Editorial

Leveraging the Internet of Things: Integration of Sensors and Cloud Computing Systems

Massimo Villari,[1] Adnan Al-Anbuky,[2] Antonio Celesti,[1] and Klaus Moessner[3]

[1] *University of Messina, Contrada di Dio No. 1, 98166 Messina, Italy*
[2] *School of Engineering, Computer and Mathematical Sciences, Private Bag Box 92006, Auckland 1142, New Zealand*
[3] *Institute for Communication Systems, University of Surrey, Guildford GU2 7XH, UK*

Correspondence should be addressed to Massimo Villari; mvillari@unime.it

Received 17 May 2016; Accepted 22 May 2016

1. Introduction

Nowadays, cloud computing is a widely debated topic. In fact, there are many scientific works that apply the cloud technology to different fields including energy efficiency [1], storage [2], eHealth [3], dataweb [4], and Internet of Things (IoT) [5].

In particular, considering the IoT scenario, the increasing penetration of sensing and actuating devices is modifying the way of how Internet services and applications are both conceived and consumed. The integration of distributed sensor networks with cloud computing systems is raising the interest of both the academic and industrial communities. Developments and progress in this area pave the way toward novel scenarios for IoT applications. Virtualisation generates pools of (virtual) sensors and actuators, and these, in turn, form new types of on-demand IoT resources available over the cloud. These IoT resources are delivered and accessible in form of IoT as a service (IoTaaS) which require to be integrated with other cloud services (e.g., regarding computing, storage, and network). As a consequence, new types of providers are rising, which combine cloud computing solutions with IoT. We talk about IoT cloud to indicate a new type of distributed system consisting of a set of smart devices interconnected with a remote cloud infrastructure, platform, or software through the Internet able to provide IoTaaS [6].

In this scenario, it is possible to build new mash-up applications and services which can be deployed in a multiprovider ecosystem in which several cloud providers are interconnected to deliver a universal decentralized computing environment where everything is driven by constraints and agreements. However, integrating IoT devices with the cloud is not trivial at all and many research challenges are yet to be addressed.

IoT and cloud computing have become new "buzz words" in the IT world, but how to combine these concepts is not clear. In fact, according to a recent Gartner report, there will be 25 billion devices connected over the Internet by 2020. The IoT phenomenon can accelerate emerging novel application on several sectors, but it can be effective only if the device and object ecosystem are organized, interoperable, and user-friendly. The main challenge of hybrid IoT cloud systems is represented by the fact that they require interoperability, scalability, self-adaption, Quality of Service (QoS), fault-tolerance, and security.

2. Background

Sensor-cloud formation is one of the areas that receive extensive research within the field of sensor network [7]. The motivation towards sensor grouping or clustering comes from number of perspectives including data mining and fusion, network energy performance, and data routing. It might relate to the type of sensing like spatial environmental conditions and/or the geographic location. It might involve homogeneous or heterogeneous sensing. Recent research activities related to IoT architectures highlight the benefits of adopting a cloud-based model [8]. Majority of the architectural setups have distributed Wireless Sensor Networks

(WSN) clouds for sensing physical data which, in turn, are supported by a more efficient and computationally powerful overall cloud computing model. In [9], the authors proposed a cloud-based architecture in which the cloud acts as a virtual sink with multiple sink points. This datum is then stored and processed in a distributed fashion within the cloud. The authors employed the NS-2 simulator and lay more focus on the packet transmission. However, the architectural organization of the physical sensor cloud besides optimizing the cloud performance does not feature in their work. Moreover, the types of adopted Operating Systems have not been specified. The combination of IoT and WSN technologies is being extensively utilized for large scale IoT projects by industries and academic researchers [10].

Quality of Service (QoS) is a fundamental networking problem affecting both wired and wireless IoT systems. IoT WSN architectures have Service Level Agreement (SLA) requirements which differ from traditional WSN [11]. Heterogeneous IoT nodes in IP-enabled sensor networks have very different SLA requirements in terms of delay, energy consumption, and reliability. Thanks to limited buffering capabilities, queue congestion can occur leading to degradation of QoS [12]. Minimizing the energy communication/computation of the low-power sensors is a major constraint for the low battery-powered sensors [9], along with increasing throughput and reliability of the overall IoT architecture [13]. The area of QoS management and QoS attributes (energy consumption, throughput, reliability, etc.) in a complex scalable IoT WSN framework has not been properly addressed and studied and the definition of QoS for IoT architectures is still not clear [14]. Built-in QoS guarantees are essential for the network algorithms and advanced energy saving protocols in an intelligent end-to-end IoT cloud framework. High level IoT sensor network applications require application scheduling and resource provisioning to satisfy SLA requirements. In this context, it is of utmost importance to optimize scheduling performance and reduce associated resource provisioning costs [14]. An IoT-enabled architecture for interconnecting a network of heterogeneous, low-power wireless transceivers through a standard interface such as the IPv6 protocol and 6LoWPAN has served as the backbone for realizing several fully pervasive and ubiquitous large scale IoT projects [15] such as Smart Campus Testbed [16], SmartSantander EU, CitySense [17], and Smart City of the ARTEMIS JU SP3SOFIA project [18] as well as for deployment in healthcare telematics, agriculture, transportation sectors, and so forth. Such large scale IoT systems require high levels of energy efficiency and QoS requirements.

Nowadays, security is seen as one of the major factors that slows down the rapid and large scale adoption and deployment of both the IoT and cloud computing. In fact, security in IoT and cloud computing is a widely discussed topic [19, 20]. In [21], the authors investigate the security issues and challenges on the IoT-based Smart Grids (SG) and define the major security services that should be considered when dealing with SG security. A Key distribution for secure eHealth applications in IoT is fundamental to enforce security [22]. Security is fundamental for scalability, flexibility, and reliability at both data and system levels [23]. Another interesting research topic regards the unification of resilient cloud systems and secure IoT environments. In [24], the authors propose an approach to provide secure IoT services using the Datagram Transport Layer Security (DTLS) as a de facto security protocol. In particular, they examined problems that can happen when applying the DTLS protocol to the IoT, which comprises constrained devices and constrained networks. To solve the problems, they separate the DTLS protocol into a handshake phase (i.e., establishment phase) and an encryption phase (i.e., transmission phase).

3. Motivation

"The social and technical IoT phenomena possess the power to disrupt our society such as the Internet before." IoT is becoming the technological innovation driving applications that have the power to change the markets across different domains. Thousands of applications can be identified in each domain and new ones appear everyday, but inevitably they now require a strong interconnection among things. The state-of-the-art witnesses the technological and methodological issues concerning aspects such as interoperability, scalability, privacy, standardization, and legal issues. Many researchers are looking at efficient and smart ways for using IoT in the near future. The scientific research on IoT looks at devices located in the edge of the Internet. They leverage techniques of proximity and locality for working, but there are not so many works investigating the interaction of IoT devices with cloud computing systems. Cloud systems in IoT are fundamental to manage the devices connected through the Internet in a given administrative domain. This special issue includes high quality and novel contributions from researchers coming from both the academic and industrial communities who work on the integration of distributed sensor networks, cloud computing, and IoT environments. In particular, it advances the state-of-the-art in IoT cloud considering the following main aspects: (i) integration of IoT devices with the cloud, (ii) configuration of IoT devices over the cloud, (iii) communication of IoT devices over the cloud, and (iv) security of IoT devices over the cloud.

4. Advances in the State-of-the-Art

This special issue advances the state-of-the-art focusing on four macroareas that are (i) integration of IoT devices with the cloud, (ii) configuration of IoT devices over the cloud, (iii) communication of IoT devices over the cloud, and (iv) security of IoT devices over the cloud.

Regarding integration of IoT devices with the cloud, J. Augustyn et al., in "Hi-Speed USB Based Middleware for Integration of Real-Time Systems with the Cloud," discuss the integration sophisticated sensors and actuators with the cloud, by means of the use of a piece of middleware. This integration results in handling streams of data produced by sensors as well as streams sent back to actuators. In cases for which both large streams and a short reaction time are required, a special real-time oriented approach is necessary to design and build an interconnected piece of middleware. In particular, the authors propose a hybrid low-cost, low-power middleware architecture for handling and processing sensor related data streams. It is based on two microprocessor boards interconnected by high speed USB links. The system includes three embedded hardware implementations of the proposed architecture, two software realizations (single and multithread ones), and two process scheduling algorithms that have been examined to evaluate their real-time performances. A series of experiments have been performed in order to measure closed loop control times and sensor data streams achievable in practice. An outcome is presented and discussed in detail. Obtained results confirm that the proposed architecture can be applied as middleware to integrate such elements of Internet of Things as robots and similarly time-constrained systems with the cloud. The results can serve as reference point in research and development of real-time middleware solutions.

Regarding configuration of IoT devices over the cloud, A. Puliafito et al., in "Towards the Integration between IoT and Cloud Computing: An Approach for the Secure Self-Configuration of Embedded Devices," focus on selconfiguration mechanisms in IoT clouds. The secure bootup and setup of Internet of Things (IoT) devices connected over the cloud represent a challenging open issue. This paper deals with the automatic configuration of IoT devices in a secure way through the cloud, in order to provide new added-value services. After a discussion on the limits of current IoT and cloud solutions in terms of secure self-configuration, the authors present a cloud-based architecture that allows IoT devices to interact with several federated cloud providers. In particular, they present two possible scenarios, that is, single cloud and federated cloud environments, interacting with IoT devices and we address specific issues of both. Moreover, we present several design highlights on how to operate considering real open hardware and software products already available in the market.

Regarding Communication of IoT devices over the cloud, F. Van den Abeele et al., in "Integration of Heterogeneous Devices and Communication Models via the Cloud in the Constrained Internet of Things," focus on communication models in IoT Clouds. As the Internet of Things continues to expand in the coming years, the need for services that span multiple IoT application domains will continue to increase in order to realize the efficiency gains promised by the IoT. Today, however, service developers looking to add value on top of existing IoT systems are faced with very heterogeneous devices and systems. These systems implement a wide variety of network connectivity options, protocols (proprietary or standards-based), and communication methods all of which are unknown to a service developer that is new to the IoT. Even within one IoT standard, a device typically has multiple options for communicating with others. In order to alleviate service developers from these concerns, the author present a cloud-based platform for integrating heterogeneous constrained IoT devices and communication models into services. An evaluation shows that the impact of our approach on the operation of constrained devices is minimal while providing a tangible benefit in service integration of low-resource IoT devices. A proof of concept demonstrates the latter by means of a control and management dashboard for constrained devices which was implemented on top of the presented platform. The results of our work enable service developers to more easily implement and deploy services that span a wide variety of IoT application domains.

Regarding security of IoT devices over the cloud, X. Li et al., in "A Method for Trust Quantification in Cloud Computing Environments," focus on analysing the trustiness in IoT cloud environments. Cloud computing and Internet of Things (IoT) are emerging technologies that have experienced rapid development in recent years. While cloud computing presents a new platform over which services are offered to the user more conveniently, IoT facilitates the collection of a large amount of data via interconnected wireless sensors for event monitoring and control. In such environments, ownership and control over the data may lead to potential conflict between the protection of data and the provision of services. Thus, cloud security has received a great deal of attention in recent years. The authors propose a method for trust quantification based on fuzzy comprehensive evaluation theory for cloud computing to protect user data through trust quantification of cloud services; after that they introduce a trust ontology for cloud services and define user preference trust values. By enhancing the existing trust concept based on dynamic requirements, the authors introduce some cloud service attributes to study layered service representation for trust preference and then apply the fuzzy comprehensive evaluation theory to perform trust quantification. Finally, some experiments are performed to prove the effectiveness of the proposed method. M. Xiang et al., in "Avoiding the Opportunist: The Role of Simmelian Ties in Fostering the Trust in Sensor-Cloud Networks," specifically focus on studying the trustiness in Wireless Sensor-Cloud Networks (WSCNs). New concepts of trust has emerged in recent studies as an alternative mechanism to address security concerns in WSCN. Most of the studies on trust are focusing on how to model and evaluate trust so as to effectively detect any malicious activity in the network and then isolate and avoid them. In addition, WSCNs are very dynamic and flexible, thus being hard to keep a static network topology and connectivity which bring more challenges to be secured. In this paper, we have introduced the new angle of adaptive network approach to discover the interplay between network nodes trust evaluation and its underlying topology change. It has been found that the network connectivity change will also have strong impact on the trust behavior running over it. Inspired from the trust studies in sociology, the authors discuss how Simmelian tie structured networks enable more positive impact on fostering trustworthiness among wireless sensor nodes and how structural hole characterized networks provide more opportunity for misbehaviors, having a negative impact on securing the sensor-cloud networks.

Acknowledgments

We wish to thank all the researchers who submitted papers to this special issue for having shared their work with us, as well as reviewers, who made a remarkable effort in reviewing

the submissions. Without their hard and valuable work, it would not have been possible to select these special issue high quality papers within the given time bounds.

Massimo Villari
Adnan Al-Anbuky
Antonio Celesti
Klaus Moessner

References

[1] M. Giacobbe, A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "Towards energy management in cloud federation: a survey in the perspective of future sustainable and cost-saving strategies," *Computer Networks*, vol. 91, pp. 438–452, 2015.

[2] A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems," *Journal of Network and Computer Applications*, vol. 59, pp. 208–218, 2016.

[3] A. Celesti, M. Fazio, A. Romano, and M. Villari, "A hospital cloud-based archival information system for the efficient management of HL7 big data," in *Proceedings of the 39th International Convention DC VIS: Distributed Computing, Visualization and Biomedical Engineering (MIPRO '16)*, IEEE Computer Society, Opatija, Croatia, May-June 2016.

[4] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How the Dataweb can support cloud federation: service representation and secure data exchange," in *Proceedings of the 2nd Symposium on Network Cloud Computing and Applications (NCCA '12)*, pp. 73–79, December 2012.

[5] A. Celesti, M. Fazio, M. Giacobbe, A. Puliafito, and M. Villari, "Characterizing IoT cloud federation," in *Proceedings of the IEEE 30th International Conference on Advanced Information Networking and Applications Workshops—Workshop on Cloud Computing Project and Initiatives (CCPI '16)*, pp. 93–98, Le Régent Congress Centre, Switzerland, March 2016.

[6] A. Celesti, D. Mulfari, M. Fazio, M. Villari, and A. Puliafito, "Exploring container virtualization in IoT clouds," in *Proceedings of the International Conference on Smart Computing Workshops (SMARTCOMP Workshops '16)*, IEEE Computer Society, St. Louis, Mo, USA, May 2016.

[7] H. Sabit and A. Al-Anbuky, "Multivariate spatial condition mapping using subtractive fuzzy cluster means," *Sensors*, vol. 14, no. 10, pp. 18960–18981, 2014.

[8] H.-I. Wang, "Constructing the green campus within the internet of things architecture," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 804627, 8 pages, 2014.

[9] R. Piyare, S. Park, S. Y. Maeng et al., "Integrating wireless sensor network into cloud services for real-time data collection," in *Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC '13)*, pp. 752–756, IEEE, Jeju, South Korea, October 2013.

[10] R. Fantacci, T. Pecorella, R. Viti, and C. Carlini, "A network architecture solution for efficient IOT WSN backhauling: challenges and opportunities," *IEEE Wireless Communications*, vol. 21, no. 4, pp. 113–119, 2014.

[11] S. E. S. N. Azlan and A. Al-Anbuky, "Modelling the integrated qos for wireless sensor networks with heterogeneous data traffic," *Open Journal of Internet of Things*, vol. 1, no. 1, pp. 1–15, 2014.

[12] J. W. Hui and D. E. Culler, "IPv6 in low-power wireless networks," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1865–1878, 2010.

[13] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the implementation of IoT for environmental condition monitoring in homes," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3846–3853, 2013.

[14] Z. Gal and G. Terdik, "On the statistical analysis of wireless sensor vs. wired data network traffics," *Carpathian Journal of Electronic and Computer Engineering*, vol. 4, pp. 41–48, 2011.

[15] M. Nati, A. Gluhak, H. Abangar, S. Meissner, and R. Tafazolli, "A framework for resource selection in internet of things testbeds," in *Testbeds and Research Infrastructure. Development of Networks and Communities*, vol. 44, pp. 224–239, Springer, Berlin, Germany, 2012.

[16] M. Nati, A. Gluhak, H. Abangar, and W. Headley, "Smartcampus: a user-centric testbed for internet of things experimentation," in *Proceedings of the 16th International Symposium on Wireless Personal Multimedia Communications (WPMC '13)*, pp. 1–6, IEEE Press, June 2013.

[17] I. Chatzigiannakis, G. Mylonas, and A. Vitaletti, "Urban pervasive applications: challenges, scenarios and case studies," *Computer Science Review*, vol. 5, no. 1, pp. 103–118, 2011.

[18] L. Filipponi, A. Vitaletti, G. Landi, V. Memeo, G. Laura, and P. Pucci, "Smart city: an event driven architecture for monitoring public spaces with heterogeneous sensors," in *Proceedings of the 4th International Conference on Sensor Technologies and Applications (SENSORCOMM '10)*, pp. 281–286, IEEE Press, Venice, Italy, July 2010.

[19] Y. H. Hwang, "IOT security & privacy: threats and challenges," in *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security (IoTPTS '15)*, p. 1, New York, NY, USA, 2015.

[20] Z.-K. Zhang, M. C. Y. Cho, and S. Shieh, "Emerging security threats and countermeasures in IoT," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS '15)*, pp. 1–6, ACM, April 2015.

[21] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia Computer Science*, vol. 34, pp. 532–537, 2014.

[22] M. R. Abdmeziem and D. Tandjaoui, "An end-to-end secure key management protocol for e-health applications," *Computers & Electrical Engineering*, vol. 44, pp. 184–197, 2015.

[23] H. Jiang, F. Shen, S. Chen, K.-C. Li, and Y.-S. Jeong, "A secure and scalable storage system for aggregate data in IoT," *Future Generation Computer Systems*, vol. 49, pp. 133–141, 2015.

[24] M. Panwar and A. Kumar, "Security for IoT: an effective DTLS with public certificates," in *Proceedings of the 2nd International Conference on Advances in Computer Engineering and Applications (ICACEA '15)*, pp. 163–166, Ghaziabad, India, March 2015.