Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

Development of a Methodology to Securitize Household IoTs

Trabajo Fin de Máster

Presentado por: González Domínguez, Paula

Director: Paniagua Diez, Fidel

Ciudad: Madrid

Fecha: 26/07/2018

Agradecimientos

A mi director de proyecto, Fidel Paniagua, por su disponibilidad y por todas las sugerencias y comentarios que han llevado a mejorar significativamente el contenido de este trabajo.

A Rodrigo Blanco y Jaume Soler, no solo por todos sus consejos y orientaciones, sino sobre todo por el tiempo y buena disposición que siempre han tenido conmigo. Sois el tipo de profesionales en el que me encantaría algún día llegar a convertirme.

Y muy especialmente, a mis padres, porque aún sin entender todavía qué me ha llevado a escoger este camino, nunca han dejado de apoyarme y de ilusionarse con cada una de mis pequeñas “locuras formativas”.

Gracias.

ABSTRACT

Along the present paper is conducted a thorough research of the current panorama regarding IoT environments, in which has been identified a significant lack of defined security methodologies or standards. Therefore, after this study and analysis of the context, it is proposed a new security methodology adapted to household environments, which is based on the examination of the elements that compose them and a specific threat model for them, as well as the need of a tailored presentation of the results for a final user. The results of this proposal are satisfactory as well as its ability to be adapted for other less specific IoT environments.

Keywords: IoT, security methodology household environments.

RESUMEN

En este trabajo se lleva a cabo una profunda investigación del panorama actual relativo a los entornos IoT, para los cuales se ha identifica que existe una carencia de metodologías o estándares de seguridad definidos. Por ello, tras este estudio y análisis del contexto, se propone una nueva metodología de seguridad adaptada a entornos domésticos, que está basada en la examinación de los elementos que lo componen y un modelado de amenazas específico para éstos, así como en su necesidad de presentación adaptada al consumidor final. Las conclusiones de esta propuesta son satisfactorias y se plantea su capacidad de adaptación a otros entornos IoT menos específicos.

Palabras Clave: IoT, metodología de seguridad, entornos domésticos.

INDEX

INDEX OF FIGURES

INDEX OF TABLES

1. INTRODUCTION

No one would trust in the security of a house without a door or even without a bolt, however it is not rare to find out that many people are interacting, using or even wearing smart devices that owe no kind of basic security measures.

What is that ambivalence due to? The answer is much easier than what it may seem at first: in general, users are simply not aware of what they are exposing themselves to.

This leads to a very worrisome problem, not only due to the large amount of people that it could affect, but also due to the direct impact that IoT devices can have in the physical world. For example, while a cyberattack targeted to obtain bank credentials would mostly lead to money loss, a cyberattack targeted to a specific IoT could put in danger the life of the people surrounding it.

Considering this approach, it is surprising that IoT producers or institutions have not taken care of this situation yet, but as it will be shown along the following study, users are not the only parties that possess an important lack of information about this ‘IoT world’.

To better understand and address this situation, along this paper will be studied the context and features of IoTs, as well as the security resources available to understand them and their related security features. Among these resources, is specially highlighted the role of the currently available security methodologies, which are studied to understand their scope, depth and versatility, and to also identify possible gaps that they may present.

Moreover, in line with the results of this analysis, it will be suggested a new approach for a security methodology that can be used in any IoT context to securitize its devices and systems, and that will also aim to cover the gaps identified in other security methodologies.

1.1. Motivation

As it was previously introduced, there is currently an important lack of information regarding IoTs. The clearest sample of this is the lack of security standards and methodologies defined to securitize IoT devices and environments, leading consequently to the deployment of very insecure devices that have a high and direct impact in the lives of millions of uniformed users.

This is a global problem, and even if there are already some institutions taking efforts towards solving this situation, such as NIST (NISTIR, 2018), no official methodology or standard to securitize IoTs has been published yet. Actually, the just-mentioned draft addresses the status of international cybersecurity standardization for IoTs, shown in Annex I.

Consequently, this paper aims to improve this situation by providing a methodology to securitize IoTs, studying its context and features, and defining a tailored solution which is also adapted for the consumers of these kind of devices.

1.2. Structure

The present paper has been organized according to the following structure:

- **Chapter 1, INTRODUCTION:** It lays out on a high level the main problematic that will be addressed along the paper, its causes, the reasons why the development of a methodology has been goal chosen by this project and what is expected to be achieved by it.

- **Chapter 2, CONTEXT AND STATE OF THE ART:** It summarizes the research conducted about IoTs, their history and evolution, their main benefits that they provide, the challenges that institutions, consumers and producers are currently facing and the particularization of a security proposal accordingly to the studied panorama.

- **Chapter 3, FRAMEWORK OF THE PROJECT:** It identifies the generic and specific goals that are expected to be achieved along the project. It also describes the methodology used in the development of the project as well as the definition of the specific environment of study, explaining the reasons of this choice.

- **Chapter 4, HOUSEHOLD IOT ENVIRONMENTS:** It describes the environment of choice, disaggregating the assets that compose it, their functions and associated risks.

- **Chapter 5, IOT SECURITY METHODOLOGY FOR HOUSEHOLD ENVIRONMENTS:** It is the core of the project. It explains in detail the security proposal, its requirements and considerations, the steps that should be followed, its evaluation and the requirements for a suitable presentation of its results. In that evaluation section, it is represented a realistic scenario where the proposed methodology can be implemented, allowing the detection of failures or further needs of development. Moreover, it is also proposed a mean of presentation for the methodology, along with a visual example of this proposal.

- **Chapter 6, CONCLUSIONS:** After the research and analysis conducted though all the previous sections, there will be extracted the main conclusions of the project, including the extent in which the previously defined goals have been achieved and the ability of implementing the methodology in other environments.

- **Chapter 7, FUTURE LINES OF WORK:** As an extension of the previous chapter, it analyses the future applications and gaps that have to be solved to ensure the applicability of the methodology in any IoT context.

2. CONTEXT AND STATE OF THE ART

In this chapter it will be studied the past and present of IoTs, going through its definition, main features, standards and other significant related circumstances, which may also be critical to fully understand the security problematic that this paper is aiming to solve.

2.1. History and Evolution of IoTs

The concept of IoT (Internet of Things) was coined by Kevin Ashton in 1999 as the title of a business presentation, in which he emphasized the need of reducing the human interference over data analytics devices (Ashton, 2009).

The term evolved along the years, drifting apart from its original use and turning into a new and wide idea, which has not always been used homogenously. In the context of this paper, the term IoT will refer to the whole ecosystem of interconnected devices and systems, as well as their resulting services, that collect, exchange and process data in order to be able to adapt dynamically to its context.

In the past years the IoT industry has been experimenting a sharp increase, and in 2011 a Cisco study estimated that by 2020 the number of devices connected to the internet would reach the 50 billion (Evans, 2011). Even though this number is nowadays being discussed and a more recent Gartner study estimates that this figure will be around 20 billion by that same date (Gartner, 2017), the numbers are still impressive to wonder what has caused this rapid growth and what might be its implications.

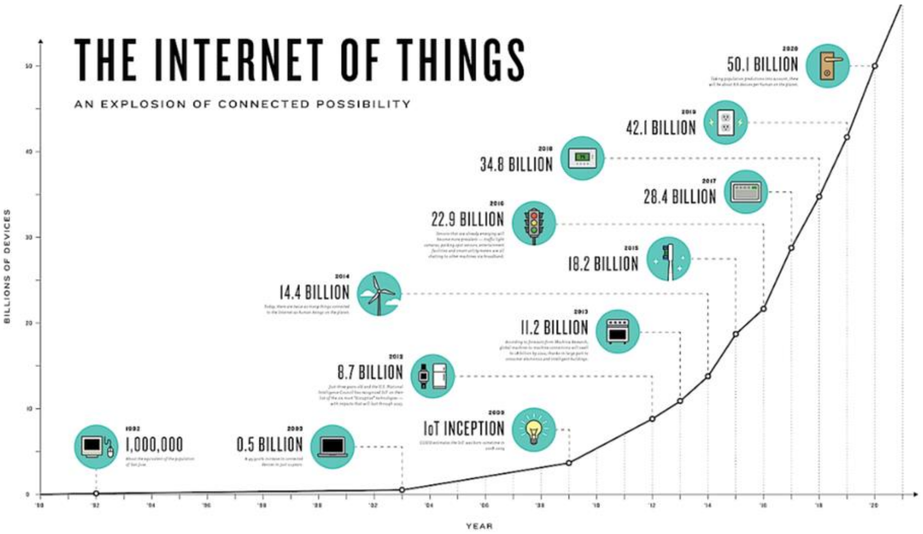


Figure 1. Evolution of IoTs. Source: CISCO data

2.2. Benefits of IoT Development

One of the main reasons why IoTs are experiencing such an exponential increase is the countless number of benefits that they can provide to both, consumers and producers.

From a business perspective, Mark Hung, Gartner Research Vice President, declares that "The IoT will have a great impact on the economy by transforming many enterprises into digital businesses and facilitating new business models, improving efficiency and increasing employee and customer engagement" (Gartner, 2017).

This is due to the features included in IoT devices, such as the capability of collecting, tracking and analyzing great amounts of data about consumers and their environment, which allow producers to optimize sales and production in terms of offering faster and more tailored releases, as well as boosting their innovation capacity.

In the eye of the customers, on top of the above-mentioned benefits, this have also led to noticeable improvements in the quality of their lives, such as through health, household or mobility devices, as well as through new leisure experience.

These reasons have motivated the early development and adoption of IoT Devices and Systems.

However, this development should also be embraced carefully, because it is important to remember that along with all those benefits may also come some significant security challenges.

2.3. Current Security Challenges for IOTs

2.3.1. New Threats and Security Breaches

Along with the inclusion of IoTs in the market, new surfaces of attack have also been deployed, leading to new security threats and concerns. It is estimated that by 2020 more than 25% of the enterprise attacks will involve the IoT, despite the IT security budgets are predicted to account for less than the 10% for IoT related issues (Gartner, 2017). Meanwhile, the number of attacks as well as their harming capacity keep on increasing over the years.

To understand the dimension of this problem, there are some examples of IoT security breaches that have taken place during the past few years and that are recalled next:

- **2009, Puerto Rican Smart Meters Hacked**: The smart meters at the Puerto Rican Electric Power Authority (PREPA) were physically accessed to carry out several power thefts.

- **2010, Stuxnet attack to PLCs:** The computer worm Stuxnet was designed to attack industrial programmable logic controllers (PLCs), accessing nuclear centrals and sabotaging some of their facilities.

- **2013, Foscam IP baby-cam hijacked:** The Foscam wireless cameras were accessed, allowing unwanted users to spy and interact with the targeted family, screaming and insulting the baby and her family.

- **2013, Target data breach:** A third party intruded the Target's system stealing 40 million credit and debit card accounts, obtaining their network credentials through an HVAC vendor, which were supposed to be used only to report temperature fluctuations in the stores.

- **2014, vulnerabilities in Hospira LifeCare infusion pumps:** The security bug could be exploited to take control over affected drug pumps, being able to change the assigned doses.

- **2015, Jeep car remotely hijacked:** Third parties took control over the whole car, sending instructions through its entertainment system to its main functions.

- **2015, Vtech Toymaker data breach:** The personal information of millions of families was exposed due to the lack of encryption provided by the digital toymaker. It included pictures, conversations, addresses, etc.

- **2016, Mirai DDoS:** The botnet Mirai infected more than one million IoT devices through their Telnet port, allowing DDoS attacks on countless devices, webpages and DNS providers.

- **2016, Cloudpets' DB held for ransom:** The personal information of thousands of customers was publicly stored in and open database, with was thereupon held for ransoms. The conversational features of the toys could also be accessed through its BLE technologies.

- **2017, Romantik Seehotel Jägerwirt:** The digital key access of the hotel had its system breached and held for a ransom, disabling customers to get into their rooms or new key cards to be reprogrammed.

Apart from the just-mentioned attacks, it is also important to remember that the IoT devices can also execute unwanted actions that may lead to security breaches, even when they are not manipulated by third parties. Good examples are provided by the smart home device Alexa, which have already been involved in unwanted behaviors, such as in 2017, when it ordered the shipping of several dollhouses (Liptack, 2017) or even in the present year, recording and sending a private conversation to a random contact of its owners (Wolfson, 2018).

2.3.2. Maturity Level of the Sector

Not only targeted attacks to IoT systems and misbehaviors of their devices can lead to security breaches. The IoT industry is currently facing also three mayor problems, as Scott Willson highlighted in a recent article for DZone (Willson, 2018), which may also affect the general security of these environments. These problems are: the lack of defined industry standards, the vast diversity of 'things' and the use of the limitless amount of IoT produced data.

A) Lack of Standardization

Nowadays, there are several international institutions working towards developing unified standards or methodologies to securitize IoTs. Due to the diversity and complexity of this ecosystem, none of them have published a definitive security proposal yet, but they have done meaningful research contributions which can help to reach this target. Some of the most significant documents, in which are also based the current paper, are the following.

- **National Institute of Standards and Technology (NIST):** In February of this year the NIST Internal Report (NISTIR) published a draft for IoT security, called *'Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)'*. This report aims to inform and enable policymakers, managers, and standards participants as they seek timely development of and use of cybersecurity standards in IoT components, systems, and services. It brings a good frame to understand the cybersecurity landscape for IoT and identify the areas where security standards are missing, but it does not provide yet a security framework itself. (NISTIR, 2018)

- **European Union Agency for Network and Information Security (ENISA):** Last year ENISA published a study titled *'Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures'*, which aims to set the scene for IoT security in Europe, providing insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying potential good practices and security measures to apply in order to protect IoT systems. It serves as a reference point in this field and as a foundation for relevant forthcoming initiatives and developments (ENISA, 2017).

- **Industrial Internet Consortium (IIC):** In late 2016 the IIC published a document called *'Industrial Internet of Things, Volume G4: Security Framework'* which explained and positioned security-related architectures, designs and technologies, as well as identified procedures relevant to trustworthy Industrial Internet of Things (IIoT) systems. This document described their security characteristics, technologies and techniques that should be applied, methods for addressing security, and how to gain assurance that the appropriate mix of issues have been addressed to meet stakeholders' expectations (IIC, 2016). As well, in 2017 it was also published a document called '*The Industrial Internet of Things Volume G1: Reference Architecture*', which provides an Industrial Internet Architecture Framework (IIAF) that is expected to serve as a foundational framework for other related technical documents and activities, as well as to provide guidance and assistance in the development, documentation, communication and deployment of IIoT systems (IIC, 2017).

- **Gartner:** Recently this year, the Gartner Advisory Company has released a paper called *'Architect IoT Using the Gartner Reference Model'* which provides an architecture blueprint that defines what functionality is required, where that functionality will operate, and how data and control will flow in an IoT project (DeBeasi, 2018).

B) Diversity of 'things'

Trying to frame the different assets, functions or results that can be related to IoT environments is a challenging task. This is due to the wide variety of items that these systems can include, as well as the diversity of vendors, functions or outcomes that those devices can be bounded to.

This situation poses an important problem of interoperability, which leads to the development of specific applications for almost each device included in the IoT system, instead of having a single central hub that controls the whole environment.

The solution to this problem would be to unify the interconnection requirements of the different IoT devices, however, there are still three main barriers that hinder this solution:

- The mentioned exponential growth of the sector, which difficult the in-time arrival of unified and aligned standards.

- The lack of commercial incentives for different vendors to build common platforms.

- The need of overhauling all the devices already in operation, that have also required significant investments to be deployed.

C) Uses of Data

By the end of 2016, an article in Network World pointed out that only an autonomous car could use 4,000GB of data per day (Nelson, 2016). IoT are active data collectors and reporters, what may also create important concerns, such as the following:

- **Confrontation with Data Protection regulations:** A clear example is the GDPR, the current General Data Protection Regulation implemented in the European Union, which establishes strict limitations to controllers and processors to collect, process, store and transfer personal data.

- **Vague definition or alignment with the purposes:** IoT devices can produce almost limitless amount of data and sorting through these volumes of data to make meaning is not always an easy task to accomplish by producers, controllers or processors.

- **Processing and storing challenges:** Along with the mass production of data, there is also the need of processing and storing it. Artificial Intelligence, Machine Learning and Cloud Computing provide solutions to these aspects, but likewise IoT, there are not yet settled technologies, adding their own challenges to IoT ones.

- **Security vulnerabilities:** The complexity of IoT environments, altogether with the all the previously mentioned circumstances have led to vulnerable environments, which can easily lead to Data Breaches.

2.4. Lines of Work in the IoT Security Field

After analyzing the whole context regarding IoTs, it is obvious that there is still much left to do concerning the security of these environments.

In particular, there are two statements that can summarize quite well the research carried out in this field:

- The IoTs ecosystems are composed by a wide variety of connected services and devices, and the protection of IoT deployments depends on the protection of all their elements (ENISA, 2017).

- There are still many areas of security in IoTs that lack of official security standards or a unified security framework, disregarding severe security gaps (NISTIR, 2018).

These statements highlight the actual need of developing a unified standard to securitize IoT environments, that has also been endorsed by the previous research.

Therefore, the present paper will aim to develop a modular methodology that starting from a very specific approach can be afterwards escalated to any IoT environment, providing at least a base for the development afterwards of an official security standard.

3. FRAMEWORK OF THE PROJECT

3.1. Generic and Specific Goals

As it has been outlined, the main goal of the present project is to improve the security of IoT users through the development of a methodology that allows to securitize IoT environments.

As a direct consequence from this goal, it is also necessary that the methodology developed has a generic approach that allows it to be implemented in any IoT ecosystem.

In the process of achieving this main goal, there are other several and specific goals that will also be pursued:

- To identify reliable sources that define and analyze IoT ecosystems. As this can be considered a still budding field, there is a lot of space for inaccurate information or misinterpretations, which is why this point is vital to develop a solid base for the project.
- To clearly identify the structure and relations within all the elements that integrate an IoT ecosystem. There should also be included clear explanations or definitions of each of the elements identified.
- To gather and define the main functions that the elements of an IoT system can deploy.
- To identify security risks directly associated to IoTs, and in the case of not finding an official classification, develop a tailored one based on the precedent research.
- To identify or propose security mitigations that improve the security of IoT users and define the way they should be implemented to guarantee that expectancy of security.
- To identify the situations in which the methodology can be used and to verify if it has the ability to be implemented in any IoT environment with profitable outcomes.

3.2. Methodology Used in the Project

To achieve the above-mentioned goals, it has been conducted a thorough research to identify similar methodologies that address total or partially some of the issues mentioned. No documentation has been identified that addresses directly the problematic posed, forcing the development almost from scratch of a new and independent methodology. Nevertheless, some existing models and publications have been used as a reference to ensure that this project is based in reliable foundations. Within the sources used to conduct the presented methodology development, could be outlined the following ones:

- The ENISA (2017), NIST (2018) and Gartner (2017) publications have carried several studies to identify the human, procedural and technical resources involved in IoT ecosystems. All these sources follow different approaches and present different classifications of all these elements, which is why, the present project has gathered and analyzed all this information to come up with a different classification that aims to keep the accuracy of the consulted sources but providing a simpler and more specific approach for the currently studied issues.
- Microsoft has developed a Threat Model (Betts & et al., 2018) that defines a path to identify these threats in very diverse contexts, which is why it has also been considered for IoTs. However, as it is not a methodology *ad hoc* for the studied environments, it cannot be used in this context to carry out the risk analysis. However, from this model has been taken the idea of dividing the different sections of an IoT ecosystem architecture. On the other hand, the risk classification has been specifically created for the present project, and not based on the STRIDE threats classification posed by Microsoft.
- The OWASP IoT Project (OWASP, 2015) presents a draft about the attack surface areas and security considerations for IoTs, which have been used to contrast and complement the classification of risks and mitigations developed in the present paper.

Consequently, the resulting methodology is not a replication or a direct application of any of the above-mentioned resources, but they have been taken as a reference of professional efforts that go towards similar directions and that have inspired or guided the design of the new proposal presented afterwards.

3.3. Environment of Study: Household IoTs

While analyzing the above-mentioned studies and papers, there have been identified some efforts towards developing standardized solutions for Industrial IoTs, especially for Critical Infrastructures, and for Health Devices.

However, there is a field which has not captivate much attention yet, but that is also worth to consider: Household environments. These particular scenarios gather some worrisome characteristics, such as the following:

- They can congregate a vast diversity of devices from different vendors and with very diverse functions and features.

- Most of their users do not have the knowledge to securely configurate their environment or event to understand the risks they can be taking.

- They can interfere directly into the private life of users, putting at risk their privacy as well as their personal integrity.

For these reasons, the present paper will be focused on the study of the characteristics of a household IoT ecosystem and propose a methodology that is adapted to the diversity of devices and the features of this particular environment, but that can also be escalated afterwards to other IoT contexts.

4. HOUSEHOLD IOT ENVIRONMENTS

The number and variety of IoT devices that can be found in a household environment are countless: smart vacuum cleaners, connected toys, lighting solutions, smart appliances, virtual assistants, Smart TVs, etc.

The features of each of these devices, as well as the interactions within them and the final users, will increase or reduce the number of threats the IoT ecosystem is exposed to.

Due to such a level of granularity, it is not possible to study all these devices and interactions as a whole, but it is possible to separate the big picture into smaller pieces that ease their analysis and consequently the proposal of security solutions that match all of them.

With this aim, in the following sections it will be described the main components and features of a Household IoT environment, as well as the interactions of every element with their users.

4.1. Basic Elements of a Household IoT Architecture

There is still some controversy about the definition of each of the elements composing IoT ecosystems. However, after some thorough research, the present section describes in broad strokes what could be considered the basic IoT architecture of a household environment, composed by the following elements:

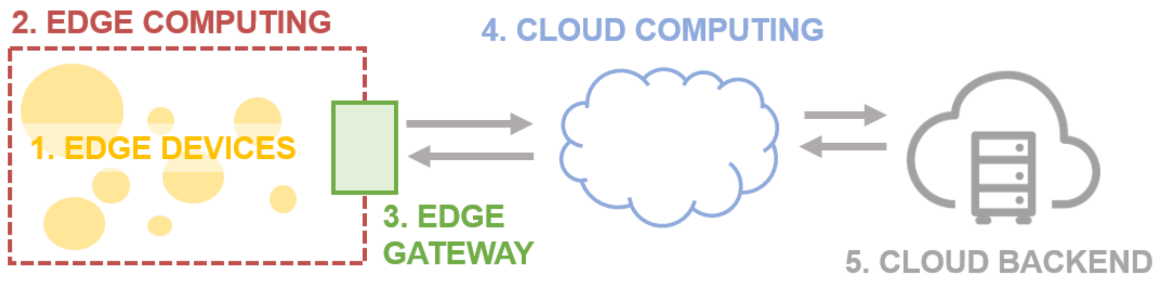


Figure 2. Basic Elements of a Household IoT architecture

1. **Edge Devices (IoT Devices):** It refers to the virtual and physical elements that integrate an IoT ecosystem. They can be very diverse, but their common features are the capacity of being identified and the ability to communicate with other devices. Moreover, they can also perform different tasks which will be detailed in further sections.

2. **Edge Computing (Fog Computing):** It refers to a distributed IT architecture, in which client data are collected, stored, exchanged and processed at the periphery of the network, but still close to the original source of the data. This allows the processing of time-sensitive data in almost real time, avoiding also the time lapse and costs derived from Cloud Computing.

3. **Edge Gateway:** It refers to the physical or virtual node that serves as the connection point between different Edge Devices, as well as between the IoT ecosystem and outsider networks. It provides system interoperability, communication and data-processing capabilities, among other features.

4. **Cloud Computing:** It refers to the use of remote services such as software, platforms or infrastructure, to store, process and retrieve data from an off-site location. In the IoT context it is generally used for historical analysis, big data analytics and long-term storage.

5. **Cloud Backend:** It refers to the server side on a Cloud Computing service where all the processes actually take place.

The present paper will be mainly focused on the study of the first three items (devices, fog and gateway) since these are the only elements that can be directly influenced by the final user actions. The remaining elements (cloud computing and backend) are mostly affected by the business partners involved in the IoT service but cannot be directly influenced by the final user actions, which is why even if they will be considered during the risks analysis, they will not be included among the assets that belong to the household IoT environment.

4.2. IoT Assets

There is not a standardized or official classification of IoTs items and features, which is why the current section presents an own blueprint that aims to gather the most relevant elements integrating an IoT architecture, keeping a simple but also a reliable approach.

Thus, the following classification has been based on two premises:

- To identify the main components integrating an IoT system, the following classification has been supported on the research carried out by Gartner (DeBeasi, 2018) and ENISA (ENISA, 2017), in addition to other complementary sources, such as IoT articles from DZone (Zhang, 2018) or from the Open Automation Software Company (OAS).

- To provide an easy aggregation of these components, the following classification has adopted the point of view of an IoT user, differentiating among the main devices that users associate to the main functions of each IoT, and other peripherical elements that provide complementary functionalities to the main device.

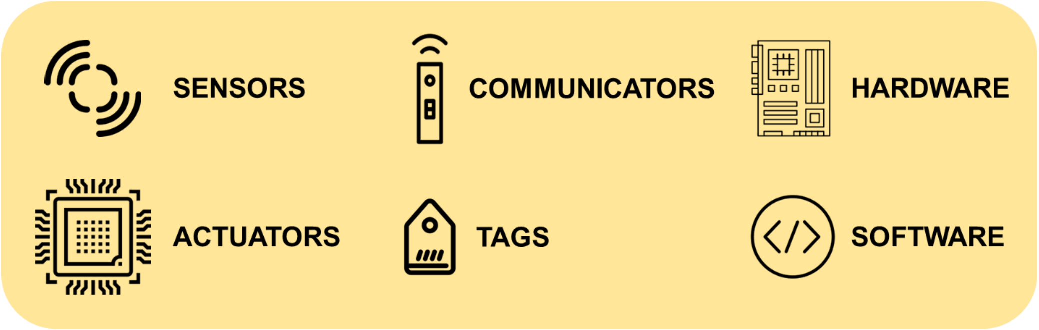


Figure 3. IoT Main Device Components

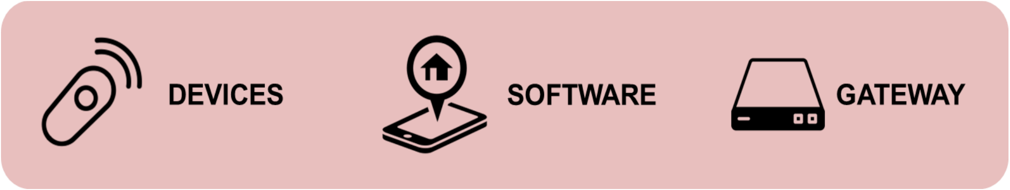


Figure 4. IoT Peripherical Elements

4.2.1. Main Devices

The Main Devices are embedded systems with a dedicated function within a larger mechanical or electrical system (Dulaney & Easttom, 2018) and constitute a physical interface to interact with the physical world, including users. For this reason, these are normally the objects that customers associate directly to the main function of a single IoT system, as it can be smart objects such as fridges, drones or thermostats.

Their technical design is directly submitted to their main function, which is why they are commonly based on a processing unit that enables them to process data on their own, providing real-time responses for the users, but their capacity of processing and storing data – among others – are also limited. Their main components are:

(*) Mandatory elements in an IoT device

(*) **Sensors** and/or **actuators**	The **sensors** are the subsystems whose purpose is to detect and/or measure events in their environment and send the information to other electronics in order to be processed. The type of data the sensors can gather are widely diverse, which is why trying to cover all of them is an almost unreachable task. However, on the section addressing the main functions of IoTs, are covered the most common examples. The **actuators** are the output units of IoT devices which execute decisions based on previously processed information, taking an electrical input and turning it into a physical action. That information is also commonly gathered by sensors and processed by electronics embedded on the same device than the actuator, guaranteeing almost real-time responses. Just like the sensors case, the type of responses produced by actuators are almost unlimited, even though some of the most common expressions will also be pointed out on the present paper.
(*) **Communicators**	They provide the ability to communicate with other devices.
(*) **Tags**	They provide identification to the device. The most common ones are: NFC, Barcode, UHF RFID, BLE and URL.
Hardware elements	They are the different physical components (except sensors and actuators) from which the IoT devices can be built. These include microcontrollers, microprocessors, the physical ports of the device, the motherboard, etc.
Software elements	They comprise the Operating System (OS) of the IoT device, its firmware and the programs and applications installed/running on the main device.

Table 1. IoTs Main Device Components

4.2.2. Peripherical Elements

The Peripherical Elements make reference to all the items that are designed to interact with the main device to display some of its elementary functions (e.g., managing the main device, activating the actuators) or that provide a complementary feature to the main device (e.g., allowing it to display new content). It is important to note that some of these elements can constitute a main device on their own, which is why they will share the components associated to those devices. One of the most remarkable features is that they generally provide user-friendly interface for the users to interact with the main device, allowing them to deploy the main function through the main device.

They are located on the Edge and the most common elements are:

Complementary devices	The main device can interact with other simple or complex devices, that can introduce core functions without which the main device would not be able to accomplish its main purpose, or that can simply introduce new or complementary features to the IoT system.
Complementary software	Likewise it happened with the complementary devices, there are software elements that can be associated to the main device by default, such as applications or web portals to ease the interaction with the users and the main device, but they can also provide extra features to the IoT system.
Gateway	The IoT Gateway is regularly a combination of both, physical and logical elements, that despite it does not belong directly with the main device or its peripherals, it can influence their behavior and interactions. It operates at an application level and provides features such as the following: - Interface features for different communication protocols, allowing devices and networks interoperability. - Networking features and hosting live data. - Data aggregation, pre-processing, cleansing, filtering and optimization. - Data caching, buffering, streaming and short-term data historian features. - Data visualization, basic data analytics and system diagnosis. - Network and user security management. - Device configuration management.

Table 2. Edge Support Devices

4.3. IoT Functions

The main function of any IoT could be summarized as gathering and processing inputs to provide certain outputs, more precisely, data, which is any information provided from or about the status of a device or its environment. This definition, however, is too vague, in special considering that some institutions, such as the European Parliament and the Council of the European Union, define processing as any operation performed on data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data (General Data Protection Regulation, 2016). For this reason, on the table below are summarized the most representative functions that can perform the main and peripherical devices that integrate the Edge.

Data collection	This function is carried out mainly by the sensors. They can detect changes in a physical or virtual level, such as the following: - **Physical changes:** Sound / Vibration, Vision / Light, Presence / Proximity, Temperature, Humidity / Moisture, Position / Tilt, Motion / Acceleration, Chemical / Biological / Gas, Force / Load / Pressure / Torque, Electric / Magnetic. - **Virtual changes:** Software, Network.
Data storing	The data gathered by the sensors or provided by other IoT elements can be stored temporarily or permanently at the edge and/or at the cloud.
Data analysis	The data gathered can be manipulated in order to obtain information that can be used by the IoT and provide a specific output in a timely manner. Common manipulations are the aggregation, organization, transformation or even deletion of data. This allows a faster and more efficient processing of the data gathered.
Data transmission	The data can be transmitted to peripherical elements using wired or wireless communication technologies. In the Annex II of this paper are summarized the most common communication protocols used in IoT communications.
Data display	The data gathered and processed allows the IoT actuators and interfaces to show or display specific behaviors, that can cause a physical and/or a digital impact.
Data Management	This concept comprises the ability of influencing data to take decisions over all the previous functions, as well as about aspects such as the purpose of the data processing, the access and security of this data, among other functional decisions.

Table 3. Functions of IoTs

4.4. IoT Risk Analysis

As it was mentioned in the previous section, the main function of any IoT could be summarized as gathering and processing inputs to provide certain outputs, or in other words, to process data.

The IoT assets studied so far can interact among them, as it is shown in the illustration below. This interaction allows for processing data and consequently accomplishing the functions the assets and the IoT in general have been designed for.

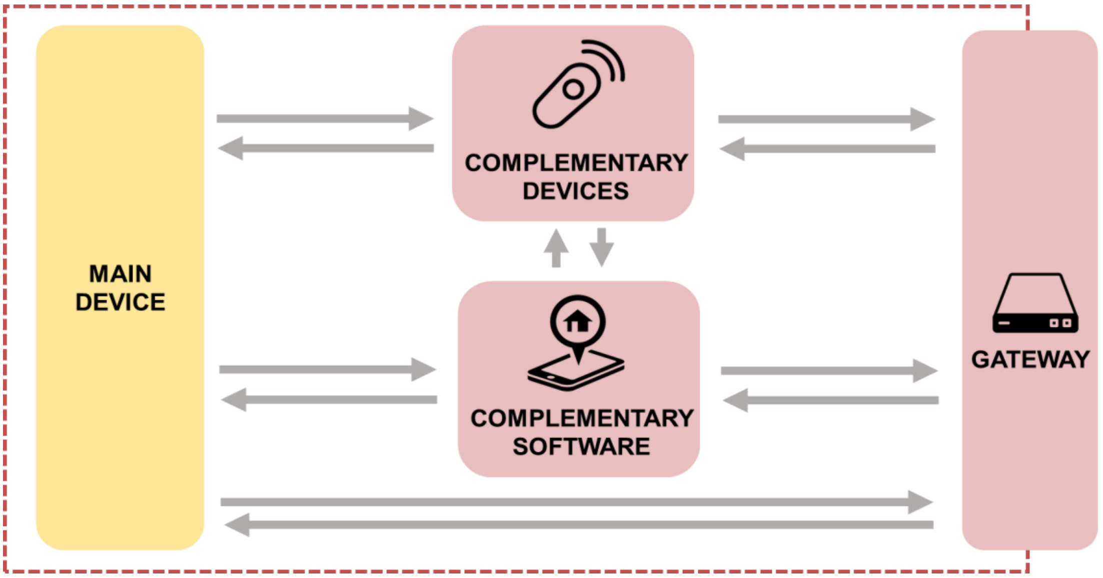


Figure 5. Data Processing at an IoT environment

Each of these assets and interactions can be exposed to internal or external threats, that taking advance of vulnerabilities can access to the IoT ecosystem, compromising part or even the whole security of it.

As it was previously mentioned, household environments are particularly sensitive to security threats, due to the lack of knowledge or resources their users possess regarding the identification, comprehension and confrontation of these threats.

Consequently, the development of a security methodology for this environment should be based on a risk analysis focused on the consequences perceived by the users in case of the materialization of any threat and the possible actions to be taken for their mitigation, and not on the nature of those threats.

5. IOT SECURITY METHODOLOGY FOR HOUSEHOLD ENVIRONMENTS

Throughout the research carried out about the context and state of the art regarding the Internet of Things, it has been observed that there are currently many security challenges in this field that still need to be tackled. One of the most significant challenges is the lack of security standards or methodologies to securitize IoT environments.

As a result, the present chapter will address this problematic, proposing a security solution that addresses it.

5.1. Focus of the Project

As it was already introduced, this project aims to define a security methodology that improves the security of IoT users. As it was also mentioned, the case of study will be focused on household IoTs, to understand the security flaws that these environments can have and give them the chance to securitize them. Moreover, this implementation can also be transposed afterwards to different environments, helping to identify and cover their security flaws.

Thus, in the following sections will be described the requirements that should be taken into account to afterwards conducting a risk analysis for household IoT environments, as well as the steps to efficiently identify and mitigate the identified risks. Finally, this proposal will also be evaluated presenting a scenario where this methodology can be applied, checking its suitability and its real ability to accomplish the purpose for which it has been created.

5.2. Identification of the Requirements

Along the previous chapters, there have been identified the particularities of IoT household environments, including the roles of the people interacting with them, their assets, functions and main security features.

All these aspects are presented and summarized just below.

	ASSET	SIGNIFICANT FEATURES
ENVIRONMENT	HOUSE	- Defined and reduced space. - There are normally no tech-specialized profiles within this environment, hindering the management of IoT security. - The most common connectivity technology is Wi-Fi. - Generally, the investment in digital and technical security is not high or specialized.
ROLES	USERS	- Low technical and threat management knowledge or comprehension. - Low influence on technical design and features. - Low access or resources for premium security solutions.
	PRODUCERS	- More interest on commercial features than security ones. - Lack of interest or knowledge about IoT security. - Lack of legislation, standards or guidelines for IoT security. - High price of commercial security solutions.
	INTRUDERS	- Benefited by the features of other roles. - Easy access to information and resources. - Ability to remain incognito.
TECHNOLOGIES	SENSORS	- Very diverse vendors, nature and features. - Normally, they cannot be directly manipulated by users.
	ACTUATORS	- Very diverse vendors, nature and features. - Normally, they cannot be directly manipulated by users.
	COMMUNICATORS	- Very diverse vendors, nature and features. - Normally, they cannot be directly manipulated by users. - They are normally the point of entry for remote attacks. - In case of being protected, normally are used low-investment solutions.

Table 4. Identification of the Requirements for the Security Methodology (I)

	ASSET	SIGNIFICANT FEATURES
TECHNOLOGIES	**TAGS**	- They cannot be easily manipulated by the users. - Some of them can be copied or even change their ID.
	HARDWARE ELEMENTS	- Very diverse vendors, nature and features - They are commonly identified by the users as 'The' IoT. - They provide the basic infrastructure that allows the device to perform its basic functions.
	SOFTWARE ELEMENTS	- Very diverse vendors, nature and features. - They provide the basic solutions that allow the device to perform its basic functions.
	COMPLEMENTARY DEVICES	- Very diverse vendors, nature and features. - They can provide core or support functionalities. - The generally act as the physical communication interface among the user and the device. - They are generally located a short distance away from the main device. - They increase the attack surface in the IoT ecosystem.
	COMPLEMENTARY SOFTWARE	- Very diverse vendors, nature and features. - They can provide core or support functionalities. - They generally provide the virtual communication interface among the user and the device. - They increase the attack surface in the IoT ecosystem. - They are generally based on platforms, infrastructures or solutions that scape to the knowledge and control of the user.

Table 5. Identification of the Requirements for the Security Methodology (II)

	ASSET	SIGNIFICANT FEATURES
TECHNOLOGIES	GATEWAY	- It allows to integrate management and security features to the IoT ecosystem. - They can also provide an interface for the user to analyze and control the IoT ecosystem. - It allows the interoperability and aggregation of devices and features. - It allows to integrate the functions of several devices in a unified platform. - It allows to control or reorganize data transmission and processing. - It allows to centralize the security of all the IoT assets.
FUNCTIONS	DATA COLLECTION	- Depending on the type of sensor and the features surrounding it, they can be physically accessed or manipulated.
	DATA STORING	- Depending on the type of sensor and the features surrounding it, they can be physically accessed or manipulated.
	DATA ANALYSIS	- It can be performed within the devices or the edge, or they can be performed remotely, on cloud or on-premise locations. - They can variate from very simple to very complex analysis.
	DATA TRANSMISSION	- It features and requirements can vary extensively, depending on the technologies and configurations settled for the transmission.
	DATA DISPLAY	- Depending on the type of actuator and the features surrounding it, they can be physically or virtually accessed or manipulated.
	DATA MANAGEMENT	- Depending on the design and configuration of the assets, the devices and their features can be (or not) easily managed by the users.

Table 6. Identification of the Requirements for the Security Methodology (III)

As it has been observed, the requirements to take into consideration are numerous and very diverse, what explains the current challenge of defining a common methodology to group and protocolize the steps for securitizing IoT environments.

Even if in this section are analyzed the specific requirements for a household adapted methodology, their nature is generic, and actually this classification could be easily transposed to any other context, where the difference would lie in the features of each asset, but not on their classification.

Thus, is precisely the just-shown requirements classification what will be used as the base to develop a security methodology which can be at the same time intuitive, coherent and complete, and that can also be adaptable for different situations or environments.

Thereby, in the following sections it will be laid out the development of a security methodology for IoT environments that will identify and evaluate all the assets and interactions integrating an IoT environment. It will mainly consist in a progressive analysis of each of the elements integrating the ecosystem and their functions, followed by a lineal association of possible risks and mitigations.

The following image is a simplified representation of the security proposal that will be explained in detail next:

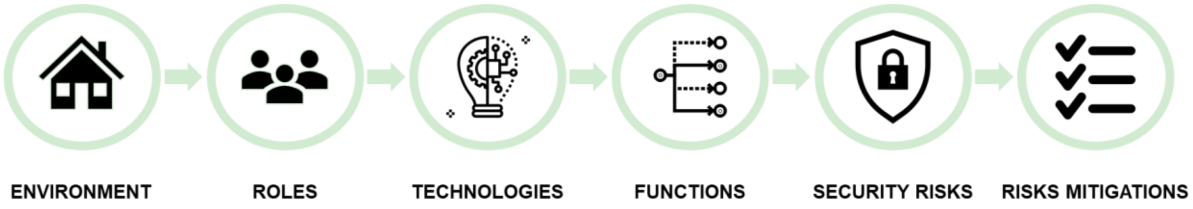


Figure 6. Graphic Representation of the Proposed Methodology

In the image, each circle represents each step of the methodology and the asset or feature that should be addressed at each point. Along the following section, each of these steps will be described in depth, indicating the factors that should be taken into consideration to properly tackle each of these phases and obtain the best outcomes out of them.

5.3. Additional considerations

While defining a new security methodology it is important not only to consider the requirements for its development, but also the requirements for presenting it to its target audience.

In the studied scenario, the present proposal could be especially interesting for two types of users: IoT devices producers and users.

IoT producers possess the technical knowledge, or at least the resources to get that knowledge, which is why the comprehension and implementation of the following methodology may not suppose a challenge for them. However, final users in general are not familiar with technical structures, which is why they may find a challenge to even identify the IoTs environment elements or IoT architecture, what would allow them to start with the subsequent security analysis. This limited comprehension or access to security resources could severely hinder the proper implementation of the security methodology, which is why, in this case, takes special relevance not only the procedures developed along it, but also the way of presenting it to its users.

Consequently, depending on the profiles implementing the methodology this should take two different approaches:

- When it is used by IoT producers, they should design and implement the risk analysis to decide which kind of features include or exclude from their products.
- When it is used by final IoT users, the risk analysis posed by the methodology should be facilitated by a technical expert party, leaving at their choice only the last step of the methodology, meaning the decision taking about the implementation of risks mitigations.

As a result, even though in both cases the procedure defined would be exactly the same, in the second case the described steps should be presented through a user-friendly interface, that manages itself the most technical-related steps and that allows the users to be informed, interact and decide about the IoT systems in a simple and intuitive manner. To address this perspective, in this project is also proposed a technical solution that would allow this presentation and implementation. It consists on the integration of a visual interface into a Gateway that can automatically scan the IoT elements of the Household ecosystem, accordingly to the presented methodology, and that would allow the user to take informed decisions based on its analysis.

5.4. Description of the methodology

5.4.1. FIRST STEP: Delimitation of the IoT environment

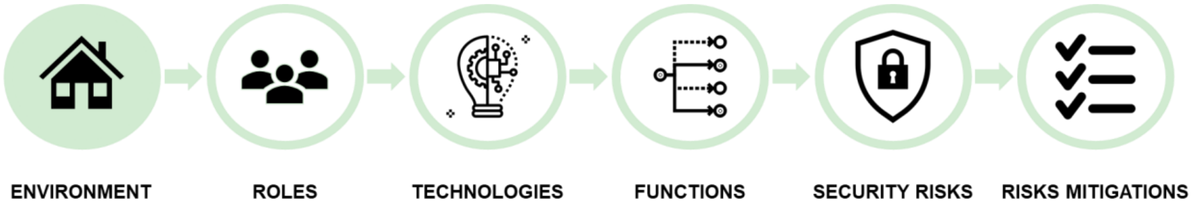


Figure 7. IoT Environment

The first step consists in the definition and delimitation of the physical and virtual space that will compose the IoT environment, also previously described as the Edge Computing for the IoT ecosystem.

More precisely, it will be necessary to consider the physical space where the IoT devices will be located (main and complementary ones), but also the area of influence of the communications among devices and their connections with external parties. On this purpose, it is important to list the elements present in the space but also to represent them graphically to better understand their connections and interactions.

The following figure shows an example of how this representation could look like, standing MD for Main Device, PE for Peripherical Elements, GW for Gateway, CL for the Cloud and the rows for the flow of data among all the elements. On a real implementation, each device should not be identified by a generic label, but by one that leads to no mistake about which element it is representing.

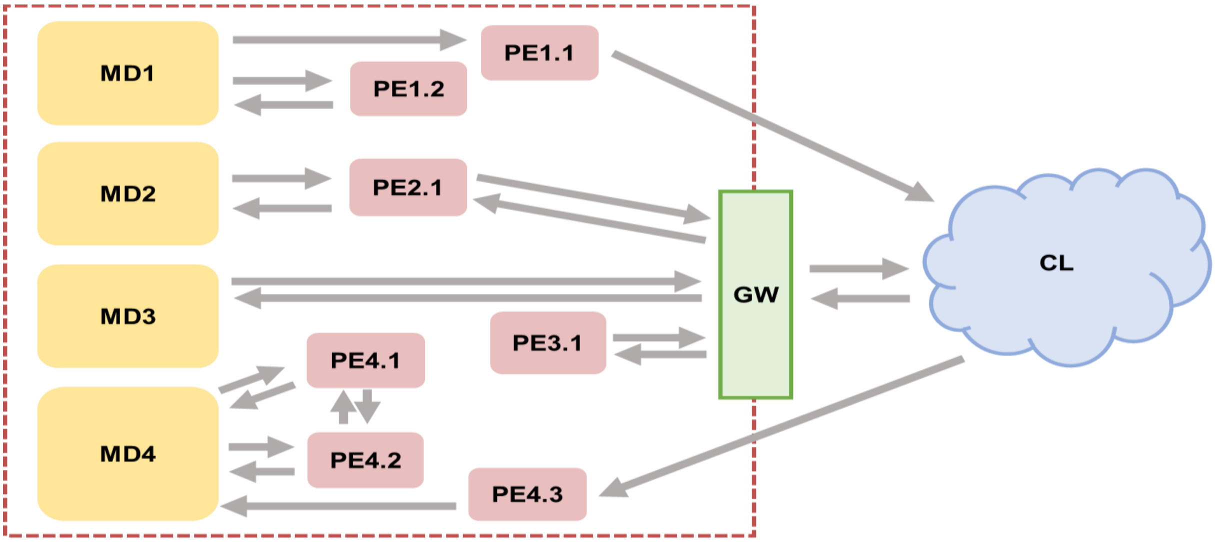


Figure 8. Example of Delimitation of the IoT Environment

5.4.2. SECOND STEP: Identification of the roles involved

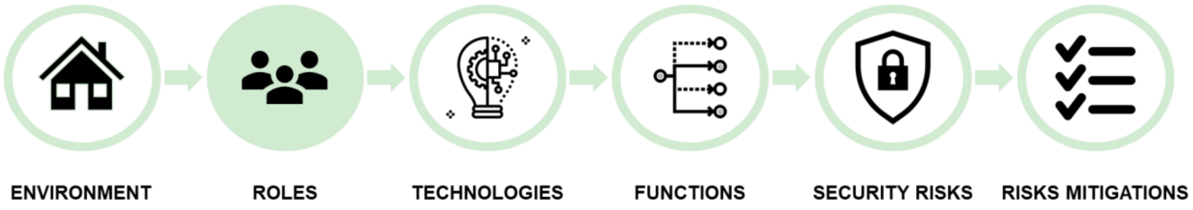


Figure 9. IoT Related Roles

The second step consists in the identification of all the roles that can interact or influence the IoT ecosystem. The role is a representation of one or several natural or legal people, that share some common particularities.

This classification is important to understand who can influence the security of the IoT ecosystem, either through the improvement of it or through the generation of risky situations. Therefore, depending on the focus of interest while implementing this methodology, it will be more or less interesting to also include certain level of granularity on the classification. This statement will be explained in detail right after the main classification of roles is presented.

The three basic roles that should be identified in any IoT environment are the following:

- **Providers:** It refers to all the authorized third parties that can influence on the design or features of the devices, as well as in the services that it provides and that are located out of the IoT physical environment. In this category can be grouped the suppliers, the producers and even the 'pre' and 'post' production service providers (for patching, updating, storing, analyzing or any other processing purposes).

- **Users:** It refers to the natural people who are intended to interact with the IoT system or device. They will be mostly located within the physical space of the IoT environment, even if they can also virtually interact with it through interfaces such as phone or web applications. They can have an active or passive interaction with the device.

- **Unauthorized third parties:** It refers to all the unintended natural or legal persons that can interact intentionally or accidentally with the IoT ecosystem, independently on where they are located.

Apart from the human roles, it is important to not forget about the **natural phenomena**, what stands for all the non-human events that can affect the security of an IoT environment, and that could also be aggregated as a different role itself.

As it has been previously mentioned, the main roles can also be subdivided into more specific categories, such as the ones mentioned as an example in the description of each role. To define the need of granularity is important to consider the following aspects:

- Who is implementing the methodology
- Which are the specific purposes of the implementation

To better understand the relevance of these two questions, just below are presented two scenarios where the proposed methodology would be used to securitize an IoT environment:

- *Scenario A*: A health company is designing a wearable IoT and wants to identify the security risks associated to the prototype of the product and its environment, to provide the best security guarantees to users and do the smartest choices while designing the product and its features.
- *Scenario B*: A consumer has just bought a smart vacuum cleaner and wants to know the security risks associated to it, as well as the possible mitigations for the identified risks.

Even though in both cases the proposed methodology has been used to securitize an IoT environment identifying its correspondent risks, there are significant differences. While in the second scenario is only relevant to identify possible risks and their available mitigations, in the first scenario is also important the source of these risks, originated by the actions or choices of specific roles.

Consequently, in the first scenario would be very important to bring to a lower level the definition of roles, to properly address each risk to its specific source and allowing the health company to take informed security decisions.

5.4.3. THIRD STEP: Identification of the technologies involved

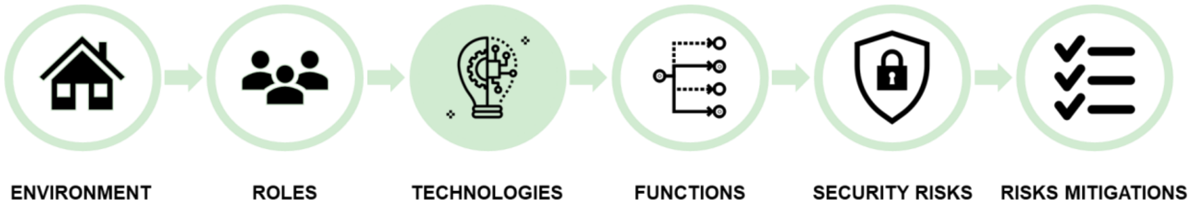


Figure 10. IoT Involved Technologies

The third step consists in the identification of all the technologies involved in the IoT ecosystem.

As it was previously studied in the section 4.2. of this paper, the main classification of IoT assets would be the following for each of the IoT systems analyzed:

- **Main Device:**
  - Sensors
  - Actuators
  - Communicators
  - Tags
  - Hardware
  - Software

- **Peripherical Elements:**
  - Complementary devices
  - Complementary software
  - Gateways

This identification and classification should be assigned to each of the IoT systems composing the IoT environment. The particularities of each of these elements have already been described in previous sections of this paper, which is why, they will not be repeated in the present section.

5.4.4. FOURTH STEP: Identification of the functions for each technology

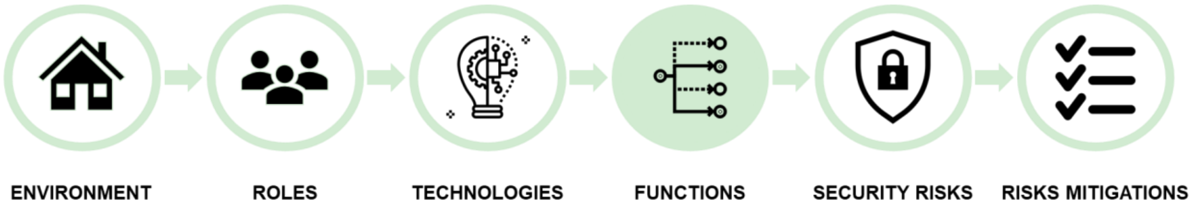


Figure 11. IoT Functions

The fourth step consists in the identification of all the functions that each of the previously identified technologies possess.

For this purpose, it is recommended to design a table, a tree diagram, or a similar structure, that allows to link each function to each of the identified technology, while it also provides a visual representation of where the most sensitive areas of the IoT can be located.

The section 4.3. of the present document provides a classification of IoT functions, which are the following:

- Data collection
- Data storing
- Data analysis
- Data transmission
- Data display
- Data Management

The features of each of these functions have also been described in detail in previous sections of this paper, which is why they will not be redefined in the current one.

5.4.5. FIFTH STEP: Identification of the security risks for each function

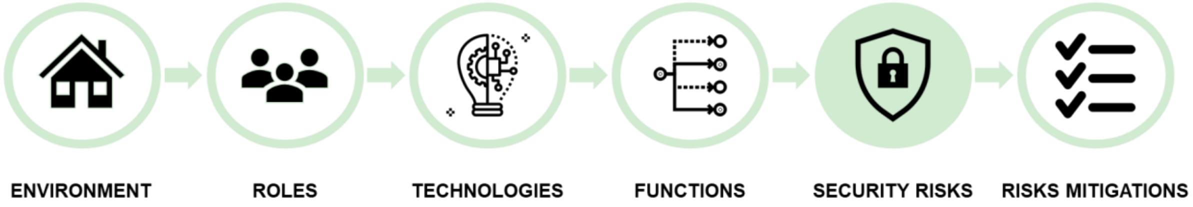


Figure 12. IoT Security Risks

The fifth step consists in the identification of security risks associated to each of the functions previously defined, as well as which of the studied roles can cause each risk

Consequently, at this point is necessary not to only identify the set of risks affecting the IoT environment, but also to correlate each of them with the roles identified in previous steps. It is suggested to continue with the representation chosen in the step 3 (table, chart, etc.), allowing an easy correlation between the function of each technology and its correspondent risk.

Regarding to the correlation of each risk with the role generating it, would be as simple as to include another section (column, brunch, etc.) in the chosen representation, where this role is indicated following the previous classification. The most common correlations would be the following:

ROLE	R/R ID	ORIGIN
Provider	**PR1**	Poor security design of the IoT architecture
	PR2	Misuse of data from this party
User	**UR1**	Poor choice of the security configurations or actions
	UR2	Misuse of the device or system

Table 7. Risks-Roles Correlation

As a consequence, unauthorized third parties or natural phenomena could intrude or affect the IoT systems endangering their confidentiality, integrity or availability and its related roles.

The identification of risks can be quite vast, and there is neither a standard classification or a specific catalog for IoT security risks that can be used as a base for this analysis. For this reason, in the present section has been developed a high-level classification of security risks that can affect IoT environments. Yet still not exhaustive, in conjunction with the rest of identified elements, it can provide a clear picture about the origin and impact of the security risks. Moreover, this classification could be complemented with Information

Security generic risks, which can be obtained from risks or threats catalogues such as the ENISA Threat Taxonomy (ENISA , 2016).

This classification risk classification is presented next:

FUNCTIONS	RISK ID	DEFINITION
Data Collection	**CR1**	The information is not collected or is not accurate
	CR2	Unauthorized information is collected
Data Storing	**SR1**	If the databases are not secured, the collected data can be accessed or tampered
	SR2	If there is no backup of the information, it can be lost
Data Analysis	**AR1**	If the software is tampered or misconfigured, the results of the data analysis could not be the intended ones
	AR2	If the data provided is not essential to carry out the main activity of the device, could be used for illegitimate purposes
	AR3	Depending on the data provided, could be used for profiling
Data Transmission	**TR1**	If someone is located in the transmission area, can eavesdrop or tamper the data collected or displayed
	TR2	If the transmission is not encrypted, it can be eavesdropped or tampered.
	TR3	If someone interferes the connection, can eavesdrop or tamper the data collected or displayed
Data Display	**DR1**	Legitimate information is not displayed
	DR2	Tampered information is displayed
Data Management	**MR1**	If there is no access control or it is inadequate, unauthorized users can access the device and its features.
	MR2	If there is no authentication control or it is inadequate, unauthorized users can impersonate legitimate ones.
	MR3	If there are no lost access procedures, or they are inadequate, legitimate users could lose access to the services provided
	MR4	If there are no update measures or they are inadequate, security vulnerabilities could not be patched
	MR5	If the password policies are not strong enough, unauthorized users can impersonate legitimate ones.
	MR6	If the application has not been securely developed, data can be accessed or tampered

Table 8. Risks-Functions Correlation

5.4.6. SIXTH STEP: Identification of mitigations for each risk

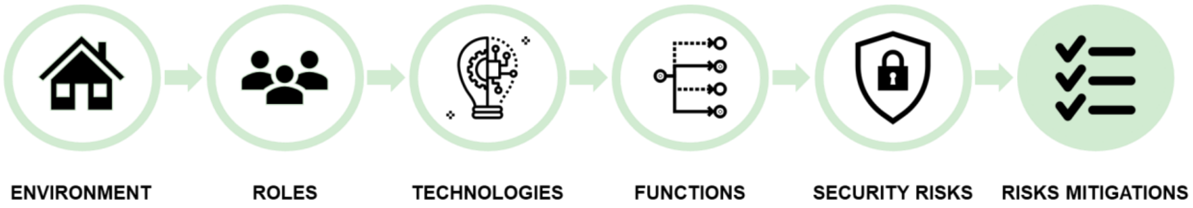


Figure 13. IoT Risks Mitigations

The sixth step consists in the identification of mitigations that can be implemented to reduce or even eliminate the risks associated to the functions of each technology that composes the IoT ecosystem, as well as which of the studied roles can mitigate that risk.

Consequently, as in the previous step, it is necessary to identify the set of mitigations for each identified risk, and to correlate it with the role that can implement the suggested mitigation. Likewise in the previous step, it is suggested to continue with the representation chosen in the step 3 (table, chart, etc.) and proceed like it is described during step 5.

Regarding to the correlation of each mitigation with the role generating it, the most common correlations would be the following:

ROLE	R/M ID	MITIGATION
Provider	**PM1**	Can only be implemented by design and before the IoT is distributed
	PM2	Can be implemented remotely and once the IoT is already operating
User	**UM1**	Can alter the security configurations of the IoT to mitigate the risk
	UM2	Cannot mitigate the risk, meaning that it is necessary to decide whether accepting the risk or rejecting the use of the IoT

Table 9. Mitigations-Roles Correlation

In the same way that it happened in the previous step, the identification of security mitigations is also too broad to be tackled in the present project, which is why in the following table are only represented the main identified mitigations for the previously described risks. Moreover, the technical implementation of each of these mitigations will also depend on the choice of the implementor and the available resources for this purpose.

However, the following list can be used as a base for future studies, where it can also be completed and updated accordingly to the evolution of the currently studied IoT field.

FUNCTIONS	RISK ID	MIT. ID	MITIGATION DESCRIPTION
Data Collection	**CR1**	**CM1.1**	To include an informing feature when the information is properly collected
		CM1.2	To include integrity solutions, such as hashing or certificates
	CR2	**CM2**	To include an information-restricted configuration, attending to the principle of *Need-to-know.*
Data Storing	**SR1**	**SM1**	If the storing service is outsourced, only use trusted vendors and solutions
	SR2	**SM2**	To define backup solutions or infrastructures
Data Analysis	**AR1**	**AM1**	To require and provide only the essential information to carry out the expected service.
	AR2	**AM2**	To require and provide only the essential information to carry out the expected service.
	AR3	**AM3**	To require and provide only the essential information to carry out the expected service.
Data Transmission	**TR1**	**TM1.1**	To monitor all the connections stablished
		TM1.2	To activate diode functionalities (only entrance/only release)
	TR2	**TM2.1**	To enable and use secure transmission protocols
		TM2.2	To include integrity solutions, such as hashing or certificates
	TR3	**TM3.1**	To monitor all the connections stablished
		TM3.2	To enable and use secure transmission protocols
		TM3.3	To close unused ports
		TM3.4	To activate diode functionalities (only entrance/only release)
Data Display	**DR1**	**DM1**	To include an informing feature when the information is displayed, or it fails to be displayed
	DR2	**DM2**	To include integrity solutions, such as hashing or certificates
Data Management	**MR1**	**MM1.1**	To include access control features
		MM1.2	To use the principle of Need-to-know
	MR2	**MM2.1**	To provide solid authentication control features
		MM2.2	To use hardened passwords, codes or methods of authentication to avoid impersonation based on easy-to-access private data of the user
	MR3	**MM3.1**	To use hardened lost access procedures control
		MM3.2	To avoid the use of unreasonable requirements for access control in non-critical cases, that would lead the user to easily lose or forget the access credentials
	MR4	**MM4.1**	To provide means of update for devices and services
		MM4.2	To verify the software keeps updated with the last released versions
	MR5	**MM5.1**	To guarantee hardened password policies
		MM5.2	To avoid unsecure practices such as the re-use of passwords or the use of data easy to guess or to obtain
	MR6	**MM6.1**	To guarantee S-SDLC practices
		MM6.2	To only use applications and devices provided by trusted vendors

Table 10. Risks-Mitigations Correlation

5.5. Evaluation of the Methodology

In the present section it is represented a realistic scenario of a Household IoT ecosystem where the methodology developed can be tested.

5.5.1. FIRST STEP: Delimitation of the IoT environment

The present environment will integrate 3 IoT Devices: A Smart Toy from the brand CloudPets, a Chromecast and a Wireless Baby Monitor from the brand Arlo.

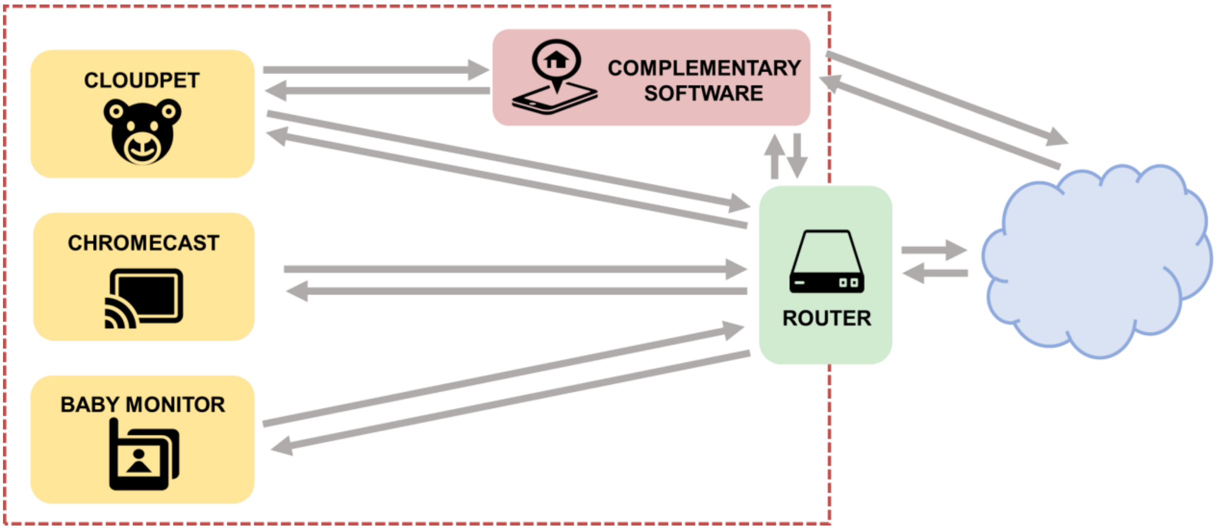


Figure 14. Household IoT Security Architecture Blueprint

5.5.2. SECOND STEP: Identification of the roles involved

The scenario will be composed by a family of three members: two parents and a baby. Consequently, the roles classification would attend to the following one:

ROLE	ID	DETAILS
Providers	**P1**	Companies involved: Spiral Toys, mReady and Linode. (CloudPet)
	P2	Google (Chromecast)
	P3	Arlo (Baby Monitor)
Users	**U1**	Parents (Active security users)
	U2	Baby (Passive security user)

Table 11. Example of Roles Identification

5.5.3. THIRD STEP: Identification of the technologies involved

At this step, should be identified the technologies involved in each of the IoT elements. To carry out a reliable evaluation, it has been conducted some research to identify the main features of the proposed devices on the following sources:

- CloudPets: Troy Hunt blog (Hunt, 2017) and CONTEXTIS (Stone, 2017)
- Chromecast: Google store (Chromecast)
- Arlo Baby Monitor: Corporate webpage (Arlo Baby)

The resulting classification would be the following one:

DEVICE	MAIN ASSETS	RELEVANT TECHNOLOGIES
Cloudpet	Main Device	· Sensor/Actuator: Sound Processor · Communicator: Bluetooth LE, Wi-Fi · Hardware/Software: Basic
	Peripherical Elements	· Complementary Software: Mobile App
Chromecast	Main Device	· Communicator: Wi-Fi · Hardware/Software: Basic
Arlo Baby Monitor	Main Device	· Sensors: Video-camera, microphone, motion sensor · Actuator: Speaker, LED · Communicator: Wi-Fi · Hardware/Software: Basic
	Peripherical Elements	· Complementary Software: Mobile App, Web browsers

Table 12. Example of Technologies Identification

5.5.4. FOURTH STEP: Identification of the functions of each technology involved

With the aim of simplifying the present analysis, in this case will be suppressed some elements that in this example have no risks associated, such as the LED technologies or the Basic Software and Hardware elements.

The resulting classification would be the following one:

DEVICE	ASSETS	TECHNOLOGIES	FUNCTIONS
Cloudpet	Main Device	Sound Processor	Data Display
		Bluetooth LE	Data Transmission
		Wi-Fi	Data Transmission
	Peripherical Elements	Web App	Data Analysis[1]
			Data Storing[1]
		Mobile App	Data Management
			Data Collection
			Data Display
Chromecast	Main Device	Wi-Fi	Data Transmission
	Peripherical Elements	Mobile App	Data Management
			Data Collection
			Data Display
Arlo Baby Monitor	Main Device	Video-Camera	Data Collection
		Microphone	Data Collection
		Wi-Fi	Data Transmission
	Peripherical Elements	Mobile App	Data Analysis[1]
			Data Storing[1]
			Data Management
			Data Collection
			Data Display

Table 13. Example of Functions Identification

[1] The Data Storing is actually conducted by cloud or on-premise servers, but it the App acts as an interface for this process.

5.5.5. FIFTH STEP: Identification of the security risks for each function

The resulting classification would be the following one:

DEVICE	ASSETS	TECHS.	FUNCTIONS	RISKS	ROLES
Cloudpet	Main Device	Sound Processor	D. Display	**DR2**	**PR1**
		Bluetooth LE	D. Transmission	**TR1, TR2, TR3**	**PR1, UR2**
		Wi-Fi	D. Transmission	**TR2, TR3**	**PR1, UR1, UR2**
	Peripherical Elements	Web App	D. Analysis	**AR2**	**PR1, PR2**
			D. Storing	**SR1**	**PR1**
			D. Management	**MR1, MR4, MR6**	**PR1**
				MR2	**UR1**
				MR5	**PR1, UR1**
		Mobile App	D. Management	**MR1, MR4, MR6**	**PR1**
				MR2	**UR1**
				MR5	**PR1, UR1**
			D. Collection	**CR2**	**PR1, UR1, UR2**
			D. Display	**DR2**	**PR1**
Chromecast	Main Device	Wi-Fi	D. Transmission	**TR2, TR3**	**PR1, UR1, UR2**
	Peripherical Elements	Mobile App	D. Management	**MR2**	**UR1**
				MR6	**PR1**
			D. Collection	**CR2**	**PR1**
			D. Display	**DR2**	**UR1**
Arlo Baby Monitor	Main Device	Camera	D. Collection	**CR2**	**UR1**
		Microphone	D. Collection	**CR1**	**UR1**
		Wi-Fi	D. Transmission	**TR3**	**UR1, UR2**
	Peripherical Elements	Mobile App	D. Management	**MR2**	**UR1**
				MR6	**PR1**
			D. Collection	**CR2**	**PR1**
			D. Display	**DR2**	**UR1**

Table 14. Example of Risks Identification

5.5.6. SIXTH STEP: Identification of mitigations for each risk

In this last step are shown the mitigations defined for each of the identified risks, as well as the roles which can implement this mitigation, following the defined model:

RISKS ID	MIT. ID	IDENTIFIED MITIGATION	ROLES
CR2	**CM2**	To include an information-restricted configuration, attending to the principle of *Need-to-know.*	**PM1, PM2, UM1**
SR1	**SM1**	If the storing service is outsourced, only use trusted vendors and solutions	**PM1, PM2, UM1**
AR2	**AM2**	To require and provide only the essential information to carry out the expected service.	**PM1, PM2, UM1**
TR1	**TM1.1**	To monitor all the connections stablished	**UM1**
	TM1.2	To activate diode functionalities (only entrance/only release)	**PM1, PM2, UM1**
TR2	**TM2.1**	To enable and use secure transmission protocols	**PM1, UM1**
	TM2.2	To include integrity solutions, such as hashing or certificates	**PM1, PM2**
TR3	**TM3.1**	To monitor all the connections stablished	**UM1**
	TM3.2	To enable and use secure transmission protocols	**PM1, PM2, UM1**
	TM3.3	To close unused ports	**PM2, UM1**
	TM3.4	To activate diode functionalities (only entrance/only release)	**PM1, PM2, UM1**
DR2	**DM2**	To include integrity solutions, such as hashing or certificates	**PM1, PM2**
MR1	**MM1.1**	To include access control features	**PM1, PM2**
	MM1.2	To use the principle of Need-to-know	**PM2**
MR2	**MM2.1**	To provide solid authentication control features	**PM1, PM2**
	MM2.2	To use hardened passwords, codes or methods of authentication to avoid impersonation based on easy-to-access private data of the user	**PM2, UM1**
MR4	**MM4.1**	To provide means of update for devices and services	**PM1**
	MM4.2	To verify the software keeps updated with the last released versions	**PM1, PM2, UM1**
MR5	**MM5.1**	To guarantee hardened password policies	**PM1, PM2**
	MM5.2	To avoid unsecure practices such as the re-use of passwords or the use of data easy to guess or to obtain	**PM2, UM1**
MR6	**MM6.1**	To guarantee S-SDLC practices	**PM1, PM2**
	MM6.2	To only use applications and devices provided by trusted vendors	**PM1, UM2**

Table 15. Example Mitigations Identification

5.6. Presentation of the results

After the whole security methodology has been put into practice and the security analysis has been carried out by security professionals, it is essential to keep in mind which will be the target audience of its results.

In the case of an information security expert, this whole analysis can be conducted simply by following the previously mentioned steps. However, if the analysis is expected to be presented to or conducted by a user with limited technical or information security knowledge, its implementation should be eased by an automatic analysis tool which can present its requirements and steps in a simple and user-friendly manner.

Complementary to the methodology development, in this paper is suggested to take advantage of the versatile nature and abilities of domestic gateways to integrate in them the two main keys of the present development, which means:

- **An automatic implementation of the methodology:** The properties of domestic gateways allow the integration of all the technological features needed to carry out an automatic 'autosensing' of the IoT ecosystem, identifying automatically the technologies, functions and risks involved on it. It also has the ability of not only analyzing, but also influencing on the IoT ecosystem, being able to modify their security configurations.

- **Provide a user-friendly interface to manage the IoT ecosystem**: It is also possible to integrate a screen into the gateway that would allow the system to present the information gathered in a simple and comprehensive way for the user. This would allow users to manipulate configurations and harden their IoT systems, whenever this would be possible. As well, in the cases that scape to the user control, it would at least inform them about the risks they may be taking in a simple language, allowing them to take informed decisions about their choices of consuming or not certain IoT products.

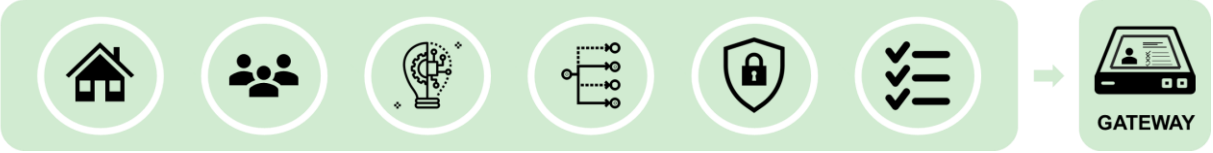


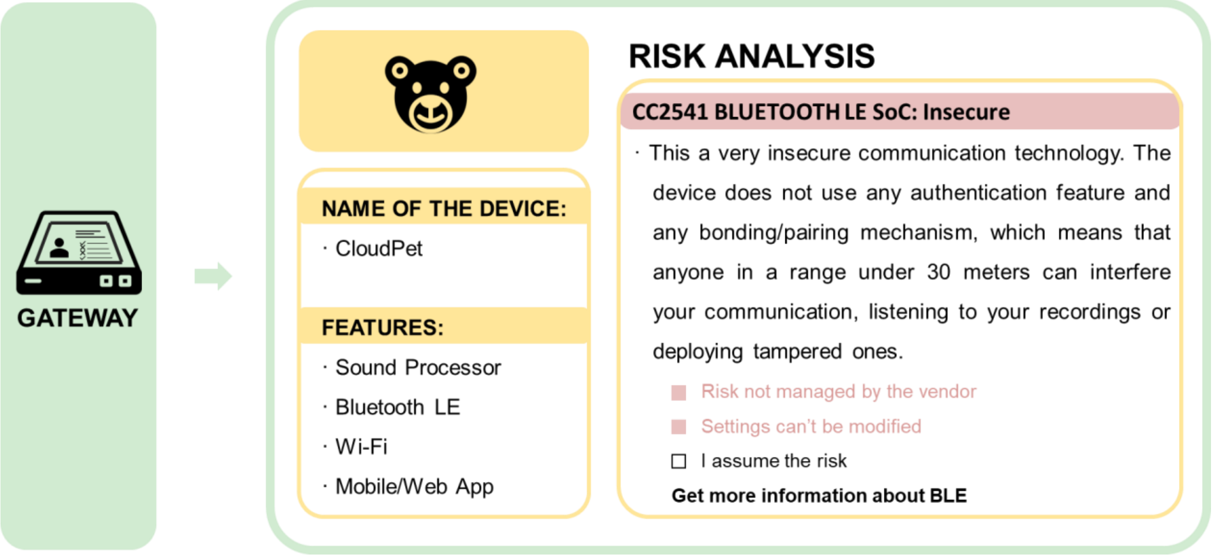
Figure 15. IoT Methodology Integration Gateway

Consequently, all the analysis carried out during the evaluation of the methodology could be presented to the legitimate user through a screen integrated in the gateway hardware or even in an app specifically designed for this purpose.

The chosen interface would be used to display all the previously collected and analyzed information in a simple and understandable way. The outcome of the whole application of the methodology should be the following:

- Display of the identified IoTs, their features and functions.
- Display of the associated risks with a checkbox that indicates:
  - Risk mitigated by the vendor (e.g., if it has a certificate or if security practices have been identified to mitigate the specific risk).
  - Risk that can be mitigated by the user (e.g., changing the configuration settings or deciding to filter the information through the gateway).
  - Risk that is assumed by the user (e.g., when the risk cannot be evaluated or mitigated by any of the previous parties, but the user has been informed about it).

In the presented case, the users with an active interaction with the IoT assets would be benefited by this analysis by easily identifying the security flaws of one of the IoT devices (The CloudPets) in comparison with another similar one from a more reliable source (Arlo Baby Monitor).



· This a very insecure communication technology. The device does not use any authentication feature and any bonding/pairing mechanism, which means that anyone in a range under 30 meters can interfere your communication, listening to your recordings or deploying tampered ones.

■ Risk not managed by the vendor
■ Settings can't be modified
☐ I assume the risk

Get more information about BLE

Figure 16. Example of Risk Analysis Feedback for CloudPets BLE Feature

6. CONCLUSIONS

Along the present paper have been studied the features and particularities of IoT environments, their components, related agents and interactions. After this deep search, all these concepts have been gathered, restructured and completed to define an outcoming security methodology that could be implemented in any IoT environment with the purpose of securitizing it. The methodology implementation was also tested in a realistic environment, leading to the following main conclusions:

- The main goal of the project, developing a methodology that allows to securitize IoT environments, has been completely achieved. The proposed methodology gathers all the key aspects that should be considered while identifying security risks in IoT environments and also provides practical solutions to mitigate those risks.

- The stemmed goal of developing a methodology with a generic approach has also been achieved, allowing the proposed methodology to be used to securitize very diverse IoT environments. Actually, concerning this approach, it is important to note that to keep its flexibility, the methodology has been developed at a very high level, indicating at the last step which mitigations should be implemented, but not the technical specifications for these implementations. Consequently, meanwhile this methodology covers up the goals of the present project, it could be interesting to bring to a lower level some specifications, to be able to identify more specific security measures depending on the type of IoT environment which is object of examination.

Regarding the specific goals defined from the main ones, could also be extracted the following conclusions:

- It has been satisfactorily achieved the specific goal of identifying reliable sources in which to base the development of the project. This point was especially challenging, due to the great amount of inaccurate or just-published material that can be found regarding the IoT topic. The effort of remaining informed and updated has also been considerable, but the outcomes can be appreciated on the contents displayed and also in on the recent dates of publication of several bibliography references.

- The achievement of the structure and relations definition goal, has been considerably satisfactory. The structure of IoT architectures is presented in a very simple and clear way and all its elements and interactions have been presented in a very simplified, but still precise way. On the other hand, related to the already mentioned high-level approach for some definitions, this point would still accept more level of concretion, however, this has not been set up as one of the priorities for the present development.

- Similarly to the previous point, the main functions of IoT technologies have been satisfactorily identified and explained, nevertheless it could be interesting to consider further ampliations in other projects that would bring more detail to all the studied elements.

- As it was outlined in the definition of the specific goals for this project, in case of not counting with an official list of security risks directly associated to IoTs, it should be defined an *ad hoc* one that could be included in the proposed methodology development here presented; this goal has also been achieved. The intended list has been developed and included, preserving the high-level approach in accordance to the general focus of the paper. The list provided however, is not intended to be taken as a static reference that should not be altered. Actually, to preserve its utility, it will be necessary to keep this list 'alive', including updates and ampliations, accordingly to the evolution of the sector.

- The goal of defining security mitigations that improve the security of IoT users, has also been achieved. Regarding their implementation, they have not been defined at a technical low-level, which allows the users to decide through which configurations or resources will be wanted to concrete the measure.

- Finally, it has been checked that this methodology can be used in a very specific IoT environment as it is a household one, providing effective measures that security effectively the risks identified along the application of the proposed methodology. Moreover, considering its structure and features it seems to owe the ability to be adapted to other different IoT environments.

Apart from the consecution of the generic and specific goals defined at the beginning of this project, there are some other aspects which are interesting to point out:

- This project has done an intense research and effort to provide simple but still accurate solutions. However, its generic features may also hinder the identification of very specific risks; e.g.: through it a user/provider can identify that the application has not been securely developed, however, it is not possible to identify the specific source of this unsecure development. As a consequence, it is remarked along the paper that it would be really interesting to go a step further, starting from this first development and concreting in more detail each of the resources defined along the present development.

- The development of this methodology has not been left only at a theoretical level, and considering the difference of knowledge, skills and resources among the different agents that can interact or influence in the IoT system, it has been suggested a practical example of how a technical tool can gather and implement automatically this security methodology in any kind of environment and managed by every kind of user.

7. FUTURE LINES OF WORK

Along the development of this project and as a conclusion for it, there have been identified possible and interesting future lines of work which are presented next:

- The possibility of complete and bring to a low-level of detail the presented development, with the purpose of providing a higher level of accuracy while identifying risks and mitigations.

- To develop a commercial solution based on the proposed methodology, such as the mentioned gateway, that would allow users to easily identify the security risks that they are exposing themselves to in an IoT environment. Such a resource, would not only help to prevent or mitigate active risks, but also to spread a security information culture among the most vulnerable agents (users). Moreover, this solution could also be presented as a business solution that would allow providers of IoT solutions to identify and correct their risk sources before deploying their solutions, preventing them from great money losses as a consequence of fines or reputation damages, among others.

8. BIBLIOGRAPHY

Ashton, K. (2009). That 'Internet of Things' Thing. *RFID Journal*. Retrieved from http://www.rfidjournal.com/articles/view?4986

DeBeasi, P. (2018, April 26). *Architect IoT Using the Gartner Reference.* Gartner. Retrieved from Gartner.

Dulaney, E., & Easttom, C. (2018). Host, Data and Application Security. In E. Dulaney, & C. Easttom, *Study Guide for CompTIA Security* + (p. 214). Indiana: John Wiley & Sons.

ENISA. (2017, November 20). *Baseline Security Recommendations for IoT.* Retrieved from ENISA: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Evans, D. (2011, April). *The Internet of Things. How the Next Evolution of the Internet is Changing Everything.* Retrieved from CISCO: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Gartner. (2017). *Leading the IoT. Gartner Insights on How to Lead in a Connected World.* Retrieved from Gartner: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

IIC. (2016). *Industrial Internet of Things Volume G4: Security Framework.* Retrieved from IIC: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

IIC. (2017). *The Industrial Internet of Things Volume G1: Reference Architecture.* Retrieved from IIC: https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf

Liptack, A. (2017, January 7). *Amazon's Alexa started ordering people dollhouses after hearing its name on TV.* Retrieved from The Verge: https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse

Nelson, P. (2016, December 6). *Just one autonomous car will use 4,000 GB of data/day.* Retrieved from Network World:

https://www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html

NISTIR. (2018, February). *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT).* Retrieved from NIST: https://csrc.nist.gov/publications/detail/nistir/8200/draft

OAS. (n.d.). *What is an IoT Gateway?* Retrieved from Open Automation Software: https://openautomationsoftware.com/blog/what-is-an-iot-gateway/

OWASP. (2015, November 29). *IoT Attack Surface Areas.* Retrieved from OWASP: https://www.owasp.org/index.php/IoT_Attack_Surface_Areas

OWASP. (2017, February 14). *IoT Security Guidance.* Retrieved from OWASP: https://www.owasp.org/index.php/IoT_Security_Guidance

OWASP. (n.d.). *Internet of Things Project.* Retrieved from OWASP: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

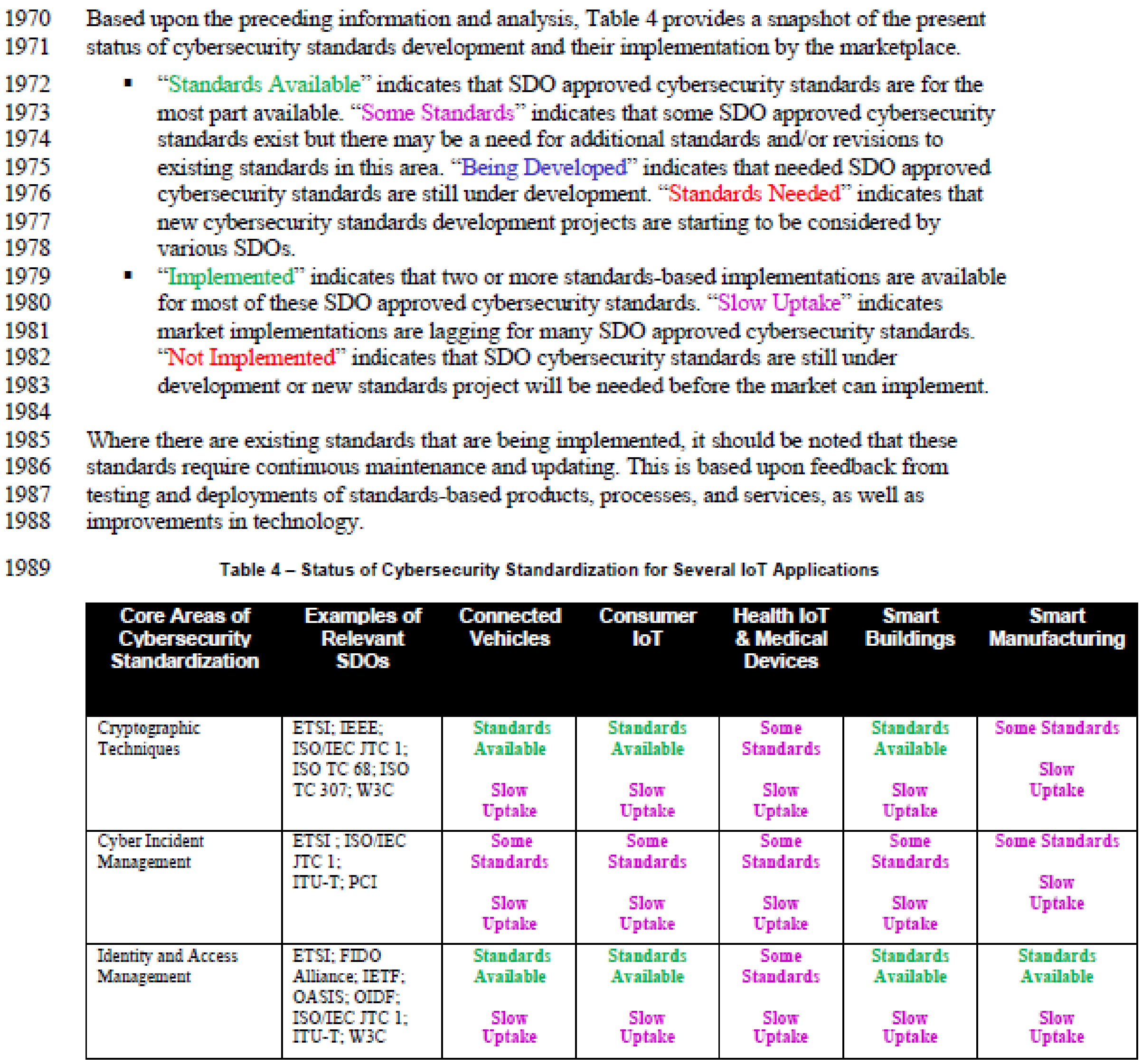
The European Parliament and the Council of the European Union. (2016, April 27). *General Data Protection Regulation.* Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Willson, S. (2018, May 29). *What the Internet of Things Is Missing.* Retrieved from DZone: https://dzone.com/articles/what-the-internet-of-things-is-missing?utm_medium=feed&utm_source=feedpress.me&utm_campaign=Feed:%20dzone%2Fiot

Wolfson, S. (2018, May 24). *Amazon's Alexa recorded private conversation and sent it to random contact.* Retrieved from The Guardian: https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation

Zhang, L. (2018, June 15). *The Building Blocks of an IoT Architecture.* Retrieved from DZone: https://dzone.com/articles/the-building-blocks-of-an-iot-architecture

9. ANNEX I: STATUS OF INTERNATIONAL CYBERSECURITY STANDARDIZATION FOR IOTS (NISTIR, 2018)



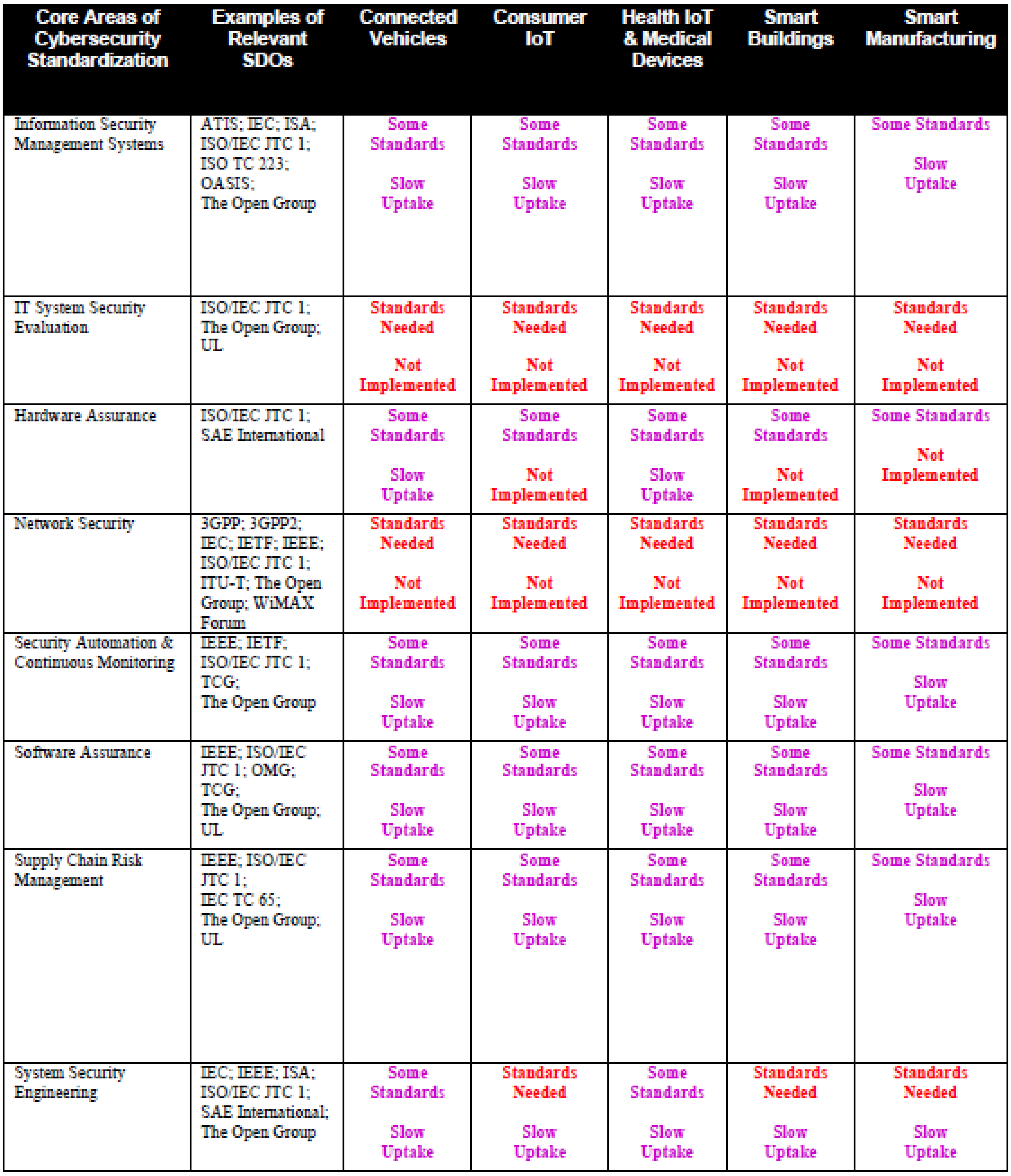
Based upon the preceding information and analysis, Table 4 provides a snapshot of the present status of cybersecurity standards development and their implementation by the marketplace.

- "Standards Available" indicates that SDO approved cybersecurity standards are for the most part available. "Some Standards" indicates that some SDO approved cybersecurity standards exist but there may be a need for additional standards and/or revisions to existing standards in this area. "Being Developed" indicates that needed SDO approved cybersecurity standards are still under development. "Standards Needed" indicates that new cybersecurity standards development projects are starting to be considered by various SDOs.
- "Implemented" indicates that two or more standards-based implementations are available for most of these SDO approved cybersecurity standards. "Slow Uptake" indicates market implementations are lagging for many SDO approved cybersecurity standards. "Not Implemented" indicates that SDO cybersecurity standards are still under development or new standards project will be needed before the market can implement.

Where there are existing standards that are being implemented, it should be noted that these standards require continuous maintenance and updating. This is based upon feedback from testing and deployments of standards-based products, processes, and services, as well as improvements in technology.

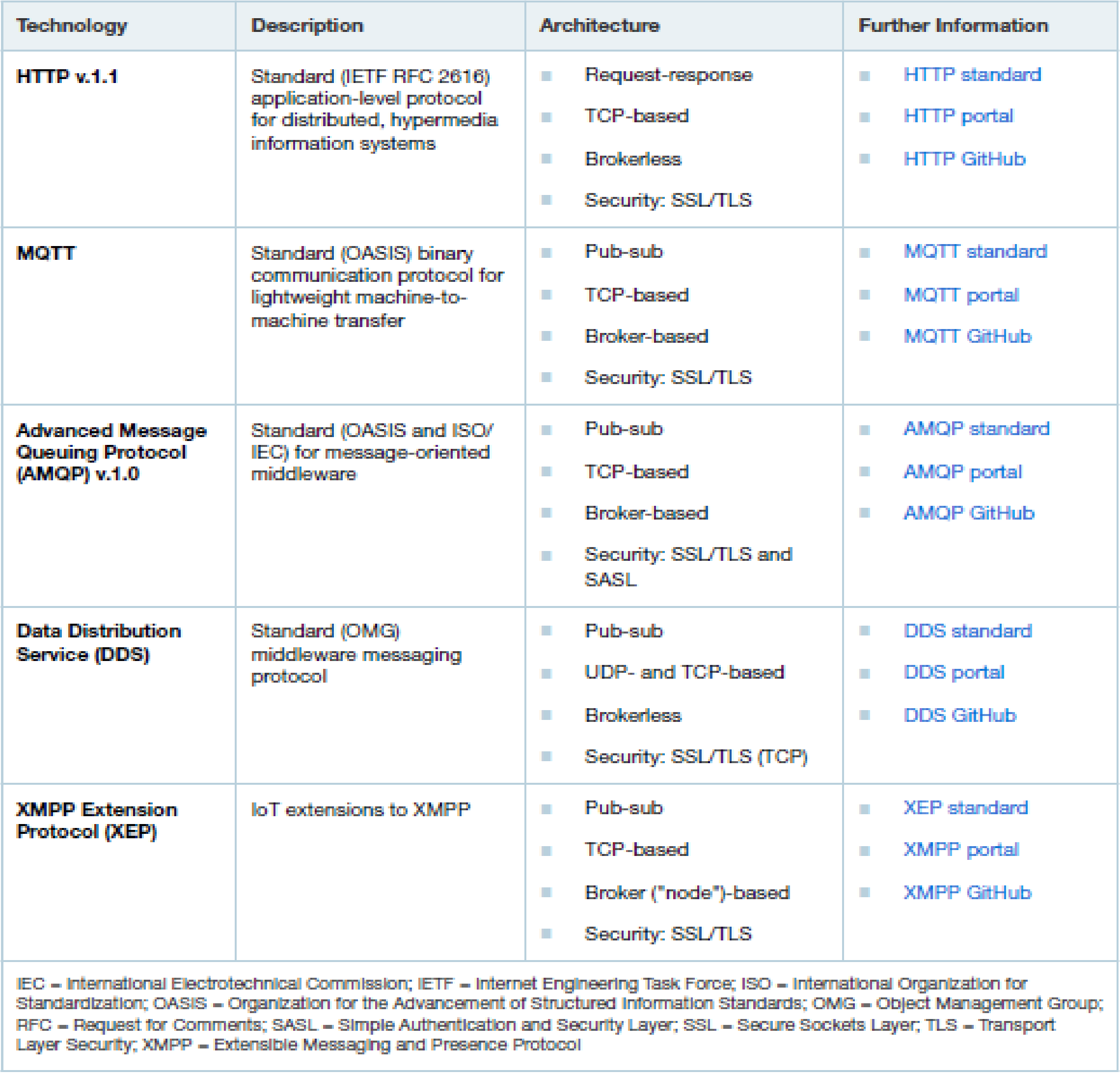
Table 4 – Status of Cybersecurity Standardization for Several IoT Applications

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Cryptographic Techniques	ETSI; IEEE; ISO/IEC JTC 1; ISO TC 68; ISO TC 307; W3C	Standards Available Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake
Cyber Incident Management	ETSI ; ISO/IEC JTC 1; ITU-T; PCI	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Identity and Access Management	ETSI; FIDO Alliance; IETF; OASIS; OIDF; ISO/IEC JTC 1; ITU-T; W3C	Standards Available Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake	Standards Available Slow Uptake	Standards Available Slow Uptake



Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Information Security Management Systems	ATIS; IEC; ISA; ISO/IEC JTC 1; ISO TC 223; OASIS; The Open Group	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
IT System Security Evaluation	ISO/IEC JTC 1; The Open Group; UL	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented
Hardware Assurance	ISO/IEC JTC 1; SAE International	Some Standards Slow Uptake	Some Standards Not Implemented	Some Standards Slow Uptake	Some Standards Not Implemented	Some Standards Not Implemented
Network Security	3GPP; 3GPP2; IEC; IETF; IEEE; ISO/IEC JTC 1; ITU-T; The Open Group; WiMAX Forum	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented
Security Automation & Continuous Monitoring	IEEE; IETF; ISO/IEC JTC 1; TCG; The Open Group	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Software Assurance	IEEE; ISO/IEC JTC 1; OMG; TCG; The Open Group; UL	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Supply Chain Risk Management	IEEE; ISO/IEC JTC 1; IEC TC 65; The Open Group; UL	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
System Security Engineering	IEC; IEEE; ISA; ISO/IEC JTC 1; SAE International; The Open Group	Some Standards Slow Uptake	Standards Needed Slow Uptake	Some Standards Slow Uptake	Standards Needed Slow Uptake	Standards Needed Slow Uptake

10. ANNEX II: IOT COMMUNICATION PROTOCOLS (ENISA, 2017)



Technology	Description	Architecture	Further Information
HTTP v.1.1	Standard (IETF RFC 2616) application-level protocol for distributed, hypermedia information systems	■ Request-response ■ TCP-based ■ Brokerless ■ Security: SSL/TLS	■ HTTP standard ■ HTTP portal ■ HTTP GitHub
MQTT	Standard (OASIS) binary communication protocol for lightweight machine-to-machine transfer	■ Pub-sub ■ TCP-based ■ Broker-based ■ Security: SSL/TLS	■ MQTT standard ■ MQTT portal ■ MQTT GitHub
Advanced Message Queuing Protocol (AMQP) v.1.0	Standard (OASIS and ISO/IEC) for message-oriented middleware	■ Pub-sub ■ TCP-based ■ Broker-based ■ Security: SSL/TLS and SASL	■ AMQP standard ■ AMQP portal ■ AMQP GitHub
Data Distribution Service (DDS)	Standard (OMG) middleware messaging protocol	■ Pub-sub ■ UDP- and TCP-based ■ Brokerless ■ Security: SSL/TLS (TCP)	■ DDS standard ■ DDS portal ■ DDS GitHub
XMPP Extension Protocol (XEP)	IoT extensions to XMPP	■ Pub-sub ■ TCP-based ■ Broker ("node")-based ■ Security: SSL/TLS	■ XEP standard ■ XMPP portal ■ XMPP GitHub
IEC = International Electrotechnical Commission; IETF = Internet Engineering Task Force; ISO = International Organization for Standardization; OASIS = Organization for the Advancement of Structured Information Standards; OMG = Object Management Group; RFC = Request for Comments; SASL = Simple Authentication and Security Layer; SSL = Secure Sockets Layer; TLS = Transport Layer Security; XMPP = Extensible Messaging and Presence Protocol			

Source: Gartner (April 2018)

Table 1 depicts an indicative listing of different protocols grouped by communication layer. The datalink layer handles the connection between IoT devices across a physical link, either wired or wireless, for example between sensors or between a sensor and the gateway that connects a set of sensors to the Internet. The network layer is divided into the routing layer, which handles the packet transfer from the source to the destination, and into the encapsulation layer, which builds the packets. The session layer defines the protocols enabling messaging capabilities among the elements of the IoT communication subsystem[46].

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

Table 1: Indicative listing of communication protocols for IoT[46]