Universitat Oberta de Catalunya

uoc.edu

Security in IoT Ecosystems

Noelia Pérez Moldón

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Seguridad en la Internet de las cosas

Amadeu Albós Raya

Helena Rifà Pous

Junio 2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Security in IoT Ecosystems*
Nombre del autor:	*Noelia Pérez Moldón*
Nombre del consultor/a:	*Amadeu Albós Raya*
Nombre del PRA:	*Helena Rifà Pous*
Fecha de entrega (mm/aaaa):	06/2019
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Seguridad en la Internet de las cosas*
Idioma del trabajo:	*Inglés*
Palabras clave	*IoT / Cloud / Security*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

Hoy en día, IoT (Internet de las cosas) está revolucionando el mundo como lo conocemos.

El Internet de las cosas (IoT) es un concepto técnico que describe un sistema compuesto por múltiples objetos físicos que ahora están conectados a Internet. Estos dispositivos tienen la capacidad de transferir datos a través de una red sin necesidad de interacción de persona a persona o de persona a ordenador. También pueden conectarse y transferir información entre ellos a través de la red.

Para permitir y crear estas interconexiones, hay diferentes elementos involucrados que crean lo que llamamos el ecosistema IoT.

El principal objetivo del ecosistema de IoT es recopilar, procesar, manejar y almacenar los datos de manera eficiente en tiempo real para brindar un mejor servicio a los clientes finales junto con la integración de los múltiples tipos de dispositivos de IoT.

En este Trabajo de Fin de Mater, estudiaremos la seguridad de los ecosistemas de IoT. Para hacerlo, analizaremos las tecnologías, productos y soluciones que algunos fabricantes y proveedores ofrecen para el entorno empresarial (principalmente en la nube). Los analizamos desde una perspectiva de seguridad y finalmente revisaremos un ejemplo de un ecosistema de IoT para empresa donde analizaremos los principales problemas de seguridad que le afectan y las mejoras de seguridad que se pueden realizar.

Abstract (in English, 250 words or less):

Nowadays IoT (Internet of Things) is revolutionizing the world as we know it.

The internet of things (IoT) is a technical concept that describes a system composed by multiple physical objects that are now being connected to the Internet. These devices have the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. They are also able to connect and transfer information between them over the network.

In order to allow and create these interconnections, there are many different elements involved that creates what we call the IoT Ecosystem.

The main objective of the IoT Ecosystem is to collect, process, handle and store the data efficiently in real time to provide a better service to the end customers along with the integration of the multiple kind of IoT devices.

In this Mater thesis report, we will study the security on IoT ecosystems. In order to do it, we will analyze the technologies, products and solutions that some manufacturers and suppliers offer to the business environment (mostly in the cloud). We analyze them from a security perspective and finally we will review an example of an IoT ecosystem for business where we will analyze the main security problems that affect it and which security improvements can be made.

Index

List of Figures

1. Introduction

5.5.1 Context and justification

Nowadays IoT (Internet of Things) is revolutionizing the world as we know it. Every day we are more connected and every day we depend more on this type of technology, both personally and professionally. In this environment, the security in this type of communications is crucial since every day we exchange a multitude of information that travels from one device to another through networks.

From the business world, we see how each day more of these services are requested and in this type of environment, security is essential.

In this Mater thesis report, we will study the security on IoT ecosystems. In order to do it, we will analyze the technologies, products and solutions that some manufacturers and suppliers offer to the business environment (mostly in the cloud). We analyze them from a security perspective and finally we will review an example of an IoT ecosystem for business where we will analyze the main security problems that affect it and which security improvements can be made.

5.5.2 Goals

- Understand the current state of IoT technologies offered to business environment.
- Review the technologies involved with IoT and the security problems related.
- Analyze the advantages and the integration of IoT on business world.
- Evaluate the main disadvantages and risk of the implementation of IoT technologies from the point of view of security on the companies.
- Study what is an IoT ecosystem and the elements and technologies related by analyzing also the products provided by suppliers nowadays.
- Define an example of an IoT ecosystem to analyze some principal security points.
- Exhibition of safety improvement plans to propose a future line of analysis.

5.5.3 Methodology

We will analyze what is IoT and the technologies related with it. We also analyze which are the main security problem to which these technologies are expose now a days. Then we will review the impact of IoT in the business world and to define the main risk to which the companies that decide to move to IoT solutions are expose. We will also review the elements that compose and IoT ecosystem and the different IoT proposals that manufacturers offer focused on the business environment. Next, we will proceed to analyze the main security problems of these elements by using a defined example of an IoT Ecosystem.

With this methodology, we intend to start from a generic analysis in which we know a wide variety of technologies and options that manufacturers offer today for the business world, to ending up performing a small analysis of the main security problems of an IoT ecosystem example defined.

5.5.4 Planning

Below a table is presented with the list of tasks scheduled for the realization of this project, as well as the start and end dates for each one of them.

For calculations, Fridays are considered as holidays.

Start date	End Date	Description	Duration (working days)
20-feb.	21-feb.	Start of classes (TFM)	1
21-feb.	24-feb.	Review of calendar and classroom documentation	2
24-feb.	28-feb.	Preparation of the work plan	4
25-feb.	26-feb.	Email - Ask questions and send the initial plan	1
28-feb.	5-mar.	Review of the work plan	4
5-mar.	6-mar.	Classroom - Delivery 1 - Work plan	1
6-mar.	12-mar.	Search for information (Analysis)	5
12-mar.	18-mar.	State of art of IoT and technologies related	5
18-mar.	23-mar.	Analysis of IoT impact on business	4
23-mar.	28-mar.	Analyze security issues	5
28-mar.	1-abr.	Update documentation 1	3
1-abr.	2-abr.	Classroom - Delivery 2	1
2-abr.	13-abr.	Analisis of IoT ecosystem: definition, elements and suppliers	9
30-abr.	13-may.	Analisis of IoT ecosystem: security issues	9
13-abr.	21-abr.	Definition of an example of a secure IoT ecosystem	7
21-abr.	27-abr.	Implementation of the IoT ecosystem	4
27-abr.	29-abr.	Update documentation 2	2
29-abr.	30-abr.	Classroom - Delivery 3	1
30-abr.	7-may.	Perform test plan	4
7-may.	11-may.	Results documentation	3
11-may.	13-may.	Conclusions of the tests	2
13-may.	16-may.	Update documentation 3	2
16-may.	20-may.	Improvement plan	3
20-may.	23-may.	Final conclusions	3
23-may.	26-may.	Update documentation 4	2
26-may.	28-may.	Review of introduction points and plan update	2
28-may.	3-jun.	Memory Writing - General Review	5
3-jun.	4-jun.	Classroom - Delivery 4	1
4-jun.	8-jun.	Recording the presentation video	3
8-jun.	10-jun.	Edition of the presentation video	2
10-jun.	11-jun.	Classroom - Delivery 5 - Video presentation	1
17-jun.	20-jun.	Defense of the TFM	3

Figure 1 – Planning Table

Following Gantt chart shows the tasks listed in the previous table sorted in chronological order:

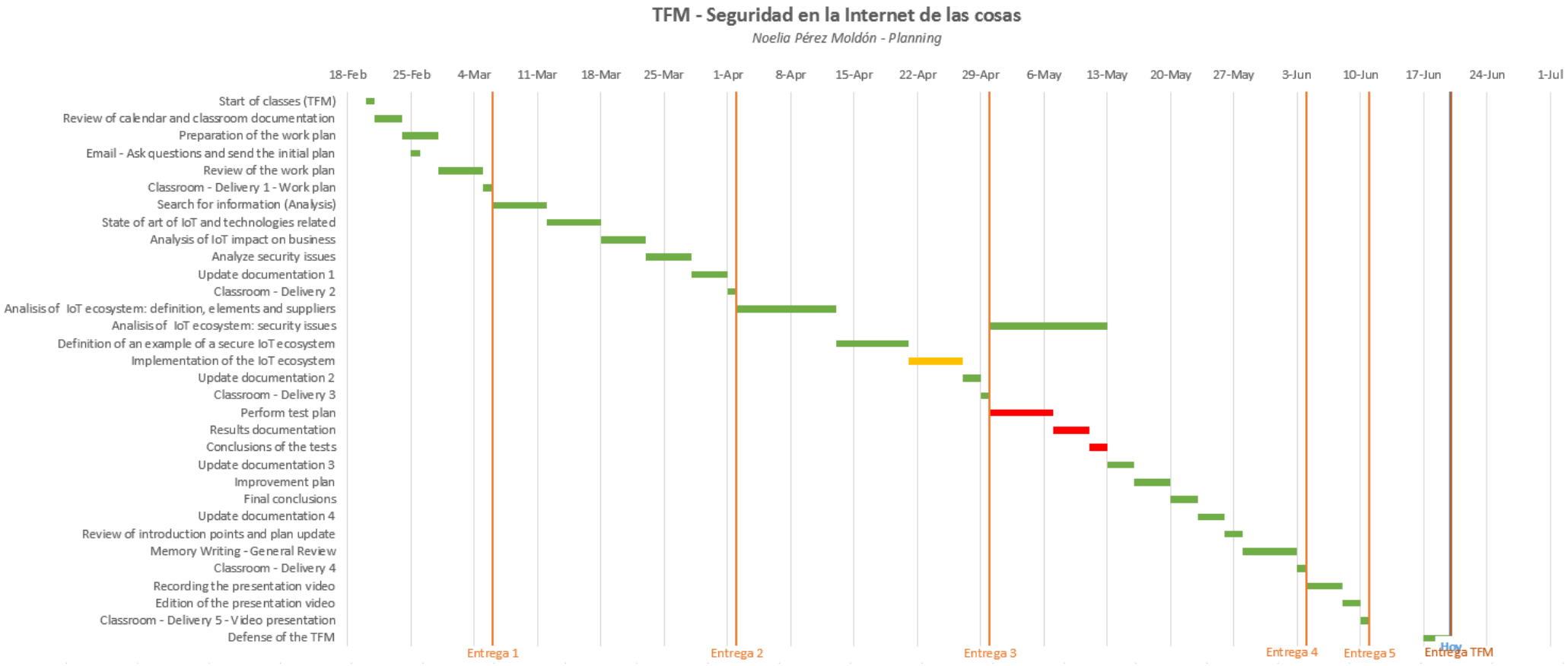

Figure 2 – Planning Graph

5.5.5 Outline

Chapter 2 presents what is IoT and the technologies related as the network virtualization, hosting, cloud, edge and fog computing. On this same chapter, we will review which are the main security problems that affect to these technologies.

On chapter 3, we will review how IoT is related with business by reviewing the IoT specialization for Industrial companies and how IoT technologies are integrated with other important services to business like analytics and machine learning. In this chapter, we will analyze also, which are the main security issues that affect to the companies that decide to use IoT technologies on their business and some recommendations they should take into account to maintain the security in their companies.

Along chapter 4, we will analyze which are the main components of an IoT ecosystem for business reviewing the different elements involved and the suppliers of each type of component. Then on chapter 5, we will define an example of an UCaaS IoT ecosystem to review in detail the high-level implementation analyzing also elements involved, the different suppliers and the main security issues that can affect this ecosystem defined.

Finally, we will review some of the security improvements that could be made on the IoT ecosystem along chapter 6 and we will summarize the conclusions obtained on this Mater thesis report on chapter 7.

2. IoT and technologies related

2.1. IoT

The internet of things (IoT) is a technical concept that describes a system composed by multiple physical objects that are now being connected to the Internet. These devices have unique identifiers (UIDs) and they have the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [1]. They are also able to connect and transfer information between them over the network.

This technology is growing every day and more devices are starting to get "smarter" and connected to the network, therefore this is an important point to be taken into account on the new network transformation.

Figure 3 – Internet of Things (Hughes Europe)

Telecommunications companies are already aware of the importance of IoT. Cisco, for example, estimates than by 2020, 27 billion devices will be connected globally with over half being machine-to-machine connections [2]. Telefónica however estimates that there would be around 20 billion at that time [3] while Ribbon mentioned 30 billion devices [4], closer to Cisco approach. Anyhow, all these big companies agrees that we will see an incredible growth during the next years.

In order to be ready to transform and adapt the network to support all these new and different devices each company is providing their own solutions and systems, but most of them have several things in common, as the technology used. Most of the solutions proposed are implemented on the Cloud over virtualized servers, as we will see next.

2.2. Network virtualization

Networks have been changing during the latest years not only in their implementations (migration from circuit-based networks to data network, introduction of new technologies 2G, 3G, 4G, 5G, LTE, VoIP…) but also on where the servers of

these networks are placed. Hardware has been improving and nowadays they have enough capabilities and resources to carry on several applications and processes at the same time without affecting the service. This is why, in order to safe costs, different suppliers are using the same HW to support several kind of SW in order to benefit of these resources saving cost to service providers.

The improvements on the HW servers allow also that virtualization could came into the picture to make the SW to work and behave like HW to manage workloads by radically transforming traditional computing to make it more scalable.

The absence of HW allows companies to save money on power supply, installations of servers and renting or maintenance of data centers, but it also provides more flexibility and scalability as you can create more HW and deeply the SW that you need in a more efficient and faster way. As mentioned before it is expected a big increase of devices connected to IoT over the next years, therefore it is important that the network can be easy to scale and flexible enough to adapt itself to these devices without causing a big impact on the overall cost.

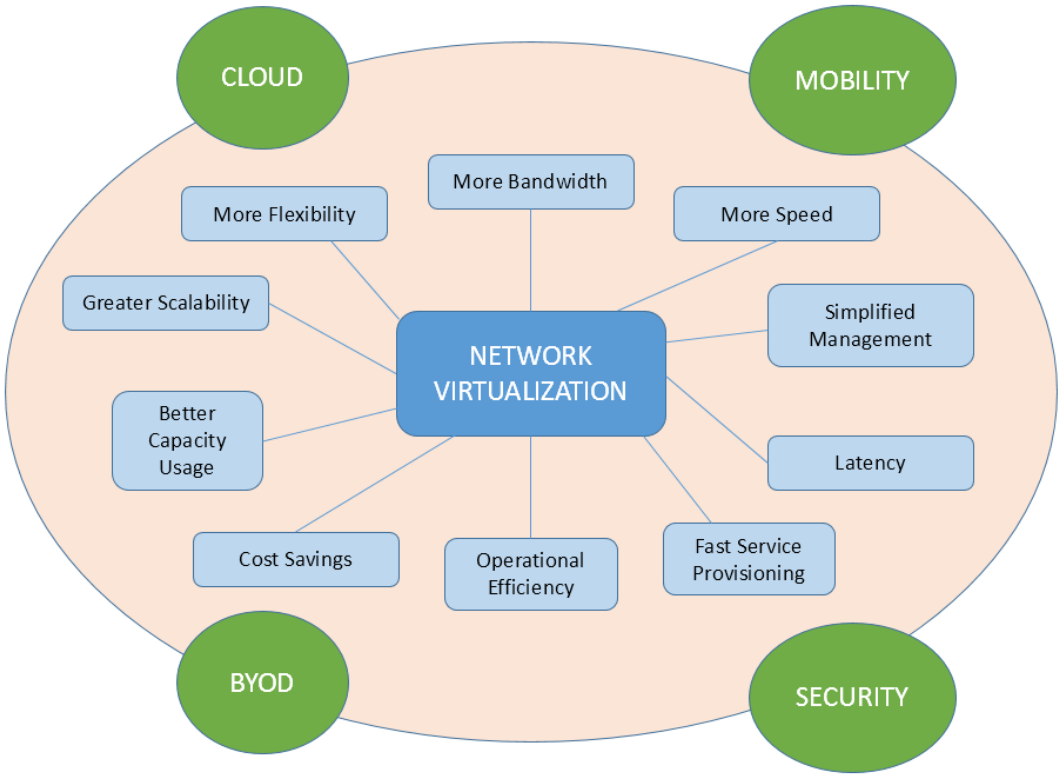

Figure 4 – Network Virtualization Advantages (Based on Data Center Dynamics graph) [5]

As ZTE explains, while Internet companies traditionally lease physical servers from internet data centers (IDCs) to develop services, their computing, storage and internal networks in data centers are now run through virtual infrastructure as a service (IaaS). Down the road, they will evolve towards the platform as a service (PaaS) model, which features integrated development and operation. With PaaS, services will be iterated and launched faster, and the ecosystem that integrates partners will become stronger [6].

Each of these models implies that the management of the servers don't need to be done by the companies itself but that these can be manage remotely by a 3rd party company specialized on these services, with this, the main companies will save costs and they won't need to have specialized people to manage their IT services. Depending on the model selected by the company there will be more or less services managed by the 3rd party companies. Below we can see a graph from Bitec that explains the different solutions from the IDCs to Iaas, PasS and finally SaaS (Software as a service) which is a full service provided by a 3rd party itself.

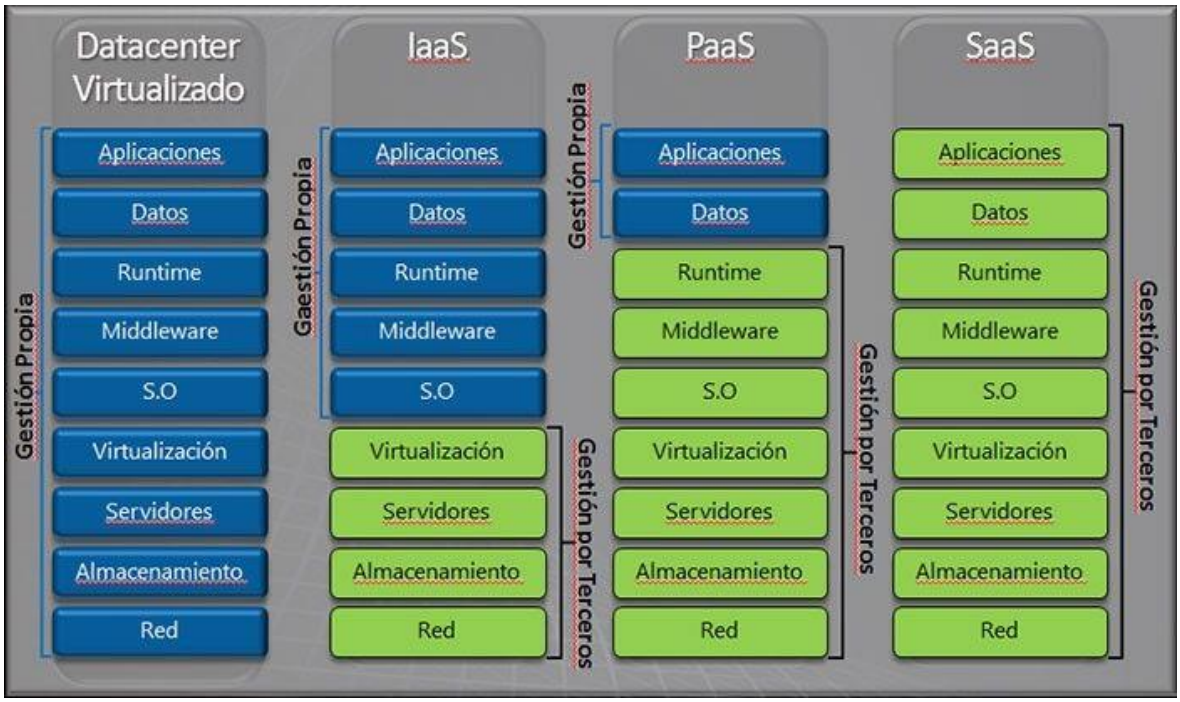

Figure 5 – Management of the different systems [7]

These services will be reviewed later from the cloud environment point of view.

2.3. Hosting

Another traditional service that is also now being virtualized is the hosting.

The servers deployed on virtualized HW are not specifically placed on one place, usually these servers are redundant and they could run on different HW servers. There are suppliers that provide this hosting service where customers can deploy their virtualized servers like Amazon Web Services (AWS) for example.

This fact of the HW in an unknown place but reachable from Internet makes us mention that these new virtualized servers are located in what we call the cloud [8].

These servers provide multiple services to end users and companies, as storage for example. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as

an electronic device has access to the web, it has access to the data and the software programs to run it.

Hosting allows users, companies and customers to deploy their own servers on a virtualized environment paying a monthly or yearly quote. Now we do not need to have access or place to create our own CPD. As Techradar described [9], hosting allows many computers working together, running applications using combined computing resources. A hosting solution works via a network, like the internet, and enables companies to consume the computing resource like a utility e.g. gas or electricity.

In order to make these servers (virtualized or not) reachable from Internet it's necessary to have an public IP address so the rest of the IoT devices connected to the network can reach them to obtain the services.

And if instead of sharing the public IP address to the IoT devices we share a domain name, the end users will be able to reach the servers behind this domain name, this means that we can change the server IP if we replace it on the DNS server so the users can map the domain name accordingly.

The services provided by these servers that are reachable via Internet is what people commonly call the cloud services.

2.4. Cloud

As mentioned, these servers (virtualized or not) provide multiple kind of services to the end users and IoT devices and that these servers are commonly placed on what we called "the Cloud". It is called that way because as we have seen, the servers are now reachable via Internet and are not necessary placed specifically just in one geographical place.

Cloud computing is a system that can provide different services depending on the level of virtualization of the servers as we have also seen before:

- Infrastructure as a service (IaaS) that involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an outsourced, on-demand service.

- Software as a service (SaaS) involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand.

- Platform as a service (PaaS) which shares some similarities with SaaS, but the main difference is that instead of delivering software online, it is a platform for creating software that is delivered via the internet.

As Jake mentioned on Investopedia [10], SaaS is expected to experience the fastest growth, followed by IaaS.

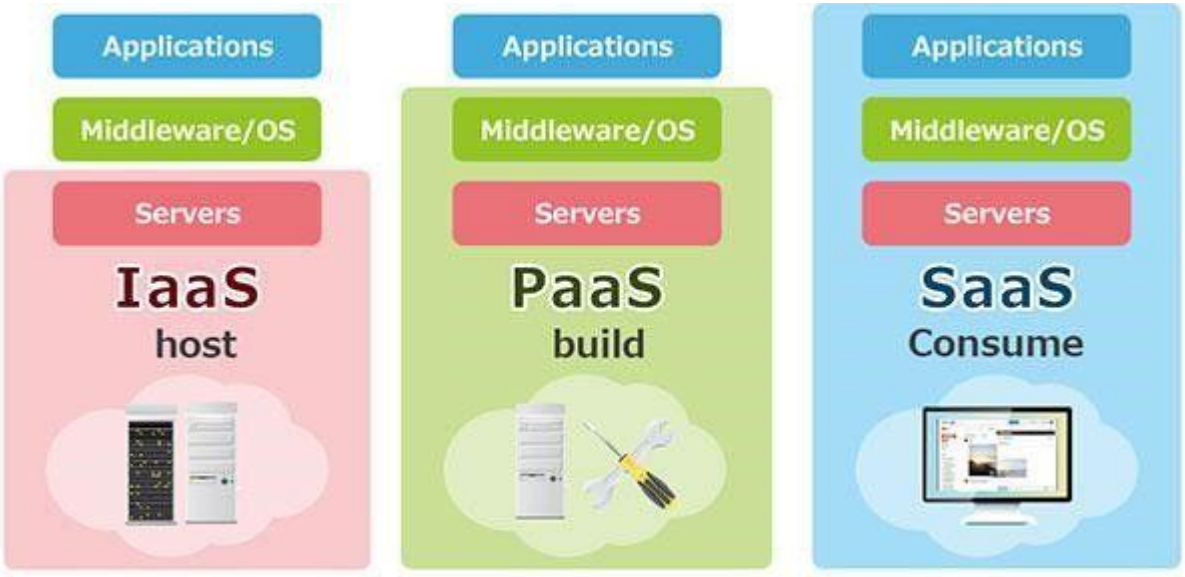

Figure 6 – Cloud services – Bitec [11]

Some of the SaaS that can be provided could be for example:

- Unified Communications as a service (UCaaS) that involves all communications functions such as voice and telephony, meeting solutions, messaging, presence and instant messaging, are clubbed together in a single package and delivered over the cloud on a pay-as-you-go model. [12]

A combination of these services with IoT devices will provide more functions to the customers such as get a call directly from their cars without needing to connect the mobile phone via Bluetooth, or having a collaboration meeting using a smart TV for example.

The cloud heritage some of the benefits for the virtualized networks, such as the greater scalability, the flexibility, the better capacity usage, the simplified management, etc. In addition, as these cloud services can be adapted in several ways, the companies can select the services that suit them better for their business and pay only for the services that they need each time.

These services are provided from one or more servers that are integrated on the cloud. As we have mentioned, most of them could be virtualized and we cannot know exactly where the HW is. However whether if the servers that compose this cloud are virtualized or not, they could be placed so far away and in order to connect from the device to these servers we would need to go through a lot of routers and maybe even travel around the world in order to reach them. This is why the use of services on the cloud is considered not suitable for the scenarios where low latency is required. In order to prevent it cloud services can use edge and fog computing.

2.5. Edge Computing and Fog Computing

The increase of devices and connections to the servers of the cloud is causing issues with the bandwidth and with the amount of data that need to be processed by the servers. We should keep in mind that we expect a big increase of these kind of connections due to the growth of IoT technology.

In order to solve the bandwidth and latency problems it has been designed a model where data, processing and applications is made on devices placed at the edge of the network, known as edge computing. [13]

This makes that we can work in a more rational and efficient way with all these generated data. For instance, companies will be able to analyze relevant data on real time since the processing of these data would be done on the edge devices closer than on the cloud so it will not take that much time to be processed. From IoT perspective, the IoT devices will get faster answers from the cloud (edge devices) so at the end IoT devices can provide a faster service to customers.

There is another concept related with this edge computing which sometimes is being wrongly considered as synonymous, named “Fog computing”. As Brandon Butler explains on NetworkWorld webpage, “Fog refers to the network connections between edge devices and the cloud. Edge, on the other hand, refers more specifically to the computational processes being done close to the edge devices. So, fog includes edge computing, but fog would also incorporate the network needed to get processed data to its final destination.” [14]

This allow large data centers in the cloud to "delegate" part of their responsibilities to Edge Computing devices. In order to do so through Fog Computing that defines requirements or needs at that end of this ecosystem as a whole. [15]

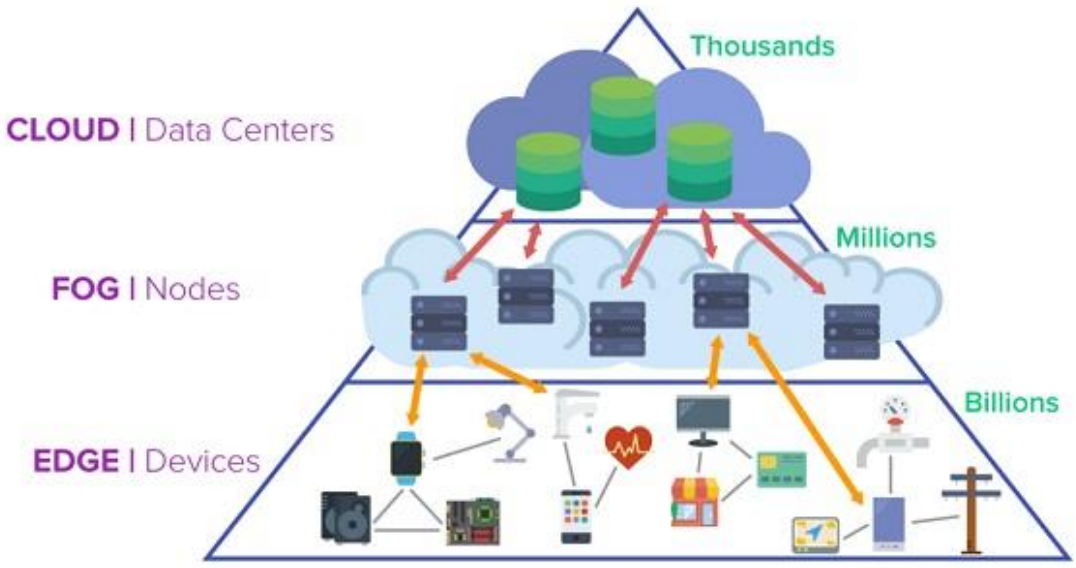

Figure 7 – Cloud, Fog and Edge [16]

As we mentioned, by these kind of connections that allow the processing of the data out of the cloud, latency is lower if we compare it with cloud computing since the data goes from one device to another without being force to pass or being processed by cloud servers that could be far away. Nevertheless, as the data is being processed there (out of the cloud – considered as safe environment), we cannot guarantee the data that arrive to the cloud servers has been processed in the correct way or not.

2.6. Main Security Issues on Cloud Networks and IoT

Data network used to be accessible only by PCs, servers and mobiles phones, but now IoT is causing that everyday more multiple and diverse devices are being also connected. Networks need to be adapted to support these kind of diverse devices and to be protected of the attacks that might come through or from them. We will analyze this part deeply once we have understood better the idea of an IoT ecosystem on chapter 4.

The virtualization brings many advantages but also bring new security threats. Now attackers could compromise VM infrastructures for example, allowing them to access other VMs on the same system and even the host. Once the attacker has gain the access to these servers they can obtain confidential information, the can modify it and even turn down the service. This will affect the three pillars of information security, which are confidentiality, availability and integrity.

This is why hosting providers review carefully security details by providing services for network monitoring, SSL, firewall, DDoS prevention, malware detection and removal, providing different levels of access depending on the type of user and always using strong passwords and allowing customers to make backups [17]. Now they do not have to take care only about the physical access of their servers but also to the remote access to prevent unauthorized people to enter into their customer's data and servers.

One of the points where security is more controlled is the cloud and the servers on it. If we can prevent attackers to access to any of the servers on the cloud, we will protect the virtualized servers also. To provide successful services to end users, the cloud should be considered as a safe and thrust environment even if the connections to this cloud are based on a non-secure environment like Internet. Usually most of these connections over internet are tried to be done over secure protocols as https that use certificates to guarantee the

However if a part of the storage and processing is made on the devices out of the cloud (edge computing) this make all these servers placed on the edge a perfect place for hackers to look for security issues in order to obtain or manipulate the data or even to try to access to the main cloud servers. Nevertheless, there is another point of view of this situation; some people argue that this kind of distribution is good because if there is less data in a corporate data center or cloud environment, then the less data there is vulnerable if one of those environments is compromised. [18]

Some of the most known security issues that we can found on these cloud scenarios are IP address spoofing [19], man-in-the-middle [20] or denial of services attacks [21].

Attack	Description	Disadvantages	Solutions	Advantages
IP address spoofing	Act of falsifying the content in the Source IP header, usually with randomized numbers, either to mask the sender's identity	- Identity theft, masquerading as a legitimate entity. - Hackers avoid discovery and implication by law enforcement and forensic cyber-investigators. - Hackers prevent targets from notifying device owners about an attack in which they are unwittingly participating. - Hackers bypass security scripts, devices and services that attempt to mitigate DDoS attacks through the blacklisting of attacking IP addresses.	- Review unexpected behaviors. - Monitoring networks for atypical activity - Deploying packet filtering to detect inconsistencies. - Using robust verification methods - Authenticating all IP addresses and using a network attack blocker.	- Prevent identity theft. - Prevent access to the servers to unauthorized users.
Man-in-the-middle	Act of interrupt communication between two computers, alter the packets, and then transmit them without the original sender or receiver knowing.	- Hacker gains instant access to your device. - Once they infiltrate this closed system, they can send spoof emails — messages that appear legitimate. - Hacker gains control of your browser cookies, which are small pieces of data that store website information when you are browsing.	- Use secure connections when browsing over Internet that encrypt the traffic. - Use a firewall. - Set up a virtual protected network (VPN) - Keep your security solution software up to date.	- Prevent personal and confidential data to be stolen. - Prevent identity theft.
Denial of service	Act of overwhelm computer networks with traffic. Is a brute-force attempt to slow down or completely crash a server.	- Systems will not respond well to legitimate requests for service - Services will not be available. - Services provided will be done slower.	- Disable any unneeded or unfamiliar network services that could be used as a DDoS infiltration point. - Establish a baseline for network performance and server traffic. - Invest in a special anti-DDoS service that features automatic scanning to detect the most common types of DDoS attacks.	- Prevent money, time, clients and even reputation to be lost.

Figure 8 – Most Known Securiy Issues Table

The main issues that we usually found when we try to avoid these kind of attacks on the cloud and on IoT elements is that servers and devices sometimes are not having enough capacity, or the firmware or OS has some limitations that we cannot skip. This is why having multiple kind of servers and devices on an IoT environment is not only a disadvantage because of the multiple points where they can be attacked, but also an advantage because we can:

- Include more servers on the cloud with extra capability than the devices to implement functions to protect the network elements.
- Have servers with different kind of firewalls and OS to prevent having the same limitations or issues in all of them.
- Distribute the HW on different geological sites to prevent risks as (fires, floods, earthquakes, power cuts, etc.)

Therefore, by joining this variety of devices, we can take the better of each one and protect ones with others creating a more secure environment but also it is important to understand and prevent the vulnerabilities of each of the specific devices to create a safe IoT Ecosystem, as we will see in Chapter 5.

3. IoT for business

3.1. IoT benefits for business

Everyone knows the importance of the data and how this could be useful in many different ways in life, for personal porpoises, for political causes, for economical ones, etc. Companies are aware of the importance to obtain, collect, store and process the data that will help them to improve their benefits and services and here is where IoT can bring to many benefits to these companies. With precise data in hand, a business is able to make intelligent product-recommendations and customize searches to attract more customers. [22]

IoT devices are collecting a huge amount of multiple data from different users across the world. If companies can get this data and with the correct processing they could get much more detail reports on which are their customer needs, which are their expectations, some details that even these customers are not even aware of but that can be extracted from their behavior.

Nevertheless, IoT is not only valid for customer or financial perspective but also from employee and productivity one. Companies can create their own IoT applications or devices to help their employees to work in a more comfortable and efficient way. For instance, a company can create or buy an application for their employee's mobile phones that will help them to connect to each other's, by chat, call or even to create virtual meeting rooms for their conferences from their phone. This will allow employees to work from home and make them feel more comfortable and therefore to work better.

3.2. Industrial Internet of Things (IIoT)

Usually the IoT term is used in all areas that involve the use of this technology of devices connected to the cloud, however many of the IoT service providers usually refer to a specific section focused only on the industrial sector and they named IIoT (Industrial Internet of Things).

Therefore IIoT is a subset of the IoT that eliminate all consumer products (for example products for home applications, such as a connected refrigerator, smart TV and portable devices), and focusing only on the part of increasing efficiency processes, health and safety. The IIoT focuses exclusively on industrial applications, such as chain production, manufacturing or agri-food industry processes. [23]

The devices and technologies involved on IIoT will required being more robust and securing than any commercial IoT device. In addition, industrial companies will request this technology to be easy scalable to adapt it to their needs.

However, even if security is one of the main concerns of this industrial sector, the analysis made shown up that the lack of budget is the part that is making the integration of this technology on the industries to be delayed as we can see from the data collected by Vector ITC group [24] on the following chart.

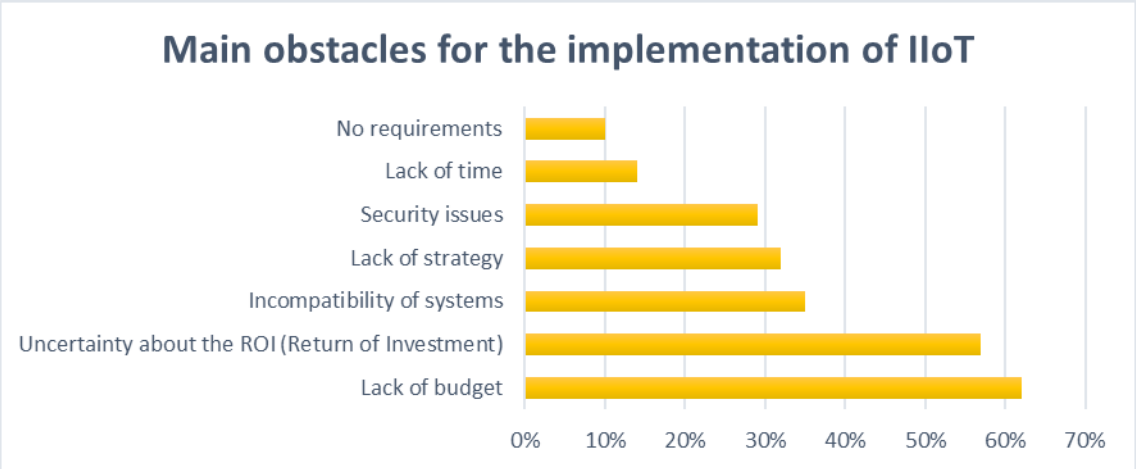

Figure 9 – Obstacles for the implementation of IIoT

For the analysis of this Mater thesis report we have decided not to focus only on this specific part of IIoT but keep a more open analysis of IoT related to all kind of business including not only industrial sector but also services providers like Internet providers, health companies, transport companies, etc. However, it is important to make this reference because of its specialized needs.

3.3. IoT Integration with Analytics and Machine Learning

As Stephen Zafarino mentioned on IoT Agenda [25] the future of IoT in business will take shape in the form of intelligent sensors, platforms and autonomous, predictive

analytics produced by bringing the advantages of cloud computing closer to where that data is being generated, aka the intelligent edge.

By analyzing this information on the edge, it can be identified which is the useful information to help the company to get the results that they need for their business. If to the analyzed data we add some "intelligence" to these devices by including machine learning software they can provide a more accurate service to customer's needs based on their behavior and on the data that is being collected related with customer profile.

As Stephen also mentioned that machine learning integration, provide IoT business devices with the intelligence they need to act on the data they are producing, rather than operating as simply data producers.

Machine learning can provide predictive analytics as well. Traditionally this kind of predictive analysis was done by high skill data scientist or high skill business analytics and now this can be improved by trying to automatized it and integrating it with IoT environment. IoT will provide the data that the algorithms made for the machine learning needs to create these predictive analysis, and these analysis can provide the information to the edge computing so it can give a faster and more personalized service to the end users.

3.4. Security Issues that can impact Companies with IoT

Despite of the benefits that IoT can provide to the companies it is important to consider also the risk or threats to which they are exposed as well. As we saw on chapter 2, the use of these technologies relates with IoT provides multiple benefits but also new vulnerabilities that can affect to the confidentiality, the integrity and the availability of the data. If this is not guarantee, the companies will be affected in several ways, as their end customers will not able to obtain the services (DoS attack) and this can impact into a loss of confidence in the company along with an economical cost if they committed to provide a rate of availably of the service. It can also bring legal problems to the company if attackers can reach to personal and confidential data of their customers than once more will cause a loss of confidence and probably an economical cost associated.

The main security, servers and telecommunications suppliers have made several researches about this. For instance, Avast mentioned some of these mayor risks to which companies are exposed [26]:

- Access to the sensitive data: IoT devices can manage multiple kind of data and some of it might be sensitive one and could be wanted by cybercriminals.
- Sabotage: Another kind of attack to which these devices and data can be exposed is sabotage. As Avast mentioned a bad actor could potentially hold a vehicle and its occupant's hostage or demand payment to stop the sabotage of an assembly line.
- Bonets: Cybercriminals can infect several devices into the network with bonets in order to coordinate attacks and cause a DDoS (Distribute Denial of Service) attack.

This kind of attack consist on sending multiple requests to the servers on the network to make it crash or at least to make it not available to handle real users requests due to the congestion.

CISCO also has made some researches and they identify which are the biggest sources of concern related with cyber-attacks:

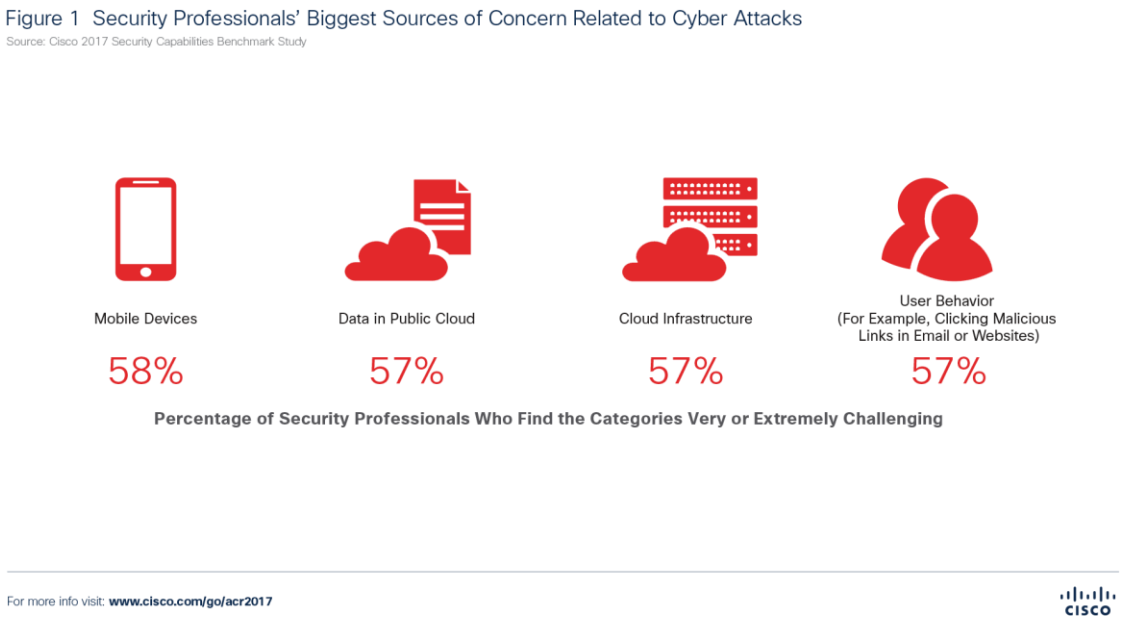

Figure 10 – Security Proffessionals' Biggest Sources of Concern Related with Cyber Attaks [27]

As we can see there's a high concern about the devices involved (in this case they focus on the mobile devices), and the cloud as infrastructure and also as if public clouds are a safe environment to store the data that in the past was stored on their on-premise solutions in most of the scenarios. Another one of the main concerns is how the users can get into hackers tricks and provide them confidential information without even realizing and providing hackers an easy authorize access to the system.

As we explained before, the data is the most valuable thing that IoT can provide to the companies. Therefore, how to deliver, transfer, process and store the data in a secure way is critical for the companies also. That is why they care about the devices in charge of this like the mobile devices, or the cloud servers.

As mentioned most of these connections are done over Internet using IP protocol, so the servers of the cloud should take care of attacks using IP spoofing. In addition, as Internet is considered a non-secure network it is important to try to use secure protocols (https, SSL, etc.) to transfer this information to prevent external attackers to intercept it and to modify it. As we saw on previous chapter this kind of attack is commonly known as man-in-the-middle.

One of the mains ideas of the cloud is that we do not know exactly the geographical place where the data is stored or transferred over. However ending raw data over the

internet can also have privacy and legal implications, especially with country-specific data regulations being adopted like the GDPR [28]. Companies should take this into account to prevent to have legal problems. In addition, from the point of view of security we have to keep in mind that once the data get out of our controlled and secure environment it can be taken if other networks do not implement secure controls correctly. From business perspective companies should review which kind of information they need to send out of their network and how and where it will be sent to minimize the risks.

3.5. How to Maintain IoT security

Some of these attacks mentioned before cannot be avoid by the companies themselves. It is important that all the actors involved on these IoT environment understand the importance of the security and their role on it.

Suppliers of HW, SW and the operators of the cloud should keep in mind all this kind of attacks and provide methods to detect stop and prevent these attacks to happen. It is so important that the network could be considered a secure environment to store and transfer the information. Mobiles should be secure, the clouds should also be considered a safe environment for the end customer and therefore they should understand that despite of the infrastructure of the cloud, the ecosystem is safe.

However, there is another part of security that should be covered by end users, as we saw on the previous diagram. Users in some cases are not aware of the importance of some details like to use strong passwords (in these cases suppliers or network operators can force the users to follow some rules in order to stablish a secure password). They should take care as well and be prevented against attacks of social engineering (an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain.[29]). If a hacker can easily obtain the password of a user because it is not strong enough or it can obtain private information or valuable data with a Phishing attack [30], hacker can commit fraud or access an organization's network. Companies should provide them information so they can understand the new risk to which they are now exposed, to prevent these kind of attacks.

Hackers can be aware of security issues of a specific firmware version, as it is already published on a public vulnerability database as NVD [31] and take advantage about this to attack the device or the server. Both, users and administrators should take care to keep the SW updated with the latest patches to prevent devices and network elements to be manipulated or sabotaged.

It is recommended that IoT devices and networks implement security technologies as:

- Blacklisting: works by maintaining a list of applications that are to be denied system access and preventing them from installing or running. [32]

- Vulnerability assessment: is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately. [33]
- Device detection: is based on analyzing the User-Agent string sent by the browser. User-Agent strings are defined in the HTTP standard, which says that a User-Agent (UA) is made up of multiple 'product tokens' indicating the software and hardware characteristics of the device. [34]
- Anomaly detection: is the identification of data points, items, observations or events that do not conform to the expected pattern of a given group. [35]
- Privacy & data protection: securing data against unauthorized access.

Companies on their side should improve their ISMS (Information Security Management System) to adapt it to the new servers and devices that IoT introduces in their company. A good implementation of the ISMS will allow the companies to detect the best way to control, monitor and improve their processes, data and devices.

4. IoT Ecosystem

4.1. Introduction

IoT is a network of smart devices, sensors, and actuators that can interconnect with each other. In order to allow and create these interconnections, there are many different elements involved that creates what we call the IoT Ecosystem.

The main objective of the IoT Ecosystem is to collect, process, handle and store the data efficiently in real time to provide a better service to the end customers along with the integration of the multiple kind of IoT devices.

The amount of components that integrates and IoT Ecosystem can vary depending on the supplier's solutions, but in general, all these IoT Ecosystem have these kind of elements: end devices (sensors, mobile devices, Wireless cameras, weather stations, etc.), network devices (routers and gateways) and data centers (application servers, analytics, databases…).

This variety of elements made the Ecosystem a rich environment, but also made it much more vulnerable, since there are multiple places where it can be attacked. In order to understand which are the risks that our IoT Environment is facing it is so important to know which are the elements that conform it.

4.2. Elements involved

An IoT ecosystem involved multiple devices; we can group these devices into 3 categories based on their functionality:

- Data centers
- Network Devices
    - Edge IT
    - Internet Gateways, Data Acquisition Systems
- End devices (sensors and actuators)

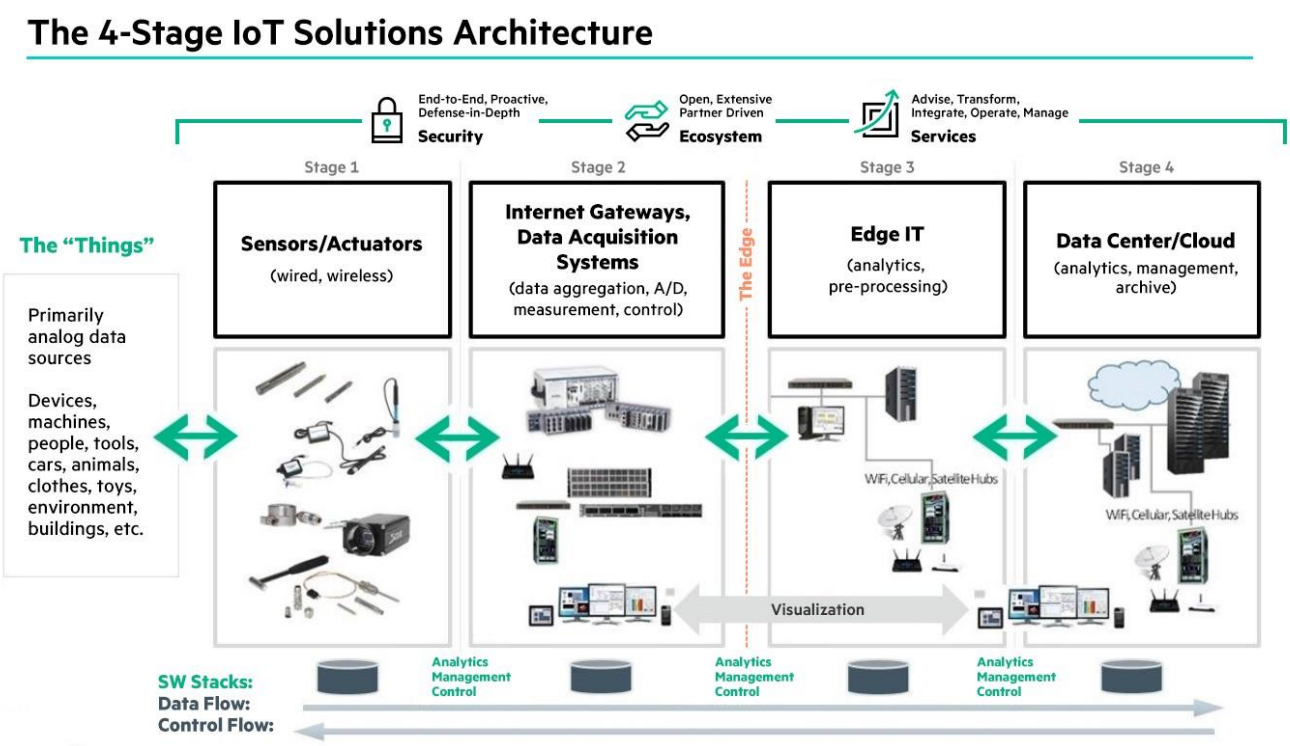

Figure 11 – IoT Solutions Architecture [36]

Data centers:

These data center are mostly placed on private or hybrid clouds and it can serve for two purposes: It can be the source of IoT device control, or it can be the endpoint for data that comes from scattered IoT devices.

On these data centers is where the process, handle and storage of the data will be made, this is why it is so important that these servers and databases are placed on a safe environment to prevent non wanted access to our data.

Here we can find different kind of servers with different objectives: like analytics, servers that provide services, intelligent servers that analyze the data and learn from it, etc.

Network devices:

Between the data center and the IoT devices are the intermediary access points for communications also called devices of the Edge network. These devices connect to the end devices using gateways. These are devices on the production floor that collect

data from distributed endpoints through a Bluetooth or WiFi connection and then send that data to the data center.

As Newgenapps explained [37], these Gateway enables easy management of data traffic flowing between protocols and networks. On the other hand, it also translates the network protocols and makes sure that the devices and sensors are connected properly.

It can also work to preprocess the data from sensors and send them off to next level if it is configured accordingly. By doing these the IoT Ecosystem will become much more efficient since the data will be sent to the servers on the cloud that should manage this information much more faster.

End devices:

These IoT devices are usually the most numerous elements of the ecosystem. They are also those that have more variety of devices and manufactured by a greater variety of manufacturers. In this section we would have all kinds of sensors, cameras, weather stations, Bluetooth speakers, Google home, Alexa, smart TV, smart vehicles, smart appliances, etc.

These devices can be connected to the network through different technologies as Wi-Fi, 4G, 3G, 2G, and Ethernet… That is why each one will connect to the cloud through different gateways depending on the technology used.

The variety of devices made that end customer can have multiple kind of services and solutions, and the variety of suppliers providing different kind of devices made that the customers can choose the ones that suits better their needs based on their economic situation.

4.3. Suppliers

For each kind of device involved on the IoT Ecosystem we can find several suppliers, each one provide different devices and solutions for IoT. However due to the variety of devices and suppliers there could be problems to integrate them on the ecosystem. That is the reason why there are some homologation tests being run by the different companies to be sure that their devices are suitable to be integrated.

The following diagram made by Frost and Sullivan [38] shows some of the main suppliers that provide devices, servers and services inside of an IoT ecosystem:

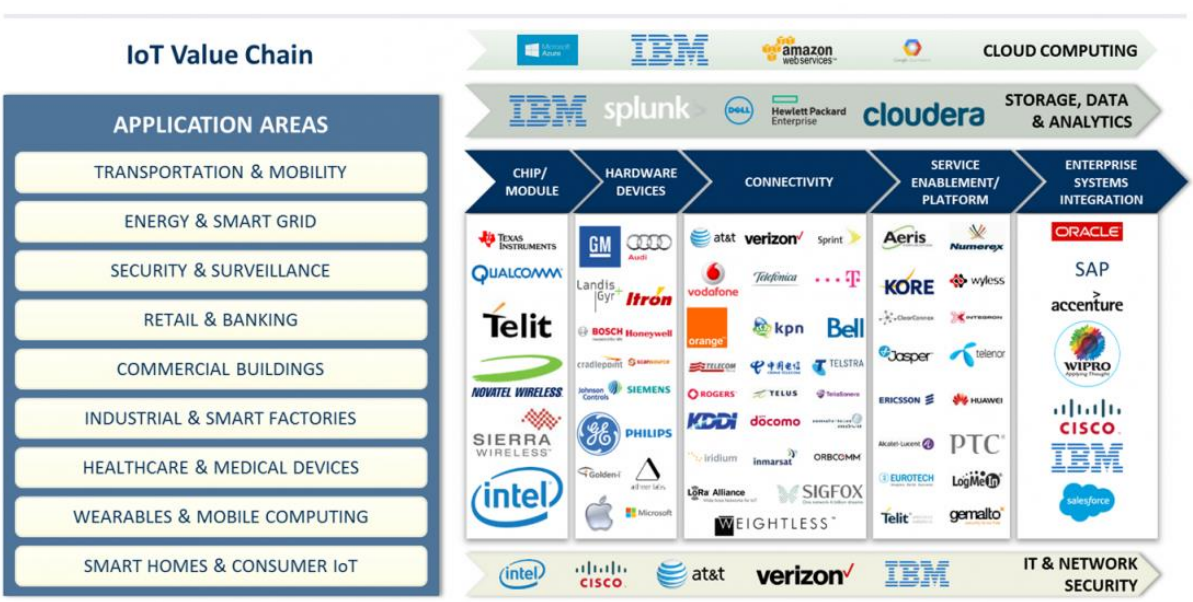

Figure 12 – Suppliers in an IoT Ecosystem

On the top of the diagram in the part of cloud computing we can see several known companies as Microsoft, IBM or Amazon. Each one of these suppliers provide their own cloud solution.

Microsoft offers Azure [39], that is a public cloud computing platform that provides a range of cloud services, including compute, analytics, storage and networking. Users can select from these services to develop and scale new applications, or run existing applications, in the public cloud.

IBM offers IBM Cloud [40], a full-stack cloud platform that spans public, private and hybrid environments. Build with a robust suite of advanced data and AI tools.
Amazon offers Amazon Web Services (AWS) [41] a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow. Explore how millions of customers are currently leveraging AWS cloud products and solutions to build sophisticated applications with increased flexibility, scalability and reliability.

Amazon also provides specific services for IoT integration named as AWS IoT [42] provides broad and deep functionality, spanning the edge to the cloud, so you can build IoT solutions for virtually any use case across a wide range of devices. Since AWS IoT integrates with AI services, you can make devices smarter, even without Internet connectivity.

Ribbon even if it is not on the previous diagram also offers Kandy as a PaaS for IoT. As Ribbon mentioned [43] Kandy communications Platform-as-a-Service (PaaS) is a real-time software development platform built from Ribbon's core communications, presence, security and real-time technologies. Kandy enables service providers, enterprises, software vendors, systems integrators, partners and developers to enrich

their applications and services with real-time contextual communications, providing a more engaging user experience.

In addition, Kandy [44] has been growing over the latest years to provide further services as CPaaS, UCaaS (Unified Communications as a Service), Wrappers, WebRTC, etc.

Multiple hardware suppliers provide elements along the whole IoT Ecosystem. These hardware elements could be part of the end devices, servers that help to provide the network services or even servers of the data center. On these hardware elements there are also chips and modules provided at the same time by other suppliers listed on the left part of the diagram.

In the middle, we have the connectivity suppliers as Telefónica, Vodafone, AT&T, Verizon… and platforms providers. These companies provide to the customers the network connectivity to get into the IoT Ecosystem; they also take care of the security on their own networks to prevent attacks.

Finally, on the right, we have some of the suppliers for enterprise system integration. One of them is CISCO [45] that announced a blend of IoT edge network appliances, developer tools, and deployment blueprints, infused with intent-based networking (IBN) to help the enterprise to build a secure IoT Ecosystem.

Even that these suppliers seems to be defined on a single area, this is not real, as each day these suppliers keep increasing their services and of them are trying to create their own IoT Ecosystem as Telefónica with Movistar Home and Aura [46] for example.

5. Example of a IoT Ecosystem for business

5.1. Introduction

As we have been reviewing each end device could be made by a different supplier and work with a different technology, this made that the integration on the IoT Ecosystem could become a hard process.

As an example, I have decided to use Ribbon UCaaS (SaaS) service named as Kandy. The Kandy platform allow us to create easily our own IoT ecosystem in a faster and simple way (we will not be stuck in interoperability issues as all belong to the same supplier). And we will have also the applications (mobile and web) to connect the end user devices (mobile and PC) into the cloud server (Kandy) only by registering with the user name and password. We will make an analysis of the different elements that are in our IoT Ecosystem and check some of the main security issues that can affect to this environment.

5.2. High level definition of the Ecosystem

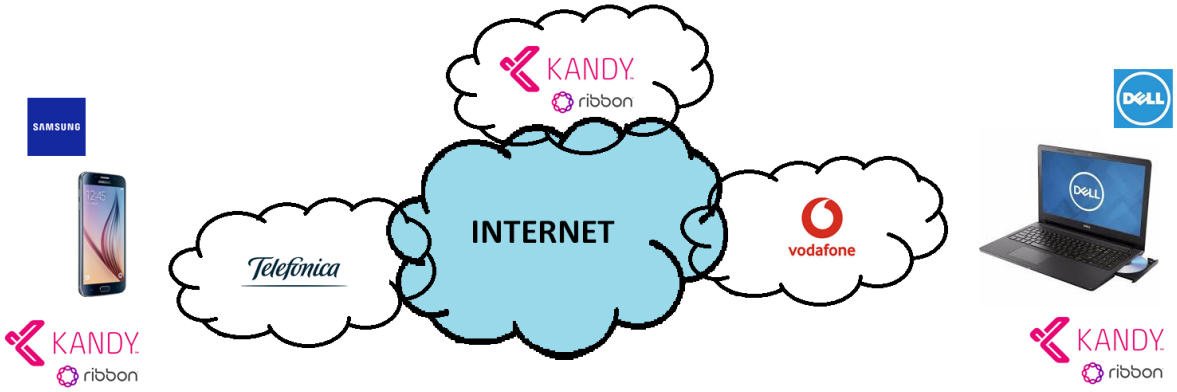

Figure 13 – UCaaS IoT Ecosystem example

On this IoT ecosystem, we will create an environment where we will connect a mobile phone trough Telefónica network to UCaaS Kandy cloud service. On another side, we will have a PC with a browser with a sw embedded that connect through Vodafone network to the UCaaS Kandy. Both, Telefónica and Vodafone can reach this Kandy cloud though the Internet.

On the next point, we will review with more detail the HW elements and the SW involved on this IoT Ecosystem that we are taking as example.

The UCaaS provided by Kandy offers the users several kind of options to communicate in a safe way with user B, as VoIP call, videoconferencing, web collaboration, voice mail…

A safe communications path will be stablished between the end devices and the Kandy cloud service. This is an important point, since the data transferred to create the communication path and the data sent during the communication will be sent though Internet which is not a safe environment and where the communication can be intercepted or manipulated.

We will consider that all the services providers' networks (Telefónica, Vodafone and Kandy) are safe environments, since these companies take care of their network security. However, none of the environments are never 100% secure, as there are always multiple kind of attacks to whom they are exposed to everyday. Most of these attacks fail because these services providers stop them, but some others succeed and it lead to several and multiple kind of projects. For instance the known WannaCry ransomware that affect to Telefónica last year [47], it ended up also affecting to other customer connected to their networks. In order to prevent problems to propagate from these networks, the services providers should also review the data that is coming from these others "trusted" networks.

5.3. Technologies, elements and suppliers involved

This is a detailed list of the elements involved on our defined IoT Ecosystem.

Device A:

- Device: Mobile Phone
- Supplier: Samsung
- Model: Galaxy S6 SM-G920F
- O.S.: Android 7.0 (Supplier Google)
- Android Patch Security Level: 1 of June 2018
- Application:
    - Downloaded from Play Store
    - Name: KANDY Communicator [48]
    - Supplier: Fringland (Ribbon)
    - Version: 7.0.3.131 -25

Network provider – Device A:

- Supplier: Movistar (Telefonica)
- Type of connection: 4G+

UCaaS / PaaS on the Cloud provider (cloud computing, Storage, Data and Analytics)

- Supplier: Ribbon
- Type of connection: Internet

Network provider – Device B:

- Supplier: Vodafone
- Type of connection: Wi-Fi & optical fiber

Device B:

- Device: Laptop
- Supplier: DELL
- Model: Latitude E7440
- O.S.: Windows 8 (Supplier Microsoft)
- Application:
    - Kandy Communicator Web Client [49]
    - Supplier: Ribbon
    - Opened in Google Chrome
    - Version: 73.0.3683.103

Using the previous diagram where we could see the different suppliers involved on the IoT Ecosystem, taking into account the elements involved on our ecosystem we will have the following picture:

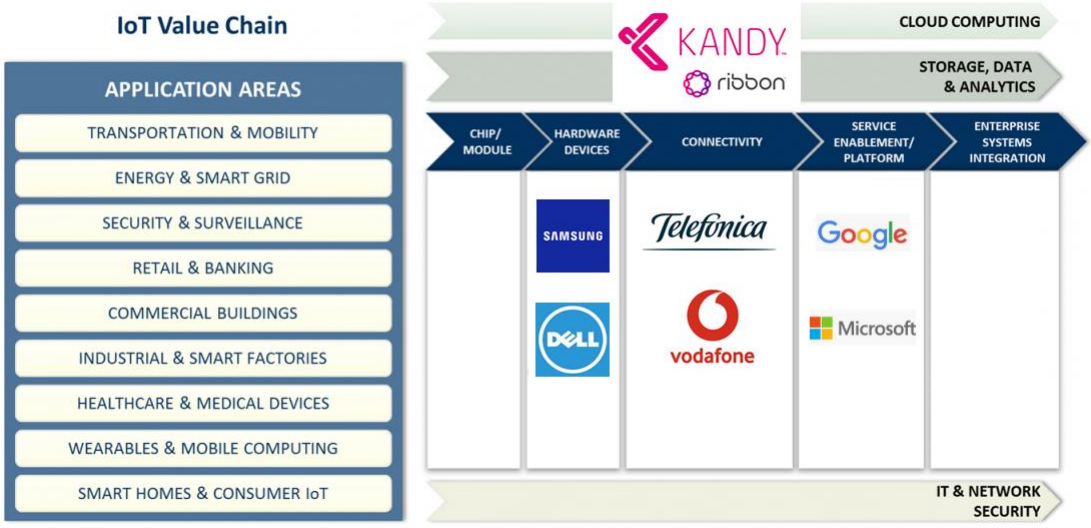

Figure 14 – Suppliers in the defined UcaaS IoT Ecosystem example

Although some areas appear in white, it does not mean that there are no other suppliers involved. The HW devices involved on the IoT Ecosystem have chips and modules made by other suppliers. As well, on the networks from the service suppliers (Vodafone, Telefónica and Kandy) there are other kind of HW devices as routers, call centers, switches, etc. However, we do not have additional information about these elements, but indeed, there are other HW suppliers, chip module suppliers and also suppliers that provide the service enablement, the enterprise system integration and the network security. As we mention before, we suppose that these suppliers' networks are safe environment and therefore we will not take into account these other suppliers, HW elements or firmware versions. This information is confidential of these companies and we cannot have access to it.

5.4. Implementation

Ribbon offers to create a user with five free tests accounts to particular users to test and try the Kandy services [50].

On the Kandy portal, I created a domain called nomial and 2 test users accounts. After signing in and creating these test users accounts users I received the following email:

> Congratulations! Your account has been activated and you've created your first Kandy Project! To help speed things along, we created two user accounts for your project for you.
>
> Here are the details:
>
> **Kandy Project:**
>
> - Test

User 1:

- Username: user1@nomial.com
- Password: a76wk8r4a

User 2:

- Username: user2@nomial.com
- Password: a1ieq0opla

Please make note of these usernames and passwords so you and your first users can log in and start using all of the great Kandy features!

Thanks,
Kandy

Recently Ribbon has decided not to offer the Kandy cloud services to end particular users and provide it only to enterprise customers. Therefore, the testplan scheduled at the beginning of this project cannot be completed. Now the access to the portal is no longer valid and the test accounts has been removed.

As we can see on Kandy web page this server is not active at the moment [51], so we cannot connect to the Kandy cloud to perform a test call.

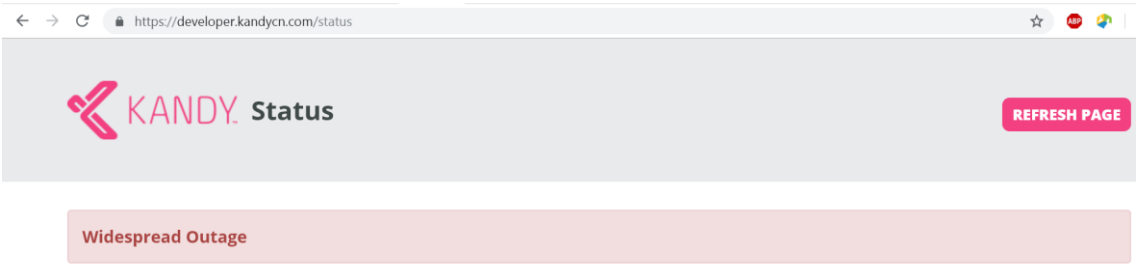

Figure 15 – Kandy for Customer Service Status

The application on the mobile app also display a red line that means that it cannot register into the Kandy cloud platform.

Figure 16 – Kandy Communicator App for Android Status

Due to these technical problems, we cannot make a real implementation of this IoT Ecosystem on this Mater thesis report and therefore the analysis of the security issues will be done only from a theoretical point of view.

5.5. Security analysis

Even in this simple IoT Ecosystem that include only 2 devices and the cloud we are expose to different security problems.

As we have done along the previous chapters, we will start locating the main security problems related with the technologies used. Then we will analyze the security vulnerabilities to which this IoT Ecosystem can be exposed due to the devices that compose it and review how the data and the information is sent, transfer, process and storage along the IoT ecosystem. Along the process, we will review the implications that these problems might have on the companies from a business perspective.

5.5.1 Security problems related with the technologies used

As we have mentioned, Kandy is a SaaS solution for UCaaS offered by Ribbon, this means that there's no need for the end clients (users or companies) to install any kind of hardware on premise in order to access to this service that is available in the cloud (accessible via Internet).

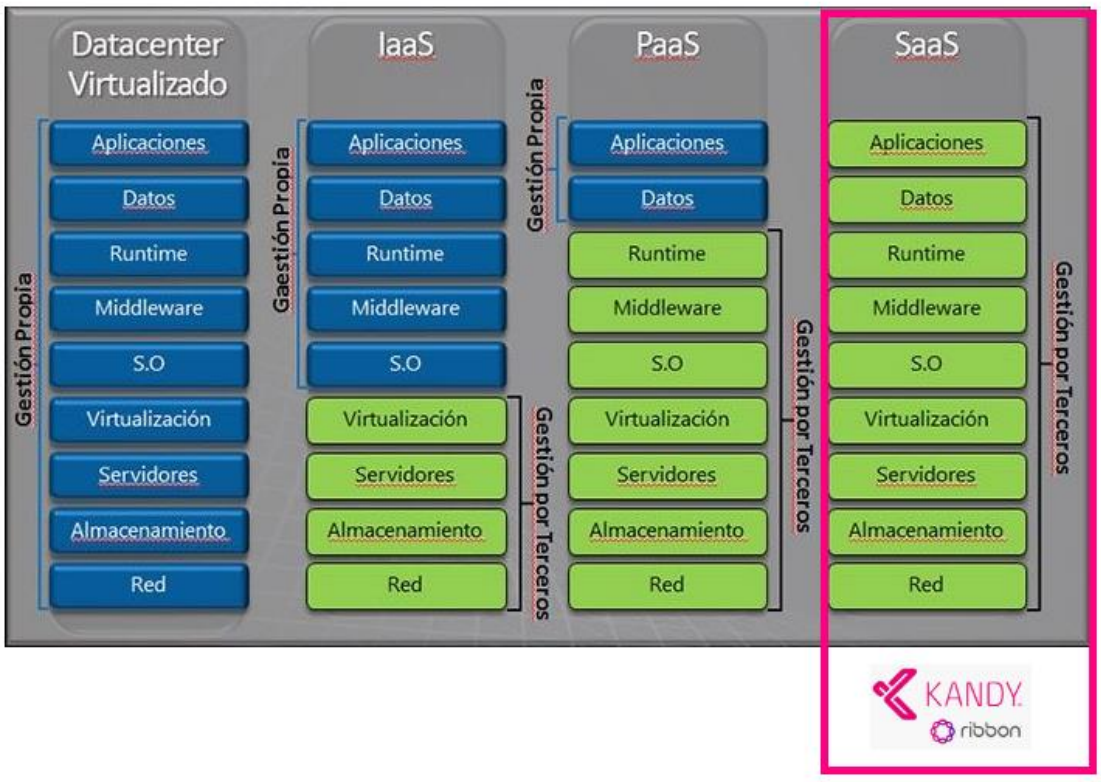

Figure 17 – Kandy SaaS for Unified Communications

This also means that Ribbon will be the company that will take care of the security at this level. They will prevent attackers to access to their virtualized servers to gain access to the different VM and also, they will cover the hosting and it security by doing network monitoring, preventing DDoS attacks, blocking unwanted connections using firewalls or backlisting and making backups to prevent data loss. As they are the cloud service providers they will take care that the cloud can be considered a safe environment and that all the information, data and process that is done over it is done in a secure way.

5.5.2 Security problems in the IoT Ecosystem

However, in order to reach the cloud the users should connect to it over Internet access. This internet access can be offered by different companies, in our example we have 2, Telefónica (Movistar) and Vodafone. Each company provide Internet access to a different end user and also using different technologies. For example, the end user connecting to the cloud using his mobile phone is connected over 4G+ connection to Telefonica's network and then Telefónica connect this user to Internet so it can reach Kandy cloud.

The data that is sent via 4G is encrypted, so it is considered a secure way to transfer data however, as Norton mentioned [52] even if it's not easy to hack a 4G connection, there has been few successful cases of people hacking it, so it can be compromised. On the other hand, using a 4G connection is much safer than using Wi-Fi for instance, as the user B is doing with Vodafone. Wi-Fi security will depend on the router configuration (most of the end users do not modify the default configuration and credentials set by the suppliers so they make easy to hackers to gain access to their Wi-Fi networks).

As Ribbon, and its customers cannot guarantee that the end users that connect to the cloud are using secure connections, the solution provide use a secure end-to-end connection. The users that connect to the cloud using the mobile or the web app will stablish a secure path between the end application and the cloud server to transfer the information minimizing attacks like man-in-the-middle caused by using non-secure connections by one or some of the end users.

On the graph below, we can see how the end devices are connected to the cloud using WebRTC sent over https connection in a secure way:

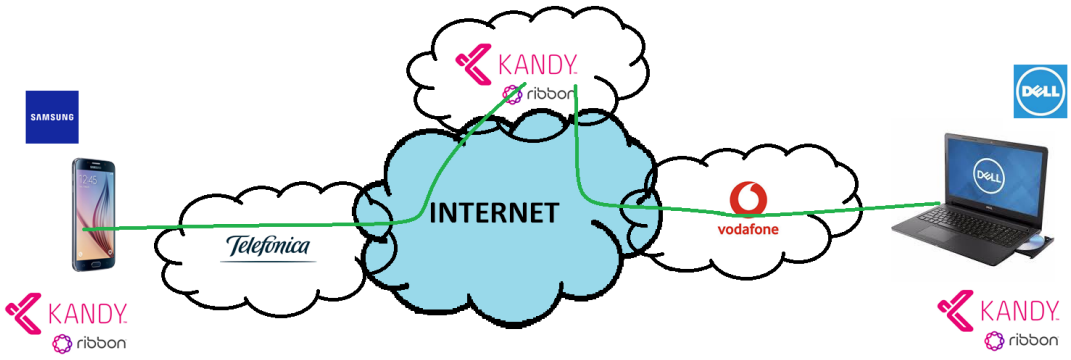

Figure 18 – UCaaS connection

With this all these points mentioned, Ribbon is taking care that the data is being transferred in a secure way along the IoT Ecosystem protecting the confidentiality and the integrity of this data, and preventing sabotage or access to sensitive data of unauthorized users.

We have analyze already how the data is being transferred and sent in a secure way. We understand that it is also process in a secure way because the main process of the service is done on the cloud, which is a safe environment, and this is where the main information is stored. However, there is other place where the information is store and processed which are the end devices.

That is why it is important to keep the devices updated to the latest firmware version. In the case of an attack, the hacker will only be able to access to the device data, which is not as critical as accessing to the cloud information that contains the data of all the users of the service. The device suppliers, in this case Samsung and Dell works with the S.O. suppliers (Google and Microsoft) in order to try to approve and provide to the end users the latest firmware version that fix the security problems already known. As we have mentioned, the security vulnerabilities found are commonly being listed and open so anyone can read them. If the users are having an old version that still contains one of these known vulnerabilities, the attackers can take advantage of this and access to the device information.

Another point that is important to know is that the mobiles and web applications are also being identified by using a User-Agent identity so the cloud can identify the different devices that are connected to their systems so it can made backlisting in case of an anomaly detection.

This is also useful to block certain kind of attacks for DDoS. Keeping the data safe it is important but if the service is not available the IoT Ecosystem do not make sense for the end users. As we have seen during the implementation, Ribbon has decided to stop offering Kandy service to particular customers, so the service is not available. In this case is the self-supplier the one that have decide to turn off the service, but actually this will be exactly the same scenario that an end user will find after a successful DDoS attack. The user will not be able to register into the Kandy cloud and therefore he will not be able to use the services neither.

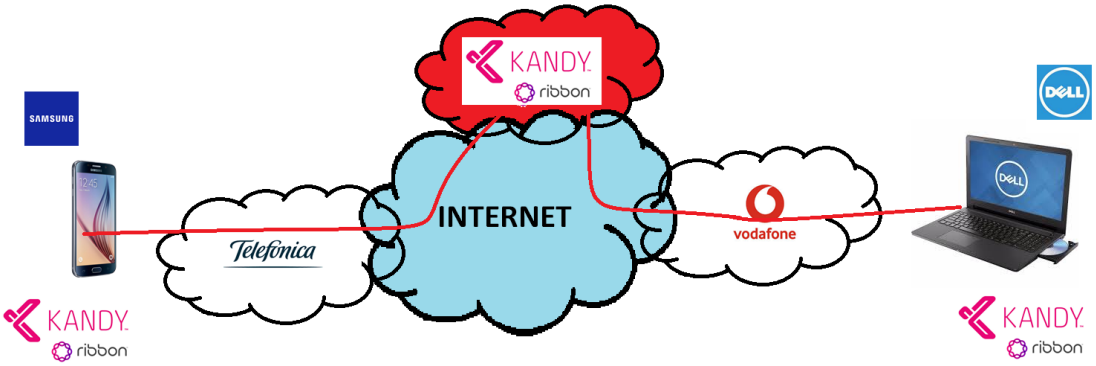

Figure 19 – UCaaS out of service

5.5.3 Business Implications

From a business perspective, the availability of the service is so important. Imagine that the company that have decided to bought this UCaaS service is Pizza Hut, if the cloud services are not available, their employees won't be able to make or received calls and therefore they will lose money and their customers confident.

Ribbon is aware of this problem and the importance of the availability of the service and the data. That is why they commits that this service have high availability. In order to obtain this, the cloud should be prepared to react and stop DDoS attacks but also to have high availability of the servers virtualized (redundancy and geo-redundancy).

This geo-redundancy is also important to cover some legal necessities. As we mentioned there are laws as the GDPR to which this service have to be compliant, therefore depending on the situation of the company's employees the solution should be provided on a different way to cover the legal requirements of each region.

Based on all this analysis we can consider this example as a secure IoT Ecosystem as it is covering that the information is secure (the IoT Ecosystem cover the confidentiality, the integrity and the availability of the data), and it also provide a high availability for Enterprise customers of the service.

6. Improvement plan

Most of the improvements related with security can and should be done on the cloud side, because here is where the most powerful processors are and where the service is provided.

The cloud should be constantly being updated to have the latest firmware of the servers that make it up to prevent open and known vulnerabilities to be available to attackers. This revision can be done manually by a user that review that all the servers are updated or automatically by a server that compares the current firmware version with the latest one provided and recommended by the suppliers.

There are some suppliers that provide products to protect different elements of the ecosystem like Sophos for example [53]. There could be an integration also between Sophos application and the Kandy app for Android and iOS, but for instance, this require the user or the company to buy extra service and licenses from Sophos which is something that will raise the price. Most of the end users are not conscious of the security problems that they might have and in most of the cases they prefer not to pay an extra service for a secure connection. Some services providers as Vodafone offer their own solution to protect the network as Vodafone Secure Net [54] as an extra service as well.

As we cannot expect that all the end customers are taking care of the security of their devices, the cloud should protect itself from attacks that might come also from these known users. The cloud cannot consider any device out of it environment as a trusted device.

The cloud can be implemented to detect some kind of attacks and block them automatically and informing the administrators about this preventive action that has been made. Based on the new technologies of artificial intelligence the cloud there would be a day when it will be smart enough to keep learning by itself the kind of attacks it is facing and how to protect from these.

As Exabeam mentioned [55] security Intelligence is the collection, evaluation, and response to data generated on an organization's network undergoing potential security threats in real-time. This company also provide a security platform based on this security intelligence named as Security Management Platform [56].

7. Conclusions

This project has help me to have a better understanding of what is an IoT Ecosystem, the technologies related and the architecture that compose it. I have also now a better understanding about the main security problems to which these IoT Ecosystem are exposed. Other point that we have covered along this project is how these security problems can affect to the business of a company.

Although one of the objectives proposed at the beginning was the implementation of the IoT Ecosystem for business example, due to the decision of Ribbon to stop offering this free service to end users I could not end the implementation and run the security test on it. However, we have defined the main security problems of this IoT Ecosystem from a theoretical perspective.

The methodology and the planning has been followed along this project as planned, the main change is related with the tasks planned related with the implementation and the test plan that has been replace by the deeper analysis of the security issues.

About the improvements, we could only define them from a theoretical perspective also, because as mentioned, the main security improvements should be done on the cloud environment to which we cannot have access. We have recommended some solutions based on the new security, automation and machine learning technologies. However probably Ribbon is aware of all these technologies and they are working on the cloud to include all the security improvements as possible.

8. Glossary

AWS	Amazon Web Services
BYOD	Bring Your Own Device
CPaaS	Communication Platform as a Service
DDoS	Distribute Denial of Service
HW	Hardware
IaaS	Infrastructure as a service
IDCs	Internet data centers
IIoT	Industrial Internet of Things
IoT	Internet of things
IP	Internet Protocol
ISMS	Information Security Management System
GDPR	General Data Protection Regulation
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
LTE	Long Term Evolution
OS	Operating System
PaaS	Platform as a service
PC	Personal computer
SaaS	Software as a service
SW	Software
UCaaS	Unified Communications as a service
UIDs	Unique identifiers
VoIP	Voice over IP

9. Bibliography

[1] Rouse, M. (2019, February). *Internet of things (IoT)*. TechTarget. Retrieved March 2019. <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>

[2] SIEMENS. CISCO. Member of the Charter of Trust. *Security at the scale of IoT*. Retrieved March 2019. <https://new.siemens.com/global/en/company/topic-areas/digitalization/cybersecurity/partner-cisco.html>

[3] Telefonica IoT. (2018, October). *Previsiones de crecimiento de IoT*. Telefonica. Retrieved March 2019. <https://iot.telefonica.com/blog/previsiones-de-crecimiento-de-iot>

[4] Ribbon. *Internet of Things Solutions*. Retrieved March 2019. <https://www.kandy.io/kandy-provides/internet-things-solutions>

[5] Hayes, Nicola. (2012, October). *Is the time now right for network virtualization?*. Retrieved March 2019. <https://www.datacenterdynamics.com/news/is-the-time-now-right-for-network-virtualization/>

[6] Yuanjiong, Diao. *Access Network Virtualization Enables Network Transformation*. ZTE. Retrieved March 2019. <https://www.zte.com.cn/global/about/magazine/zte-technologies/2016/4/en_711/459173>

[7] Marketing Bitec. (2017, June). *Adoptando la nube: ¿Nube híbrida, privada, IaaS, PaaS, o SaaS?.* Bitec. Retrieved March 2019. <https://www.bitec.es/servicios-cloud/adoptando-la-nube-nube-hibrida-privada-iaas-paas-o-saas/>

[8] Frankenfield, Jake. (2019, April). *Cloud Computing*. Investopedia. Retrieved April 2019. <https://www.investopedia.com/terms/c/cloud-computing.asp>

[9] Athow, Desire. (2018, June). *What are the different types of web hosting?*. Techradar. Retrieved April 2019. <https://www.techradar.com/news/what-are-the-different-types-of-web-hosting>

[10] Frankenfield, Jake. (2019, April). *Cloud Computing*. Investopedia. Retrieved April 2019. <https://www.investopedia.com/terms/c/cloud-computing.asp>

[11] Marketing Bitec. (2017, June). *Adoptando la nube: ¿Nube híbrida, privada, IaaS, PaaS, o SaaS?.* Bitec. Retrieved March 2019. <https://www.bitec.es/servicios-cloud/adoptando-la-nube-nube-hibrida-privada-iaas-paas-o-saas/>

[12] Banerjee, Sukamal. (2019, February). *IoT and UCaaS: Changing face of corporate communication (and how to get it right).* IoT Agenda. Retrieved April 2019. <https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/IoT-and-UCaaS-Changing-face-of-corporate-communication-and-how-to-get-it-right>

[13] Cabello, Carlos. (2016, July). Por qué si aprendiste a manejarte en la nube (cloud), ahora tendrás que hacerlo en la niebla (fog computing). Nobbot. Retrieved April 2019. <https://www.nobbot.com/redes/fog-computing/>

[14] Butler Brandon. (2017, September). *What is edge computing and how it's changing the network.* NetworkWorld. Retrieved April 2019. <https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html>

[15] Pastor, Javier. (2018, December). *Edge Computing: qué es y por qué hay gente que piensa que es el futuro.* Xataka. Retrieved April 2019. <https://www.xataka.com/internet-of-things/edge-computing-que-es-y-por-que-hay-gente-que-piensa-que-es-el-futuro>

[16] Lance, Eliot. (2018, January). *Edge Computing for AI Self-Driving Cars*. Aitrends. Retrieved April 2019. <https://www.aitrends.com/ai-insider/edge-computing-ai-self-driving-cars/>

[17] Balaban, David. (2019, January). *Web Hosting Security Best Practices*. Tripwire. Retrieved April 2019. <https://www.tripwire.com/state-of-security/featured/web-hosting-security-best-practices/>

[18] Butler Brandon. (2017, September). *What is edge computing and how it's changing the network.* NetworkWorld. Retrieved April 2019. <https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html>

[19] *What is IP spoofing?.* Kasperksy. Retrieved April 2019. <https://usa.kaspersky.com/resource-center/threats/ip-spoofing>

[20] *Defending Yourself from a Man in the Middle Attack*. Kasperksy. Retrieved April 2019. <https://usa.kaspersky.com/resource-center/threats/man-in-the-middle-attack>

[21] *Distributed Denial of Service: Anatomy and Impact of DDoS Attacks*. Kasperksy. Retrieved April 2019. <https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work>

[22] Coppol, Sofia. (2018, August). *How Internet of things (IoT) is transforming the future business landscape.* Hackernoon. Retrieved April 2019. <https://hackernoon.com/how-internet-of-things-iot-is-transforming-the-future-business-landscape-e6ef7fea5b2b>

[23] T-Systems. (2018, February). *¿Qué es IIOT y en qué se diferencia de IOT?.* Retrieved April 2019. <https://www.t-systemsblog.es/que-es-iiot-diferencia-iot/>

[24] Vector ITC. (2018, March). IIoT: Cuando el Internet de las Cosas llega a la Industria. Retrieved April 2019. <https://www.vectoritcgroup.com/tech-magazine/innovation-trends/iiot-cuando-el-internet-de-las-cosas-llega-a-la-industria/>

[25] Zafarino, Stephen. (2018, September). *What businesses need to know about the future of IoT*. IoT Agenda. Retrieved April 2019. <https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/What-businesses-need-to-know-about-the-future-of-IoT>

[26] Avast Business Team. (2019, February). *What risks do IoT security issues pose to businesses?.* Avast. Retrieved April 2019. <https://blog.avast.com/iot-security-business-risk>

[27] CISCO. (2017). Security Professionals' Biggest Sources of Concern Related to Cyber Attacks. Retrieved April 2019. <https://www.cisco.com/c/dam/assets/prod/sec/images/1080/Figure-1-Security-Professionals-Biggest-Sources-of-Concern-Related-to-Cyber-Attacks.png>

[28] Zafarino, Stephen. (2018, September). *What businesses need to know about the future of IoT*. IoT Agenda. Retrieved April 2019. <https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/What-businesses-need-to-know-about-the-future-of-IoT>

[29] Rouse, Margaret. (2018, May). *Social engineering*. TechTarget. Retrieved April 2019. <https://searchsecurity.techtarget.com/definition/social-engineering>

[30] ForcePoint. *What is a Phishing Attack?.* Retrieved April 2019. <https://www.forcepoint.com/es/cyber-edu/phishing-attack>

[31] NVD. *National Vulnerability Database*. NIST. Retrieved April 2019. <https://nvd.nist.gov/>

[32] Rouse, Margaret. (2011, June). A*pplication blacklisting.* TechTarget. Retrieved April 2019. <https://searchsecurity.techtarget.com/definition/application-blacklisting>

[33] Rouse, Margaret. (2018, April). *Vulnerability assessment (vulnerability analysis).* TechTarget. Retrieved April 2019. <https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis>

[34] Piejko, Pawel. (2016, March). *What is device detection?*. Device Atlas. Retrieved April 2019. <https://deviceatlas.com/blog/what-is-device-detection>

[35] Techopedia. *Anomaly Detection*. Retrieved April 2019. <https://www.techopedia.com/definition/30297/anomaly-detection>

[36] Chandrayan, Pramod. (2017, December). *All About Edge Computing- How It Is Changing The Present Past & Future Of IoT?.* Codeburst.io. Retrieved April 2019. <https://codeburst.io/edge-computing-iot-a-partnership-that-will-rule-the-connected-world-in-2018-70737afade84>

[37] Newgenapps. (2018, May). *IoT Ecosystem Components: The Complete Connectivity Layer*. Retrieved April 2019. <https://www.newgenapps.com/blog/iot-ecosystem-components-the-complete-connectivity-layer>

[38] Frost and Sullivan. Retrieved May 2019. <https://ww2.frost.com/>

[39] Microsoft Azure. *What is Azure?.* Microsoft. Retrieved May 2019. <https://azure.microsoft.com/en-us/overview/what-is-azure/>

[40] IBM. *What is IBM Cloud?.* Retrieved May 2019. <https://www.ibm.com/cloud/>

[41] AWS. *Start Building on AWS Today*. Amazon. Retrieved May 2019. <https://aws.amazon.com/>

[42] AWS. *AWS IoT*. Amazon. Retrieved May 2019. <https://aws.amazon.com/iot/>

[43] Ribbon. (2017, February). *Kandy Platform Brings "Human Element" to IoT Connectivity with Contextual Real-Time Communications Solutions*. Retrieved May 2019. <https://ribboncommunications.com/company/media-center/press-releases/kandy-platform-brings-human-element-iot-connectivity-contextual-real-time-communications-solutions>

[44] Kandy. *Cloud Communications Platform as a Service*. Ribbon. Retrieved May 2019. <https://www.kandy.io/>

[45] CISCO. *Internet of Things (IoT).* Retrieved May 2019. <https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html?dtid=osscdc000283>

[46] AURA. *Movistar Home*. Telefonica. Retrieved May 2019. <https://aura.telefonica.com/movistarhome>

[47] Lacort, Javier. (2012, May). *WannaCry, el ransomware del ataque a Telefónica*. Hipertextual. Retrieved May 2019. <https://hipertextual.com/2017/05/wannacry-ransomware-ataque-telefonica>

[48] Fringland. (2016, September). *Kandy Communicator*. Google Play. Retrieved May 2019. <https://play.google.com/store/apps/details?id=com.kandy&hl=en>

[49] Ribbon. *Kandy Communicator Web*. Retrieved May 2019. <https://communicator.kandy.io/>

[50] Ribbon. *Kandy Registration*. Retrieved May 2019. <https://www.kandy.io/register>

[51] Ribbon. *Kandy for customers Status*. Retrieved May 2019. <https://developer.kandycn.com/status>

[52] Symantec employee. *How safe is surfing on 4G vs. Wi-Fi?.* Norton. Symantec. Retrieved May 2019. <https://us.norton.com/internetsecurity-wifi-how-safe-is-surfing-on-4g-vs-wi-fi.html>

[53] Sophos. *Business products.* Retrieved May 2019. < https://www.sophos.com/en-us.aspx>

[54] Vodafone. *Vodafone Secure Net*. Retrieved May 2019. <https://securenet.vodafone.es/>

[55] Exabeam. *What is security Intelligence?.* Retrieved May 2019. <https://www.exabeam.com/glossary/security-intelligence-definition/>

[56] Exambeam. *The Exabeam Security Management Platform*. Retrieved May 2019. <https://www.exabeam.com/product/>