Smart Campus: Trends in cybersecurity and future development

Campus inteligente: Tendencias en ciberseguridad y desarrollo futuro

Brayan Sánchez-Torres[*]
Jesús Alberto Rodríguez-Rodríguez[**]
Dewar Willmer Rico-Bautista[***]
César D. Guerrero[****]

Fecha de recepción: 19 de septiembre de 2017
Fecha de aprobación: 24 de diciembre de 2017

Abstract

Smart Campus is an entity of any kind that uses technology and infrastructure to support and improve its processes, so people can use them better. This paper reviews the literature to contextualize the Internet of Things and its vital importance for the Smart Campus, as well as its relationship with the concepts of cybersecurity and wireless sensor network. We describe the various interrelationships, tendencies, and future development of a Smart Campus, as well as the differences and similarities with the emerging concept of Smart University. This review revealed that the Internet of Things is involved in all fields and can influence and improve the university's processes to contribute to decision-making, technological development, and academic learning. To conclude, Smart University focuses on improving the

[*] Universidad Francisco de Paula Santander Ocaña (Ocaña-Norte de Santander, Colombia). ORCID: 0000-0002-8579-6591. bsanchezt@ufpso.edu.co.

[**] Universidad Francisco de Paula Santander Ocaña (Ocaña-Norte de Santander, Colombia). ORCID: 0000-0002-2827-894X. jarodriguezr@ufpso.edu.co.

[***] M. Sc. Universidad Francisco de Paula Santander Ocaña (Ocaña-Norte de Santander, Colombia). ORCID: 0000-0002-1808-3874. dwricob@ufpso.edu.co.

[****] Ph.D. Universidad Autónoma de Bucaramanga (Bucaramanga-Santander, Colombia). ORCID: 0000-0002-3286-6226. cguerrer@unab.edu.co.

infrastructure of universities through technology, with the main purpose of enhancing the quality of the education provided by institutions.

Keywords: communication system security; Internet of things; security data; smart campus; wireless communication.

Resumen

Un Smart Campus es una entidad de cualquier tipo que utiliza la tecnología para apoyar su infraestructura y sus procesos, con el fin mejorarlos para el uso de las personas. El propósito de este trabajo es presentar una revisión de literatura, en donde se contextualiza el *internet de las cosas* y su vital importancia para el Smart Campus y su relación con los conceptos de ciberseguridad y red inalámbrica de sensores. Se presentan las diferentes interrelaciones, tendencias y desarrollo futuro del Smart Campus, así como las diferencias y similitudes con el concepto emergente de Smart University. Esta revisión reveló que el *Internet de las cosas* se involucra en todos los campos y puede influir en los procesos de una universidad para mejorarlos, ayudar en la toma de decisiones y apoyar el aprendizaje académico y el desarrollo tecnológico. Se concluye que Smart University no se queda en mejorar la infraestructura de las universidades a través de la tecnología, pues su fin principal es mejorar la calidad de la educación impartida por las instituciones.

Palabras clave: campus inteligente; comunicación inalámbrica; Internet de las cosas; seguridad de los datos; seguridad del sistema de comunicación.

Como citar este artículo:
B. Sánchez-Torres, J. A. Rodríguez-Rodríguez, D. W. Rico-Bautista, and C. D. Guerrero, "Smart Campus: Trends in cybersecurity and future development," *Rev. Fac. Ing.*, vol. 27 (47), pp. XX-XX, Jan. 2017.

I. INTRODUCTION

Technology has generated main changes in society, like IoT (Internet of Things) is doing it nowadays. Technology enables objects to connect and thus offers control and better performance of things. IoT embraces everything, therefore, generates subfields of this concept. This article addresses the main IoT subfields and their applicability to generate future revolutions, as well as the use of IoT to improve the university’s processes and overall education. The main objective of this article is to explain the applicability of IoT to develop Smart Campus and its influence on security, using as a referent the Universidad Francisco de Paula Santander Ocaña (UFPSO) located in the department of Norte de Santander, Colombia.

The Internet of Things (IoT) is a complex network that connects millions of devices and people with multiple services and objectives, through multi-technology, multi-protocols, and multi-platforms [1, 2]. The main vision of IoT is an intelligent world where the real, digital, and virtual converge to help all areas of daily life [3, 4]. Society is full of changes and IoT might have an important role in future changes, but IoT will only be applicable when it becomes a much more developed, robust, resistant, safe, and easy to understand concept [5, 6].

Understanding internet’s governance as the development and application by governments [7], the private sector, and the civil society could argue whether this governance applies to IoT. However, it seems evident that the governance of IoT should be discussed along with the general Internet. Several IoT problems, such as security, interoperability standards, and protocols can be solved by implementing governance mechanisms, like occurs for the Internet in general [8].

Applications developed under the IoT umbrella are more convenient to people, but if the security of the information is not guaranteed, problems would arise. In addition, IoT not only stores information, but also connects users between platforms, allowing an attacker to collect personal information from people and devices [9, 10]. For instance, an IoT system was implemented to treat diabetes, which impacts directly the patient's daily welfare; because the system handles the patient's information, the network security is critical from a personal security perspective [11].

This article is divided into three main sections: (i) the methodology used to select articles, magazines, books, and literary reviews; (ii) the literary review that analyzes the selected papers; and (iii) the conclusions based on the Smart Campus.

II. METHODOLOGY

For this study, we used a descriptive methodology, beginning with a general database search on the subject by using the keyword "IoT". Afterwards, we combined the main keyword with others to reduce the number of articles linked to our field of interest. [12]

We used the ACM, Scopus, and ScienceDirect databases because they are among the most relevant resources the UFPSO can access. We considered articles, literature reviews, lectures, and books when selecting the documents to be analyzed. The search and selection process were determined by the following considerations:

- The main search keywords were Internet of Things (IoT), sensor networks (WSN), cybersecurity, and Smart Campus [13-15].
- We limited the search to articles, journals, and reviews, among others, published since 2013 to analyze the most recent developments and research about this topic.
- We limited the research to the areas of computer science, energy, and engineering.
- Constraints related to authors or research journals were no taken into consideration to access more topics and concepts.

III. LITERATURE REVIEW

IoT must have a security chain in the connections and in the privacy of the assets, which can be solved if it has security policies, restart mechanisms, secure software, and bug reporting systems, as well as methods to discover and reshape vulnerabilities [16, 17]. The four main IoT connectivity models are (i) device-to-device, (ii) device to the cloud, (iii) device to gateway, and (iv) data exchange through back-end. These models give IoT flexibility in connecting their devices [18].

The company BITAG suggests considering issues such as encryption, software update, and system validation against vulnerabilities when developing IoT, in addition to follow the best practices for security and encryption. Regarding the specific IoT system, it should have backup measures or continue working in case connection problems and power failures arise [16].

the necessary requirements to offer quality IoT systems are (i) heterogeneity, which refers to the management of various devices, systems, and services, (ii) scalability to adapt to changes without losing the quality of the system, (iii) minimization of costs to apply economic but highly functional systems, (iv) flexibility to integrate new devices and reprogramming, (v) quality of service (QoS) that the system must offer to its stakeholders, and (vi) secure environment that offers robust communications, authentication, encryption, privacy, and confidential transfer [19].

One of the most relevant technologies applied to IoT is the Internet protocol ipv6, which is one of the bases for its proper functioning. Since the ipv6 has a greater number of addresses, it can deal with all the devices expected to connect [20]. Based on the IPV, the 6LowPAN is created, which is a standard that uses ipv6 to allow sensor networks to communicate with other IP devices [21, 22].

A. IoT evolution

IoT is a technology that advances at a rapid pace based on the automation of tasks; for this reason, analyzing the design principles for cloud environments is necessary, as well as taking advantage of known technologies such as sensors and standards, like W3C semantic sensor network ontology, a service provision scenario that can generate smart campuses [23, 24].

B. Wireless sensor networks

Wireless sensor networks (WSN) are composed by sensor nodes distributed to collect information. The constant flow of data handled in the wireless environment makes the system vulnerable to attacks at different levels; therefore, Suspect Detection Systems (SDS) are important for data protection [25-27]. One of the main disadvantages of the networks of nodes or sensors is the elevated energy consumption; an easy way to save energy is to make the devices to interact with the connection through rules or protocols, minimizing the connection time, and allowing the connection only for delivering urgent data [28, 29]. Projects focused on connections between sensor networks have proposed the use of dynamic keys as a solution to offer more security when people log into devices that belong to the IoT system [30, 31].

Sensor networks must have a QoS that supports and offers a reliable system. QoS is the ability to guarantee that the required service for the network is supported; although it can also be seen as the ability of the network to customize the treatment of specific classes of data. The characteristics that a network must meet to offer QoS to a network of sensors are priority, periodicity, term, availability, reliability, confidentiality, security, latency, variation, and recovery of failures [32, 33].

C. Cloud computing and big data

IoT collects a large amount of information from the sensors and handles the information that must be stored. According to the amount of compiled information, some researchers argue that a new family of data mining algorithms is necessary to help with the decision-making [34, 35]. The cloud service storage model is one of the most accepted for working with big data through the web and networks. However, many cloud users are worried about the access that cloud operators have to their high sensitive data. For problems like this, cryptography with the Security-Aware Efficient Distributed Storage system, designed to obtain an efficient massive distributed storage service and high-level security protection, has been proposed to encrypt all the data and distribute it across the different servers in the cloud without causing large overhead and latency [36, 37].

IoT aims to transform and improve the quality of health service by optimizing medical care, reducing costs, and providing good and fast care in urgency cases; this is achieved by cloud computing, taking advantage of wireless broadband coverage and the wide use of smartphones that allow monitoring and diagnosing the patient remotely [38]. IoT processes aligned to the cloud generally work with a layer of cloud processing, which hosts a multi-agent architecture, a database, and an ontology used by agents to increase the general reliability and interoperability characteristics of cyber-physical systems, and a web server that allows any device with Internet connectivity to access stored data [39, 40].

D. IoT in data security

With the increasing number of devices connected to the internet, the chances of finding vulnerabilities increase, so the target of cybercriminals will be IoT devices. Due to a poor design, IoT devices may present vulnerabilities that expose the user’s data leaving the information unprotected. The main issue is that people are becoming more dependent on IoT systems for many services. Therefore, these devices should be more secure [18, 41, 42].

The major security problems of IoT focus on insecurities: (i) unsafe networks, because they are generally open, allowing intruders to access through the device´s MAC address, perform “Man in the Middle” or “Deny of Service” attacks, (ii) authentication practices, because the hardware used in IoT often has limited capacities, which generates insecurity in connections, authentications, and dissemination of information [43].

Security solutions have already been considered as frameworks that focus on security and privacy designed from other models, those models are adapted to work on IoT [44, 45]. Below, we list several proposed solutions on security of IoT systems:

- Diverse ways to fortify security as a model of differential game that determines the optimal amount of network resources to invest in the security of the system. This proposal considered the vulnerability of the information as the main variable of the model [46].
- Solutions based on the study of anomalies to prevent attacks to the IoT system. These solutions work from a neural network that takes various data sets as input parameters, covering both valid and invalid cases, to detect any anomalous behavior and prevent its propagation. Furthermore, this solution acts as a health monitoring system for the IoT sensor nodes, analyzing the transmitted data and sending it to a base station, which in case of failure, the valid sensor node can stop functioning and transmit invalid data to a base station [47].
- One of the solutions designed for information security in IoT systems is the proxy, which controls the traffic generated by the devices in the network. The proxies proposed for this type of IoT systems use an algorithm that allows them to have their messages encrypted, delivering the data without knowing the recipient, thus offering one more level of security to the system. [48].

- The cloud has also been used for teaching cybersecurity, allowing teacher and student to use resources more appropriately, and providing controlled and safe environments by enabling instructors to monitor [49, 50]. These types of cloud use can favor the development of Smart University; in addition, they have been used to develop systems in virtual environments that help learning and decision-making for developments focused on IoT [51].
- The chip AWS-ECC508 was designed to make devices safer at least for developers who use Amazon's IoT cloud, and to offer end-to-end security between the IoT device and the cloud infrastructure; the device uses Amazon's authentication system [52].

E. Impact of IoT on energy consumption

IoT can contribute to the field of energy management, which is where companies and natural persons usually have the highest operating expenses. However, the regulation of energy use is linked to social responsibility of green areas, regulatory requirements, and financial results. In particular, IoT is great meeting these needs, with developments such as BMS that are centralized systems that monitor, control and record construction services systems, such as mechanical systems, elevators, electrical systems, HVACs, lighting, plumbing, security/surveillance, and contingency alarms. It is noteworthy that larger facilities can achieve greater relative efficiency gains, based on the idea that more wasted energy encourages more saving possibilities [53, 54].

IoT revolutionized the energy sector, managing electrical networks with devices that transfer secondary workloads to low hours; where tariffs are lower, it is possible to save up to 20%, and to manage micro networks by using online devices [55]. Managing energy through IoT allows thinking in terms of providing accurate information about the CO_2 emissions resulted from the production processes. The energy awareness questions are grouped into three levels: conscious energy at the operation level, conscious energy at the product level, and conscious energy at the order level, which if treated with IoT can reduce the energy costs, and the CO_2 emitted throughout the production [56].

F. Smart Campus and University

The Smart Campus, a concept that arose since the emergence of the new IoT fields, is an entity of any kind that uses technology and infrastructure to support and improve its processes, so people can use them better. The Smart University concept derived from the Smart Campus concept [57], and refers to the integration of computing in the cloud and the IoT, providing smart campuses that help managing, teaching, and researching in universities [58, 59].

The main advantages of Smart University are (i) to know the traffic of people in relation to the university, (ii) to control the academic flow (classrooms, class hours, and faculties, among others), (iii) to analyze risks and decision making through statistics, (iv) to systematize all processes, and (v) to reduce energy consumption [60]. For example, Wang [61] proposed to construct green campus with IoT concepts, developing an architecture to manage the application systems that provide data to computer labs to facilitate the decision-making process, and thus reduce the energy consumption. Other examples are the project focused on developing architecture for an intelligent library based on RFID technology that protects and standardizes the selection of books in Donghua University [62], and Smart Uji that unifies all the information of the Jaume I University in Castellón, Spain, which is a Smart Campus focused on locating areas of interest and consulting useful information, through maps on responsive web pages; this Smart Campus serves as a foundation for implementing new functionalities in the university [63].

IoT is involved in everything and influence the processes in a university, helping to improve them regarding the decision-making, technological development, and support in academic learning.

IV. Discussion

Among the IoT fields, it is important to highlight the difference between Smart Campus and Smart University. According to their future projection, they might be fairly the same, but they have different approaches: Smart Universities focus on applications to improve infrastructure and the provision of academic services, whereas Smart Campus is applied by entities outside education with economic purposes.

Many literature reviews consider that security is the weakest point of IoT, due to the standardization issues and to the fact that the technologies intended to solve IoT problems do not offer enough security for the information that may pass through the IoT system. However, solutions for each IoT problem are starting to arise, as we have expressed in this article. The next step is to implement and improve these possible solutions.

Currently, encryption is proposed to solve the issues of information transmission through radio frequency; however, other potential solutions come with specific hardware, such as the AWS-ECC508 chip; the implementation of this solution will begin in the near future. Surely, in the future there will be web development frameworks that support IoT-based systems, specific frameworks for statistics, and information presentation, among other features that manage IoT systems; artificial intelligence will also help the treatment and decision-making of the data that IoT handles.

V. CONCLUSIONS

Universities should pay attention to the following fast-growing IoT fields for developments in the IoT and Smart University: (i) health, (ii) industrial processes, (iii) agriculture, (iv) mobility, (v) safety, and (vi) smart homes.

The Smart University generation focuses on improving the university infrastructure through technology, aiming at improving the quality of education provided by the institutions.

The solutions given to safely develop IoT must be standardized because the independent realization of frameworks and methodologies can present a problem to focus security solutions.

ACKNOWLEDGMENTS

The authors thank the Universidad Francisco de Paula Santander Ocaña (UFPSO), in particular, the Division of Research and Extension (DIE) for the support developing this research. The authors would like to acknowledge the cooperation of the Center of Excellence and Appropriation on Internet of Things under project ID: FP44842-502-2015, supported by the Colombian Ministry of Information and Communication Technologies and the Colombian Agency of Science, Technology and Innovation.

AUTHORS' CONTRIBUTIONS

Sánchez-Torres and Rodríguez-Rodríguez conducted the search, the recompilation and the analysis of the papers referenced in this article, and contributed to write the manuscript. Rico-Bautista and Guerrero helped writing the manuscript and reviewed it. All authors read and approved the final manuscript.

REFERENCES

[1] Y. Medina-Cárdenas, and D. Rico-Bautista, "Modelo de gestión de servicios para la universidad de pamplona: ITIL," *Scientia et technica*, vol. 2 (39), pp. 314-319, 2008.

[2] Y. Medina-Cárdenas, D. Rico-Bautista, and Y. Areniz, Modelo estratégico para la gestión tecnológica en la organización: plan táctico de la calidad (ITIL & ISO 20000), I. T. Metropolitano, Ed., Medellín: Fondo Editorial ITM, 2016, p. 90. DOI: http://doi.org/10.22430/9789585414006.

[3] A. Liñán Colina, A. Vives, A. Bagula, M. Zennaro, and E. Pietrosemoli, Internet de las cosas, W. S. Science, Ed., 2015.

[4] C. Restrepo, O. Salcedo-Parra, and J. Sánchez-Céspedes, "Traffic model for the interconnection of networks and operators using MPLS-TE," *Revista Facultad de Ingeniería*, vol. 26 (44), pp. 87-96, 2017. DOI: http://doi.org/10.19053/01211129.v26.n44.2017.5774.

[5] L. Atzori, A. Lera, and G. Morabito, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Networks*, vol. 56, pp. 122-140, Mar. 2017. DOI: http://doi.org/10.1016/j.adhoc.2016.12.004.

[6] A. Tejero López, "Seguridad en el Internet de las cosas," Master Thesis, Universidad Politécnica de Madrid, 2014.

[7] L. Rueda, and D. Rico-Bautista, "Modelamiento inicial de ciudades de países en vía de desarrollo, utilizando dinámica de sistemas," *Scientia et technica*, vol. 1 (34), pp. 421-426, 2007.

[8] V. Almeida, D. Doneda, and M. Montero, "Governance Challenges for the Internet of Things," *IEEE Internet Computing*, vol. 19 (4), pp. 56-59, Jul. 2015. DOI: http://doi.org/10.1109/MIC.2015.86.

[9] Q. Jing, A. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20 (8), pp. 2481-2501, Nov. 2014. DOI: http://doi.org/10.1007/s11276-014-0761-7.

[10] K. Kobara, "Cyber physical security for Industrial Control Systems and IoT," IEICE Transactions on Information and Systems, vol. E99.D (4), pp. 787-795, 2016. DOI: http://doi.org/10.1587/transinf.2015ICI0001.

[11] S. Thiel, J. Mitchell, and J. Williams, "Coordination or Collision? the Intersection of Diabetes Care, Cybersecurity, and Cloud-Based Computing," *Journal of Diabetes Science and Technology*, vol. 11 (2), pp. 195-197, Mar. 2017. DOI: http://doi.org/10.1177/1932296816676189.

[12] M. Callejas-Cuervo, L. Martínez-Tejada, and A. Alarcón-Aldana, "Emotion recognition techniques using physiological signals and video games –Systematic review–," *Revista Facultad de Ingeniería*, vol. 26 (46), pp. 19-28, 2017. DOI: http://doi.org/10.19053/01211129.v26.n46.2017.7310.

[13] P. Alves, S. da Silva Santos, and J. Abreu de Faria, "Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime," *Sociologia: Revista da Faculdade de Letras da Universidade do Porto*, vol. 23, pp. 95-113, 2017.

[14] M. Sastoque-Caro, G. Puerto-Leguizamón, and C. Suárez-Fajardo, «Oportunidades para la implementación de radio definida por software en redes de sensores," *Revista Facultad de Ingeniería*, vol. 26 (45), pp. 137-148, 2017. DOI: http://doi.org/10.19053/01211129.v26.n45.2017.6422.

[15] P. Alves, S. da Silva, and J. de Faria, "Clusters de Percepções sobre cibersegurança e cibercriminalidade em Portugal e as suas implicações para a implementação de políticas públicas nesse domínio," *Revista da FAE*, vol. 19 (2), pp. 22-37, 2016.

[16] BITAG, Internet of Things (IoT) Security and Privacy Recommendations, Broadband Internet Technical Advisory Group Technical Working Group Report, BITAG, 2016.

[17] H. Ning, H. Liu, and L. T. Yang, “Cyberentity Security in the Internet of Things,” *Computer*, vol. 46 (4), pp. 46-53, Apr. 2013. DOI: http://doi.org/10.1109/MC.2013.74.

[18] K. Rose, S. Eldridge, and L. Chapin, La internet de las cosas—una breve reseña, I. Society, Ed., 2015.

[19] E. Borgia, “The Internet of Things vision: Key features, applications and open issues,” *Computer Communications*, vol. 54, pp. 1-31, Dec. 2014. DOI: http://doi.org/10.1016/j.comcom.2014.09.008.

[20] J. Lobo, and D. Rico-Bautista, “Implementación de la seguridad del protocolo de internet Versión 6,” *Revista GTI*, vol. 11 (29), pp. 35 - 46, 2012.

[21] I. Robles, and A. Acosta, “IPv6 y el Internet de las Cosas (IoT),” in *Cisco Support Community Expert Series Webcast*, 2016.

[22] L.-O. Vargas, G. Romaniello, M. Vučinić, M. Favre, A. Banciu, R. Guizzetti, C. Planat, P. Urard, M. Heusse, F. Rousseau, O. Alphand, É. Dublé, and A. Duda, “GreenNet: An Energy-Harvesting IP-Enabled Wireless Sensor Network,” *IEEE Internet of Things Journal*, vol. 2 (5), pp. 412 - 426, 2015. DOI: http://doi.org/10.1109/JIOT.2015.2425431.

[23] J. Soldatos, and N. Kefalakis, “Design principles for utility-driven services and cloud-based computing modelling for the Internet of Things,” *International Journal of Web and Grid Services*, vol. 10 (2-3), pp. 139-167, 2014. DOI: http://doi.org/10.1504/IJWGS.2014.060254.

[24] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen Porisini, “Security, privacy and trust in the Internet of Things: The road ahead,” *Computer Networks*, vol. 76, pp. 146-164, Jun. 2015. DOI: http://doi.org/10.1016/j.comnet.2014.11.008.

[25] N. A. Alrajeh, S. Khan, and B. Shams, “Intrusion Detection Systems in Wireless Sensor Networks: A Review,” *International Journal of Distributed Sensor Networks*, vol. 9 (5), pp. 1-7, May. 2013. DOI: http://doi.org/10.1155/2013/167575.

[26] T. Cao Minh, A self-organizing management platform for wireless sensor networks, Universitat Pompeu Fabra, 2014.

[27] N. Cong Luong, D. Thai Hoang, P. Wang, D. Niyato, D. In Kim, and Z. Han, “Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 18 (4), pp. 2546 - 2590, 2016. DOI: http://doi.org/10.1109/COMST.2016.2582841.

[28] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT Urban Scenarios,” *IEEE Sensors Journal*, vol. 13 (10), pp. 3558-3567, Oct. 2013. DOI: http://doi.org/10.1109/JSEN.2013.2272099.

[29] M. Barceló Lladó, Wireless Sensor Networks in the Future Internet of Things: Density, Mobility, Heterogeneity and Integration, Universitat Autònoma de Barcelona, 2015.

[30] C. C. Chang, W. Y. Hsueh, and T. F. Cheng, “A Dynamic User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks,” *Wireless Personal Communications*, vol. 89 (2), pp. 447-465, Jul. 2016. DOI: http://doi.org/10.1007/s11277-016-3281-1.

[31] F. Ishmanov, and Y. Bin Zikria, “Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues,” *Journal of Sensors*, vol. 2017, Article ID 4724852, Feb. 2017. DOI: http://doi.org/10.1155/2017/4724852.

[32] J. Hing Fong Chen Gallardo, Un middleware fiable para el desarrollo de aplicaciones sobre redes inalámbricas de sensores y actores, Universidad de Málaga, 2014.

[33] M. Guizani, D. He, K. Ren, J. Rodrigues, S. Chan, and Y. Zhang, “Security and privacy in emerging networks: Part 1,” *IEEE Communications Magazine*, vol. 53 (4), pp. 18-19, 2015. DOI: http://doi.org/10.1109/MCOM.2015.7081098.

[34] F. Alama, R. Mehmoodb, I. Katiba, and A. Albeshria, “Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT),” *Procedia Computer Science*, vol. 98, pp. 437-442, 2016. DOI: http://doi.org/10.1016/j.procs.2016.09.068.

[35] T. Tsai, S. Huang, and Y. Tseng, “SIBSC: Separable Identity-Based Signcryption for Resource-Constrained Devices,” *Informatica (Netherlands)*, vol. 28 (1), pp. 193-214, 2017. DOI: http://doi.org/10.15388/Informatica.2017.126.

[36] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, “Intelligent cryptography approach for secure distributed big data storage in cloud computing,” *Information Sciences*, vol. 387, pp. 103-115, 2017. DOI: http://doi.org/10.1016/j.ins.2016.09.005.

[37] I. Weber, S. Nepal, and L. Zhu, “Developing Dependable and Secure Cloud Applications,” *IEEE Internet Computing*, vol. 20 (3), pp. 74-79, 2016. DOI: http://doi.org/10.1109/MIC.2016.67.

[38] M. A. AL-Zoube, and Y. Alqudah, “Mobile Cloud Computing Framework For Patients' Health Data Analysis,” *Biomedical Engineering - Applications, Basis and Communications*, vol. 26 (2), Article ID 1450020, 2014. DOI: http://doi.org/10.4015/S1016237214500203.

[39] T. Sanislav, S. Zeadally, and G. D. Mois, “A Cloud-Integrated, Multilayered, Agent-Based Cyber-Physical System Architecture,” *Computer*, vol. 50 (4), pp. 27-37, 2017. DOI: http://doi.org/10.1109/MC.2017.113.

[40] F. Wu, L. Xu, S. Kumari, and X. Li, “A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 8 (1), pp. 101-116, Feb. 2017. DOI: http://doi.org/10.1007/s12652-016-0345-8.

[41] Q. M. Ashraf, and M. H. Habaebi, “Autonomic schemes for threat mitigation in Internet of Things,” *Journal of Network and Computer Applications*, vol. 49, pp. 112-127, 2015. DOI: http://doi.org/10.1016/j.jnca.2014.11.011.

[42] F. Luo, J. Zhao, Z. Y. Dong, Y. Chen, Y. Xu, X. Zhang, and P. K. Wong, “Cloud-Based Information Infrastructure for Next-Generation Power Grid: Conception, Architecture, and Applications,” *IEEE Transactions on Smart Grid*, vol. 7 (4), pp. 1896 - 1912, 2016. DOI: http://doi.org/10.1109/TSG.2015.2452293.

[43] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, “Learning Internet-of-Things Security "Hands-On",” *IEEE Security and Privacy*, vol. 14 (6), pp. 37-46, Nov. 2016. DOI: http://doi.org/10.1109/MSP.2016.118.

[44] J. L. Hernández Ramos, Development of a security and privacy framework for the internet of things, Universidad de Murcia, 2016.

[45] G. Yongan, Z. Hongbo, and Y. Longxian, “Smart Service System(SSS): A Novel Architecture Enabling Coordination of Heterogeneous Networking Technologies and Devices for Internet of Things,” *China Communications*, vol. 14 (3), pp. 130-144, Mar. 2017. DOI: http://doi.org/10.1109/CC.2017.7897329.

[46] Y. Ding, X. W. Zhou, Z. M. Cheng, and F. H. Ling, “A Security Differential Game Model for Sensor Networks in Context of the Internet of Things,” *Wireless Personal Communications*, vol. 72 (1), pp. 375-388, Sep. 2013. DOI: http://doi.org/10.1007/s11277-013-1018-y.

[47] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, “Intelligent Intrusion Detection in Low-Power IoTs,” *ACM Transactions on Internet Technology*, vol. 16 (4), Art. 27, Dec. 2016. DOI: http://doi.org/10.1145/2990499.

[48] D. Díaz-Sánchez, R. S. Sherratt, P. Arias, F. Almenárez Mendoza, and A. Marín, “Secure store and forward proxy for dynamic IoT applications over M2M networks,” *IEEE Transactions on Consumer Electronics*, vol. 62 (4), pp. 389-397, Nov. 2016. DOI: http://doi.org/10.1109/TCE.2016.7838091.

[49] K. Salah, M. Hammoud, and S. Zeadally, “Teaching Cybersecurity Using the Cloud,” *IEEE Transactions on Learning Technologies*, vol. 8 (4), pp. 383 - 392, Oct. 2015. DOI: http://doi.org/10.1109/TLT.2015.2424692.

[50] M. Coccoli, P. Maresca, L. Stanganelli, and A. Guercio, “An experience of collaboration using a PaaS for the smarter university model,” *Journal of Visual Languages and Computing*, vol. 31, pp. 275-282, 2015. DOI: http://doi.org/10.1016/j.jvlc.2015.10.014.

[51] A. Furfaro, L. Argento, A. Parise, and A. Piccolo, “Using virtual environments for the assessment of cybersecurity issues in IoT scenarios,” *Simulation Modelling Practice and Theory*, vol. 73, pp. 43-54, 2017. DOI: http://doi.org/10.1016/j.simpat.2016.09.007.

[52] S. Cass, “A chip to protect the internet of things [Resources_Beyond the datasheet],” *IEEE Spectrum*, vol. 54 (1), pp. 20-21, 2017. DOI: http://doi.org/10.1109/MSPEC.2017.7802735.

[53] D. Minoli, K. Sohraby, and B. Occhiogrosso, “IoT Considerations, Requirements, and Architectures for Smart Buildings-Energy Optimization and Next-Generation Building Management Systems,” *IEEE Internet of Things Journal*, vol. 4 (1), pp. 269-283, 2017. DOI: http://doi.org/10.1109/JIOT.2017.2647881.

[54] Y. Simmhan, S. Aman, A. Kumbhare, R. Liu, S. Stevens, Q. Zhou, and V. Prasanna, “Cloud-Based Software Platform for Big Data Analytics in Smart Grids,” *Computing in Science and Engineering*, vol. 15 (4), pp. 38-47, 2013. DOI: http://doi.org/10.1109/MCSE.2013.39.

[55] Bankinter, Internet de las cosas en un mundo conectado de objetos, Bakinter, Ed., 2011.

[56] F. Shrouf, Utilizing the Internet of Things to promote energy awareness and efficiency at discrete production processes: Practices and methodology, E.T.S.I. Industriales (UPM), 2015.

[57] D. Rico-Bautista, J. Parra-Valencia, and C. D. Guerrero, “IOT: Una aproximación desde ciudad inteligente a universidad inteligente,” *Revista Ingenio UFPSO*, vol. 13 (1), pp. 9-20, 2017.

[58] X. Nie, “Constructing Smart Campus Based on the cloud computing and the internet of things,” in *2nd International Conference on Computer Science and Electronics Engineering*, 2013. DOI: http://doi.org/10.2991/iccsee.2013.395.

[59] T. Marcos Alves, C. André da Costa, R. da Rosa Righi, and J. L. Victória Barbosa, “Exploring the Social Internet of Things concept in a Univeristy Campus using NFC,” in *41st Latin American Computing Conference*, 2015.

[60] M. Cata, “Smart university, a new concept in the internet of things,” in *14th RoEduNet International Conference - Networking in Education and Research*, 2015. DOI: http://doi.org/10.1109/RoEduNet.2015.7311993.

[61] H.-I. Wang, “Constructing the green campus within the internet of things architecture,” *International Journal of Distributed Sensor Networks*, vol. 10 (3), pp. 1-8, Mar. 2014. DOI: http://doi.org/10.1155/2014/804627.

[62] Y. Luo, J. Cao, and J. Qian, “Exploration and construction of smart library based on RFID technology,” *Advanced Materials Research*, vol. 765-767, pp. 1743-1746, Sep. 2013. DOI: http://doi.org/10.4028/www.scientific.net/AMR.765-767.1743.

[63] M. Benedito-Bordonau, D. Gargallo, J. Avariento, A. Sanchis, M. Gould, and J. Huerta, UJI Smart Campus, Centro Nacional de Información Geográfica, 2013.