Analysis of Security Mechanisms Based on Clusters IoT Environments

Paulo Gaona-García[1], Carlos Montenegro-Marin[1], Juan David Prieto[2], Yuri Vanessa Nieto[3]

[1]*Universidad Distrital Francisco José de Caldas*
[2]*Fundación San Mateo*
[3]*Corporación Unificada Nacional de Educación Superior, Bogotá – Colombia,*

***Abstract* — Internet of things is based on sensors, communication networks and intelligence that manages the entire process and the generated data. Sensors are the senses of systems, because of this, they can be used in large quantities. Sensors must have low power consumption and cost, small size and great flexibility for its use in all circumstances. Therefore, the security of these network devices, data sensors and other devices, is a major concern as it grows rapidly in terms of nodes interconnected via sensor data. This paper presents an analysis from a systematic review point of view of articles on Internet of Things (IoT), security aspects specifically at privacy level and control access in this type of environment. Finally, it presents an analysis of security issues that must be addressed, from different clusters and identified areas within the fields of application of this technology.**

***Keywords* — Internet of Things, Network Security, Information Security, Privacy of Data, Secure Connections.**

I. Introduction

Internet of things (IoT) is considered as an integrated part of Internet, also defined as a global network infrastructure and dynamic composed of a large number of objects, able to communicate and interact with each other, with end users [1][2][3]. These objects must have unique identities which allow interactivity.

Due to the accelerated enhanced of devices connected to Internet, and the need to create networks that interact with them, privacy and data protection is substantial [4]. Therefore, the information security is an actual well known aspect, due to devices connected to internet is growing rapidly, which represents an exposure increase on data at the network.

This paper proposes a security infrastructure to neutralize vulnerabilities at IoT, using mechanisms such as (PKI) that allow identity authentication based on a combined public key, giving solution to the excessive amount of authentications. In this issue it is found a solution given by [5] performing an analysis of fingerprint recognition, they proposed a 3-layer model (sensor, transport, application), enabling the analysis of each of the components involved in the process. Another security problem is related to the communication media, this problem is addressed in [4], in this project authors using RFID systems and incorporate a microchip combined memory, create a system which allows to receive a signal and return it with some additional data (unique serial number).

This study is intended to present an overview of challenges presents in IOT security levels. Thus, it is presented the state of the art related to safety in environments Internet of things, specifically about security mechanisms involved in it and on the other hand, present an analysis of factors involved in performance application and security, and identify security methods that allow be implemented in IOT environments. In order to achieve this purpose, we will introduce classification as a proposal to identify which aspects should be considered for raising safety issues under the principles of authentication, access control and authenticity. For this model, it is important to characterize the type of RFID devices, work settings, connection types and security mechanisms that could be applied for the purpose in order to facilitate the acquisition of devices to be used in different work environments such as industrial level, SmartGrid or home.

This paper is organized as follows. In Section 2, we presents the theoretical framework, problems identified in the area of security and related work. Section 3 describes the methodology for the literature review and analysis of our study is presented. Section 4 a proposed security model according to areas of interest to today worked in IoT is presented. The final section conclusions and future work is presented.

II. Background

A. Review Stage

Recently, Internet of Things (IOT), has become a trend at homes given the evolution and mass communications through the network, which facilitates the exchange of goods and services globally [6]. In accordance with [7] monitoring households through security cameras, motion detectors and other various sensors which are connected to the Internet allow to handle them easily, and the flow of valuable information for the user. These factors creates tranquility, for example, being able to monitor home from anywhere in the world having a smartphone connected to Internet. Nevertheless, in accordance with a study handle by [8] these constant monitoring levels are exposed to confident levels to analyze the risks, for example, the network points and transmission thereof. The authors finally conclude the need to review the processes of encryption and authentication of this. That means, now the user is not the only one who can see and monitor his home, but this would be a relatively easy task for an intruder, exposing and becoming the privacy and security of a house vulnerable.

Some of the most popular devices are leading the expansion of IoT are called wearables; They are small devices that can be wear by a person and can capture information from certain activities carried out. They can also provide other information to the user such as time, weather or even notifications received on the same or on a mobile phone linked. In addition to synchronize activity with other devices or social networks, they are able to receive mail, messages, and even calls, so in most cases the information is stored in the cloud.

IoT links computer systems to the real world through physical objects, which allow having real-time information [7]. This means that a lot of information should travel safely from objects (sensors, actuators, RFID tags, etc.), to the data center and from there to devices such as PC or smartphone, from they can make decisions based on the information it reaches. It is the development of IOT which brings new challenges in security aspects.

DOI: 10.9781/ijimai.2017.438

B. Related work

The rapid development of information technology and Internet security information about IoT, I a new problems and potential security over information has been rise. Therefore, it becomes a focus aspect to build a safety and reliability system in the IoT context. Form this problem, it has been worked in a general architecture of trust [9] this architecture mainly includes a trust module (users being the central part of the system) perception of trust module (full authentication) terminal confidence module (operate according to rules of control), trusted network module (designed to analyze, evaluate and manage security situations) and a trusted agent module (avoid the potential risks caused by access terminals do not reliable). According to the results of these modules development, was a development model to address security issues, but does not provide a specific solution to the security problem.

As the communications infrastructure of the Internet evolves to include detectable objects, appropriate mechanisms will be needed to ensure communications with these devices in the work done by [10] in the context of future applications of IoT, in areas as diverse as health (eg, remote patient monitoring or control of the elderly) and smart cities (eg distributed pollution monitoring, intelligent lighting systems), among many others. This trend is also reflected in the efforts carried out by normative agencies such as the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF), to design communication technologies and safety the IOT.

C. Identify security problems

The atmosphere of Internet of things can be summed up as a virtual representation in the network of physical objects. Data interception is real and possible, this can be proof thanks to studies that have managed to activate windshield wipers and brakes of cars only through text messages [11], handling electronic devices of the vehicle [12], tracking the vehicle navigation system [13], annulment of the navigation system of a luxury yacht running aground in the middle of the Mediterranean [14] sea, among others.

Security is a factor that should be taken into account from the start design of any product. Such problems could be trivial if other violations that have occurred at industrial sector where signals are forged through networks or wireless sensors are analyzed; but even more worrying when heating systems, lighting and security of households are tapped to be changed and transgressed [6] [7] [15] [16].

According to a study from Hewlett Packard [17] about 70% of Internet things devices are vulnerable to attack. Security cameras, thermostats, alarms, door controllers were studied, among others; each of these had a service oriented to the cloud and had a mobile application. About 25 vulnerabilities for each device and the following were highlighted:

i) Privacy issues (where you can delve respect to the rights inherent human beings to this principle).

ii) Insufficient authorization, iii) lack of encryption

iii) Insecure web interface

iv) Inadequate protection software.

The report of the most common threats in IoT [17] is presented in Fig. 1.

Hewlett Packard's report also highlighted that information such as credit cards, social security numbers and other sensitive data travel over the network without proper security. While this study has certain commercial purposes, it is important to identify issues facing the industry determines as relevant in this market.

On the other hand with the development of the IoT, RFID and ubiquitous network technology sensors have become two major parts of it. RFID as a type of automatic identification technology without

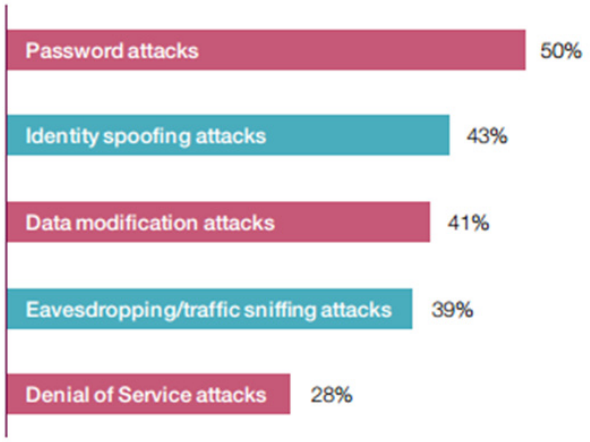


Fig. 1. Top the most common threats of IoT products (Capgemini consultant

contact identifies objects through RF signal and collect data. It is possible to work in different environments and identifying objects, according to [18] RFID is now often seen as a prerequisite for the IoT. In general, the IoT can be divided into three layers:

- *The lower level,* is the perception layer used mainly to capture, gather, distinguish and identify object information. The layer includes RFID tags and literacy devices, cameras, GPS, sensors, laser scanner, and so on.
- *The second level is the network layer,* which is used to transmit and process information obtained by the layer of perception and provides such information to the application layer, with the support of reliable communication.
- *The upper level* is the application layer, used to process data intelligently, and aggregation of data from various sources with different types. The layer implements control and information management, making use of cloud computing, data mining etc.

This model provides a theoretical framework for building a reliable security information, enabling IoT to be a creditable, controllable and independent network.

As the communications infrastructure of the Internet evolves to include detectable objects, appropriate mechanisms will be needed to ensure communications with these devices in the work done by [10] in the context of future applications of IoT, in areas as diverse as health (eg, remote patient monitoring or control of the elderly) and smart cities (eg distributed pollution monitoring, intelligent lighting systems), among many others. This trend is also reflected in the efforts carried out by normative agencies such as the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF), to design communication technologies and safety the IOT. Such technologies currently form a stack of protocols required for IoT with various communication technologies; work done by [19] is discussed detailed.

Some applications such as a monitoring system houses by [20], works using open microcontrollers such as Arduino code. Arduino Atmel AVR uses a processor that can be programmed in C language computer through the USB port also allows you to interact with other devices. The Ethernet module acts as a bridge to connect the Home Gateway to the local proxy. This application consists of three main modules: Web micro server, hardware interface modules and software package (smartphone app). This work proposes the implementation of a new architecture for the surveillance system using Android-based smartphone ensuring low costs and home control flexibly. The proposed architecture uses Web services based on Representational State Transfer (REST), as a layer of interoperable communication between the remote user and the application home devices.

From these references, then the analysis work related work, it was classified aspects from clusters defined on IoT area.

III. Methodology

In order to make an analysis of literature review, we carry out three phases to identify related works. The first preliminary phase we used keywords in fields related to security issues in IoT environments in databases such as IEEE, ACM and Scopus (Table I).

TABLE I. REVISIÓN PRELIMINAR DE ARTÍCULOS EN BASES DE DATOS ESPECIALIZADAS

Keyword of search	Data base	# of results	Reviewed articles	Related articles
Security IOT	Scopus	1.134	89	32
Security internet of things	ACM	224	29	23
Security IOT	IEEE	143	27	21
Total	--	1501	145	76

For this phase a review of the abstracts and conclusions from the preview identified 76 potential publications directly related to the security area in IoT was done. However when checking a large number of related work, it was identified that majority was not related to security issues.

Therefore it held a a second phase where a combination of the greatest number of occurrences of words used in IoT and safety was performed. Study was conducted which in advance by [21] (Table II).

TABLE II. WORD FREQUENCY IN IOT ENVIRONMENTS (YAN, ET AL, 2015)

No.	Frequency	Keywords
1	379	Internet of things
2	112	Wireless sensor networks
3	54	RFID
4	28	Security
5	22	Cloud computing
6	14	6LoWPAN
7	11	CoAPs
8	11	Future internet
9	10	IPv6
10	10	Machine to machine
11	10	Privacy
12	10	Ubiquitous computing
13	10	Web of things
14	10	Web services
15	9	Environmental internet of things
16	9	Internet
17	9	Middleware
18	8	Cyber physical system
19	8	Quality of service
20	7	Energy efficiency
21	7	Machine-to-machine communications
22	7	Performance
23	7	Smart objects
24	7	Social networks
25	6	Cloud manufacturing
26	6	Pervasive computing
27	6	Semantic web
28	6	Trust

For this study purposes, it was taken the fisrt five most frequently phrases, such as: 'IoT and security', 'Middleware', 'RFID', 'Internet', 'Cloud computing', 'Wireless sensor networks' and '6LoWPAN'. To complement this studio, the final third phase was to classify the most frequent problems from the basic security principles. Table III shows the results of this studio.

From the related work summed up in table III, It was identified the two most frequent problems: user authentication, followed by data encryption.

TABLE III
PAPER REVISION IN SPECIALIZED DATA BASES

PROBLEM	# PAPERS	%
User Authentication	33	45,2%
Traffic filter	18	24,6%
Data encryption	25	34,2%
Intrusion detection in real time	1	1,3%
Devices and applications protection	17	23,2%
Secure localization	7	9,5%
Quality service	1	1,3%
Secure connectivity between objects	12	16,4%
Secure protocols	15	20,5%
Information storage	2	2,7%
User resistance	1	1,3%
vulnerable Interfaces	1	1,3%
Cost	3	4,1%
Malware	4	5,4%
Unsecure Software, Hardware	11	15,0%
Unsecure Web interface	2	2,7%
Information theft	9	12,3%

IV. Security model proposed

Due to Internet of Things is a large field with various technologies, a categorization of the issues and technologies was made, this categorization is the basis for analyzing some details of security and privacy in the respective fields.

Figure 2 shows a categorization of the issues and their respective technologies used in each of the topics that make up the Internet of Things.

According with Figure 2, it can be identified eight major areas within IoT which must be specified level of security related studies. They are described detalied below.

- *Communication*: Research on communication protocols has come up with solutions that provide the integrity, authenticity and confidentiality, such as TLS or IPSec. Privacy needs have been addressed by different routing schemes as Onion Routing or Freenet, but these are not widely used.
- *Sensors*: Integrity and authenticity of the sensor data is an objective of the current research that can be handled as watermarking, which was previously described by [22]. The confidentiality of data sensors is a very vulnerable condition; therefore, the need for confidentiality in the sensor is low, so that confidentiality is based on the confidentiality of communication. Mechanisms such as face blurring video data are important to implement in order to preserve the privacy of individuals and objects.

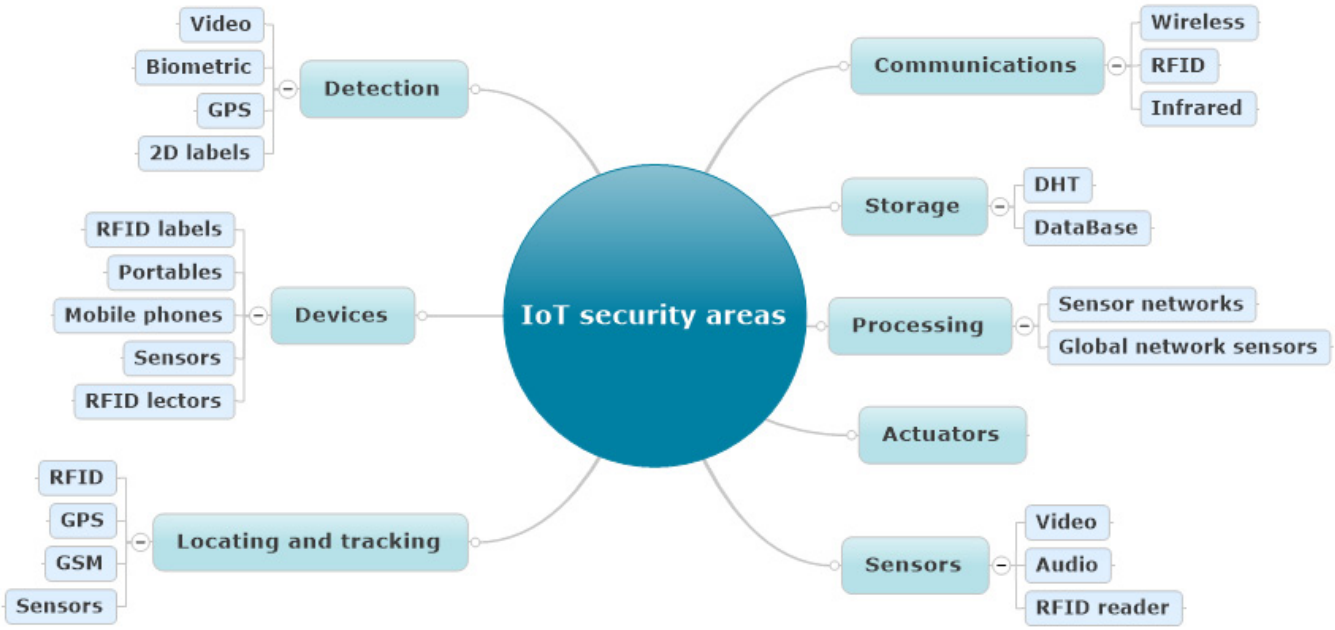


Fig. 2. IoT security areas identified

Sensor availability depends mainly on the communication infrastructure. Regulations are necessary to preserve the privacy of individuals who are currently most often unconscious on the sensors, such as video cameras.

- *Actuator*: Integrity, authenticity and confidentiality of data in an actuator depends primarily on the security of communications.
- *Storage*: Security mechanisms for storage devices are well established. Data storage is highly sensitive to privacy and there are many cases of violation of privacy regulations should be widely distributed to provide an adequate response to user privacy protection. Storage availability depends mainly on the availability of the communication infrastructure and well-established mechanisms for redundancy storage.
- *Devices*: Within the field of integrity of the devices, a device is free from malware. This property has also been called "admissibility" worked by B. Schneier, a presently open issue, researched Trusted Computing Platform (TPM) and highly sensitive. The authenticity of a device handles all the communication parts, not seen such as the end point of connection. Confidentiality is a device with integrity to ensure that no third party has access to internal data devices.

Devices privacy depends on the physical privacy and privacy of communication.

- *Processing*: Integrity in data processing services is based on the integrity of communication devices. Also, it depends on the design and proper execution of algorithms for processing. The authenticity of processing depends solely on the authenticity of the device and the authenticity of the communication.

The property of confidentiality in processing depends only on the integrity of the device, and in the case of distributed processing, depends on the integrity of the communication. The availability of processing depends on the device and the availability of communication exclusively.

- *Location and Tracking*: The integrity of Location and Tracking is based on the integrity of Communication and the integrity of the reference signals used in the location, such as GSM or GPS. It also depends on the authenticity of the authenticity and integrity of communication devices. The confidentiality of data tracking and tracing are of great importance to ensure user privacy and therefore is very sensitive. Confidentiality in this context means that an attacker is not able to disclose the location data and therefore is primarily based on the confidentiality of communication. Data privacy location means that there is no way for an attacker to reveal the identity of the person or object and the location and tracking is not possible without the agreement or explicit knowledge.

TABLE IV
RECOMMENDATION CRITERIA IN SECURITY AREAS

Properties	Security principles					
	Integrity	Authenticity	Confidentiality	Privacy	Availability	Regulation
Communication	High	High	High	Media	High	Low
Sensors	High	Medium	Low	High	Low	High
Actuators	Low	Low	Low	Medium	Low	Media
Storage	High	Medium	High	High	Low	High
Devices	High	Low	Low	Medium	Medium	Medium
Processing	Medium	Low	Low	High	Low	High
Location and tracking	Low	Low	High	High	High	High
Identificación	Media	Baja	Alta	Alta	Alta	Alta

- *Identification:* It uses same sensitivities than Location and Tracking. One difference is the higher sensitivity on the integrity part. It is easier for an attacker to manipulate the identification process as it is handling the localization process. This translates mainly due to technology used (eg RFID or biometrics) is more likely that an attacker manipulate location technologies (eg, GSM).

From this basic classification criteria are defined to determine the relevance of the security level on each of the areas identified in table IV.

V. Conclusions

Since the IOT devices are eminently focused on sending information between devices, or from them to Internet; one of the key measures to be taken, would be the protection of information traveling through them. In most cases this information travels through wireless networks or through public networks, which are vulnerable to being attack.

If communication channel is not adequately protected by encrypting data, it can be easy for an attacker to carry out attacks. The attacker can capture customer traffic, rectify it to pretend to be the originator of it, and send it to the legitimate server, so that it acts as an intermediate point in communications, invisible to both: the source and destination of traffic. Thus, people can get all the information they want even modify it, in order to alter the behavior or performance of the device, or even send false information to users, so they will not take the right decisions regard of the original information.

Another common feature characteristic to a large quantity of IOT devices, is that they use cloud services. In this case these applications have other potential risk; for instance; if there are deficiencies in the management or update the platforms; intruder would be able to access the information store and even take control of the IOT device.

There is a specific need for research into the availability of communication due to DDoS and service provided by IP. In addition, the integrity of the devices must ensure their freedom from malware such as spyware or rootkits, seeing the need for more research. Finally, almost all areas lack mechanisms applicable in the privacy of Internet of Things. The guidelines for Langheinrich are very useful for system designers, but regulations are needed to ensure that systems comply with these guidelines, and mechanisms must be developed to provide users with opportunities to actively protect their privacy rather than relying systems of Internet of Things respect their privacy and implement respective mechanisms.

Finally, it is very well known to use mobile applications that are installed on a Smartphone for any type of management, either obtain data or control the device. As a result, mobile applications can also be the target of attacks, either exploiting vulnerabilities or deficiencies in its implementation, or by developing malicious applications that emulate the behavior and appearance of legitimate access to the IOT devices.

As future work, is foreseen to carry out a characterization of these problems, so that from an ontological model and intelligent agents it can be carried out the appropriate identification of security mechanisms from most frequent problems in clusters of application of IoT. This would facilitate security alternatives identification, deployment access models IoT devices first.

References

[1] D. Boyle, R. Kolcun, and E. Yeatman, "Devices in the internet of things," J. Inst. Telecommun. Prof., vol. 9, no. 4, pp. 26–31, 2015.

[2] D. Pavithra and R. Balakrishnan, "IoT based monitoring and control system for home automation," in 2015 Global Conference on Communication Technologies (GCCT), 2015, pp. 169–173.

[3] V. Vujovic and M. Maksimovic, "Raspberry Pi as a sensor web node for home automation," Comput Electr Eng, vol. 44. pp. 153–171.

[4] R. Aggarwal and M. L. Das, "RFID security in the context of internet of things," in Proceedings of the First International Conference on Security of Internet of Things, 2012, pp. 51-56.

[5] W. Huan, "Studying on Internet of things based on fingerprint identification," in 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), 2010.

[6] R. Weber, "Internet of Things–New security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[7] L. Atzori, et al., "The internet of things: A survey," Computer networks, vol. 54, pp. 2787-2805, 2010.

[8] G. Gang, et al., "Internet of things security analysis," in Internet Technology and Applications (iTAP), 2011 International Conference on, 2011, pp. 1-4

[9] X. Li, et al., "Research on the architecture of trusted security system based on the Internet of things," in Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on, 2011, pp. 1172-1175.

[10] J. Granjal, et al., "Security for the internet of things: a survey of existing protocols and open research issues," Communications Surveys & Tutorials, IEEE, vol. 17, pp. 1294-1312, 2015.

[11] T. Bécsi, et al., "Security issues and vulnerabilities in connected car systems," in Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2015 International Conference on, 2015, pp. 477-482.

[12] M. L. Han, et al., "A Statistical-Based Anomaly Detection Method for Connected Cars in Internet of Things Environment," in Internet of Vehicles-Safe and Intelligent Mobility, ed: Springer, 2015, pp. 89-97.

[13] M. Schellekens, "Car hacking: Navigating the regulatory landscape," Computer Law & Security Review, 2016.

[14] J. Schumann, et al., "R2U2: Monitoring and Diagnosis of Security Threats for Unmanned Aerial Systems," in Runtime Verification, 2015, pp. 233-249.

[15] L. Da Xu, et al., "Internet of things in industries: a survey," Industrial Informatics, IEEE Transactions on, vol. 10, pp. 2233-2243, 2014.

[16] Z. Yan, et al., "A survey on trust management for Internet of Things," Journal of network and computer applications, vol. 42, pp. 120-134, 2014.

[17] D. Meissler, "HP study reveals 70 percent of internet of things devices vulnerable to attack," Retrieved June, vol. 30, p. 2015, 2014.

[18] B. Zhang, et al., "Security architecture on the trusting internet of things," Journal of Electronic Science and Technology, vol. 9, pp. 364-367, 2011.

[19] M. Palattella, et al., "Standardized protocol stack for the internet of (important) things," Communications Surveys & Tutorials, IEEE, vol. 15, pp. 1389-1406, 2013.

[20] R. Piyare, "Internet of things: Ubiquitous home control and monitoring system using Android based smart phone," International Journal of Internet of Things, vol. 2, pp. 5-11, 2013.

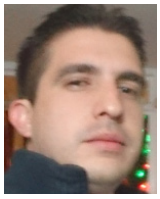
[21] B. Yan, T.-S. Lee, and T.-P. Lee, "Mapping the intellectual structure of the Internet of Things (IoT) field (2000–2014): a co-word analysis," Scientometrics, vol. 105, no. 2, pp. 1285–1300, Sep. 2015.

[22] H. Juma, et al., "On protecting the integrity of sensor data," in Electronics, Circuits and Systems, 2008. ICECS 2008. 15th IEEE International Conference on, 2008, pp. 902-905.

Paulo Alonso Gaona-García is Associate Professor and active member of GIIRA research group at Engineering Faculty of Universidad Distrital Francisco José de Caldas, Bogotá – Colombia. He obtained his Ph.D. in Information of Engineering and Knowledge at University of Alcalá in 2014. He finished a degree on System Engineer on 2003 and obtained an MSc in Information Science and Communication in 2007 at Universidad Distrital Francisco José de Caldas. His research interest include Web science, network and communications, information security, e-learning, information visualisation and semantic Web.

Carlos Enrique Montenegro Marin is a Ph.D.in systems and computer services for internet from University of Oviedo, Asturias, Spain (2012). He has a Diploma of advanced studies 2008 of the Pontifical University ofSalamanca.He is MSc.Science in Information and Communication Systems from the Universidad Distrital Francisco José de Caldas. He is a System engineer. His research interests include Object-Oriented technology, Language Processors, Modeling Software with, DSL and MDA.

Yuri Vanessa Nieto Acevedo is a MSc. Science Information and Communications from the Universidad Distrital Francisco Jose de Caldas and Industrial Engineer (2012). Is a full time researcher at AXON Investigation Group form CUN University and GIIRA (Investigation Group of Academic Interoperability) member. Her research interests include Learning Analytics, e-Learning, machine learning and virtualization.



Juan David Prieto Rodríguez is Associate Professor at Engineering Faculty of San Mateo Unversity, Bogotá – Colombia. He´s specialist in informatic security at Piloto University. He finished a degree on electronic and telecommunications Engineer on 2009 and obtained graduate postgraduate in 2014. His research interest include, network and communications, information security, information visualisation and digital signal processing.