IoT and cloud utilization. We try to grasp how

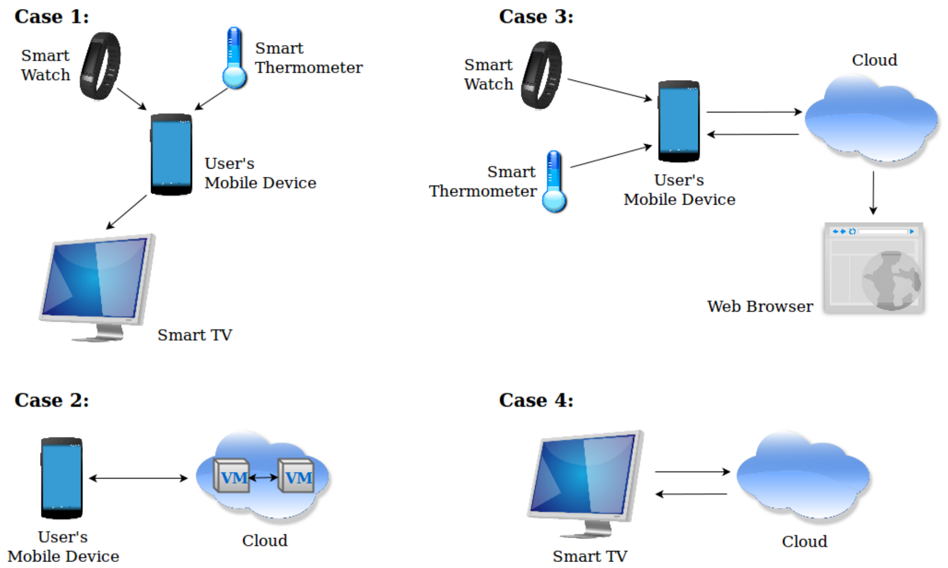

Figure 1. Identified general IoT cases

IoT and security issues are considered in these works, and depict their architectural views for each project. Finally we map these views to the four general cases identified before.

iCore

The iCore project [10] defined a cognitive framework, stating that all the accessible, observable and controllable real world or digital objects can be represented in the IoT world with a Virtual Objects (VOs) and there are Composite Virtual Objects (CVOs) using the services of VOs, a mash-up of semantically interoperable VOs. Therefore CVOs enable the reuse of existing VOs outside their initial context and domain. Innovative cross-domain systems and apps can be developed with iCore. This solution allows us to create services with the combination of local and generic service objects referring to global scale. The Usage Control Toolkit is an important element of the framework since it addresses aspects of Governance, Security and Privacy by using metamodels for specification of computer system structure, behavior, context, information and organizational roles. Figure 2 shows a general use case of iCore. VOs are composable and can form a CVO, which is able to use the services of VOs for further processing. In our visualization, not only CVOs, but VOs can store or process data in clouds or locally, which is similar to Case 3 of Figure 1, where smart sensors can communicate with the cloud only through a mobile device acting like a gateway or bridge.

BUTLER

The BUTLER project [11] covers a platform to support the development of the IoT. It must be able to support different smart domains by providing them communication, location and context awareness capabilities, although guaranteeing security and privacy is a must as well. BUTLER aims for data protection especially at communication level, not at data storage level. A security service called Authorization Server authenticates users and applications with OAuth2.0, and with the use of generated session keys and access tokens. Moreover, it has a new security and privacy service called the Identity Management. This platform provides a bootstrapping mechanism between the sensor nodes and the gateway at WSN (Wireless Sensor Network) level for large scale deployment of sensor devices. These mechanisms mentioned before address end-to-end and hop-by-hop security problems as depicted in Figure 2. BUTLER also supports information-theoretic security to increase the privacy of wireless communication and implements secret key generation for short-range communication systems. A hop-by-hop mechanism is depicted in Figure 2. The gateway, serving as a bridge between the WSN and the Internet world, responsible for the communication of these two sides. The workflow is the following: the gateway authenticates to the Autorization Server, the sensors in the IoT domain can bootstrap to the gateway in the WSN and the Autorization Server generates the needed security credentials, which can be pushed back to the sensors by the gateway. This mechanism is similar to our derived Case 3 shown in Figure 1 since the Authorization Server can be placed in a cloud and the sensors can use a smart mobile device as a gateway to the cloud.

The two approaches of BUTLER differs a little, since in an end-to-end mechanism the sensor nodes can authenticate directly to the Authorization Server to acquire the security credentials. Nevertheless both cases can be mapped to Case 3 of Figure 1.

GAMBAS

The GAMBAS project [12] developed an adaptive middleware for privacy-preservation and automated utilization of behavior-driven services. Instead of today's ordinary mo-

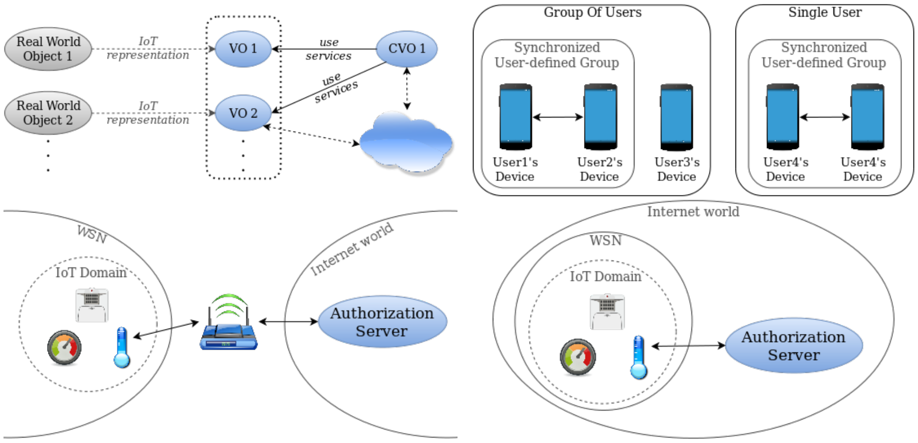

Figure 2. Use cases for: iCore framework (top-left), GAMBAS capabilities (top-right), hop-by-hop security mechanism of BUTLER (bottom-left) and end-to-end security mechanism of BUTLER (bottom-right)

bile information access, on-demand searches via browsers or apps, GAMBAS provides proactive access to the right information at the right point in time. The experience for users feels seamless due to the reduction of the complexity of application development. According to this solution, data acquisition, storage and processing also controlled by the user. Since data is acquired via users' internet connected devices, security and privacy plays a very important role. Users can define groups for themselves for information-synchronization and they are granted full control over locally stored data, acquired through built-in sensors. In other words, a secure distributed data processing system can be formed by connecting users' local data storages. A mechanism is also provided, which disables subsets of sensors in order to prevent data accumulation. GAMBAS provides security and privacy with a data discovery system using pseudonyms to avoid revealing users' identity. In addition, the middleware embrace a policy generator tool to define sharing behavior.

Figure 2 also shows the GAMBAS middleware capabilities as mentioned above, representing a distributed data processing system. Users can own devices with built-in sensors to acquire data, which can be shared among devices of a single user or a group of users with synchronized user-defined groups. This idea could be projected to Case 1 of Figure 1, where data is also acquired via a mobile device from sensors, and then it is shared with another smart device. In this case, no data is moved to the cloud.

SPaCIoS

The acronym SPaCIoS [13] stands for Secure Provision and Consumption in the IoS (Internet of Services). The new opportunities IoS brings up requires a high level of security, since services are designed, implemented, deployed, aggregated and used by different entities. This approach states that security validation should be applied at production time and also when services are deployed and consumed. Thus analyzers are used to achieve these goals by developing and combining state-of-the-art technologies. Techniques has been also developed for property-driven security testing and for vulnerability-driven testing, which enables generating test cases with e.g. model checking. A special tool has been implemented for this reason, called the SPaCIoS Tool which uses formal inputs, the expected security goals and the capabilities of the attacker to automatically generate the test cases and it also executes them. This tool have been applied on various security testing problem cases of both industrial and open source IoS application scenarios.

All the techniques described above are involved by the SPaCIoS Tool as illustrated in Figure 3 as well. The Tool demand a formal description of the SUV (System Under Validation) as an input. Then it apply the mentioned techniques using the SUV model and its source code, the security goals and the model of the attacker to produce a results to a Security Analyst through a User Interface. This approach is similar to our identified Case 4 of Figure 1, since the SPaCIoS Tool can be operated in a cloud and the user (Security Analyst) can run the Tool using a PC.

IoT@Work

The IoT@Work project [14] uses IoT technologies to provide Plug-and-Work functionality of production units. It is based on capability tokens with which possession, a subject can access a resource or service exercising the rights granted by the token. Each subject (e.g. user) owns a capability token that holds what rights that subject has over the given resources, in other words what operations can be done to the resources by the subject. The first capability token, as depicted on Figure 3, is created by the Resource Manager and assigns owner rights to itself on resources. This token is also needed to be trusted by the server which manages accesses and has a full visibility of the authorization chain. Each token contains information about itself. Additional tokens can also be generated for other users granting specified rights to them over resources by the Resource Manager. Moreover, these additional tokens can hold flags for the rights as delegable, so the owners of these tokens can generate further capability tokens. When the

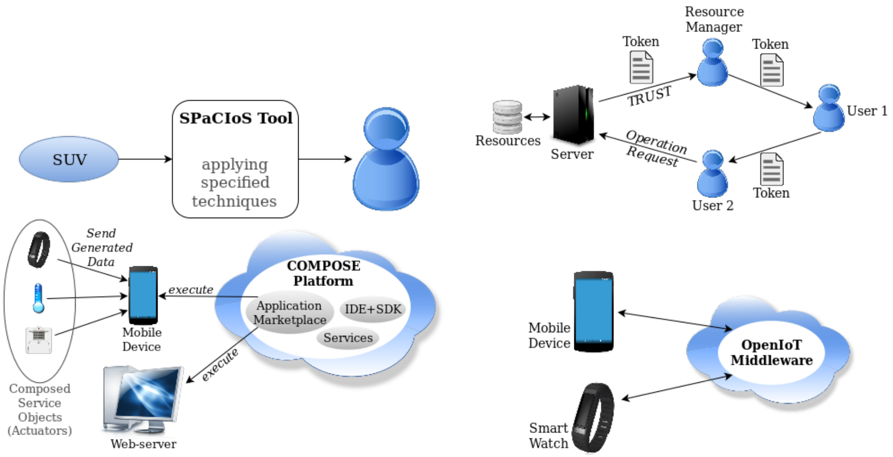

Figure 3. Use cases for: SPaCIoS (top-left), IoT@Work (top-right), COMPOSE (bottom-left) and OpenIoT (bottom-right)

chain comes to an operation request, the Resource Manager needs to check if the access request is valid or not according to the requester's capability token. It also provides encrypted and anonymous capability tokens to increase privacy.

Figure 3 also shows a workflow about how IoT@Work operates. This approach can be mapped to all of the cases of Figure 1, if we consider IoT devices (e.g. sensors, smart phones, etc.) instead of users (subjects), and a cloud instead of the server. In the light of this, every IoT device can come up with an operation request to the cloud and will have the access, if it has the right for it.

COMPOSE

COMPOSE [15] stands for Collaborative Open Market to Place Objects at your Service. As the previous long name foreshadows, the main goal of COMPOSE is to simplify the development of IoT applications. It is similar to iCore, since both of them models physical entities as virtual objects. These service objects can generate data for further processing and interact with services which also can be composed. There is a very flexible security framework in COMPOSE controlled by fine-granular data security policies which supports new IoT applications and user needs for security and privacy. Static analysis and the using of security primitives and services also helps maintain security and privacy. In addition, a possibility is given to use user feedback and to monitor functionality as well as non-functionality about the reputation of service objects, services, developers, etc. Last but not least, COMPOSE deals with data provenance. Since it means tracking the origin of data and the operations performed on them, security and privacy needs to get special attention.

The functioning of COMPOSE is visualized in Figure 3. As explained above, the generated data by the composable service objects is sent to a smart device for further processing. The cloud-based COMPOSE platform provides services, integrated IDE so does SDK and in addition, a marketplace for applications which can be executed on different platforms like mobile devices or web-servers. It is obvious that an analogy shows up between this concept and our identified Case 3 of Figure 1.

OpenIoT

OpenIoT [16] is an open source middleware built for acquiring information from internet connected ”things”. This solution can easily deploy IoT use cases (e.g. smart cities), supports large-scale intelligent and dinamically defined IoT applications and also enables on the fly deployment of services. The aim is to provide a security and privacy module for open source trusted, structured, configurable and integrated middlewares for the cloud-based delivery of IoT services. Thus it places great emphasis upon security and privacy by supporting role-based authentication and authorization to ensure authorized access to connected sensors and services. One of its seven modules is the Trust-Module, which owns the metadata descriptions and is responsible for the secure authentication using OAuth2.0 among the components. Moreover, the middleware uses utility-driven privacy and security mechanisms as well. Figure 3 demonstrates that the internet-connected IoT devices communicate with the OpenIoT middleware, which runs in a cloud. This approach is very similar to Case 4 of Figure 1, as in both of the ideas smart devices communicate with a cloud and with the services running there.

3.2. Mapping European projects to the identified use cases

Table 1 shows a comparison of these approaches, matching them to the identified IoT cases. We can see that all four cases are covered by the overviewed projects, and Case 3 is the most popular or generic.

In order to comply with the European legislation on data protection we need to identify data controller and data processor roles [4] in these cases. In case 2, the user with its mobile device can be both the controller and a processor, while in case 4 the cloud provider plays the controller and processor roles. In case 3 both cases are possible, the user

TABLE 1. SUMMARY TABLE FOR THE IOT CASES.

	Case 1	Case 2	Case 3	Case 4
iCore			x	
BUTLER			x	
GAMBAS	x			
SPaCIoS				x
IoT@Work	x	x	x	x
COMPOSE			x	
OpenIoT				x

and the cloud service provider can also play controller and processor roles, depending on the application. The EU DPD [4] states that in general the data controller is responsible for obeying the legal regulations. Our future work is to revise and extend these cases, and specify role mappings more precisely. We also plan to identify new legal constraints to be brought by the recent EU legislation reform discussed in the next section.

4. New European Regulation for IoT Cloud Environments

The European Union is currently in the process of reforming the European data protection rules, where the main objectives are: to modernize the EU legal system for the protection of personal data to respond to the use of new technologies; to strengthen users' influence on their personal data and to reduce administrative formalities; and to improve the clarity and coherence of the Member States' rules for personal data protection. To achieve these goals, the European Commission created a new legislative proposal, called General Data Protection Regulation (GDPR) [5], a regulation that sets out a general EU framework for data protection to replace the currently effective DPD.

Personal data is increasingly being transferred across borders and stored on servers in multiple countries both within and outside the EU. The globalised nature of dataflows calls for strengthening the individuals data-protection rights. This requires strong principles for protecting individuals data, aimed at easing the flow of personal data across borders, while still ensuring a high and consistent level of protection without loopholes or unnecessary complexity. Therefore the GDPR will establish a single rule that applies directly and uniformly.

As a summary, due to the legal nature of a regulation under EU law, the proposed data protection Regulation will establish a single rule that applies directly and uniformly. Considering our revealed use cases: according to the Article 4 of the current DPD, the location of the data controller's establishment determines the national law applicable, which can be variable as we have seen in the use cases mentioned in our previous work [3]. However, the proposed Regulation with its unified rules after enter into force must be applied in every Member State in the same way, so there would be and could be not discrepancy among them. Moreover where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the EU, such as in a Member State's diplomatic mission or consular post (Preamble (22) of [5]).

5. Conclusions

In this paper we introduced IoT cloud application scenarios and extracted four common usage patterns by examining recent, corresponding European projects. We also discussed legal and regulative constraints of data protection in current European legislation to be applied to these IoT cases, in order to help users to better understand IoT ecosystems and companies to design better applications for IoT cloud environments. Our future work will address extending these patterns and examining the corresponding new European Regulation in more detail.

6. Acknowledgment

The research leading to these results has received funding from the European COST programme under Action identifier IC1304 (ACROSS), and it was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

References

[1] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelffle. Vision and Challenges for Realising the Internet of Things. CERP IoT - Cluster of European Research Projects on the Internet of Things, CN: KK-31-10-323-EN-C, March 2010.

[2] R. Garg, B. Stiller, Factors Affecting Cloud Adoption and their Interrelations. 5th International Conference on Cloud Computing and Services Science (CLOSER 2015), pp 87–94, Lisbon, Portugal, 2015.

[3] A. Kertesz, Sz. Varadi, Legal Aspects of Data Protection in Cloud Federations. In S. Nepal & M. Pathan (Ed.), Security, Privacy and Trust in Cloud Systems, pp. 433–455. Springer-Verlag, 2014.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, pp. 31–50, 1995.

[5] COM (2012) 11 final, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, Jan. 2012.

[6] R. Want, S. Dustdar, Activating the Internet of Things. Computer, Vol. 48, No. 9, pp. 16–20, 2015.

[7] L. Atzori, A. Iera, and G. Morabito, The Internet of Things: A Survey. Comput. Netw., Vol. 54, No. 15, pp. 2787–2805, 2010.

[8] B. Escribano, Privacy and Security in the Internet of Things: Challenge or Opportunity. OLSWANG. Online: http://www.olswang.com/media/48315339/privacy_and_security_in_the_iot.pdf, Nov. 2014.

[9] Opinion 8/2014 on the on Recent Developments on the Internet of Things. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, 2014.

[10] iCore project website: http://www.iot-icore.eu/, May, 2016.

[11] BUTLER project website: http://www.iot-butler.eu/, May, 2016.

[12] GAMBAS project website: http://www.gambas-ict.eu/, May, 2016.

[13] SPaCIoS project website: http://www.spacios.eu/, May, 2016.

[14] IoT@Work project website: https://www.iot-at-work.eu/, May, 2016.

[15] COMPOSE website: http://www.compose-project.eu/, May, 2016.

[16] OpenIoT project website: http://academics.openiot.eu/, May, 2016.