About Security in Internet of Things

José Adame

Lusofona University of Porto, Portugal
joseangelromeroadame@gmail.com

Abstract. In this work, we start with an introduction to know what the IoT (internet of things) is, what are the Some examples. Then its main problems in security and privacy are explained. As for the solution, it is determined according to the purpose for which it is used device and not the device itself, this is also explained in two final examples. And finally a small conclusion for the future about security and privacy in IoT.

Keywords: Internet of things, IoT, Security, Security Services, Privacy, Personal Data Protection.

1 Introduction

Nowadays, information architecture based on The Internet allows the exchange of goods and services among all elements, equipment and objects connected to the network. The IoT refers to the network interconnection of all objects everyday, who are often equipped with some kind of intelligence. In this context, The Internet can also be a platform for devices that communicate electronically and share specific information and data with the world around them. Thus, the IoT can be seen as a true evolution of what we know as the Internet adding more interconnectivity extensive, a better perception of information and more complete intelligent services. In its For the most part, the Internet was used for protocols aimed at connecting applications such as HTTP (Hypertext Transfer Protocol) and SMTP (Simple Mail Transfer Protocol). However, today a large number of intelligent devices communicate with each other and with other control systems. This concept is known as M2M (machine-to-machine communications).

IoT (Internet of Things) is an emerging architecture based on the Global Internet that facilitates the exchange of goods and services between networks of the chain of supply and that has a major impact on the safety and privacy of the actors involved [1].

Some highlights in the history of the IoT are the following:

- The term: Internet of Things was first used by Kevin Ashton in 1999 that I was working in the field of network RFID technology (identification by radiofrequency) and emerging detection technologies.

- However, the IoT "was born" sometime between 2008 and 2009 [2].

- In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Currently there are about 25 billion devices connected to the IoT. More or less an intelligent device per person [2].

- It is expected that the number of smart devices or "things" connected to the IoT will be more than 50 billion in 2020.

IoT introduces a radical change in the quality of life of people, offering a great number of new opportunities for access to data, specific services in education, in safety, health care or transport, among others fields. On the other hand, it will be the key to increasing the productivity of companies, offering a wide distribution of the network, smart local networks of devices smart and new services that can be customized according to the needs of the client. The IoT brings benefits to improve the management and monitoring of assets and products, increases the amount of information data and allows the optimization of equipment and use of resources that can translate into cost savings. In addition, it offers the opportunity to create new intelligent interconnected devices and explore new models of deal.

Next we will see what makes up any "thing" exposing at the end of that point concrete examples as the case of Amazon echo that is so controversial nowadays. Finally I am making a step to the possible solution and specifying in it with a good level of details ending with two simple examples that make it easier to understand and visualize it as a summary.

And finally a brief and concise personal conclusion about all this.

2 Development and demonstration of results

IoT can be seen as a combination of sensors and actuators that are capable of provide and receive information digitizes and place it in bidirectional networks capable of transmit all the data to be used by a lot of different services and end users [3].

Multiple sensors can be attached to an object or device to measure a wide range of physical variables or phenomena and then transmit all the data to the cloud. Detection can be understood as a service model. Nowadays, the state-of-the-art devices, such as conventional items of households such as refrigerators or televisions, include communication and detection. These capabilities will be increasing with the incorporation of communication smarter and detection tools.

The architecture of IoT systems can be divided into four layers: detection layer objects, the data exchange layer, information integration layer, and the layer of application services [4].

Smart devices can already be connected through the traditional Internet. Without However, the IoT incorporates the detection layer that reduces the capacity requirements of those devices and allows their interconnection. Data consuming sensors communicate with sensors or owners thereof through the integration layer of information that is responsible for all communication and transactions. Meanwhile, new requirements and challenges for data exchange, filtering and integration of the information, the definition of new services for users, as well as an increase in

complexity of the network architecture. On the other hand, the use of cloud technologies is growing exponentially New infrastructure platforms and applications software are offered within the framework of the IoT. Some of the main advantages and benefits of the IoT will be the creation of innovative services with better performance and solutions added value, together with the reduction of data acquisition costs of services existing and the opportunity to create new sources of income in a context of a model of sustainable business These applications can be oriented to consumers, businesses, commercial activities, and survey activities, to the industrial and scientific community through use of application developers.

The number of applications and services they can provide is practically unlimited and it can adapt to many fields of human activity, facilitating and improving its quality of life in multiple forms.

As for specific devices, it is worth highlighting the case of Google home and Amazon echo, According to a study made by Mozilla these products (and others) can track the user and share your data with third parties for no apparent reason. The Mozilla report adds that, in the case of Google, its Smart speaker can listen to conversations but, as it is difficult to know what else you can do with that information. As for Amazon Echo, this device is in a position similar to that of the device Google. According to the document, the intelligent speaker of Amazon does not eliminate the stored data, it has a complex privacy policy and share data with other companies. In addition, the application is able to access to the user's camera and microphone and trace their location.

2.1 Security and Privacy

Security presents a significant challenge for IoT implementations due to the lack of a common standard and architecture for IoT security.

In heterogeneous networks, as in the case of the IoT, it is not easy to guarantee security and privacy of users. The main functionality of the IoT is based on the exchange of information among the billions or even billions of objects with an Internet connection. One of the security problems in the IoT that has not been considered in the standards is the distribution of the keys between devices.

On the other hand, privacy issues and profile access operations between the IoT devices without interference are extremely critical. Still, ensure the Exchange of data is necessary to avoid losing or compromising privacy. Increasing of the number of intelligent things that surround us with sensitive data requires management of transparent and easy access control so that, for example, a provider only can read the data, while another is allowed to control the device. In this meaning, some solutions have been proposed such as the grouping of devices integrated into virtual networks and only those devices desired within each virtual network. Another approach is to maintain an access control in the application layer in function of each seller.

In order to have a widespread adoption of any identification system for objects, there is a need to have a technically sound solution to guarantee the privacy and security of the clients. Although in many cases, security has been done As an added bonus, the feeling is that public acceptance of the IoT will occur only when Apply sound security and privacy solutions. In particular, the attacks must be intercepted, authenticated data, controlled access and customer privacy (natural and legal persons) guaranteed. It could be hybrid security mechanisms that

combine, for example, hardware security with key diversification for offer superior security that makes attacks significantly more difficult or even impossible. The selection of security features and mechanisms will continue being determined by the impact on business processes; and the counterparts will be between chip size, cost, functionality, interoperability, security and Privacy. Security and privacy issues should be addressed by future standards that must define the different security functions to provide services of confidentiality, integrity or availability.

There are also a number of issues related to the identity of people. These should be addressed in policy and legislation, being of vital importance for the efficient public administrations of the future.

As to how this situation must be faced [5], first you must understand that you can offer different levels of security depending on the service that the device needs. The Recommendation X.800 defines the following security services [6]:

- Authentication: to identify the communicating entity and the data source.
- Access control: to prevent the unauthorized use of resources.
- Confidentiality of the data: to protect them against unauthorized disclosure.
- Integrity of the data: to ensure that they have not been altered or destroyed an unauthorized way.
- Non-repudiation: to give proof of the origin of the data or delivery thereof.
- Availability: to guarantee the continuity of accessibility and use by the authorized entities.

These services are provided through security mechanisms alone or in combination, such as: encryption, digital signature, mechanisms for access control, data integrity mechanisms, authentication exchange, traffic filler, control of routing and notarization.

Low power consumption and light processing protocols are used to make the most of WSN resources. In this sense, you also have to prevent attacks whose objective is not to violate privacy but to overload the nodes and cause consumption extra [7].

The levels of security and privacy on the elements that must be protected depend on the imperatives imposed by the framework legal to which the final service is subject.

At European level, the Council of the European Union Convention n. 108, Strasbourg 28/1/1981, 5 ratifications 1/10/1985, established common data protection criteria for all members of the CE [8], coordinated by Directive 95/46 / CE of the European Parliament of 24/10/1995 [9].

In its report on the Data Protection Directive of 24/02/2004, the EU recognizes the legislative heterogeneity of its member countries and emphasizes the need for European states and institutions to adopt a equivalent level of protection of the rights of individuals [10]. Highlights

that this heterogeneity of national legislations on data protection hinders the development of the European internal market. As a result of the lines of action established by the European Parliament in the Communication of the European Economic and Social Committee [11], Europe is moving towards a common regulatory framework with the Proposal for a general regulation on data protection [12]. Once approved will be of direct application in two years for the entire European Union. This Regulation will affect those who process data of a personal nature and have an establishment in a member state, even if the information is processed performed outside the European Union. Companies not established in Europe will be affected if they process personal data for provide goods and services to residents of the EU.

Working Party Working Group 29 (WP29) has approved the first joint opinion on internet of the things, the Opinion 8/2014 on the new developments in the Internet of the things of 09/16/2014 [13], whose preparation has been led by the Agency Spanish Data Protection Agency (AEPD) together with the French authority Commission nationale de l'informatique et des libertés (CNIL).

The General Data Protection Regulation [14] will homogenize the legislation European Union on the protection of personal data, although in a global market It will still be necessary to live with the legislative heterogeneity.

In the technological field there are numerous works such as Dener, Fatema and Brad, Maw et al. , Kumari and Shukla, Shukla and Kumari, Malik, Kuthadi, Rajendra and Rajalakshmi, Karlof and Wagner and others [15-20], who have elaborated efficient security mechanisms for WSNs, and to avoid putting at risk the quality of the service for excessive consumption of resources. Companies and suppliers of equipment and networks They are very active in devising services for society and increasing their commercial catalog.

Among the proposals that exist, one gathers the knowledge about security and privacy generated for internet of things by the legal, technological and business areas, in a computer system able to channel collaboration between these areas. The purpose is to select automatic security and privacy policies that should be applied to new products and services. The collaboration between these three areas, would allow the issuance of certifications of trust for stakeholders and eliminate possible barriers of distrust. This proposal proposes the following collaborative environment:

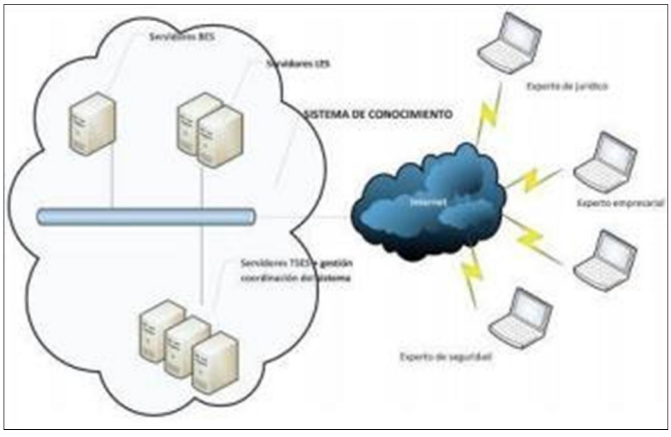

Fig.1. Collaborative environment among experts from the three knowledge areas BES (business expert system); LES (legal expert system); TSES (technological solutions expert system).

Companies dedicated to the design of new products and services can perform simulations virtual events prior to making decisions about the real market. In the legislative field, the impact on society and the market of possible modifications and new legislations in this matter, being able to know how and to what extent they would affect the products and services existing and their future developments. Technological areas can quickly know the critical aspects that need new research and innovations. To carry out complete tests, a model has been designed to test the possibilities of automation from the decision of the security policy to the configuration of the operation of the elements of the WSN. These tests have been carried out in the GRyS team (Group of Next Generation Networks and Services) of the Citsem (Center for Research in Software Technologies and Multi- media Systems for Sustainability) of the UPM (University Polytechnic of Madrid).

The design and test model (figure 2) consists of a WSN, a middleware platform oriented to services, Aware Project [21], and PDPS-IOT expert system (personal data protection system - internet of things) [22].

The PDPS-IOT expert system decides the security and privacy policy to be applied to the service (object of this article), which is communicated to the Aware platform, which knows the WSN to which it connects (its technology, the way in which it must dialogue with them, its possibilities, the security mechanisms they support) managing their configuration possibilities. Generate the commands and actions to configure them remotely using their middleware. PDPS-IOT knows the set of security mechanisms that Aware is able to manage, with that a homogeneous level of security can be established for all WSN networks.

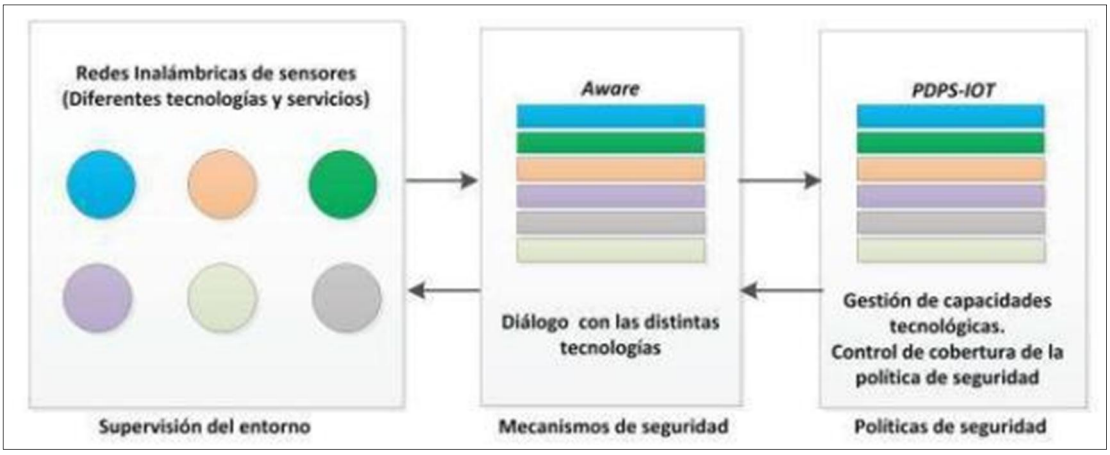

Fig.2. The design model presented.

The final service used for testing monitors health by collecting pulse data and body temperature. These data are processed and sent to the base station to inform a medical equipment. This final service involves health data of people, protected in Spain by Royal Decree 1720/2007, of 21/12/2007, on the protection of personal data, and in Europe by general regulation of data protection. Through the PDPS-IOT expert system (figure 3), which has the service specifications as input, the policy is obtained as output of security and privacy (security level) that the service should have.

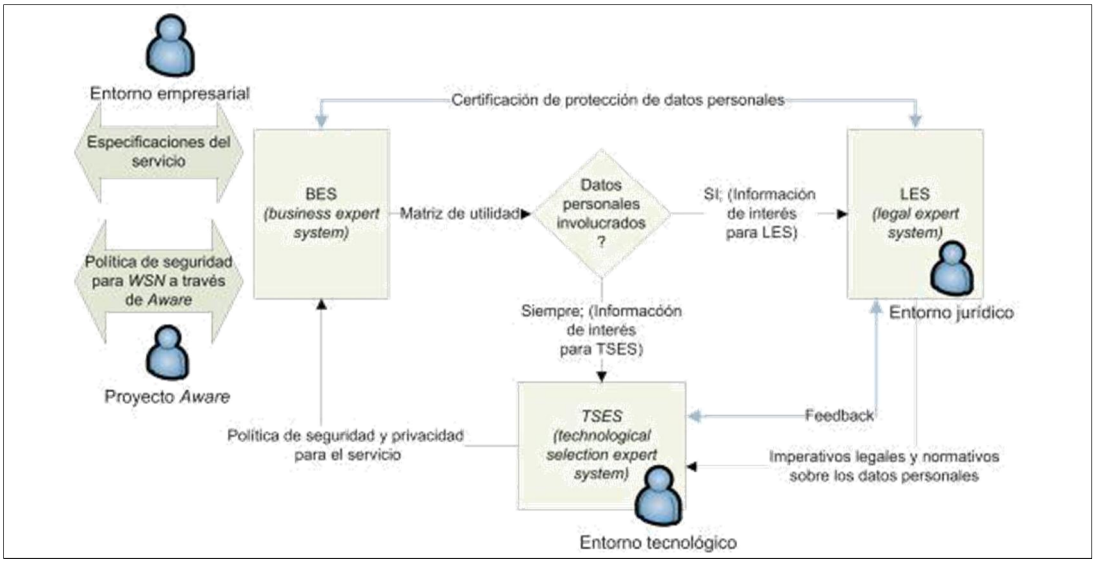

Fig.3. Personal data protection system for internet of things services (PSPS-IOT). BES (business expert system); LES (legal expert system); TSES (technological solutions expert system).

This is possible thanks to the fact that the relevant information has been formalized in what we call the matrix of utility, from which the legislative framework that affects the service is obtained. What you are looking for is to obtain the security and privacy imperatives that must act on the elements of information that should be protected. These imperatives will be transformed into a set of services and security and privacy mechanisms. In the event of a change in the use or reuse of a WSN to provide another service, or the same service in another area, after communicating it to the managers and duly update the utility matrix generates the process that culminates with the Remote reconfiguration of security in the WSN, if necessary.

As an example of the different behaviors to be had, two examples of cases of uses in which the IoT is the same, a cardiac belt:

In the case of a farm, own service to control the health of livestock. Does not involve data personal The information collected is not useful for anyone else. It is not a critical service (it does not replace food controls) and has no special continuity requirements. Access to the system does by user and password without additional mechanism.

In the case of a football team, own service to control the health of the players. There are data personal (health) protected by law before disclosure / disclosure (hide everything, or separate identity of the person of his measurements). This data must be managed and managed only by staff authorized: veracity of the actors and authorization of access. Content is required, according to the law, personal data must be true (we assume that the sensors are calibrated). It is a service that is not critical and without special continuity requirements.

3 Conclusion

In short, everything depends on the control of the bodies that regulate and can create new laws for the security and privacy in IoT and that these measures evolve at the same time as these devices and do not are left behind, this way we can have that confidence in the products that are certified by these entities (in principle) and little by little in the future will go through much safer terrain. All this does not mean that there are always some non-certified or simply new devices that have certain innovative data treatment that endangers privacy and security as it is impossible guarantee a perfect security and that there are not things that always escape us but ultimately for a standard user of these devices (like me) is worth using these devices even with that possible danger of security and privacy.

References

1. R. H. Weber, (2010). "Internet of Things - New Security and Privacy Challenges". Computer Law & Security Review 26: 23-30. Consulted in 2018.
2. Dave Evans. (2011). How the Next Evolution of the Internet Is Changing Everything. Cisco Internet of Things White Paper. Consulted in 2018.
3. Charith Perera et. al. (2014). Sensing as a Service Model for Smart Cities Supported by Internet of Things. Transactions on Emerging Telecommunications Technology 25 (1): 81– 93. Consulted in 2018.
4. Ma HD. (2011). “Internet of things: Objectives and scientific challenges”. Journal of computer science and technology 26 (6): 919-924. Consulted in 2018.
5. Al-Ameen, Moshaddique; Liu, Jingwei; Kwak, Kyungsup (2012). “Security and privacy issues in wireless sensor net- works for healthcare applications”. Journal of medical systems, v. 36, n. 1, pp. 93-101. Consulted in 2018.
6. Unión Internacional de Telecomunicaciones (1991). Recomendación X.800. Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CITT. Consulted in 2018.
7. Comisión Europea (2012). Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), n. 2012/0011/ COD, 25/01/2012. Consulted in 2018.
8. Council of Europe Treaty Office (1981). Convention for the protection of individuals with regard to automatic processing of personal data, n. CETS 108, Strasbourg, 28/1/1981, pp. 110. Consulted in 2018.
9. Unión Europea (1995). “Directiva 95/46/CE del Parlamento Europeo y del Consejo, 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos”. Diario oficial, n. L 282 de 23/11/1995, pp. 0031-0050. Consulted in 2018.
10. Parlamento Europeo (2004). “Resolución del Parlamento Europeo sobre el primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)”. Diario oficial n. C 102E de 28.4.2004, pp. 147-153. Consulted in 2018.
11. Comité Económico y Social Europeo (2009). “Dictamen sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Internet de los objetos - Un plan de acción para Europa [COM(2009) 278 final]”. Diario oficial, n. C 255, 22/09/2010, pp. 116-120. Consulted in 2018.
12. Comisión Europea (2012). Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), n. 2012/0011/ COD, 25/01/2012. Consulted in 2018.
13. European Commission (2014). “Opinion 8/2014 on the on recent developments on the internet of things”, n. 14/EN WP 223, adopted on 16 September 2014, pp. 1-24. Consulted in 2018.
14. Palafox-Maestre, Luis E.; García-Macías, J. Antonio (2008). “Security in wireless sensor networks”. En: Yan Zhang; Miao, Ma. Handbook of research on wireless security. Hershey, PA: IGI Global, pp. 547-564. ISBN: 978 1 59 904899 4 . Consulted in 2018.
15. Dener, Murat (2014). “Security analysis in wireless sensor networks”. International journal of distributed sensor networks, v. 2014, pp. 1-9. Consulted in 2018.
16. Fatema, Nusrat; Brad, Remus (2014). “Attacks and counterattacks on wireless sensor networks”. International journal of ad hoc, sensor and ubiquitous computing, v. 4, n. 6, pp. 1-15. Consulted in 2018.

17. Karlof, Chris; Wagner, David (2003). “Secure routing in wireless sensor networks: Attacks and countermeasures”. Ad hoc networks, v. 1, n. 2-3, pp. 293-315. Consulted in 2018.
18. Kumari, Babli; Shukla, Jyoti (2013) “Secure routing in wireless sensor networks”. Ijarcsse, v. 3, n. 8, pp. 746-751. Consulted in 2018.
19. Kuthadi, Venu-Madhav; Rajendra, C; Rajalakshmi, Selvaraj (2010). “A study of security challenges in wireless sensor networks”. Journal of theoretical and applied information technology, v. 20, n. 1, pp. 39-44. Consulted in 2018.
20. Malik, M. Yasir (2012). “An outline of security in wireless sensor networks: Threats, countermeasures and implementations”. En: Zaman, Noor; Ragab, Khaled; Abdullah, Azween. Wireless sensor networks and energy efficiency: protocols, routing and management. Hershey, PA: IGI Global, pp. 507-527. ISBN: 978 146 660102 4.Consulted in 2018.
21. Santos-Familiar, Miguel; Martínez-Ortega, José-Fernán; López, Lourdes (2012). “Pervasive smart spaces and envi- ronments: A service-oriented middleware architecture for wireless ad hoc and sensor networks”. Architecture for wire- less ad hoc and sensor networks, v. 2012, pp. 1-11. Consulted in 2018.
22. Sánchez-Alcón, José-Antonio; López, Lourdes; Martínez-Orte- ga, José-Fernán; Castillejo, Pedro (2013). “Automated deter mination of security services to ensure personal data protection in the internet of things applications”. En: 3rd Intl conf on innovative computing technology (Intech), August, pp. 71-76. Consulted in 2018.