Editor's Note

The Internet of Things is the networks of physical devices, embedded with electronics, software, sensors, actuators and security and connectivity mechanisms that enables them to collect and exchange data. It is a very important research topic nowadays in which many scientific papers are focusing on its bases [1].

This Special Issue tries to show some of the latest researches related to IoT with special emphasis on the basic components of IoT [2], some of the major applications in which researchers and practitioners are working [3] and especially in aspects related to security, one of the main areas of research related to IoT [4], with a special emphasis on cloud-based systems [5][6]. Next, I present a summary of the works that are included in this special issue.

Some of the key elements related to IoT are smart objects, sensors and actuators. So, González et al. present a review that explains the main concepts related to such elements, which can now be present in cities, houses, cars, through almost any physical item, capable of interconnecting with others in order to create a great range of opportunities. Authors also present one object classification system.

Wireless sensor networks are other determining factor for IoT. Bahuguna et al. show a study of the key factors that impacts the design and routing techniques of such networks. This is a very important topic since networks contains nodes with sensing, processing and communication capabilities, that have energy limitations as well as other requirements like connectivity and coverage.

IoT also opens the door to an unlimited number of applications. Dhall and Solanki present a use case on the automobile industry, using IoT-based technology and analytics. The goal is to provide a way to transmit information about the current status of vehicles and based on that information, create workflows to take actions related to car maintenance (e.g., scheduling a service with the manufacturer). The underlying idea is based on the concept of connected cars used to perform predictive car maintenance.

Continuing with the same topic, the collaboration between vehicles and the road side is very important to create intelligent transportation systems [7][8]. Vehicular Ad Hoc Networks (VANET) are important to provide comfort, safety and entertainment for people in vehicles. However, in order to give stable routes and adequate performance, there is a need of proper routing protocols. Rathi and Welekar, propose a routing protocol for such networks and evaluate its performance through a simulation.

In addition to the concept of connected cars, other authors such as Solanki et al., have also addressed issues related to smart cities. They present a method to preserve energy as well as water, in urban and rural areas through IoT. An autonomous system is proposed based on Arduino that is monitored with Lab View to control and interact with all the infrastructure located at various points in a city (parks, subways and highway lighting modules).

One extremely important factor in IoT is connectivity. Now we have a very different range of devices (both taking into account the hardware and the software), that are very difficult to communicate since they use different programming languages, protocols and interfaces. On that topic, Martínez et al., propose a migration process from classic C/C++ software applications to different mobile platforms. The proposal integrates standards with Haxe, a programming language that allows writing applications that target all major mobile platforms.

Cyber-physical attack attempts in IoT-based manufacturing systems are now very common. New threats to supply chain security have arisen, allowing attackers to manipulate physical features of pieces, resulting in more manufacturing costs. Pan et al., present two taxonomies: one for classifying cyber-physical attacks against manufacturing process and another for quality control measures for counteracting these attacks. They also provide a scheme for linking emerging vulnerabilities to possible attacks and quality control measures.

Since IoT is based, among other factors, on sensors, communication networks, data and processes that send information between devices, the protection of information traveling through them become very important. Gaona-García et al., present an analysis of previous works on security aspects related to the IoT, focusing at privacy levels and control access. They also provide a list of security issues that should ideally be addressed in these type of systems built with clusters.

Also related to security aspects, IoT relies on cloud computing to integrate and allow access to shared and configurable resources through the network. However, security is one of the biggest issues related to cloud-based and distributed systems. Thus, intrusion detection systems are required. Achbarou et al. present a classification of attacks against the availability, confidentiality and integrity of cloud resources and services, providing models to identify and prevent these types of attacks.

Given its proximity, and as stated in the previous work, security is a key aspect in both IoT and cloud computing. In Talbi and Haqiq, authors present a multi-agent based cloud service brokering system with the aim of analyzing and ranking different cloud providers, making decisions to know the more secured providers and justifying the business needs of users in terms of reliability and security.

Again with the idea of intrusion attacks in the huge amount of data that is generated in the IoT and the applications that are being moved to the cloud, Toumi et al. propose a collaborative framework between a hybrid intrusion detection system that is based on mobile agents and virtual firewalls. So, they propose three different layers to create a more reliable detection system.

To finish with proposals created to improve the cloud computing security, Saidi et al., show the most used techniques to avoid Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks in the cloud (e.g., HCF and CBF filters), which aims to break down the availability of a service to its legitimate users.

Dr. Vicente García-Díaz

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[3] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wirel. Pers. Commun., vol. 58, no. 1, pp. 49–69, 2011.

[4] R. H. Weber, "Internet of Things--New security and privacy challenges," Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30, 2010.

[5] C. G. García, J. P. Espada, E. R. Núñez-Valdez, and V. García-Díaz, "Midgar: Domain-Specific Language to Generate Smart Objects for an Internet of Things Platform.," in IMIS, 2014, pp. 352–357.

[6] K. Venkateshwaran, A. Malviya, U. Dikshit, and S. Venkatesan,

DOI: 10.9781/ijimai.2017.430

"Security Framework for Agent-Based Cloud Computing.," Int. J. Interact. Multimed. Artif. Intell, vol. 3, no. 3, pp. 35–42, 2015.

[7] G. Cueva-Fernandez, J. P. Espada, V. García-Díaz, C. G. García, and N. Garcia-Fernandez, "Vitruvius: An expert system for vehicle sensor tracking and managing application generation," J. Netw. Comput. Appl., vol. 42, no. 0, pp. 178–188, 2014.

[8] G. C. Fernandez, J. P. Espada, V. G. Díaz, and M. G. Rodríguez, "Kuruma: the vehicle automatic data capture for urban computing collaborative systems," Int. J. Interact. Multimed. Artif. Intell., vol. 2, no. 2, pp. 28–32, 2013.