Analysis and study of data security in the Internet of Things paradigm from a Blockchain technology approach

Titulació: Màster Universitari en Enginyeria de Telecomunicació UOC-URL
Autor: David Rull Aixa
Consultor: Raúl Parada Medina

Responsable: Carlos Monzo Sánchez
Àrea del TFM: Sistemes de comunicació
Data Lliurament 11/01/2018

a Déu

FITXA DEL TREBALL FINAL

Títol del Treball:	Analysis and study of data security in the Internet of Things paradigm from a Blockchain technology approach
Nom de l'autor:	David Rull Aixa
Nom del consultor/a:	Raúl Parada Medina
Nom del PRA:	Carlos Monzo Sánchez
Data de lliurament (mm/aaaa):	01/2018
Titulació o programa:	Màster Universitari en Enginyeria de Telecomunicació UOC-URL
Àrea del Treball Final:	Sistemes de Comunicació
Idioma del Treball:	Anglès
Paraules clau	Blockchain technology, IoT paradigm, security and data privacy, smart contracts, IoT vulnerabilities

Resum del Treball (màxim 250 paraules): *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball*

La tecnologia Blockchain ha guanyat interès en els últims anys d'ençà que es va presentar el seu concepte per primera vegada l'any 1991 per Stuart Haber i W.Scott Stornetta, gràcies a la seva capacitat de millorar la integritat de les transaccions a través de la xarxa entre qualsevol entitat.
L'aplicació d'aquesta tecnologia en el camp de la IoT (Internet of Things) busca garantir la seguretat i privacitat de les dades de la interconnexió digital de dispositius físics via Internet.

En aquest projecte s'analitzen les vulnerabilitats de les tecnologies i escenaris més importants de la IoT i les millors contramesures per combatre aquestes vulnerabilitats. També es fa un estudi de les contribucions i solucions més importants d'alguns investigadors per protegir les dades.
Després es fa una anàlisi de la tecnologia Blockchain i els beneficis de la combinació d' aquesta amb la IoT a través de l' estudi dels projectes i contribucions d' articles i publicacions més importants.

Finalment, proposo alguns escenaris innovadors en els quals es podria treure benefici de la convergència de la IoT amb la Blockchain.

En conclusió, aquest projecte és un espai d' informació i coneixement del paradigma IoT i la tecnologia Blockchain amb l' anàlisi d' articles de recerca més rellevants i l' estudi de les amenaces més importants de les tecnologies i escenaris del IoT. Tanmateix, s'ofereix una visió general de l'estat actual del paradigma des de la perspectiva de la seguretat i les oportunitats que la seva combinació amb la tecnologia Blockchain pot aportar a la societat.

Abstract (in English, 250 words or less):

Blockchain technology has gained interest in recent years since its concept was first introduced in 1991 by Stuart Haber and W.Scott Stornetta, thanks to its ability to improve the integrity of transactions through the network between any entity.
The application of this technology in the field of IoT (Internet of Things) seeks to guarantee the security and privacy of the data of the digital interconnection of physical devices via the Internet.

This project analyzes the vulnerabilities of the most important technologies and scenarios of the IoT and the best countermeasures to combat these vulnerabilities.
Besides, I expose the most important projects and contributions of some researchers and their solutions to protect data.

Then, an analysis of the Blockchain technology is done, and the benefits that the combination of this technology with the IoT can provide.
Finally, I propose some innovative scenarios that could benefit from the convergence of IoT with Blockchain.

In conclusion, this project is a space for information and knowledge of the IoT paradigm and the Blockchain technology with the analysis of the most relevant research articles and the study of the threats of the main technologies and scenarios within IoT.

Besides, I expose a general overview of the current state of the paradigm from the perspective of security and the opportunity that its combination with the Blockchain technology can bring to our society.

Índex

1. Introduction

During the last decade the IoT (Internet of Things) has been gradually introduced into our lives thanks to the availability of wireless communication systems.
IoT paradigm embraces many concepts; intelligent devices that collect data from the environment, many different technologies to allow their connection, services and standards, and all the elements that take part.

1.1 Context and justification of the project

IoT can bring many benefits to society in many different ways, but it is very important to be mindful so the best solution can be found to protect data privacy.
The great challenge of the IoT is to find a reliable communication environment that guarantees the security of the data transmitted between all the connected devices.
One of the possible solutions could be the convergence between IoT and Blockchain technology, and it is analyzed in this project.

There are three core elements referenced in a IoT architecture:

1.Things. Devices that have a means of connecting to a wider network.

2.Network. Connect the multiple devices to the cloud.

3.Cloud. Remote servers in a data centre which function is to consolidate and store the data in a safe way.

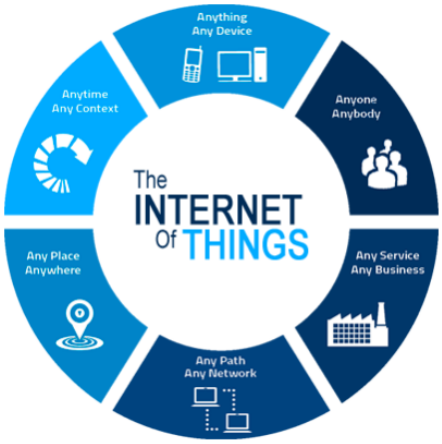

Figure 1. IoT paradigm illustrated
Source. http://mozitech.com/internet-of-things-beyond-our-current-imagination/

Blockchain technology has the potential to secure this environment thanks to cryptography, which seeks that all consumers have a secret and unique key through which access your data.

Open protocols based on Blockchain can standardize the use of RFID, GPS, all types of common sensors in the assembly lines of the industrial sector to automate data safely. Many sectors would be beneficiaries of this technology such as Healthcare or the transport and logistics sectors, which will also be able to obtain great benefits from using it to integrate the advantages of the IoT.

The advantages it offers include decentralization and transparency of information, everyone is at the same hierarchical level, preventing a main organizer from incorrectly using the data.
Although currently it cannot ensure the desired environment in a completely safe way, many companies and organizations work to improve this Internet coverage of things more and more. It does not make impossible to avoid attacks, but it does make them much more difficult to produce.
Many studies are currently focused on using homomorphic encryption. In the past, it has already been shown that this encryption was feasible, but requires much more time than conventional processes, and still works to improve it. At the moment there is not a robust plan to maintain the desired security in this environment and attacks on devices are the main danger to address.

This project focuses on the need to analyze all the information through several studies and research carried out in the field of IoT, Blockchain and its convergence, and expose what are the best solutions to fight against the vulnerabilities of the main technologies that take part of Internet of Things.
The expected result is to gather the key information of IoT paradigm related to security and the best mechanisms to guarantee the integrity and privacy of data within IoT.
Another goal is to allow other people interested in this field to access easily to information and knowledge collected in this project and also the information from many research articles that are organized by topics.
Besides, I propose some scenarios where could converge IoT and Blockchain technology in the future.

1.2 Aims of the project

-Expose the concepts of IoT (Internet of Things) and Blockchain in detail, make a study of their current impact on society, and their future perspectives as potential applications.

-Make a study with research articles and publications that relate these concepts, highlighting the most important contributions.

-Analyze the data privacy in the exchange of data between the main IoT technologies and what are the best countermeasures to avoid the possible threats.

-Analyze the challenges and opportunities of the convergence between IoT and Blockchain technology.

-Propose some possible scenarios of Internet of Things using Blockchain technology, which could be applied in the future.

1.3 Approach and method followed

The strategy to carry out this project is to look for information and study the most important measures that have been presented until nowadays of the IoT paradigm and also of its convergence with Blockchain technology through articles about research and publications. Then, expose the most important information that is related to the study of the privacy and security of the data, as well as the best mechanisms and protocols that can address the vulnerability issues and promote trusted environments that can prevent attacks.

The chosen strategy is the result of having access to valuable information due to the fact that many projects related to IoT and Blockchain technology are still undergoing experimentation and they bring different interesting approaches and concepts.
It is important to consider what is called the IoT system, that represents not only the IoT device, but the whole ecosystem that makes it work, such as web interfaces, related applications, cloud services, and the other devices that interact with it. It also represents the connection that is created between organizations, suppliers and competitors.

The detection and correction of attacks on IoT systems will become an increasingly important part of business security and the privacy of consumers' data that uses technology devices for almost all sectors of society.

1.4 Plan of the project

The realization of this project is divided into different tasks. Here I list these tasks that have to be done, related to different PACS with the start and end dates. Below, figure 2 shows the Gantt Chart.

Tasks	Start	End
PAC 1: Introduction	22/09/2017	02/10/2017
Define the topic of the Project	22/09/2017	29/09/2017
Present the motivation and structure	28/09/2017	01/10/2017
Define and plan the aims	28/09/2017	01/10/2017
Check and deliver PAC 1	02/10/2017	02/10/2017
PAC 2: State of art	03/10/2017	16/10/2017
Study of the IoT paradigm and related concepts	03/10/2017	07/10/2017
Analysis of the Blockchain technology	08/10/2017	15/10/2017
Study of the convergence between IoT and Blockchain	08/10/2017	15/10/2017
Check and deliver PAC 2	16/10/2017	16/10/2017
PAC 3: Results of research and analysis	17/10/2017	17/12/2017
Study of the protocols and technologies of the IoT	17/10/2017	25/10/2017
Study and analysis of the vulnerabilities of IoT technologies	17/10/2001	25/10/2017
Analysis of IoT solutions through research articles	26/10/2017	07/12/2017
Study of IoT-Blockchain research articles	26/10/2017	07/12/2017
Propose scenarios IoT-Blockchain for future applications	06/12/2017	16/12/2017
Check and deliver PAC 3	17/12/2017	17/12/2017
PAC 4: Redaction of the Thesis	18/12/2017	11/01/2018
Redaction of the Thesis	18/12/2017	08/01/2017
Conclusions	08/01/2017	09/01/2018
Appendix	09/01/2018	10/01/2018
Check and deliver PAC 4	11/01/2018	11/01/2018
PAC 5: Master's Thesis defense	12/01/2018	21/01/2018
Review the memory	12/01/2018	12/01/2018
Plan and assemble the presentation	13/01/2018	20/01/2018
Check and deliver PAC 5	21/01/2018	21/01/2018

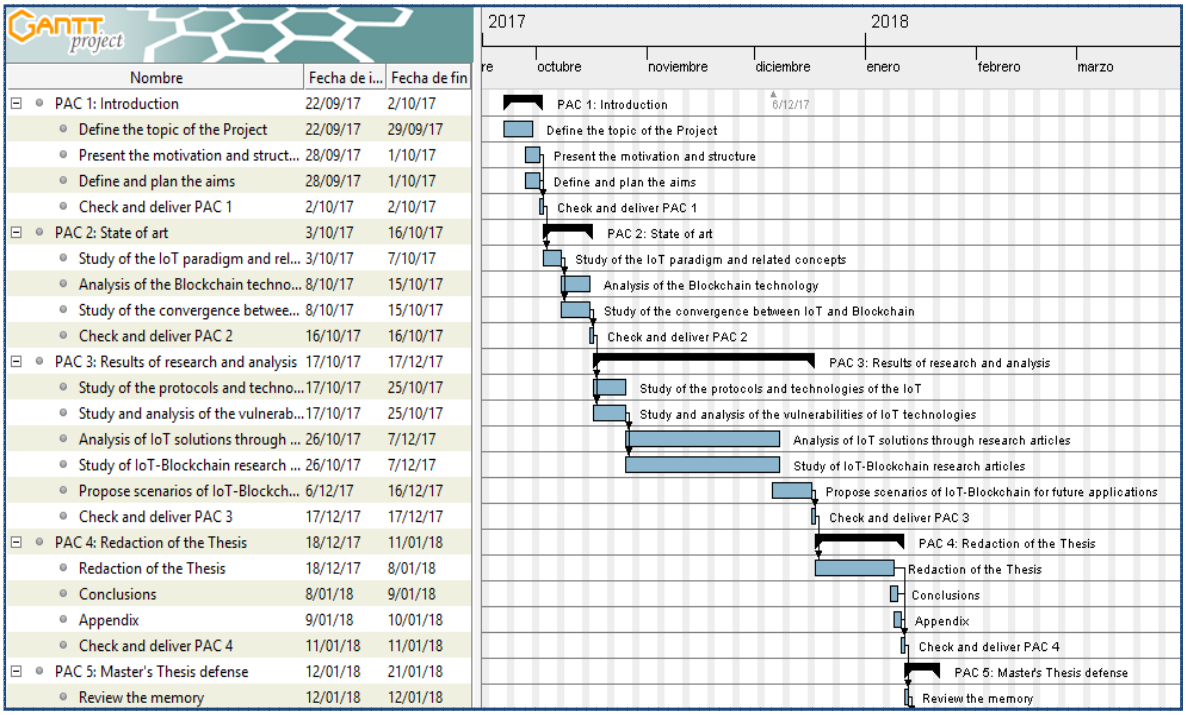

Figure 2. Gantt Chart with the project schedule

1.5 Summary of products obtained

I have detailed the most important attacks that can be done with the different IoT technologies and possible countermeasures to mitigate them.

It has been explained which are the most important threats in the most commonly IoT environments and how to avoid these threats.

On the other hand, I have summarized the most important contributions of research articles in two subjects:

-Articles that provide security solutions and present mechanisms and tools to protect data within the IoT paradigm.

-Articles that provide solutions based on the convergence of the IoT with Blockchain technology.

Finally, some scenarios have been proposed where the convergence between the IoT and the Blockchain technology could be applied in the future, explaining the key concepts and general features.

1.6 Description of the other sections of the memory

In section 2 I present the IoT paradigm with its most important protocols and architectures introducing the most important IoT technologies: RFID (Radio Frequency Identification), WSN (Wireless Sensor Networks), NFC (Near Field Communication), Bluetooth, BLE (Bluetooth Blow Energy), Wi-Fi, WiMAX (Worldwide Interoperability for Microwave Access), Z-Wave, LoRa and the Cloud Computing paradigm.
In section 3 I introduce and explain Blockchain technology with its most important features and the related concepts.
In section 4 I explain the vulnerabilities of IoT technologies (that are presented in Section 2) and I propose mechanisms to fight against them.
In section 5 I expose the vulnerabilities of the most common scenarios, and the countermeasures that mitigate them. These scenarios are: Smart Home, Smart Grids, Connected Industry, Connected Health, Connected car and Supply Chain.
In section 6 I summarize important proposals of several articles that seek solutions to guarantee the data security and privacy within the IoT.
In section 7 I explain the advantages of the convergence between the IoT and Blockchain technology and the most important solutions that have been done taking the opportunities of their combination.
In section 8 I propose scenarios and ideas where the combination of IoT with Blockchain could be applied in the future.

2. Internet of Things

The term *the Internet of Things* it is about to connect daily elements to the Internet to take advantage of the possibilities provided by the almost immediate communication between different elements and systems. This is possible, above all, thanks to the improvement of communication networks and storage and processing systems, as well as the enormous evolution of the technology that allows to provide the necessary connectivity to any device.

2.1 IoT

The concept of ***IoT*** was established by Kevin Ashton in 1999, a British technology pioneer who founded the Auto-ID Center, Massachusetts [1] at MIT (Massachusetts Institute of Technology), a private university in Cambridge, which is often ranked as one of the world's most prestigious universities.

Internet of Things brings promising challenges and opportunities. Research on IoT has important economic and social value for the development of the next generation of information, network, and communication technologies.

2.2 IoT paradigm

There is no universally accepted definition of IoT, because this paradigm not only describes a new type of technical architecture but also a new concept that defines how we interact with the physical world.

Here I expose two definitions of the concept that I have chosen from IEEE *(Institute of Electrical and Electronics Engineers)* and ITU (International Telecommunications Union) [2]:

-*IEEE* defines IoT as "*a* network of items (each embedded with sensors) which are connected to Internet". (Special report on Internet of Things in March 2014).

-*ITU* defines IoT as "ubiquitous network in which the concept of ubiquitous is founded upon the all inclusive us of network and network devices". (2005 IoT report, ITU series Y,20).

If I had to define the Internet of Things with my words, I would say that it is the connection of all kinds of objects with each other through Internet to achieve a digitally communicated environment.

An important concept related to the Internet of Things is ***M2M*** *(Machine-to-Machine).* Represents a set of technologies that enable the machines to communicate with each

other and drive action. M2M uses wireless networks to connect Internet and devices to each other with minimal direct human intervention, to deliver services on the needs of a wide range of industries. On the other hand, IoT represents the coordination of devices, appliances, machines connected to the Internet through multiple networks with human interaction as a key factor.

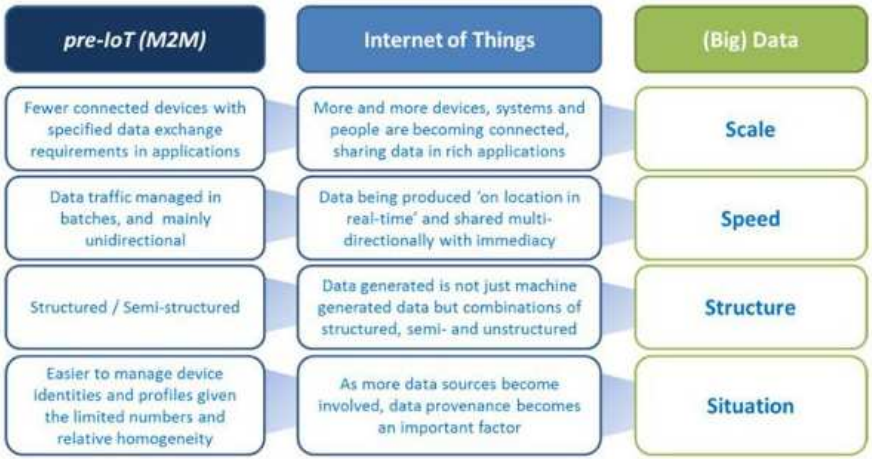

Figure 3. Comparision between M2M and IoT

Source. Machina Research report "Why NoSQL Databases are needed for the IoT

Figure 3 illustrates different aspects related to M2M and IoT. Generally, both concepts are similar. The main differences are the scalability, the structure and the speed. IoT has more connected devices than M2M and it is more used in the consumer space while M2M has a stronger industrial connotation.

The concept of M2M was used during World War II for identifying friend or foe to prevent pilots from hitting friendly targets. Nowadays is used in several applications such as machine maintenance, measuring, security, chain supplying, asset tracking or remote monitoring [2]-[4].

Organization	Objectives
ITU-T JCA IoT	Networking aspects, identification, USN
ISO/IEC JT1 SWG WG5	Identification of IoT-related market requirements, standardization gaps
CEN TC 225 WG6	Identification technologies, data gathering protocols, and communication protocols
ETSI TC M2M	M2M e2e network reference architecture, identification, addressing, security, privacy
TIA R-50	Ubiquitous protocols for industrial smart devices communications
ATIS M2M Committee	Service layer and interfaces towards application and transport layers
IEEE 802.16 M2M TG	IEEE 802.16 improvements to support M2M applications
OMA M2M	Device management extension, location services
CCSA TC10	Green community, vehicle communication systems, e-health monitoring
ARIB M2M Study Ad Hoc Group	Smart grid, smart cities, smart home
TTA M2M PG	Service requirements, data structure, identification
oneM2M	M2M service layer platform, service architecture, resource/data access protocols and management, security, privacy

Table 2 Objectives of the most important organizations focusing on IoTand M2M

Source. The Internet of Things vision: Key features, applications and open issues [4]

Table 2 shows some objectives of the main organizations working on IoT as a whole.

There are different organizations working in the IoT and M2M standardization process that focus on the different aspects, protocols, and other important parts of the Internet of Things.

At the international level, ***ITU-T*** work on IoT including network aspects of identification of things, and ubiquitous sensor network.

In North America many standard organizations work in promoting IoT standards:

-IEEE works in M2M applications. It investigates efficient ways to support lower power consumption of the device, a significant large number of devices at the base stations, small burst transmissions, and improved device authentication.

-ATIS (Alliance for Telecommunications Industry Solutions) aim to define a common service layer for multiple M2M applications and the corresponding interfaces between the application and the transport layers.

-TIA (Telecommunications Industry Association) is interested in specifying ubiquitous protocols for communicating with smart devices used in industries and releasing its Smart Device Communications Reference Architecture standard (TIA-4940).

-OMA (Open Mobile Alliance) is interested in extending the device management protocol for M2M communications and works on location services for mobile M2M applications.

At the European level ***CEN*** focus on identification technologies, data gathering protocols and communication protocols. ***ETSI*** is more focused on M2M standardization activities.

In Asia, the IoT standardization is done by different organizations. In China, by ***CCSA*** *Technical Committee 10*, which works mainly in the area of e-health monitoring and vehicle communication systems. In Korea, ***TTA*** founded M2M PG (PG708) working on service requirements, data structure and identification scheme, and in Japan the standardization is done through ***ARIB*** which focus on smart grid, smart cities and smart homes [4].

To understand more in detail how IoT operates it is important to know some other key concepts; sensors, connectivity, *middleware*, *addressing and scalability, data storage and visualization.*

Sensors convert a non-electrical input into an electrical signal that can be sent to an electronic circuit. They are responsible of creating information for the IoT network through the collection of data from the environment for different purposes. They must be small, versatile and energy efficient. All IoT applications have one or more sensors, have a low cost and consume less power [5].

Connectivity allows devices to communicate with each other and also with services and applications that works in the Cloud. Network design is very important in the IoT paradigm because of the huge volume of interconnected elements and also to the impact that the design can have to the global performance of the system.

Middleware interconnects and integrates all the elements that make the Internet of Things possible. It is part of the architecture enabling connectivity for huge numbers of divers things by providing a connectivity layer for sensors and also for the application layers that provide services that ensure effective communications between software [2],[6].

It acts as an interface enabling the various applications on heterogeneous systems to easily communicate with each other.

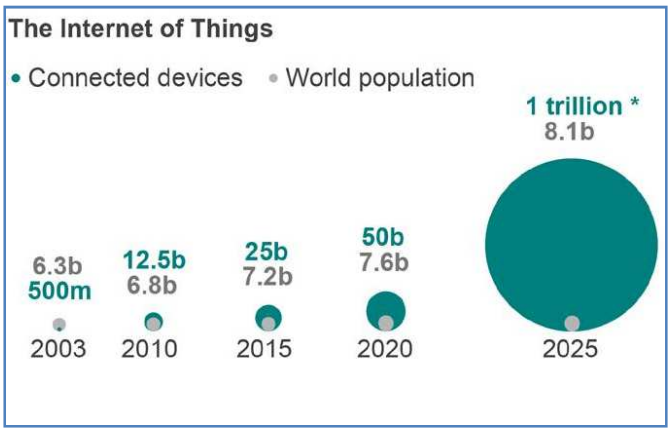

Figure 3. Comparision between connecte devices and World population
Source. Cisco IBSG

Figure 3 illustrates the comparison between connected devices and world population by years and their expected evolution.

We can observe the enormous growth potential of connected devices. While in 2003, the world population was 6.3 billion and connected devices 500 million, in 2025 is expected to have around 1 trillion devices connected and 8.1 billion people in the world.

Addressing and Scalability are very important, because all the objects included in the IoT network must have a unique identifier. IoT embraces a very large number of devices, therefore addressing schemes is essential to distinguish all the elements, their functionalities, their locations and also to control these elements through the Internet. As we know, an IP address is like a phone number or street address and when you connect to the Internet, every device is assigned to an IP address, as well as every site you visit has an IP address. Everything that is connected and other elements that are going to be connected, must be identified by their unique identification, location and

functionalities. The features to be considered of creating a unique address are: reliability, uniqueness, persistence and scalability.

IoT needs an architecture that allows scalability, which means the capacity to connect one day one hundred devices, and the following day one million.

The addressing system that has been used since the birth of the Internet is called IPv4, and the new addressing system is called IPv6.

The reason the IPv4 system has to be replaced with IPv6 is because the Internet is running out of IPv4 address space, and IPv6 provides an exponentially large number of IP addresses; 340,282,366,920,938,463,463,374,607,431,768,211,456.

The IPv6 is used for the IoT due to the fact IPv4 inability to meet the quick growth of addressing space requirements. It has introduced supported,scalable addressing schemes to provide secure access to the resources uniquely and remotely [3].

Data storage and analytics. The extremely large amount of data within IoT must be intelligently gathered, analyzed, processed and stored for more efficient and smart monitoring, actuation and real time decision making. Developing intelligent algorithms is a requirement to make sense of an efficient data management.

Cloud computing, cloud-based storage and cloud based analytics provide a great solution for handling, storing and real time processing the data from an unpredictable number of devices. Through different IoT devices the data is collected and can be shared with other data using cloud-based services. These services provide valuable information for users. Besides, it may be used for better automatic actuation and remote control [3].

Visualization is the most important aspect in the IoT global design because all the things and devices need interaction with the users. In this age of technology and communication, smart phones and tablet devices have become very popular in part because their ease of use and the capacity to access data information in a fast way.

The 2D and 3D screens have provided users with large amount of useful information in several ways. The use of smart tablets and phones has become very important to allow this interaction.

The systems are able to model the obtained data, consider how to detect events, and provide different ways to visualize the data, but always trying to show the representation of the information following the requirements of the consumers [7,8].

The IoT runs over the TCP/IP networking model and uses 4-layers and connect all the devices through the Internet. These levels are: data link level, networking level, transport level and application level [9].

-Data Link Level. At this layer you will have a requirement to connect devices that are nearby, and those that are more distant with appropriate networks.

-Networking Level. The protocol that is set to dominate at the networking level is IPv6.

-Transport Level. At this level, TCP (Transmission Control Protocol) has dominated and is used by HTTP and many other protocols such as SMTP, POP3 and IMAP4. TCP is a transport layer protocol used by applications that require guaranteed delivery. UDP (User Datagram Protocol) is one of the core members of the Internet protocol suite. TCP and UDP are the protocols more used on IP protocol [10].

-Application Level is responsible for data presentation. HTTP is probably the best known protocol at this level that powers the Web, but is not suitable in resource constrained environments because it requires complex headers with a minimum of nine TCP packets. Besides, HTTP does not guarantee message delivery. The IoT environment requires very small interactions with small devices and with very little power consumption [9].

2.3 IoT Protocols

Many protocols have been developed specifically for IoT environments. Here I explain the main protocols which are CoAP, MQTT, AMQP, XMPP and Rest [6],[11]-[16].

CoAP *(Constrained Application Protocol)* was designed by IETF Constrained RESTful Environment, and is a specialized web transfer protocol that was created for constrained device connectivity in the IoT and for M2M applications such as smart energy and building automation. It works with UDP only and is very fast in device to device communication. CoAP architecture is divided into two main sub layers: messaging and request/response. The messaging sub layer is responsible for the reliability and duplication of messages while the request/response is responsible for communication. There are four types of messages in CoAP: no confirmable, confirmable, reset and acknowledgement.

For reliable transmission over UDP, confirmable messages are used. Besides, it uses the Efficient XML Interchange data format, which is a binary data format and is more efficient in terms of space compared to plain text HTML/XML.

Because UDP allows broadcast and multicast, you can transmit to multiple hosts using less bandwidth. This makes it good for local network environments where devices need to speak with each other quickly, which is traditional for some M2M settings.

It is intended to be used in lower power and constrained networks such as 6LoWPAN and LLN/IoT that requires remote monitoring and manipulating [3],[6],[13],[16].

MQTT *(Message Queue Telemetry Transport)* is a publish protocol that runs over TCP. It was developed by IBM as a client/server protocol to meet device to gateway messaging requirements. It is a protocol that makes it suitable for IoT applications. Due to the fact that it runs over TCP, it cannot be used with all types of IoT applications.

Supports the major IoT message patterns: publish/subscribe and request/reply. This protocol implements QoS and secure communication.

MQTT-SN (*Message Queue Telemetry Transport*-Sensor Network) is an extension of MQTT which is designed for low power and low cost devices. It is based on MQTT but has some optimizations for WSN. Some wireless protocols are supported by MQTT-SN such as Bluetooth, ZigBee and UDP [13],[14].

AMQP (*Advanced Message Queue Protocol)* is a protocol maintained by OASIS, and also an open standard to exchange messages between applications (M2M). It supports both TCP and UDP and it is the only protocol viable for end-to-end use for selected IoT use cases. The key factors of AMQP are open, security, interoperability, reliability [15].

XMPP *(Extensible Messaging and Presence Protocol)* is an open standard for presence and messaging. This protocol operates through XML messages. This protocol enables users to send real-time messages and handles the user presence. The IoT XMPP version enables users to send and receive messages from machines. The key features are extensible, flexible and open standard [15].

Rest *(Representational state transfer)* is used as IoT protocol to exchange data between applications and to integrate applications that belongs to different domains. Besides, it uses HTTP as based protocol and uses client/server paradigm [12].

There are other protocols that are used specifically for security, QUIC and DTLS [17].

QUIC (*Quick UDP Internet Connections)* is a protocol that uses User Datagram Protocol and support a group of composite connections that are present between two endpoints. QUIC have the ability to provide security protection like Secure Sockets Layer or Transport Layer Security and minimize transport latency. QUIC can estimate the bandwidth in either direction so that congestion problem should be avoided.

DTLS *(Datagram Transport Layer)* is the protocol responsible for providing the communication privacy for UDP. With the use of DTLS many threats can be prevented such as eavesdropping, message tampering and message forgery. The base of DTLS is TLS, which is used for providing security.

Within IoT there are four different kinds of connections across which data moves [12], [18]:

-*Device to device* means the connection between two or more devices with each other. Different types of networks can communicate them and the main protocols used are Bluetooth, Z-Wave and ZigBee. This model is used in different scenarios, for example in smart home environments where it requires a low data rate. It can be used also in connected cars environments to share information in order to enhance many issues such as safety and traffic flow.

-*Device to cloud* represents a device connecting to an Internet cloud service in order to exchange data and control message traffic. In this model, Ethernet or Wi-Fi can be used.

-*Device to gateway* involves application software, operating on a local gateway device that acts as an intermediary between an IoT device and a cloud service. This gateway could provide security and other functionality such as data or protocol translation.

-*Back-End data sharing.* With this model, users can export and analyze smart object data from a cloud service in combination with data from other sources, and send it to other services for aggregation and analysis. An example of this model is a connected car that updates the navigation system with new route data.

2.4 IoT architectures

The Internet of Things can be capable of interconnecting various heterogeneous objects through the Internet, so there is a need for a flexible layered architecture. It represents vast range technologies and for this reason is not possible to consider only one IoT architecture as a reference model that can be used for all IoT operations. There is no standard architecture for IoT and depending on the context of these architectures are used based upon the requirements desired. The key factors that should be considered when a new architecture is developed are security, reliability, privacy, QoS, interoperability. The most used architectures are the *3-layer architecture and the 5-layer architecture* [4],[6],[8],[14],[17],[19],[20]-[28].

The 3-layer architecture was the first IoT architecture proposed. It is composed of the perception layer, the network layer and the application layer.

The objective of *the perception layer* is to acquire the data from the environment through sensors and actuators, which perform several functionalities such as location, humidity, acceleration, identifying temperature, vibration, weight, etc.

The proper functioning of an IoT system will depend on the capacities in the management of the data and the intelligent use that is made of them. For this reason the system must be able to collect information from these sensors, then store and analyze them. There are several types of sensors used in the different available applications. This layer is divided in two parts: the perception node (controllers, sensors..) responsible of data acquisition, and perception network that communicates with transportation network and sends collected data to the gateway or control instruction to the controller. The common well known sensor today is the Smartphone. It is armed with different type of embedded sensors; light, movement, proximity, camera and microphone. There are other sensors used in different sectors and with other goals. They can be laptops, mobile devices, embedded chips, ships, vehicles, and every device. Each of these objects is considered a data source for the IoT network. Before transmitting, the data is preprocessed by the units of perception layer, then filtered and send it to the network. Such units normally have little room for temporary storage, a small processing unit and security features. RFID, NFC and WSN are technologies used in this layer.

The network layer is the most important layer, the core of the IoT, and transmits the information gathered by the perception layer. It comprises of convergence network, intelligent processing, management of network and information centers.

IPv6 is considered the key protocol for this layer and 3G, Wi-Fi, FTTX, Bluetooth Low Energy, ZigBee are some of the technologies used on this layer.

The application layer allows the convergence between the IoT social needs and industrial technology. The objective of this layer is to give informational service consisting of three parts that are IoT client side, data storage and data inquiry module. It involves Cloud Computing, ubiquitous computing, intelligent processing and mega databases. Some examples of IoT applications are identity authentication, logistics management, intelligent transportation.

Due to the IoT development, the 3-layer architecture was not sufficient to cover all the demands within IoT paradigm. For this reason, other architectures were proposed [4],[6],[8],[14],[17],[23],[24],[27],[28].

The 5-layer architecture contains the perception layer, transport layer, processing layer, application layer and business layer.

The perception layer corresponds with the perception layer of the 3-layer architecture, and the *transport layer* corresponds with the network layer of the 3-layer architecture.
In the processing layer all the data transmit from the transport layer is stored, processed and analyzed. The key elements of this layer are Cloud Computing, ubiquitous computing, database, intelligent processing.
The application layer creates the distinct IoT applications and provide applications to industrial usage. Acquiring, storing, analyzing and processing of data received from the transport layer is done through this layer.
The business layer is responsible about all related to IoT applications and user privacy [17],[21],[23],[27],[28].

<table>
<tr><td rowspan="2">Application Layer</td><td>Business Layer</td></tr>
<tr><td>Application Layer</td></tr>
<tr><td rowspan="2">Network Layer</td><td>Processing Layer</td></tr>
<tr><td>Transport Layer</td></tr>
<tr><td>Perception Layer</td><td>Perception Layer</td></tr>
</table>

Table 3. The 3-layer architecture on the left, and 5-layer architecture on the right

Table 3 shows the 3-layer and 5-layer architectures. On the left, 3-layer architecture composed of Perception Layer, Network Layer and Application Layer. On the right, 5-layer architecture composed of Perception Layer, Transport Layer, Processing Layer, Application Layer and Business Layer.
There are some other architecture models which are used for special purposes, but they cannot be treated as standard architectures. These architectures are [22]:

-IoT-A is a business driven architecture that generates different reference architectures depending on domain specific requirements.

-BeTaaS is an architecture to provide communication between machine to machine. In BeTaaS there are four layers; physical layer, adaptation layer, TaaS layer and the service layer.

-OpenIoT is an architecture constructed from the reference model defined in IoT-A. The main objective is to provide the infrastructure that is cloud-based middleware.

-IoT@work is a European Commission project. The main purpose of this architecture model is to create the industrial automation domain. The layers in this architecture depend on its area of deployment.

Vasilomanolakis et al. [22] survey these four IoT architectures. They devised a list to establish a standard set of security requirements for the IoT technologies. These requirements are Network security, Identity management, Privacy, Trust and Resilience.

2.4.1 Perception Layer

As I remarked before, the most common technologies used in the perception layer which now I explain in more detail are; Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), Near Field Communication (NFC).

RFID *(Radio Frequency Identification)* is a non-contact technology used for automated identification of people and objects. Is one of the main technologies that made possible the IoT paradigm. The RFID system is composed of signal transmitter, signal receiver and transmitter receiver. It is a small microchip designed for wireless data transmission. Data is transferred between a data sender and the data receiver device through radio waves. The sender data piece is known as a tag, and recipient information piece is known as a reader. These tags are placed on the objects. There are three types of RFID tags, active, passive.

The active tags have their own transmitter and power source which is a battery the most times. Active RFID operates in the UHF (Ultra-High Frequency) (860 MHz to 960 MHz) band and offer a range of up to 100m. These active tags broadcast their own signal to send the information stored on their microchips.

In the passive tags, the reader sends energy to antenna, and then uses the transmitted signal and converted into a Radio Frequency wave (frequencies that are located in the range extending from around 3 KHz to 300 GHz), and it is sent into the read zone

Passive tags can function in the LF (Low Frequency) (125 KHz to 134.2 KHz), HF (High Frequency) (13.56 MHz) or UHF.

The last type of RFID tags is a BAP (Battery-Assisted Passive), which use an integrated power source to power on the chip.

The RFID is able to apply in many areas such as access control systems, inventory tracking, personnel tracking, animal tracking, asset tracking and collection system [2]-[4],[6]-[8],[14],[17],[20],[21],[23],[25],[29]-[31].

WSN (Wireless sensor networks) are networks of thousand of sensor nodes that sense and control the environmental conditions such as temperature, sound, pressure, etc. using wireless technologies and reporting sensible changes on a field to a specific server. It allows the interaction with different persons or computers. A WSN consists of a centralize base station that controls a multi-hub relay system that connects the source nodes. One of the applications of WSN is large area monitoring, where sensor nodes are placed in far fields with limited power sources. The popular network topologies used in a WSN are a star, a mesh and a hybrid network. Most of the communication in WSN is based on the IEEE 802.15.4 standard.

WSN can cooperate with RFID systems. In fact, both systems play a crucial role in the IoT. These networks consume low power, have good efficiency and are cost effective.

The development of wireless sensor networks was motivated by military applications, but today such networks are used in several industrial and consumer applications such as machine health monitoring and industrial process monitoring and control [3],[6]-[8],[17],[21],[23],[29].

NFC *(Near Field Communication)* is a wireless communication technology and the core technology of IoT, which was introduced when was a need to allow the communication with a few centimeters (typically a distance of 10 cm or less) and with low power and data rate required. This technology is based on RFID, so it uses variations in the magnetic field to communicate data between two NFC enabled devices. There are two modes of operation: active and passive. In the active, both devices generate magnetic fields, while in the passive mode, only one device generated the field and the other uses load modulation to transfer the data. The passive mode is useful in battery powered devices to optimize energy use. It works within the globally available and unlicensed radio frequency ISM band of 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 Kbit/s to 424 Kbit/s.

It works in the 13.56 MHz band, which means that no restrictions are applied and it does not require any license for its use.

NFC tag can be modified by potential attackers who can replace the original tag with a fraudulent one with the intention to steal valuable user information.

An advantage of close proximity between devices is that it is useful for secure transaction such as payments.

The difference between NFC and RFID is that the first one can be used for two-way communication, and for this reason many smart phones in the market are NFC enabled. Near Field Communication can be used for a wide range of services in IoT systems such as authentication, data exchange, payments, etc. It is useful for many services such as access control, transport, smart cards [4],[6],[14],[17],[32]-[34].

2.4.2 Network Layer

There are many technologies that operates mainly in the network layer. Here I explain some of the most important, which are Bluetooth and Bluetooth Low Energy, Wi-Fi, WiMAX, ZigBee, Z-Wave and LoRa. Later, I expose their vulnerabilities.

Bluetooth is a short-range communications technology that has become important in computing and many consumer product markets. It has been considered as a cheap, reliable and power efficient replacement of cables for connecting electronic devices. Bluetooth has become a smart technology for the flexible wireless communication system.
It operates in a license-free Industrial, Scientific and Medical (ISM) band ranging using 2.45 GHz. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations and it is very used to transfer sound data.
BLE *(Bluetooth Low Energy)* is a wireless personal area network technology designed by the Bluetooth Special Interest Group aimed at novel applications in the healthcare, security, home, and fitness entertainment industries. BLE uses multiple network topologies, including P2P. Compared to Classic Bluetooth, BLE is intended to provide considerably reduced power consumption (10mW) and cost while maintaining a similar communication range. The range is approximately 35 meters and the data rate is 1Mbps [5],[6],[14],[15],[35]-[39].

Wi-Fi is for many developers an obvious choice due to the fact that can offer fast data transfer, handle high quantities of data and there is a wide existing infrastructure.
The most common Wi-Fi standard used in many businesses and homes is 802.11n, which offers a range of hundreds of megabits per second, and it is fine for file transfers, but perhaps too power-consuming for several IoT applications. Wi-Fi wireless network connections use radio signals in either 2.4 GHz or 5 GHz.

The typical data rates work from 150 to 200 Mbps, and maximum are 600Mbps depending on the channel used and number of antennas. The range covers approximately 50m [4],[5],[8],[14],[38].

WiMAX is a family of wireless communication standards based on the IEEE 802.16 and WMAN (Wireless Metropolitan Area Network).
WiMAX would operate similar to Wi-Fi, but at higher speeds over greater distances and for a greater number of users. WiMAX provides service in area that are difficult for wired infrastructure to reach and has the ability to overcome the physical limitations of traditional wired infrastructure.
The IEEE 802.16 is standard operating from 2 to 11 GHz and it is expected to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the technical configuration selected. It provides speeds of approximately 70 Mbps over a range of 50 kilometers [38],[40].

ZigBee is a wireless networking standard, especially designed for wireless low-power devices. It is used for PANs (Personal Area Networks) and it is suitable for operation in isolated locations and hard radio environments. ZigBee builds on IEEE standard 802.15.4. ZigBee was developed to achieve reliable, low energy and cheap communication. The distances that can be achieved by a Zigbee device is about 10 to 100 meters.
The main purpose of this technology is home automation, including actuators and sensors. It operates at 2.4 GHz supporting data rate of 250 KB/s, at 915 MHz supporting data rates of 40 KB/s and 250 KB/s, and 868 MHz supports data rates of 20 KB/s, 100 KB/s and 250 KB/s.
Sensors, lighting controls, security and many more applications are all candidates for the new technology [6],[14],[15],[29],[38].

Z-Wave is an implementation of a complete Internet of Things substrate, containing communication, networking and application layer protocols. Z-Wave is designed to provide reliable, low-latency transmission of small data packets at data rates up to 100kbit/s. The throughput is 40kbit/s and suitable for control and sensor applications. Communication distance between two nodes is about 30 meters. A Z-Wave network can consist of up to 232 devices with the option of bridging networks if more devices are required. It uses a source-routed mesh network topology and has one primary controller [38],[41].

LoRa is a proprietary radio modulation technology licensed by SemtechCorporation [14]. It is designed to be a low power protocol and data rates can vary from 0.3 kbps to 250 kbps, and it can be used within a suburban or urban environment (from 2 to 50 km range in a crowded urban area).

LoRa operates at 868-900 MHZ ISM bands and provides long-range connectivity by using the chirp spread spectrum technique.

LoraWAN is the standard of LoRa, and provide low-power WANs with features specifically needed to support low-cost mobile secure bi-directional communication in IoT, M2M and industrial applications [38]-[39].

Main features	BLE	Wi-Fi	WiMAX	ZigBee	Z-Wave	LoRa
Standards	IEEE 802.15.1	IEEE 802.11 ah	IEEE 802.16	IEEE 802.15.4	Z-Wave alliance	IEEE 802.15g
Spectrum	2.4 GHz	2.4-5 GHz	2-11 GHz	2.4 GHz	908.42 MHz	868-915 MHz
Range	35m	1 Km	50 km	100m	30m	50 Km
Rate Mbps	1	150 kbps	70	0.25	0.1	250 Kbps
Network type	PAN	WLAN	MAN	PAN	PAN	WAN

Table 4. Main features of the main IoT Technologies

2.4.3 Application Layer

The application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. Cloud Computing is an Information technology, which operates in this layer.

Cloud Computing is the delivery of computing services such as servers, storage, databases, networking, analytics and more through the Internet. It distributes the computation task into a resource pool composed by great amounts of computing resources and allow users to obtain storage space and information service.

It is large a amount of virtual computing resources which have abilities to maintain and manage themselves in the system. The integration of IoT and Cloud Computing can enable the creation of smart environments. In the development of the mobile Internet, the Cloud Computing services based on mobile devices such as tablet, mobile phones, etc. have emerged and been used for information sharing environments. [3],[7],[8],[14],[20],[26],[29],[42]-[45].

Cloud Computing can be used in multiple contexts and there are three fundamental classes:

-*SaaS (Software as a Service).* In this model a company serves the

maintenance, support and operation that the clients will use during the time they have contracted the service. An example of SaaS is Salesforce.

-*IaaS (Infrastructure as a Service).* In this model of distribution, the service is provided through a virtualization platform. Instead of acquiring servers, network equipment or space in the data center, customers buy all these resources from an external service provider. The provisioning of these services is done through the web. One example is Amazon Web Services EC2.

-*PaaS (Platform as a Service)*. PasS offers multiple services provisioned as an integral solution on the web. Google App Engine is an example of this model.

IoT subjects	IoT concepts	Research
Architectures	3-layer	[4],[6],[8],[14],[17] [23],[24],[27],[28]
	5-layer	[17],[21],[23],[27],[28].
	IoT-A, BeTaaS, OpenIoT, IoT@work	[22]
Technologies	RFID	[2]-[4],[6]-[8] [14],[17],[20],[21] [23],[25],[29]-[31]
	WSN	[3],[6]-[8],[17] [21],[23],[29]
	NFC	[4],[6],[14],[17] [32]-[34]
	Bluetooth and BLE	[5],[6],[14],[15] [35]-[39]
	Wi-Fi	[4],[5],[8],[14],[38]
	WiMAX	[38],[40].
	ZigBee	[6],[14],[15],[29],[38].
	Z-Wave	[38],[41]
	LoRa	[38],[39]
Paradigm	Cloud Computing	[3],[7],[8],[14],[20] [26],[29],[42]-[45].

Table 5. Articles classified by subjects: Architectures, technologies and paradigm

2.5 IoT applications

IoT has the potential to transform all major segments and develop new applications in every field. The IoT main applications are:

-Smart Home. *R*efers to the connectivity through smart devices inside homes. It includes windows, door locks, smoke detectors, thermostats and entertainment systems.

-Smart City. Include a wide variety of use cases, for example, urban security, traffic management, water distribution, environment monitoring, or waste management. The goal of Smart City is to enhance the lives of the citizens through solving traffic congestion problems, noise and pollution issues.

-Smart grids**.** It uses IoT to use information about the behaviors of electricity suppliers and consumers in order to improve the reliability, efficiency and economics of electricity.

-Smart Farming emphasizes the use of information and communication technology in the cyber-physical farm management cycle. Internet of Things and Cloud Computing are expected to enhance this development and introduce more tools and artificial intelligence in farming.

-Connected Industry**.** In this field many market researches see the IoT concept with the highest overall potential. Applications among others include connected industrial equipment or smart factories.

-Connected car is about to use technology to enhance driver comfort, whether it is driver-assisted or self driving: mapping services, connectivity with other cars, or traffic control. Also remote monitoring and the concept of next generation in-car entertainment systems will be an important part of IoT applied to cars.

-Connected Health is one of the most valuable applications of IoT paradigm, due to will to improve well-being of people through connecting the health care systems and smart medical devices. Some of these benefits are improved medical decision-making based on large sets of patient data or new kinds of real-time health monitoring.

-Smart retail is based on intelligent payment solutions, in-store shopping behavior, and proximity-based advertising as the most important IoT projects in this area.

-Smart supply chain tries to enhance the tracking of products while they are on the road, and also to allow the suppliers to exchange inventory information as a big part of IoT in this field.

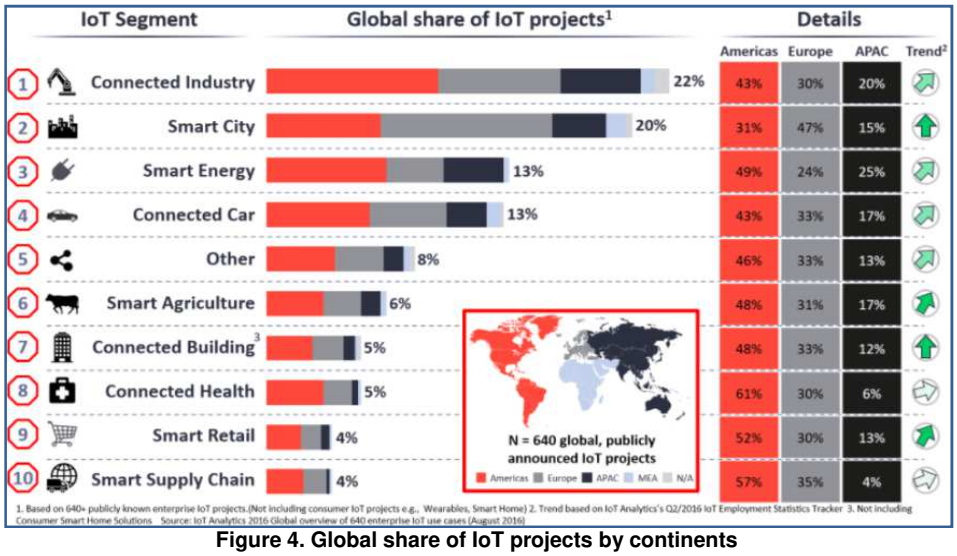

Figure 4. Global share of IoT projects by continents

Source. IoT analytics 2016 Global overview of 640 enterprise IoT use cases, August 2016

Figure 4 illustrates The main IoT projects by segment and by continents. The leading projects involve Connected Industry, followed by Smart city and Smart energy. [46]

3. Blockchain technology

The technology behind Bitcoin and other cryptocurrencies is a distributed ledger database for recording transactions, usually known as blocks. Blockchain technology enables users to share their ledger of transactions.

The first concept of Blockchain was applied in 2009 as a part of Bitcoin which was created by an unknown person using the alias Satohi Nakamoto [47].

3.1 Blockchain concept

Blockchain is a distributed database that registers an ordered list of records of transactions which are immutable linked together through a chain, on blocks.

The blocks form a linear sequence where each block references the hash of the previous block, forming a chain of blocks. Blockchain is maintained by a network of nodes and each one of them executes and records the same transactions. Any node in the network can read the transactions [48]-[57].

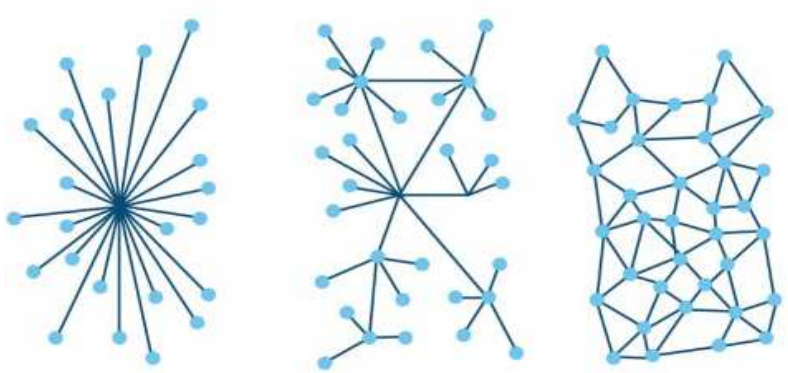

Figure 5. From left to right centralized, descentralized and distributed (Blockchain) networks
Source. http://cyberfrat.com/wp-content/uploads/2016/10/1.jpg

Figure 5 shows the different network topologies; centralized, decentralized and distributed (which is the Blockchain technology network type).

The main advantages of Blockchain networks are:

-It is public. This is the most important advantage. Everyone participating can see the blocks and the transactions stored in them. This does not mean that everyone can see the actual content of your transaction, however; that's protected by your private key.

-It is decentralized, so there is no single authority that can approve the transactions or set specific rules to have transactions accepted. That means there is a huge amount of trust involved since all the participants in the network have to reach a consensus to accept transactions.

-It is secure. The database can only be extended and previous records cannot be changed (at least, there's a very high cost if someone wants to alter previous records).

3.2 How Blockchain works

In this section I explain the main concepts related to Blockchain technology and how it operates. These concepts are; *transactions, blocks, peer to peer (P2P), DLT (Distributed Ledger Technology), smart contract, Ethereum, ether, Dapp, hash, mining, PoW and gas.*

A ***transaction*** is a transfer of Bitcoin value that broadcasts to the network and collected into blocks. Transactions are not encrypted, so it is possible to view every transaction collected into a block and they are bundled into blocks and executed on all the participating nodes.

A ***block*** contains a transaction list, the most recent state, a block number and a difficulty value. If there are conflicting transactions on the network (for example, transactions that do double spending), only one of them is selected to become a part of the block. The blocks are added to the Blockchain at regular intervals.

P2P (*Peer to Peer)* is a network in which their computers act as a node for sharing files within the group. The devices or computers that participate in this network are called peers and each peer are equal to others, so there is no central administrator device in the center of the network and there are no privileged peers.

DLT *(Distributed Ledger Technology) is a* type of database that is consensual shared, replicated and synchronized across the members of a network and the main characteristic of this database is that the transactions and their details are recorded in multiple places at the same time. DLT has no central data store.

A ***Smart contract*** is a piece of code that resides on a Blockchain, it is identified by a unique address and includes a set of executable functions and state variables. These functions are executed when transactions are made to these functions. Input parameters are included in the transactions and are required by the functions in the contract. The most popular language used to write a smart contract is Solidity. This language is quite simple and only allows to perform basic operations of its basic type.

The goal is to reduce transaction costs associated with hiring and to ensure security of the contract traditional law.

Traditional contracts	Smart contracts
1-3 days	Minutes
Manual remittance	Automatic remittance
Escrow necessary	Escrow may not necessary
Expensive	Fraction of the cost
Physical presence	Virtual presence
Lawyers necessary	Lawyers may not necessary

Table 6. Comparision chart between traditional contracts and smart contracts
Source. https://www.linkedin.com/pulse/smart-contracts-its-applications-sudip-nair

Table 6 shows the benefits of smart contracts compared to traditional contracts. The smart contracts can be executed very fast and there is no requirement of physical presence.

Ethereum is an open and programmable Blockchain platform that is powered by the peers who run the Ethereum nodes. Everybody can sign up for the platform and create an Ethereum account and create smart contracts, and also build decentralized applications. In the Ethereum network decentralized applications allow anybody to create cryptocurrencies but also anything else that is programmable.

Ether is the currency which is used in the Ethereum network. Unlike bitcoin, ethers were not created to become a decentralized global digital currency and their aspirations go beyond the sending or transfer of money.

Dapp *(Decentralized Application)* is an application that provides an interface to Smart Contracts. One example of Dapp could be a crypto currency application.

Hash. It is equivalent to the fingerprint concept, it is the unique identifier of a person. When two objects are sent to the Blockchain they will have different hashes. Moreover, if you have the object it is very easy to create the hash, but it is almost impossible to perform the opposite operation. To ensure that the reverse does not exist, the output is shorter than the inputs, and there are more than two inputs that give the same output. This way of operation makes it impossible to calculate the inverse one.

Mining. Refers to the distributed computational review process performed on each "block" of data in a Blockchain. This allows for achievement of *consensus* in an environment where nobody knows each other.

PoW *(Proof of work)* is a piece of data which is moderately difficult to produce (costly) but is very easy to verify, and it is used to avoid unwanted behaviour, for example, denial of service attacks or spam. It is a small mathematical problem every miner has to solve before sending a block back to the node.

Gas is the name of the crypto fuel, which is consumed in performing the operations on a Blockchain network. The gas quote paid is proportional to the amount of work that is required to execute the transaction.

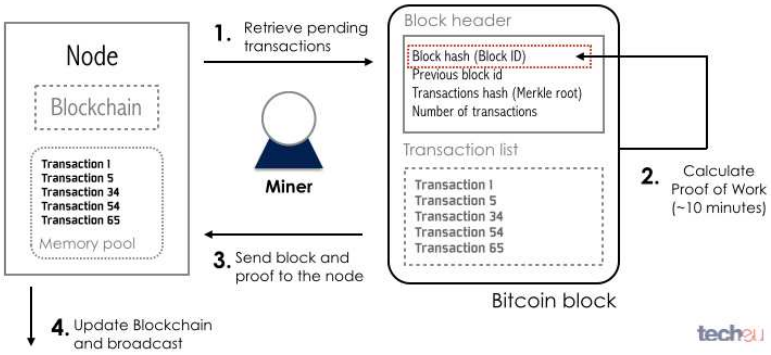

Figure 6 Blockchain structure
Source http://tech.eu/features/808/bitcoin-part-one/

Figure 6 shows the steps of the mining process and the PoW mechanism which takes on average approximately 10 minutes to complete.

There are three types of Blockchain [58]-[60] according to the way of operating:

-Public Blockchain. Everyone can read or write data and the only requirement is to have a computer and Internet connection. Some of this type of network restricts the access only to read or write. Ethreum and Bitcoin are examples that use approach where everyone can write.

-Private Blockchain. Is not open to the public, but can only be accessed by invitation and all the members who are participating know each other and are trusted. This is very useful when the Blockchain is used between companies that are part of the same branch. Some of the most famous are Hyperledger (from the Linux Foundation) and Ripple (protocol to allow international money transfers).

-Permissioned Blockchain. Also known as Consortium Blockchain, is an hybrid between public and private Blockchain. In this type, only a few selected nodes are predetermined and the participating nodes are invited, but all transactions are public. That means that the nodes participate in the maintenance and security of this network, but that all transactions are visible to users around the world.

The right to read may be public, or restricted to the participants. Consortium Blockchains maintain data privacy like Private Blockchains. BigchainDB is an example of consortium Blockchain.

The *connection steps* to join Blockchain network are:

-The user enters the system through their mobile app or web platform.

-In order to make a transaction to some, you need a digital signature. The user can obtain the public key of the receiver by scanning a QR code from another person's mobile or their payment address.

-Any person with a public key can send money to one address, but only one signature generated with a private key can take money from it.

-The app warns the miners of the pending transaction network and they verify that the customer has enough money to pay and initiate a process to group pending transaction data in the Blockchain as well as a nonce (number) and apply a hash that produces a unique fingerprint that converts the transaction into verified.

In the case of Etherum, a transaction is verified when 12 confirmations are received.

-The encrypted block must have a certain number of zeros at the beginning. It is unpredictable to know which nonce will generate a hash with the correct number of zeros, so the miner needs to prove different nuances to find the correct value.

-When you discover it, it is advertised on the rest of the network. Other miners accept the operation and look for the next block.

-The miner gets an economic compensation (25 bitcoins in the Bitcoin network) and the transaction is published in the Blockchain.

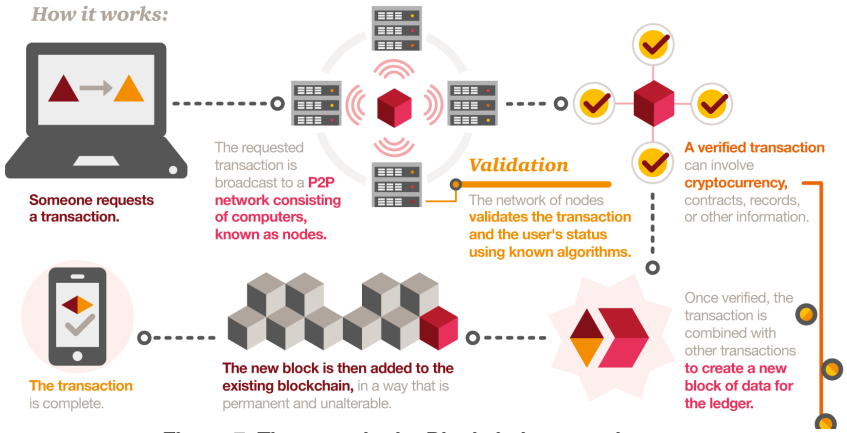

Figure 7. The steps in the Blockchain network

Source http://notibytes.blogspot.com.es/2017/08/blockchain-el-futuro-de-la-seguridad.html

Figure 7 illustrates the operation mechanism of transactions in the Blockchain network [61],[62].

The steps of this mechanism are:

-Someone requests a transaction.

-The transaction is broadcasted to a public P2P network (Blockchain network) consisting of multiple nodes.

-The network of nodes validates the transaction using known algorithms.

-Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
-The new block is added to the existing Blockchain, in a form that is unalterable permanent.
-Finally the transaction is successfully done.

3.3 Advantages of Blockchain tecnhology

Blockchains can increase security mainly on three aspects: blocking identity theft, preventing data manipulation, and stopping DoS (Denial of Service) attacks [63].

-Blocking identity theft. Blockchain's structure of network miner proof of work and its distributed ledger of data transactions reduce the possibility of data theft and data corruption.
-Preventing data manipulation and fraud. In the Blockchain technology the combination of cryptography, hashing and a decentralized structure, make it virtually impossible for any member to alter data on the ledger. This prevents and detects any form of manipulation and allows organizations to maintain the protection of the information. An important solution that has been developed to avoid fraud and manipulation is KSI (Keyless Signature Infrastructure), which ensures the protection of the networks and the security and privacy of the data.
With KSI, nobody can manipulate the data, and the authenticity of electronic data can be mathematically proven. KSI stores the digital signatures of the original files in a Blockchain and then verifies the copies through re-checking the signatures of the copies against those stored in the Blockchain.
If any manipulation is done, it is very quick detected, cause the hashes stored in the Blockchain reside in thousands of nodes.
KSI Technology is being used actively in the Aerospace and Defense Industry, and also in the Health sector to provide better control over the patient's medical record.
-Preventing Distributed Denial of Service attacks. There are a large number of critical infrastructures to protect. Blockchain can help with DNS (Domain Name System) which provides access to websites using domain names rather than IP addresses. The DNS system is dangerously centralized in a few root servers under control of ICANN (Internet Corporation for Assigned Names and

Numbers), which is responsible of the IP protocol addresses, protocol identifiers, domain system management functions and root server system management.

Blockchain could build a distributed and much more transparent DNS to make it virtually impossible for a single entity to manipulate records.

There are some differences between Blockchain networks and Cloud Computing paradigm.

In the cloud model, IoT devices are identified, authenticated and connected through cloud servers, where processing and storage are often carried out. IoT networks that have high costs are concerned in the centralized cloud model. IoT devices are vulnerable to DDoS attacks, data theft, hacking and remote hijacking. If an IoT device connected to a server is breached, everyone connected to the server could be affected. Besides, the centralized cloud model is susceptible to manipulation. The data collected does not ensure that the information is put to an appropriate use.

Blockchain can eliminate these issues of Cloud Computing. In Blockchain, message exchanges between devices can be treated in the same ways as financial transactions in a bitcoin network. Devices rely on smart contracts which guarantees more security. The fact that Blockchain verifies cryptographically signs transactions eliminate the possibility of man-in-the-middle attack, replay or other attacks [52],[64].

3.4 Blockchain applications

In this section I present some of the potential applications of the Blockchain technology [65]-[68]. These applications are; Supply chain, digital identity, voting, healthcare and government.

-Supply chain. The supply chain is very complex segment and having a transparent visibility across the whole supply chain has become more difficult. It became more difficult to track the flow of material and the distribution channels, and consequently it has led to various unethical businesses behaviours ranging from illegal trade, counterfeit products or environment damage. At the very end of the supply chain, consumers do not have the information where a final product has gone through across the supply chain.

Nowadays you can lose your parcels in the post. Taking advantage of the convergence of IoT paradigm and Smart Contracts you will be able to record the location in every moment of your parcels through the connection of sensors in every step of the way.

The smart contract brings reliability all the way along the line, allowing with security where to find the package.

-Digital identity. This application could allow consumers to have an identity recorded on a shared ledger and can add devices to their identity.

Digital Identity ensures a more secure way to verify the authenticity of someone and avoid and reduce the possible fraud.

-Voting. Blockchain can transform the traditional paper-based voting system to a digitized one and can provide a secure voting platform serving as the medium for all the process; casting, tracking and counting votes and avoid issues such as lost records and voter-fraud. Voters could count the votes themselves and verify that no votes were removed, manipulated or changed.

-Healthcare. Healthcare institutions have to deal with security and privacy issues when they share data across platforms. Enhancing data collaboration between providers means the improvement of many parts of the health field such as accuracy of diagnoses, effectiveness of treatments.

Blockchain can create this secure environment to allow healthcare institutions, payers and other parties in this field to share access to their network with data integrity guarantees.

-Government. Blockchain could be used to assure the public that the politicians are acting correctly with the money, and it also can fight against financial crime. With the technology, every transaction can be recorded without manipulation, making the ultimate destination transparent to the public.

4. IoT technologies and vulnerabilities

In this section I present the vulnerabilities of the main technologies involved in IoT that I have presented before classified by layer. I also analyze the most common IoT scenarios and what are their concerns to become secure and reliable environments for data privacy.

Then I review important security solutions that have been proposed by some researchers in order to address some of these issues. Finally, I expose Blockchain technology as an important technology to protect data within IoT.

I explain all these concepts through four main themes: IoT technologies and vulnerabilities, IoT scenarios and security issues, IoT security solutions, IoT with Blockchain technology [6],[21],[23],[24],[69].

Every day millions of new devices are connected, and the number of attacks has increased exponentially. Secure the data privacy in the IoT is important also in the control of our physical integrity because if many devices are controlled electronically, for example the lock and security system of a smart house, they can be hacked by someone and enter the house. No matter how secure a network is, when two or more devices are connected through wireless networks it will exist vulnerabilities.

Another problem of this environment of sensors and connected devices, is the fact that exist too many protocols and interfaces in the same ecosystem to control them. If we have several devices connected, it is common for each to be controlled by a different application.

These issues include a web interface, cloud interface and mobile interface. The easiest way to attack a device is by physical access. Many people can use the same devices and it is important to have conscience of this fact and activate all the possible mechanisms that any device has to.

Internet of Things devices is vulnerable to many potential cyber attacks.

To ensure the deployment of a secure IoT some requirements must be considered:

-Authentication is the process to validate if someone is who is declared to be. Is one of the biggest concerns due to the number of devices in IoT. The process of determining whether someone or something is, in fact, who or what it. Many entities are involved in the IoT (services, devices, people, service providers and processing units) and it is important to authenticate entities for these interactions. Authenticating all devices is not easy and is critical to prevent compromised enterprise networks.

-Authorization is the process of allowing someone to do or have something. It allows the users access to resources based on the user's identity. The majority of security systems is based on a two-step process which are authenticated as the first step and authorization the second one.

-Integrity*.* Techniques to restrict the modification of data to authorized persons. The IoT is based on exchanging data between lots of devices, so it is very important to ensure the protection of data. Integrity protection includes preservation against sabotage. Another key factor that influences data integrity is the fault tolerance capabilities and the robustness of the IoT System. Data integrity is ensured by password-based solutions.

-Availability**.** The users of the IoT should have all the data available wherever they need it. IoT systems need to display enough resiliency to sustain availability under desired levels as well as they need to guarantee a certain level of performance request by their applications.

-Privacy. This requirement wants to prevent attacks from malicious entities maintaining the information in safe locations with strong protection mechanisms. The growth of the IoT has shown during the last year, several privacy issues and also that many devices at the moment do not offer all the desired warranties.

-Confidentiality it is important to ensure that the data is only available to authorized users. These users can be machines and services, humans and internal objects. Confidentiality can be obtained through encryption schemes.

-Non-repudiation. Techniques to prove the involvement of an entity in a data exchange. Oftentimes is used for signatures, digital contracts and email messages. Non-repudiation can be obtained through the use of confirmation services, digital signatures and timestamps.

-Lightweight Solutions represents a unique security feature that is introduced because of the limitations in the power and computational capabilities of the devices involved in the IoT. It refers to a program, protocol, device or anything that is simpler, faster and easier to manage than other communication protocols used on a local or wide area network.

-Heterogeneity. The IoT allows the connection between different entities with different capabilities, complexity and the devices use different interfaces and are designed for different functions, therefore protocols must be designed in order to work in different situations and in different devices as well. The IoT aims to allow the connection between heterogeneous networks and things. Each device works and communicates differently as if we compare to other

devices. This issue can also affect other aspects such as privacy, difficulty in integration and identification.

The security in the perception layer is an important issue due to devices in this layer do not usually have enough memory for complete security technology. These attacks happen for external sources at the nodes where the data is passed on to the transport layer.

The major attacks in this layer aim to disrupt object identification through attacking network that connect sensor nodes. Some countermeasures in this layer, apply Intrusion detection and wireless encryption mechanisms.

I expose the security issues of the main technologies used in the perception layer which are RFID, WSN, NFC.

4.1 RFID

The most common vulnerabilities of the RFID technology are [17],[21],[70]-[75]:

-DoS Attacks. These attacks want to consume the resources of the system. Denial of Service attack is accomplished by flooding the targeted machine with superfluous requests in an attempt to overcharge systems and prevent requests from being fulfilled.

-Eavesdropping. An unauthorized individual uses an antenna in order to record communications between legitimate RFID tags and readers. Eavesdropping attacks can be done in both directions: tag to reader and reader to tag.

-Skimming. In this case, the attacker observes the information exchanged between a legitimate tag and legitimate reader. Through the extracted data, the attacker attempts to make a cloned tag which imitates the original RFID tag. The data stored on RFID chips in credit cards, and passports can be read without your knowledge and then duplicated.

-Replay Attack. In Replay attacks, the communicating signal between the reader and the tag is intercepted, recorded and replayed.

-Side Channel Attack. In these attacks, the information that is usually targeted includes power consumption, timing information and electronic fields. These attacks require a deep knowledge of the internal system on which cryptographic algorithms are implemented.

-Cloning attacks. An attacker captures tag's identifying information. The ability to create clones of tags can be used before a theft scheme or to overcome counterfeit protection.

In the case of *DoS attacks,* it is easier to detect it than prevent them from happening. Some countermeasures are enhancing the mechanical connection between the tags and items and adding an alarm function to active tags.
Some ways to fight against *Eavesdropping* include encrypting the communication between the tag and reader and establishing a secure channel. An important aspect also, is to only write the tag with enough information to identify the object.
Skimming attacks can be mitigated being more aware of the use of RFID credit cards and using blocking wallets that are designed specifically to block any potential digital hack.

To mitigate *replay attacks,* counter-based and time-based schemes can also fight this type of attacks. The tag's response must be unique for every server challenge.
To avoid *side-channel attacks,* there are two ways: reduce the release of information emitted through a side channel and eliminate the relationship between the emitted information and the secret data.
Cloning attack can be addressed by having the server share a private key with each tag.
Gross et al. [75] proposes an IPsec-conform privacy-aware authentication mechanism between RFID tags and clients on the Internet. This authentication protocol is compatible with restrictions imposed by the IP sec standard. With their contribution, they show that privacy in the IoT can be achieved without relying on the basis of existing Internet standards and on proprietary protocols.

RFID vulnerabilities	
Main threats	**Countermeasures**
DoS Attacks	Enhance the mechanical connection between the tags and items Add an alarm function to active tags
Eavesdropping	Encryption of the communication between the tag and reader
Skimming	Use of block wallets
Replay Attack	Counter-based schemes Time-based schemes
Side Channel Attack	Reduce the release of information emitted Eliminate the relationship between emitted information and secret data

Table 7. RFID vulnerabilities (main threats and countermeasures)

4.2 WSN

WSN most common attacks are [17],[21],[72],[76]-[79]:

-Wormhole. This attack causes relocation of bits of data from its original position. An attacker receives packets at one point in the network, relocates them to another point in the network, and then replace them into the network from that point.

-Sybil. In this case, the attacker makes multiple identities and replicates a single node. The identities could be stolen identities or fabricated. Those who are fabricated are fake identities which are randomly generated by the attacker. For example, if a node ID is represented by 64 bits, an attacker can randomly create 64 bits identities.

-Spoofing. It refers to the use of identity theft techniques with malicious purposes, where an attacker falsifies the origin of the packages, making the victim believe that they are from a trusted host to prevent the victim from detecting it.

-Ping Flood. It is a DoS attack where the attacker overwhelms the victim with ICMP "echo request" packets. If the target system is slow enough, it is possible to consume enough its CPU cycles for a user to notice a significant slowdown.

The way to fight against *wormhole attacks* are;

-Using synchronized clocks

-Using directional antennas

-Using multidimensional scaling

The most strong techniques to resist Sybil attacks are;

-Trusted certification

-Location verification

-Economic incentives

-Random key redistribution

-Resource testing

A common mechanism to avoid *spoofing attack* is to implement a WSN authentication protocol and data encryption, which increases the cost and technology complexity needed for a successful attack.

To mitigate a *ping flood attack* is important to reconfigure the firewall perimeter to disallow pings to not allow attacks originating from outside your network. It is important to use an IDS (Intrusion Detection System), which is a software application that

monitors a network for malicious activity to help identify patterns in network packets that may indicate an attack on the client.

WSN vulnerabilities	
Main threats	**Countermeasures**
Wormhole	Use of synchronized clocks Use of directional antennas and use of multidimensional scaling
Sybil	Trusted certification, location verification, economic incentives Random key redistribution and resource testing
Spoofing	Implement an WSN authentication protocol and data encryption
Ping Flood	Reconfiguration of the firewall perimeter Use of IDS (Intrusion Detection System)

Table 8. WSN vulnerabilities (main threats and countermeasures)

4.3 NFC

Near Field Communication common vulnerabilities are [17],[80]-[82]:

-Phishing attack. Is a computer abuse committed through the use of a type of social engineering, characterized by trying to acquire confidential information in a fraudulent way (such as detailed information on credit cards or other banking information). The attacker, known as phisher, is posing as a trusted person in an apparent official electronic communication.

-User Tracking. When tags use the same unique ID for anti-collision, an attacker could easily track the tags. User Tracking attack compromises the secrecy of an NFC system.

-Relay attack. Type of hacking technique related to *man-in-the-middle attack*. In a classic man-in-the-middle attack, the attacker intercepts and manipulates communications between two parties initiated by one of the parties. In the case of relay attacks, communication with both parties is initiated by the attacker, and then relays messages between the parties without necessarily reading or manipulating them.

Some countermeasures against *phishing attacks* include;

-Filter emails for malicious URLs and attachments to prevent phishing emails using security analytics to filter out these threats.

-Update client-side operating systems, software and plug-ins.

-Implement 2-Factor Authentication[1] to any externally-facing system to stop attackers from using stolen passwords.

-Enable SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail) standards. These two standards help determine if an email actually came from the sender domain it claims to detect email spoofing and help filtering a lot of mass phishing.

Unauthorized tracking can be prevented by making certain that the values of the response appear to an attacker as random.

To avoid *NFC relay attacks*, three countermeasures can be applied.

-Limit maximum latency; determine how long it should take for a tag to return a response to a command in order to code the application reader-side to refuse to communicate with any tag that appears to be taking significantly longer than expected.

-Limit latency variation; If the kind of latency variation that the reader experiment when communicating with the card is characterized, then it is possible to program the reader to detect communications that exceed these levels of fluctuation and reject them.

-Pay attention to the terminal many times to make more difficult an attack to be done.

NFC vulnerabilities	
Main threats	**Countermeasures**
Phishing attack	Implement 2-Factor Authentication Enable SPF and DKIM Filter emails for malicious URLs
Relay attacks	Limit maximum latency Limit latency variation Pay attention to the terminal

Table 9. NFC vulnerabilities (main threats and countermeasures)

4.4 Bluetooth

The attacks from the network layer can directly target the sensor and actuator nodes and alter the destination of information, alter the information source or block the connections between the perception layer and the application layer hence complete breakdown of the service [20].

[1] 2-FA is a security process in which the user provides two authentication factors to verify they are who they say they are. *http://searchsecurity.techtarget.com/definition/two-factor-authentication*

Bluetooth main vulnerabilities are [83],[84]:

-Bluesnarfing. These attacks forces a connection to the device, such an attack can gain access to stored data and the IMEI (International Mobile Equipment Identity) which may lead to rerouting incoming calls to the attacker's device.

-Bluejacking. This attack is similar to a phishing attack. In this case, unsolicited messages are sent to a Bluetooth enabled device in order to conduct activities such as adding an entry to the contact list.

-Bluebugging. In these attacks, commands and devices can be accessed through exploiting a flaw in the firmware of legacy devices.

-Denial of Service. It is similar to a DoS in other types of wireless communication. The attacks overwhelm the target by sending large number of messages.

The countermeasure to avoid *Bluesnarfing* is to update Bluetooth devices with an up-to-date operating system and software. It is important to keep Bluetooth devices in non-discoverable mode anytime they are not actively exchanging data. Countermeasures include turning off Bluetooth device in certain public areas when they are not being used. Another important thing is to ignore suspicious messages, refusing or deleting them.

Countermeasures to mitigate *Bluejacking* include update both software and hardware of Bluetooth devices and requiring authentication.

To mitigate *Bluebugging* is important to limit device discoverability and connectivity by turning it off or hiding it in undiscoverable mode.

To prevent *DoS attacks* it is recommended to switch off Bluetooth when you are not using it.

Bluetooth vulnerabilities	
Main threats	**Countermeasures**
Bluesnarfing	Update Bluetooth devices with an up-to-date operating system and software Turning off Bluetooth device when it is not being used
Bluejacking	Update both software and hardware of Bluetooth devices Require authentication
Bluebugging	Limit device discoverability and connectivity by turning it off Hiding it in undiscoverable mode
Denial of Service	Switch off the Bluetooth when you are not using it

Table 10. Bluetooth vulnerabilities (main threats and countermeasures)

4.5 BLE

In Bluetooth Low Energy, some of the main attacks which can be done are [85]:

-MITM *(Man in the Middle attack).* An attacker secretly relays and possibly alters the communication between two devices that believe are communicating with each other.

The attacker can annul the system and send commands that compromise user security. The attacker will passively extract encrypted packets that the IoT devices communicate during authentication. The IoT device being attacked would receive the encrypted packet and would decrypt it using the same old keys.

-Attacks on exposed BLE services. These attacks can be done through different ways, for example, attacking AT interface. Oftentimes vendors leave hardware module's serial AT interface open. Then, attackers can easily exploit this open interface to change BLE module's configuration. Other attacks take advantage of the fact of having poorly written logic, poor or no random number generators or failing with the protection against brute force.

To avoid MITM, it is advisable to use the Bluetooth link layer security features. The use of a proprietary higher layer protocol can add a layer of security against MITM attacks.

Countermeasures to mitigate *attacks on exposed BLE services* such include:

-Apply time-limited provisioning. With this option, BLE device would expose the services for a limited time when at a deployment state.

-Build a list of the services. Build a checklist of all inputs and logic flaws before the device goes into production.

Bluetooth Low Energy vulnerabilities	
Main threats	**Countermeasures**
Man in the Middle atttack	Use the Bluetooth link layer security features
Attacks on exposed BLE services	Apply time-limited provisioning Build a list of the services

Table 11. BLE vulnerabilities (main threats and countermeasures)

4.6 Wi-Fi

There are some ways within Wi-Fi which are [86]:

***-Wi-Fi Password Cracking*.** Wireless access points that use older security protocols are easy targets because these passwords are easy to crack.

***-Planting Malware*.** Customers that join a guest wireless network are susceptible to unknowingly walking out with unwanted malware, delivered from bad-intentioned neighboring users.

***-Data Theft*.** Cyber thieves can intercept data being sent through the network.

***-Bad Neighbors*.** Due to the large number of wireless users on the network, the risk of a pre-infected device entering the network.

The countermeasures to avoid *Wi-Fi attacks* are:

-Implement WPA2 wherever possible. It is one of the hardest encryption methods and can provide extra security that network deserves.

-Enable web content filtering to prevent unsuspecting Wi-Fi clients from accidentally clicking that invites malware, exploitation, and backdoors to be loaded into the network.

-Implement application ID and control for monitoring. Inspect all Wi-Fi traffic.

Wi-Fi vulnerabilities	
Main threats	**Countermeasures**
Wi-Fi Password Cracking, Planting Malware, Data Theft, Bad Neighbors	Implement WPA2 and enable web content filtering

Table 12. Wi-Fi vulnerabilities (main threats and countermeasures)

4.7 WiMAX

Even if WiMAX has complex authentication and authorization methods and strong encryption techniques is still vulnerable to different threats such as [87],[88]:

-Masquerade attack. The masquerading consists of assuming, by a system, the identity of another one. These attacks can be made through spoofing or sniffing.

-Scrambling attacks. In this case the attacks affect all wireless systems with precise injections of RF interference during the transmission of specific management messages.

-Water torture attack. The attacker sends a series of frames to consume the receiver's battery.

A standard strategy to resist *masquerade attacks* is to create innovative algorithms that can efficiently detect the suspicious actions, which could result in the detection of attackers.
A possible solution for *scrambling attacks* is based on a key-dependent one way function and the Diffie-Hellman protocol [89].
To prevent a *water torture attack*, is very important to implement a sophisticated mechanism to reject the false frames.

WiMAX	
Main threats	**Countermeasures**
Masquerade attack	Create innovative algorithms
Scrambling attacks	Key-dependent one way function Diffie-Hellman protocol
Water torture attack	Sophisticated mechanism

Table 13. WiMAX vulnerabilities (main threats and countermeasures)

4.8 ZigBee

Some important attacks are Replay attacks, End-device Sabotage Attack and Network Key Sniffing attack [90],[91].

-Replay attacks in ZigBee are based on the interception of network traffic and the re-transmission as if the original sender is sending the data again.
-End-device sabotage attack is based on sabotaging the Zigbee end-device by sending a special signal that makes it wake-up constantly until the battery runs out.
-The network key sniffing attack is based on exploiting the key exchange process in ZigBee when using the Standard Security level defined by the ZigBee specification.

To avoid Replay attack can be used a 32-bit frame counter, which is a value that is constantly updated by the communicating devices every time a new frame has been received.

End-device sabotage attack can be prevented with the using of a remote alerting system for warning about power failures of ZigBee devices, but it is a requirement to have an active role of a network administrator. Another countermeasure is to configure the legitimate ZigBee End-device in a cyclic sleep mode that allows modules to wake-up constantly for checking data. The advantage of this countermeasure is that does not require continuous maintenance and actions of the network administrator.

Network key sniffing attacks. An important countermeasure against this attack is to preinstall the network key using the Standard Security level. The best option is using the High Security level in safety-critical ZigBee-enabled systems because then the network key is never transported unencrypted over the air.

ZigBee vulnerabilities	
Main threats	**Countermeasures**
Replay attacks	Use of a 32-bit frame counter
End-device Sabotage Attack	Configure the legitimate ZigBee End-device in a cyclic sleep mode Use of a remote alerting system for warning about power failures
ZigBee Network Key Sniffing attack	Preinstall the network key using the Standard Security level Use of the High Security level in safety-critical ZigBee-enabled systems

Table 14. ZigBee vulnerabilities (main threats and countermeasures)

4.9 Z-Wave

The vulnerabilities of Z-Wave protocol [92],[93]:

Using the Z-Wave physical layer, messages are asynchronously exchanged over the RF medium as MPDU (MAC Protocol Data Unit) frames. A MPDU contains a header, consisting of identification and control fields.

Impersonation attacks. These attacks violate the source integrity of the protocol. With the exception of the controller, Z-Wave devices, implicitly trust the source and destination fields of the MPDU frame.

Arbitrary SR cache modification. The attacker change the routing behaviour of target source nodes.

Black Hole attack. Is a type of Denial-of-service attack in which a router discards packets instead of relaying them because it is compromised for different reasons.

A way to avoid *impersonation attacks* is to use Z-Wave devices with security layer. Secure frames are signed and encrypted using keys exchanged during network

inclusion. An attacker who is not in possession of the encryption and authentication keys cannot transmit a valid secure frame.

Other countermeasures to prevent other attacks include:

-Use an asymmetric key system, where each node has a public and private authentication key. Devices may authenticate messages from the controller.

-Hop by hop authentication.

Z-Wave vulnerabilities	
Main threats	**Countermeasures**
Impersonation attacks	Use Z-wave devices with security layer
Arbitrary SR cache modification Black Hole attack	Use an asymmetric key system, hop by hop authentication

Table 15. Z-Wave vulnerabilities (main threats and countermeasures)

4.10 LoRa

The security vulnerabilities of Lora are [94]:

-Jamming attacks. In these attacks, malicious entities can transmit a powerful radio signal in the proximity of application devices, and disrupt the radio transmissions. Usually, those attacks require dedicated hardware, which minimizes the possibility of be done in real world devices.

-Compromise Devices and Network keys. LoRaWan provides end-to-end security using application and network keys. Someone with physical access can compromise the LoRa end-devices and attack them extracting the keys.

The *jamming* of the whole network can be detected since all the devices that communicate in that frequency would suddenly start to drop out from the network. One action could be switching the operational frequency when abnormal behaviors are detected.

Other countermeasures to *protect devices* are key management and frame counters.

LoRa vulnerabilities	
Main threats	**Countermeasures**
Jamming attacks	Switch the operational frequency when abnormal behaviors are detected
Compromise devices/network keys	Key management and frame counters

Table 16. LoRa vulnerabilities (main threats and countermeasures)

4.11 Cloud Computing paradigm

As data is being exchanged between different entities such as databases and applications, it is exposed to several kinds of attacks before it gets to the users of the information security threats can be from within the layer through mainly unauthorized access, theft of data, supply of fake data, worms and viruses. or the network layer through alter of data destination and source information [20],[21].

The security issue is the main concerned aspect in cloud computations [95]. Cloud Computation involves certain key information of companies and becomes the target of hackers. Due to the security issue, companies sensitive to data such as financial and medical companies are not recommended to adopt Cloud Computing technology.

The security issues within the Cloud Computing include:

-Wrapping attack. This attack is made by duplication of the user account and password in the log-in phase, and the SOAP[2] messages that are exchanged during the setup phase between the Web browser and server are affected by the attackers.

-***Flooding attack*.** These attacks happen when an attacker generates fake data, which could resource some type of code to be run in the application of a legitimate user.

-Data Stealing problem. In this attack, the user account and password are stolen. As a result, the storage integrity and security in the cloud can be attacked.

To avoid *wrapping attack,* Zunnurhain et al. [95] propose to increase the security during the message passing from the web server to a web browser by using the SOAP message. The way is adding a redundant bit with the SOAP header that will be triggered when the message is interfered with by a third party during the transfer. This bit will be checked and if it is found triggered, a new signature value will be generated.
To mitigate *Flooding attack* all the servers in the cloud could be organized as a group of servers. Each group can be designated for a specific job. When a server is overloaded, a new server will be deployed in the group.

[2] SOAP is a protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to induce extensibility, neutrality and independence
https://en.wikipedia.org/wiki/SOAP

To address *data stealing*, at the end of every session, the customer can send an email about the usage and duration with a special number to be used to access the system at the next time.

Cloud Computing vulnerabilities	
Main threats	**Countermeasures**
Wrapping attack	Add a redundant bit with the SOAP header
Flooding attack	Create a group of servers
Data Stealing	Send an e-mail about the usage and duration with a special number

Table 17. Cloud Computing vulnerabilities (main threats and countermeasures)

Stergiou et al. [97] analyze the security issues of both IoT and Cloud Computing technologies and their combination. To protect data they propose the combination of AES[3] and RSA[4] algorithms in the integration of IoT and Cloud technologies.

[3] AES is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption. The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits.
https://www.techopedia.com/definition/1763/advanced-encryption-standard-aes

[4] RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. *https://simple.wikipedia.org/wiki/RSA_(algorithm)*

5. IoT Scenarios

Daubert et al. [98] presents a formal model to manage the balance between trust in the service provider and need for privacy of individuals in IoT scenarios. This model establishes a relation between sensitivity of information, privacy, PII (personally identifiable information) and trust, and automatically maps between these terms are done, while maintaining user control. They expect to apply this model in M2M and Big Data scenarios as well.

In this section, I expose the issues of the main IoT scenarios and different ways to address them. These scenarios are Smart Home, Smart Grids, Connected Industry, Connected car, Connected Health and Smart Supply Chain.

5.1 Smart Home

There has been a significant growth in the demand for smart home devices. Smart home means automation of daily work with electrical equipments used in homes [99].

This concept provides a comfort and luxury life with security as well. Smart homes combine multiple numbers of IoT devices and services and provide users with different possibilities to control and learn the status of their home. The interconnections of these devices are done through wired, wireless protocols or wireless sensors such as Wi-Fi, Bluetooth or others for controlling and optimizing functions.

Razzaq et al. [99] highlight major security issues of IoT in a smart home, focusing the security attacks and their countermeasures. Here I summarize the main concepts of their contribution.

The possible security threats in a smart home include:

-DoS and DDoS attacks. In this case attackers may access the network and send messages to devices as RTS/CTS[5]. Other attacks are done using malicious codes to perform DoS attacks in the devices connected in the smart home.

The way to fight these attacks is applying authentication to block and detect unauthorized access. Apply cryptographic techniques to ensure security of the network.

-Monitoring and personal information leakage. The sensors can be hacked by an attacker and then it can monitor the home personal information.

[5] RTS/CTS is the optional mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem *https://en.wikipedia.org/wiki/IEEE_802.11_RTS/CTS*

The countermeasure for this threat is to apply encryption between gateway and sensors and user authentication.

-Falsification. When the communication between devices and the application server is done, an attacker may collect the packets by changing routing table in the gateway. The attacker can leak the confidentiality of data.

To avoid this threat, SSL techniques with proper authentication mechanisms should be applied. SSL (Secure Sockets Layer) is a computer networking protocol for securing connections between network application clients and servers over an insecure network, such as the Internet.

Another countermeasure is to block unauthorized devices that may try to access the home network.

-Trespass. The smart door may be accessed by an attacker and then trespass on the home.

Countermeasures to trespass are access control and authentication mechanism, and passwords should be changed frequently and must contain many characters because it is very difficult for attackers to break long passwords.

Cho et al. [100] propose *IoT security platform* based on a central node for a IoT home environments. This central node collects and store information of each sensor module related to IoT services by mounting a small PC (Raspberry pi) on a Wi-Fi routing functioning as Central Node and IoT equipment and manages the communication between things and sensors by determining each thing through the small PC. The small PC monitors the traffic and watch traffic attacks in order to detect, analyze and block it, and also monitors abnormal traffic patterns.

Smart Home vulnerabilities	
Main threats	**Countermeasures**
DoS and DDoS attacks	Apply authentication Apply cryptographic techniques
Personal information leakage	Apply encryption between gateway and sensors and user authentication.
Falsification	Apply Secure Sockets Layer (SSL) techniques
Trespass	Control and authentication mechanism Passwords should be changed frequently and contain many characters

Table 18. Smart Home vulnerabilities (main threats and countermeasures)

5.2 Smart Grids

Smart Grids are another important segment of IoT [101]. It seeks to optimize the distribution network of electric power to the maximum in order to make an efficient and sustainable use of this resource.

Smart Grids and their cyber-physical nature has rendered it vulnerable to different type of attacks that can happen to their networks, communications and physical and entry points.

Sanjab et al. [101] expose the key threats targeting smart grids and the potential solution approaches that can help mitigate these threats.

I explain the main information and aspects of their contribution highlighting the most important threats in smart grid environments and possible countermeasures.

In Smart Grid environments the common attacks are:

-DIA attacks *(Data injection attacks).* These attacks are meant to manipulate exchanged data, such as feedback control signals, sensor readings and electricity price signals. This type of attack can be done through compromising the hardware components or interception the communication links.

-Time synchronization attacks*.* These attacks, manipulate the time reference to create a false visualization of the actual system conditions.

-Availability attacks. This means the accessibility to grid components and also to the information transmitted and collected. DoS attacks belongs to availability attacks and block key signals to compromise the stability of the grid.

-Dynamic system attacks. The adversaries inject input data in the system without causing changes to the measurable outputs. The attacker compromises sensors, intercept their outputs while injecting its attack signal.

-Physical attacks. These attacks target physical components such as transmission lines, generation or substation.

-CAs *(Coordinated attacks)* can be launched by resourceful adversaries that exploit the dense interconnections between grid components to launch simultaneous attacks of different types targeting various components.

Countermeasures that mitigate these threats include:

-Prevention. This phase involves reinforcing the security of the system to prevent attacks to be done successfully. Two types of analyses can be performed:

-*Vulnerability assessment and risk management:* consists of determining which grid components are vulnerable to which types of threats. This is done with the analysis of past data to identify the components that have been more vulnerable.

-*Security reinforcement:* application of security policies for reinforcing the grid security after characterization of the main threats and their effects.

-*Detection*. It is important to take preventive measures. The operator must continuously scan the system to detect threats which have passed the attack prevention mechanisms.

-*Mitigation.* When an attack is detected, mitigating the effect of the attack and eliminating it is very important to restore the normal operating state.

After threat elimination, Smart Grids elements that had been disconnected such as generators, transmission lines and loads can be reconnected to restore normal operation.

Smart Grid vulnerabilities	
Main threats	**Countermeasures**
Data Injection Attacks, Time synchronization attacks, Availability attacks, Dynamic system attacks, Physical attacks, Coordinated attacks	Prevention, Vulnerability assessment and risk management Security reinforcement, Detection, Mitigation

Table 19. Smart Grid vulnerabilities (main threats and countermeasures)

5.3 Connected Industry

The next industrial paradigm, known as Connected Industry and often called Industry 4.0 brings self-organizing, fully connected and intelligent factories [102].

The intensive communication and huge amounts of data brings new challenges.

Smart Factories have to provide a safe environment to protect the complex IT systems that compose them and face all the threats that can cause serious damages to the data, computers, and all the elements that take part in the manufacturing process.

In the Industry 4.0 paradigm, cyber security strategies should be secure and integrated into organizational strategy from the beginning.

The main security issues in connected Industry are:

-Virus scanners constraints. Firewalls and virus scanners provide basic protection mechanisms, but they have limited value in Smart Factories because the most virus scanners cannot fight against unknown cyber threats that are oftentimes designed for a specific attack, and large amounts of data requires real-time analyses to isolate suspect data quickly.

-Smart tags manipulation. In the Industry 4.0, the smart tags attached to components may be manipulated by an attacker, and then travel through the supply chain carrying all the way with the malicious contents.

-Remote maintenance. Maintenance done by subcontractors creates potential risk, as it requires a connection to their computers and networks.

-Lack of digital identification and authentication. Some traditional machines can be operated directly by someone touching control panels and manipulate them easily.

Some important countermeasures to address these security threats are:

-ISMS (Information Security Management System). It helps to monitor and improve IT-security processes, and it addresses organizational and technical aspects, but must be managed by specialized employees. There are standards such as ISO/IEC 27001 and IEC 62443 that assures that the right processes are followed.

-Penetration Tests help to find security weaknesses that will exist in a complex IT-system, even though with very secure IT designs. It is important to have experts that perform these penetration tests and then find the best preventive solutions. *IT-Security Audits* should be done and implemented properly.

-End-to-End Encryption and Electronic Signing of sensitive communications to ensure that unauthorized persons or machines cannot successfully steal the information being transmitted.

-Strong Authentication of all people, machines and processes involved in potentially critical systems are a second design principle.

-Separation of subsystems in the overall Smart Factory architecture to assure that potential attacks can be constrained to one subsystem, by decoupling it from the rest of the Smart Factory.

Connected Industry vulnerabilities	
Main threats	**Countermeasures**
Virus scanners constraints, Smart tags manipulation, Remote maintenance, Lack of digital identification and authentication	Information Security Management System (ISMS), Penetration Tests, IT-security Audits, End-to-End Encryption Electronic Signing, Strong Authentication, Separation of subsystems

Table 20. Connected Industry vulnerabilities (main threats and countermeasures)

5.4 Connected Health

The Healthcare field fight against cyber risks much more than other sector due to the inherent weaknesses in its security posture.

Martin et al. [103] present the IoT issues in the connected health environments. Here I highlight the most important aspects and concepts of their report.

The most common cyber threats in connected health:

-Data theft for financial gain. Steal personal data for the monetary gain, for example; addresses, names, financial information and social security details.

-Data corruption. Alter test results for some interest.

-Data theft for impact. Steal personal data of politicians, celebrities or other high profile people.

-DoS attacks. These attacks are motivated by activism, revenge or blackmail and are intended to disrupt the healthcare networks.

Some ways to improve cyber security:

-Network security. Ensure the protection of the networks, filtering out unauthorized access or malicious content.

-Establish effective anti-malware defenses and control or limit the access to removable media (such as memory sticks).

-Monitoring. Continuously monitor all the networks and systems and seek unusual activity that may indicate an attack is in process.

-User privileges. Control and limit user privileges to essential systems to protect medical records.

Connected Health vulnerabilities	
Main threats	**Countermeasures**
Data theft for financial gain, Data corruption, DoS attacks, Data theft for impact	Effective anti-malware defenses, Filter out malicious content, Monitoring continuously all the networks, Control and limit user privileges

Table 21. Connected Health vulnerabilities (main threats and countermeasures)

5.5 Connected car

The connected cars and the communication with the external world expose vulnerabilities that can be threatened by malware to attack. These vulnerabilities could be in the design and implementation of hardware, software, applications and communication systems of the car. Vulnerabilities on the external data that enters a vehicle and in the operating systems used on them.

Zhang et al. [104] present main security issues in connected vehicles and different ways to fight against malware attacks. I expose the main information of their work related to these aspects and what are the mitigation options to address the issues.

The main ways where the malware can attack a car are:

-On-board Diagnostic Ports. This port enables someone to have access to the internal networks of the car and eavesdrop on messages over these networks, send malicious messages. Attacks can be done through installing malware on the ECUs[6].

-OTA Firmware and Software updates. Some smart cars have more than a hundred million lines of software code, and the remote OTA[7] firmware update can be a way for malware to infect cars.

-Embedded Web Browsers. Accessing the Internet and downloading applications to vehicles provide an easy way for malware to be downloaded to the vehicle.

-Removable Media Ports. Modern vehicles have USB ports to connect brought-in-devices. The remove media ports can be infected, and can in turn spread into the systems.

Traditional vehicle networks are MOST, CAN and LIN and cannot provide reliable security protections. The methods that have been used in order to protect vulnerabilities are:

-Physical Network Separation. Separate networks have been used to isolate different electronic subsystems on a vehicle, but this becomes a less effective way to protect networks due to the need of different electronic subsystems to communicate more with each other to support advanced vehicle functions. Close communication with the different subsystem is important to ensure more network protection.

[6] ECU (Electronic Control Unit) is any embedded system that controls one or more of the electrical system or subsystems in a transport vehicle *https://en.wikipedia.org/wiki/Engine_control_unit*

[7] Over-the-air is any method of making data transfers or transactions wirelessly using the cellular network instead of a cable or other local connection *https://www.gsmarena.com/glossary.php3?term=ota*

-Predefined messages. Some ECUs accept only predefined message types. This approach helps reduce virus infection and it is effective when all the traffic consists of only predefined messages.

-Signature-Based Malware Detection. This mechanism consists of two sequential steps. The first one, malware must be identified and a unique signature of each one of them is generated. Second step, each computer retrieves the malware signatures.

-Behavior-based malware detection. This mechanism determines whether a program is malicious by observing what it does when it executes. They detect polymorphic, metamorphic and any type of malware that mutate when replicating themselves.

Zhang et al. [104] present also an important security solution; a cloud assisted vehicle defense framework that can address the malware threats.

Connected car vulnerabilities	
Main threats	**Countermeasures**
Onboard Diagnostic Ports, OTA Firmware and Software updates, Embedded Web Browsers, Removable Media Ports	Physical Network Separation, Predefined messages Signature-Based Malware Detection, Behavior-based malware detection

Table 22. Connected car vulnerabilities (main threats and countermeasures)

5.6 Supply Chain

Within supply chains, deliberate cyber attacks usually involving malware can easily reach the business in the chain through vulnerable access points.

Kirby [105] expose the major threats and what are the main countermeasures. I present the different key aspects of these threats.

The attackers can identify vulnerabilities of the weakest member of the chain to gain access to the other members of the supply chain.

Supply chain attacks usually happen from websites and watering holes that are used to distribute malware and also third party (data storage and software providers).

Some solutions to fight these threats are:

-Encryption. Make sure that all business hard drives are encrypted.

-Cyber Security Training. Staff awareness to provide training to all employees to know well the threats and the best countermeasures in each case.

-Back up. Ensure the business has a secure backup and disaster recovery service in place and also the partners that have access to the business data.

-*Update*. Ensure the business run with automatic updates to reduce the risk of running on an unsupported or out of date system that hold vulnerabilities.
Implement *data security policies*. Use endpoints for devices that have been checked and approved.

Supply Chain vulnerabilities	
Main threats	**Countermeasures**
Third party software providers, third party data storage, websites and watering holes,	Encryption, cyber security training, back up update, implement data security policies

Table 23. Supply Chain vulnerabilities (main threats and countermeasures)

6. IoT security solutions

There are many solutions proposed for IoT by some researchers in terms of data protection. I highlight and summarize the most important contributions.

Radomirovic' et al. [106] propose a IoT model which consists of an asynchronous communication network and a Dolev-Yao adversary with fingerprints abilities. A Dolev-Yao is a formal model used to prove properties of interactive cryptographic protocols. They expose that the communication between devices should be considered under the control of this formal model.

Alshammari [107] propose a methodology to mitigate the effect of attacks in Data Centers in order to decrease the vulnerability for the security of the network. This methodology evaluates the parameters in the presence of attacks; Energy consumption of the DC (to execute the request),Time delay (to reach the request) and Number of packets received. Then it mitigates the attack by excluding the request coming from the same IP after exceeding Time delay. Finally, compare these parameters with the parameters in the presence of attack.

Hodo et al. [108] presented an *ANN (artificial neural network)* based approach for intrusion detection on IoT network to identify DDoS and DoS attacks. These networks are inspired by the biological neural networks. The ANN algorithm was validated against a simulated IoT network demonstrating over 99% accuracy and can detect several attacks. It also helps in order to improve stability of the network at an early stage of the attack, avoiding major network disruptions.

Huuck et al. [109] propose a specific software lifecycle solution to minimize the potential security threat and implications at low cost. They explain why static program analysis is one of the main tools for risk mitigation and security improvement. One example of the static program analyzer is Goanna by Red lizard Software [110] which is able to detect use of data without protection and can warn quickly in these cases.

Karolewicz et al. [111] propose and analyze eight variants of the distributed data storage with different database structure in order to design an effective IoT data storage service. The proposed variants differ in the rules on how data records are propagated, stored and retrieved inside the network.

O'Neill [112] describes an alternative approach for providing authentication and identification for IoT devices through PUF (physical unclonable function). PUFs use the manufacturing process variations of silicon chips to generate a unique digital fingerprint.

Chetterjee et al. [113] propose a solution with PUFs as well. They explain the development of a light weight identity-based cryptosystem suitable for IoT in order to provide secure authentication and message exchange across the device and this development is done through a PUF.

Huang et al. [114] present a security framework that named as SecIoT and that provides robust and transparent security protection. They study the data security behaviour in different IoT scenarios. The framework addresses the main concerns of users and ensures communications, supports use authorization and provides essential authentication.

Rehman et al. [17] focus on the major issues related to security, such as Identification, authentication, data management and heterogeneity.

To address the authentication problem the available solutions proposed are handshake process and public key cryptography. In the case of data management the solution proposed is SQL Lite [115], and to address identification issues, the solutions is to use IPv6 and hardware address. To remove the issues of heterogeneity such as latency and processing speed and communication between different types of devices, it must be used IDRA architecture which is specially designed to integrate all the devices. IDRA can connect objects directly without any gateway. It supports communication between devices that uses different MAC protocols.

Niu et al. [116] uses the attack tree model proposed by Bruce Schneier [117] on the study of the perception layer of IoT. Attack Tree is a tree structure to stimulate the method of various attacks and attacking steps depend on each other. The conclusion of the analysis is that perception layer should be strengthened with intrusion detection mechanisms, establish of identity authentication scheme and also strength node authentication.

Sadeghi et al. [118] provide an introduction to Industrial IoT systems with security and privacy challenges. They highlight the fact of securing the IoT industrial systems with a holistic perspective. The requirement is a holistic cyber security framework that covers all abstraction layers of heterogeneous IoT systems and across platform boundaries in order to address the various security and privacy risks. This includes different aspects such as, platform security, security engineering, security management, identity management and industrial rights management.

Hernandez-Serrano et al. [119] propose three recommendations that need to be followed by any IoT ecosystem participant. These recommendations have been done following solutions for BIG IoT project[8].

[8] The objective of the BIG IoT project is to ignite really Internet of Things ecosystems *http://big-iot.eu*

Regarding privacy, IoT platforms must accomplish three requirements: First of all, data minimization to limit the collection of personal information to what is directly necessary to accomplish a specified purpose. Secondly, provide strong accountability to provide mechanisms to securely loc any action by any member dealing with sensitive data. Finally, transparency and easy access to the data; those who control data must bring transparent and easily accessible data protection policies that show in a clear way how their data is being processed to the end users.

Cheng et al. [120] propose quantum-resistant algorithms for securing communication in the IoT based upon the advances in quantum computing. Depending on the different security purposes different algorithms are proposed such as AES-256 and XMSS.

Marin et al. [121] present an ECC (Elliptic Curve Cryptography) for secure communications in heterogeneous IoT networks. The ECC is a variant of asymmetric or public key cryptography.

Liu et al. [122] present an IoT middleware layer that connects heterogeneous hardware in local IoT systems. They propose an IoT name resolution service (IoT-NRS) which is a device registration service that provides naming and key management as a core component of the middleware layer, and develop a lightweight keying protocol that establishes trust between an IoT device and the IoT-NRS.

Wang [123] provides an overview of privacy preserving techniques in IoT. Anonymization methods are the primary techniques used to maintain privacy preservation in IoT.

Cirani et al. [13] propose a scalable, reliable and self-configuring, peer-to-peer based architecture for IoT networks, aiming at providing automated service and resource discovery mechanisms, which require no human intervention for their configuration. It is proposed this architecture for both local and global service discovery (SD knows as the automatic detection of devices and services offered by these devices on a computer network). They show how the proposed architecture allows the local and global mechanisms to successfully interact, while maintaining their mutual independence.

Tanaka et al. [124] presents approaches to ensure availability. Two key points are: detecting problems as soon as happens, and taking provisional measures to prevent the spread of damage while the system continues functioning. The technology proposed is based in three functions: first, a server internal operation monitors function to detect suspicious behaviors, secondly a traffic anomaly detects suspicious communications and finally evaluation function is done.

IoT subjects	IoT concepts	Research (vulnerabilities)
Technologies	RFID	[17],[21],[70]-[75]
	WSN	[17],[21],[72],[76]-[79]
	NFC	[17],[80-82]
	Bluetooth and BLE	[83]-[85]
	Wi-Fi	[86]
	WiMAX	[87],[88]
	ZigBee	[90],[91]
	Z-Wave	[92],[93]
	LoRa	[94]
Paradigm	Cloud Computing	[20],[21],[95],[97]
Scenarios	Smart Home	[99],[100]
	Smart Grids	[101]
	Connected Industry	[102]
	Connected Health	[103]
	Connected car	[104]
	Supply Chain	[105]

Table 24. Articles classified by subjects: Technologies,paradigm and scenarios

7. IoT and Blockchain convergence

The fast development process of both Blockchain and IoT-based technologies will bring changes over the next decade in the way we live and connect, as long as the objectives of protecting user privacy and data are maintained.

7.1 Concept

The converge of IoT and Blockchain may create a good environment to maintain data privacy and also to protect all connected devices from possible attacks.
The use of Blockchain can provide higher security compared to storing all data in a central database. In the data storage and management aspect, damage from attacks on a database can be prevented. Moreover, since the Blockchain has an openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data.

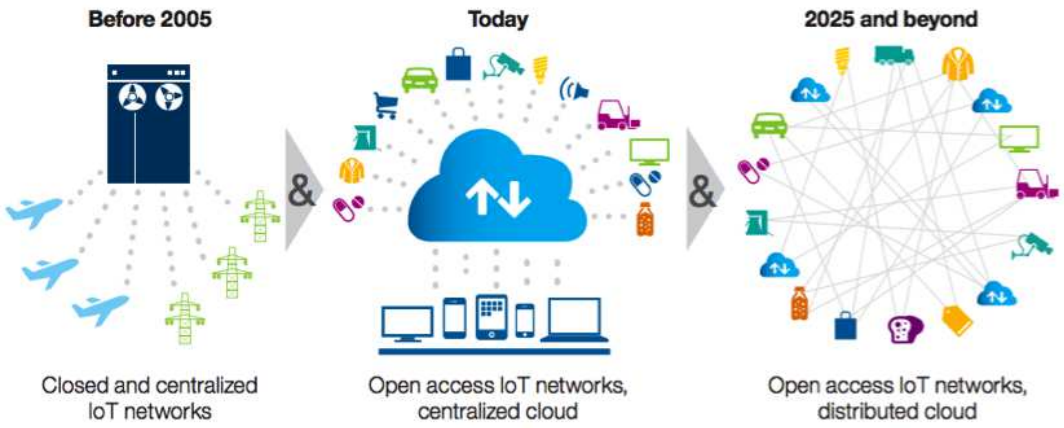

Figure 8. The IoT network topologies used in the past, today and in the future
Source https://securityledger.com/2015/01/ibm-and-samsung-bet-on-bitcoin-to-save-iot/

Figure 8 illustrates the IoT networks evolution and how it is expected to be in the future with the integration of Blockchain technology.
The fast development process of both Blockchain and IoT-based technologies will bring changes over the next decade in the way we live and connect, as long as the objectives of protecting user privacy and data are maintained.

Although the convergence of IoT and Blockchain will bring many opportunities and advantages, there are some disadvantages that will have to be considered. The main disadvantages are [125]-[127]:

-*Legal issues*: It is a completely unknown territory without any legal code to follow, and this could be a problem for manufacturers and service providers.

-*Storage* could be a problem. The ledger has to be stored on the nodes themselves. As time goes on the size of the ledger will increase.

That is far away of the capabilities of a wide range of smart devices that have very low storage capacity.

-*Time issues*: time required to encrypt all the objects IoT involved in a Blockchain network. One of the main problems is that the different types of devices could not be able to operate at the desired speed with the same encryption algorithms due to their different computing capabilities.

-Lack of maturity and standards to promise interoperability among competing ledgers and platforms.

On the other hand *the advantages of IoT using Blockchain are:*

-*Security (avoid attacks and manipulation).* A private Blockchain can store cryptographic hashes of individual device firmware. This record can prove that a specific device has not been manipulated or attacked. When that is proved, that device is allowed to connect with other services or devices.

Blockchain-based identity and access management systems can fight successfully against attacks related to IP address forgery or IP spoofing.

Due to the fact that is impossible to alter approved Blockchains, any device cannot connect to a network with fake signatures. Immutability and decentralized access prevent and detect malicious actions.

Blockchain avoids the issues of cyber attacks in cloud servers, software bugs or other similar problems because records are on many computers. The network is resilient to failures because it is a decentralized P2P network with no points of failure, and where the transactions cannot be manipulated.

-*Strength of the architecture.* IoT architecture can be vulnerable in every part of the system. Different attacks can be done such as DDoS, hacking, remote hijacking and data theft. Blockchain provide secure and more integrity for data vulnerabilities through verification; transactions are signed and verified cryptographically to prove that the originator is the one who have sent the message.

-*Solve capacity constraints.* The quick growth of connected devices must be managed properly to be able to adapt the network capacity for all these devices.

Blockchain solves the problem of a centralized entity because through smart contracts, devices can communicate in a secure way with each other and execute actions automatically.

-*Instantaneous transfer*. It is working all the hours, seven days a week. Reconciliation and paymeny of transaction can be done in less than 10 minutes.

-*Autonomous*. Blockchain can allow IoT devices to communicate with each other and for transactions in an autonomous way as each device has its own Blockchain account and there is no requirement for a trusted third-party.

-*Scalable.* Blockchain network is scalable due to the fact it is maintained by a network of peers. The computing capability of the network scales as more and more peers join the Blockchain.

7.2 Internet of Things applications using Blockchain

Blockchain is ready to transform practices in a number of IoT sectors, including [128]:

-Automotive. The automotive industry is adopting measures based upon Blockchain and IoT convergence. These solutions want to provide reliable information and allow to do transactions between the main business partners; insurers, manufacturers, auto financing companies, regulators, service providers and customers.

-Healthcare. Blockchain can enhance this sector by providing the perfect environment to store patient data that comes from several medical devices.

-Supply chain. Blockchain can address many problems in the supply chain industry such as optimization visibility and demand. It can create a reliable environment for all the members participating in the supply chain, allowing a secure access to shared data. Some of the applications in this industry can include the identification of contaminated food in the chain or tracking food items for specific goals related to packaging.

-Home automation. A Blockchain-IoT enabled technologies are being used in smart cities and smart buildings to enhance operations, security, and to also to enhance the protection of devices and the data collected from them.

7.3 IoT solutions using Blockchain technology

Many solutions have been developed for providing security within IoT taking the advantage of Blockchain technology. I summarize in this section the most important contributions.

Dorri et al. [129] propose a secure, private and lightweight architecture for IoT based on Blockchain technology that eliminates the overhead of Blockchain while maintaining most of its security and privacy benefits. The proposed architecture consists of an overlay network and cloud storages coordinating data transactions with Blockchain to provide privacy and security for smart home environments.

Zhang and Wen [130] propose an IoT electric-business model specially designed for the IoT E-business by redesigning many elements in traditional E-business models and using P2P based on the Blockchain and smart contract to realize the transaction of smart property.

Xia et al. [131] propose a solution to address the medical data security issues. They present a blokchain-based data sharing framework that addresses the access control challenges associated with sensitive data stored in the cloud. The system is based on a permissioned Blockchain which allows access to invite and hance verified users. The system permits users to request data after their identities and cryptographic keys are verified.

Shafagh et al. [132] present a data-centric design for IoT with a focus on sharing, resilience and auditable protection of information. They introduce an initial design of a Blockchain-based end-to-end encrypted data storage system.

B.Lee and J.Lee [133] present a firmware update scheme that securely checks a firmware version, validates the correctness of firmware and enables downloading of the latest firmware for embedded devices in an IoT environment. This scheme relies on a Blockchain technology for firmware checking and validation. An embedded device requests its firmware update to nodes in a Blockchain network and tests a response to determine if it is up-to-date or not. If not, the embedded device downloads the latest version from a peer-to-peer firmware sharing network of the nodes. In the case that the version is updated, its correctness are checked. This proposed scheme avoids tampering attacks.

Ouaddah et al. [134] propose a framework for access control in IoT based on the Blockchain technology. They present a fully decentralized pseudonymous and privacy preserving authorization management framework that enables users to own and control their data. To implement this model they use and adapt the Blockchain into a

decentralized access control manager and establishes an initial implementation with a Raspberry PI device.

Rodrigues et al. [135] present a BloSS (Blockchain Signaling System), which is a novel approach deploying hardware to simplify the signaling of DDoS attacks in a cooperative network defense system.

Zyskind et al. [136] describe and implement a protocol that ensures users to own and control their data without the requirement of a third party. It is done through a decentralized personal data management system.

Conoscenti et al. [50] focus on the scalability issue that Bitcoin has to deal with. Their research work analyses by different simulations how scalability behaves. They highlight the Bitcoin Lightning Network [137] as one of the possible solutions.

Outchakoucht et al. [138] focus on access control in the IoT context by proposing a dynamic and fully distributed security policy. This proposal is based on the concept of Blockchain to ensure the distributed aspect and also on machine learning algorithms in order to provide a dynamic, optimized and self-adjusted security policy. This solution gives people total control of their devices without the need to trust in an outside entity and bring an automatically-improved and dynamic security policy.

Dinh et al. [59] present a benchmarking framework [139] designed to evaluate performance of private Blockchains agains data processing workloads. With this framework called Blockbenck and their contribution, they want to guide for the future Blockchain systems design implementations.

Gaetani et al. [52] focus on a case study from the European Sunfish project [140] which seeks to facilitate the formation of secure federations of various Public-sector cloud implementations to be able to securely share data and services. With this approach, they present a first design of an effective Blockchain-based database for Cloud Computing environments based upon a total consensus mechanism.

Park et al. [141] focus on the study of Blockchain concept and what are the issues that must be considered when this technology is used in Cloud Computing environments. They present a method of secure Blockchain use and removal protocol.

O' Dair et al. [142] discuss the potential of Blockchain technology to transform the music industries associated with recorded music. Blockchain could enhance the availability and accuracy of the copyright data, and also improve the transparency of the value chain.

Crainy et al. [143] present a variant of the Byzantine consensus algorithm for consortium Blockchains. Byzantine consensus allows a group of peers to reach agreement on some value, even if a fraction of the peers is controlled by an active adversary. This algorithm avoids Sybil attacks.

Rasheed [144] exposes the opportunities Blockchain could bring to the IoT devices. He discusses the improvements that wearable devices could take from the IoT and Blockchain convergence. These solutions are focused on payments, advertising, healthcare and events.

Payments. The cryptocurrency could be uploaded in the wearable devices via online or an ATM. This wearable devices can offer payments in a faster way without the need to show anything as in the case of credit cards.

Advertising. Sometimes the companies penetrate into the privacy of a consumer to obtain valuable information. Blockchain can protect the privacy of consumers to avoid bad habits.

Healthcare. In this field, wearable devices can also benefit from Blockchain technology and IoT, with patients who have some medical devices implanted in their bodies and are installed with sensors. These sensors can send data to the medical staff through smart contracts.

Events. It proposes the use of wristband to collect and send information between the celebrities and fans. With this approach, the artists can interact with the fans and obtain valuable information.

Ruta et al. [145] expose a novel SOA (Service-Oriented Architecture) which is a style of software design where services are provided to the other components through application components over a network [146]. This architecture is based on a semantic Blockchain for different operations: selection, payment, discovery and registration. These operations are implemented by smart contracts.

Sharma et al. [147] propose a distributed secure SDN architecture for IoT using Blockchain to address the issues of the high amount of connected devices such as availability, flexibility, security, scalability and efficiency. This architecture is called DistBlockNet and combines the best of Blockchain and SDN technologies. The aim of the architecture is to protect data and mitigate DoS and DDoS attacks, spoofing and other network attacks.

Sun et al. [148] explain the advantages that Blockchain could bring to smart city development through sharing service. With this approach they want to be a start-point for more research and discussions on the design of Blockchainbased sharing services for smart cities.

Bahga et al. [48] present a peer-to-peer platform for the IoT based on the Blockchain technology. This platform, called BPIIoT allow the interaction between the members in the network with each other without an intermediary.

Ghuli et al. [149] present a method for peer to peer identification of ownership of IoT devices in a Cloud Computing that is secure with all kinds of malicious attack. This method consists of device being added by its manufacturer and then being transferred to a user based on Blockchain technology.

Walker et al. [150] present a platform to test transactive IoT Blockchain applications. This platform uses Ethereum, it is called PlaTIBART and it is used to develop,test and analyze fault-tolerant IoT Blockhain applications.

Shae et al. [151] present a Blockchain platform for precision medicines and also clinical trial. This platform consists of 4 new system components to develop new Blockchain based distributed parallel computing paradigm:

-A new Blockchain based general distributed and parallel computing paradigm.

-Blockchain application data management component for data integrity, big data integration and integrating disparity of medical related data.

-Verifiable anonymous identity management component for identity privacy for IoT devices and secure data access.

-The trust data sharing management component to provide a trust medial data ecosystem for collaborative research.

Mustard et al. [152] discuss the role of Blockchain in the ICS (Industrial Control System application). They expose many industrial scenarios where Blockchain is used. Some of them are:

-In *retail* to record every action that happens in a retail supply chain and make all the data searchable in real time for consumers.

-In the *Healthcare Industry* to maintain a backup of the people's DNA that can be securely accessed for medical applications.

-In the *Energy management* to allow customers to trade directly, sell and buy without the need of a central provider.

Cocco et al. [153] focus on the challenges and opportunities for the use Blockchain technology in banking markets. They highlight the potential of Blockchain to manage the financial processes in a more efficient way than the current system.

Beck et al. [154] discuss the Information Systems Research programs with the implementation of Blockchain technology. They defend to foment the development of IS research programs and taking advantage that each time the Blockchain is more mature.

Lin et al. [155] discuss the importance of Blockchain technology in the next step in the evolution of ICT e-agriculture that will increase economic efficiencies and food safety.

They propose a system with a Blockchain infrastructure for use at the local and regional scale.

Baxendale [156] discusses whether Blockchain could revolutionise EPRS (Electronic Patient Records). EPRs provides the information of patients visit to a hospital by storing scheduling, clinical and emergency department information. He highlights the main benefits of Blockchain technology to enhance EPR which are:

-Encryption and tamper resistance.

-Immutable and verifiable transactions.

-Decentralization, ensuring the integrity of stored data.

-Global accessibility.

Heston [157] exposes the benefits of Blockchain technology to improve gun control. The enhancing of gun tracking can avoid many suicides, which are the most common way the guns are used to kill. Blockchain implemented in this field will improve gun laws and also the gun tracking from manufacturer to end user making the process much safer.

Cai et al. [158] discuss the opportunities that Blockchain could bring to avoid fraud through online business. Blockchain systems are reliable in preventing objective information fraud where fraudulent information is fact-based (for example loan application fraud).

Russo [159] discusses the importance of implementing Blockchain in every industry that requires to ensure confidentiality and integrity of the data they manage. Blockchain will become a key element of the digital industry in the future. He highlights the impact of this technology in different fields such as banks, government and Healthcare.

Yin et al. [160] introduce and design a Blockchain solution to secure communication within M2M for CPS (Cyber-physical systems). CPS is a mechanism that is monitored by computer-based algorithms integrated with the Internet and its users [161]. They present a case study on cotton spinning production and prove that Blockchain technology can expand machines and protect the communication of data between them.

Lier [162] discuss the importance of the combination between Blockchain technology and CPS (Cyber-physical systems). Cyber-physical systems can take advantage of the Blockchains' features and be able to acquire more independence and autonomy in performing the required tasks.

Lehmacher et al. [163] discuss the advantages of implementing Blockchain technology in trade and specifically in the international supply chains. The inspections and stops across the supply chain drives up prices and it prejudice business and consumers.

Blockchain can ensure that records are protected and cannot be manipulated or faked, and the visibility in parts of the supply chain brings confidence to the whole participants.

Khaqqi et al. [164] propose an ETS model which aims to reduce emission production, personalized for Industry 4.0 integration. It works through Blockchain technology and smart device to enhance compliance measure of ETS policy. This model wants to address ETS's fraud and management issues.
Wolfond [165] discusses the potential that Blockchain-based solutions to address the present and future challenges of authentication and identity verification. His contribution wants to improve service delivery in public and private sectors within a Canadian context.
McCorry et al. [166] present a smart contract solution that works on Ethereum for the OVN (Open Vote Network) [167]. This implementation was successfully proved with forty simulated voters with a reasonable cost ($0.73 per voter) and with the guarantee of providing maximum voter privacy.
Korpela et al. [168] present a case study to bring more knowledge about digital supply chain integration to accelerate its implementation in business process.

Subjects	Research
IoT security solutions	[13],[17] [106]-[124]
Blockchain and IoT convergence	[50],[52], [129]-[136] [139]-[143], [144]-[145] [147]-[160], [162]-[166], [168]

Table 25. Articles classified by subjects: IoT security solutions, and Blockchain and IoT convergence

Conclusions of the articles

The main concerns within the IoT paradigm are the security issues of the devices due to the rapid increase in their use and also the security of the networks that allow their connectivity. The main mechanisms to mitigate the attacks are focused on cryptographic techniques and protocols to guarantee authentication and identity of the devices.
The other concern is to ensure the privacy and security of the data on the platforms that offer services to store and process the data.
Due to the fact that the IoT represents many different technologies and types of intelligent devices and the ways to connect them are increasing, keeping the privacy and security of the data is a challenge to achieve increasingly difficult.

Blockchain technology is still in an experimental phase, but the solutions that have been developed have very interesting implementation perspectives to protect the data and avoid or minimize attacks.

Many solutions focus on the Healthcare sector to improve the EPRs where data privacy plays a critical role in the relationship between patients and the health system.

Within medical environments connected records that contains personal information are attractive targets for identity thieves (Social Security number is all over the medical records). Compromising a medical IoT device could result in a breach of these records.

Other solutions focus on the Industry 4.0 where technology and data security determines the competitive value of the company, for example the projects that take the advantage of the combination between Blockchain technology and M2M to improve the communication security of the different machines that take part in the manufacturing processes of the industries. Most of these projects within smart factories work on enhancing Cyber-Physical Systems.

It is important to highlight the benefits that smart contracts can bring to various applications, for example, in the supply chain processes of the businesses, which will allow the members to access in a more reliable and secure way to the data shared every moment.

8. Proposed scenarios

I propose three hypothetical scenarios where the convergence between IoT and Blockchain could be applied in the future. It is not the aim of this project to design the architecture of these scenarios, but to present the main concepts and the important ideas related. These scenarios are a sport center, a smart museum, and a football club.

1. Sport center with IoT and Blockchain technology

This hypothetical scenario is a sport center, which has paddle courts, a gym and a pool. All the center has Wi-Fi connection inside and around.
In this scenario, there is a local private Blockchain that stores data. It keeps track of transactions and has a policy header to manage the transaction of the members of the sport center.
There is also a device that functions as a miner and processes incoming and outgoing transactions to and from the sport center. The miner collects all transactions into a block and appends the full block to the Blockchain.
This system could be used also for the other proposed scenarios as well.

In this sport center, Blockchain technology could be applied through the smart contracts for:

-*Digital Identity*. The partners of the sport center may use this application to ensure that the identity of the members is recorded on a shared ledger and no one else can have authorization to access the data and information or physically enter the center.

-*Reservation of paddle tracks*. Through the smart contracts, it is possible to reserve the tracks according to the availability of both parts (the client and the center) and avoiding mediation through other mechanisms such as calls or physical presence.

2. Smart museum with Blockchain technology

This hypothetical museum has six floors. On the ground floor there is a store with products related to the art world. On the first floor there are projection halls and a conference room. From the second to the fourth floor, there are artworks permanently

exhibited and the fifth and sixth floor would have the artworks that are frequently changed for other ones.
The museum has all kinds of sensors, controllers and actuators to monitor and manage temperature, lights and the security of the museum.

The technologies used would be:

-*Bluetooth Low Energy (BLE).* The connection between intelligent devices can be done with BLE technology. BLE networks do not require an additional gateway device like other WPANs requires. The handheld devices can act as a free gateway to the Internet for the BLE networks. Besides, BLE allows the devices to have a longer battery life and is also more resistant to interference and noise and therefore safer against attacks.

-*Wi-Fi* connection available to all users who access the museum through authentication. WPA2 (Wi-Fi Protected Access 2) protocol can be implemented, although it is vulnerable, guarantees more security than the WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) protocols.

-*RFID* technology could be used for two main purposes:

1. Protection of artworks. One of the purposes would be to control the state of the artworks through constant monitoring to avoid robberies. Through the RFID system, it can be controlled in real time if unusual movements or vibrations occur. The tag establishes some initial parameters of the location of the artworks and any change or minimal modification of it activates a signal that is immediately detected.

2. Control of entry and exit of artworks. It would also be used for organizational aspects. The inventory of entries and exits of the works could be done and know at all times where they are located and what is their state.

-*QR codes* can be used to give information about the artworks. They could be located next to the artworks.

This information can be obtained directly with a smart device like a smartphone using applications designed to read these codes. The information available would be the author, the year and a description of the artwork.

-*NFC.* The museum store would allow payments using NFC technology through a smartphone.

The museum also has *smartphone applications* to allow the people interact with all the information related to the museum.

On the other hand, the smart contracts would serve as:

-Payment of employees' salaries. The members of the museum would receive the payment of wages in cryptocurrency through the Blockchain system. Smart contracts in this case can increase the employee's guarantees in comparison with the traditional employment contract. This will allow the transfer of wages in the period specified in the contract without delays and also will protect the employees from possible bad practices of the company.

-Supply chain. The museum could have some of the artworks exposed indefinitely and others exposed temporarily. For the temporary exhibition artworks, smart contracts may be used to close the assignment contracts. This will allow closing agreements without the need for physical presence and avoiding additional costs that occur in traditional contracts with many intermediaries and other administrative expenses. It will allow the possibility of monitoring of the state of the artworks every moment in their way from their departure to the arrival at the museum through secure and protected networks.

-Hiring. Smart contracts will be used also to hire experts from the art world to hold conferences. The methodology would be recruiting people who are being offered to the museum through another company. The convergence between this company and the museum through the Blockchain technology would guarantee the correct function of this hiring process.

-Purchase of museum products. The store of the museum has the possibility of purchasing physically and virtually.

-Virtual auctions. Another potential application that Blockchain technology could bring is to allow virtual auctions of the artworks. It is a new trading system in which, in a certain way, the personal relationship with the client disappears to turn it into a negotiation through the Internet.

3. Football Club with Blockchain technology

The benefits of Blockchain technology can be applied in the field of sport in many ways, for example, in a Football club to improve the relation between the club members and the followers of the football team.

Within the stadium, cameras monitor peoples' behaviour, secure entry into restricted areas and detect movement in parking garages.

Sound, parking, temperature and other sensors detect and measure what is happening around the stadium. Wi-Fi connection is available around the stadium.

Smartphone apps can be a hub for all the club's information and communication needs, allowing the interaction and participation of fans.
In this case, smart contracts could be used to:

-*Purchase of tickets*. This could be done using Blockchain to avoid queues at sales booths and also allow the buyer to easily choose the seat location in the stadium.

-*Voting*. Another important feature would be to allow members to make virtual votes on decisions that affect the monetary investments that they pay annually, such as the election of the presidency and management team, and all the other decisions related to the club.

Having a voting system implemented through Blockchain technology would facilitate participation and ensures a safer and more reliable way than traditional methods.

-*Payment of employees' salaries*. The members of the Club would receive the payment of wages in cryptocurrency through the Blockchain system the same way as I have presented in the smart museum scenario.

9. Conclusions

This project presents an overview of the IoT paradigm and the Blockchain technology from a security approach. The fact that every day there are more and more devices connected to the Internet, increases the possibility to receive attacks in many different ways. We have seen the protocols and also the most typical architecture of the IoT, which are the 3-level architecture and the 5-layer architecture. There is no general consensus to establish a reference architecture, but I have used the 3-level as a model to develop and study the different issues of the most important technologies classified by layers.

The most important technologies within IoT have been analyzed, studying the main threats of them and what countermeasures can be applied.

RFID, WSN and NFC are the technologies more used in the perception layer, they play a key role collecting the data of the environment through sensors and require further measures in the authentication and identification of devices to guarantee the confidentiality and integrity of the data. Due to the limit computation capability of sensor nodes, the option of recive attacks is very high.

Some of the attacks that target the perception layer are Eavesdropping, Phishing, Replay attacks and Information Tracking.

The network layer is responsible for transmitting the data received from the perception layer to the application layer through various networks. This layer handles the transfer of data to places where it can be processed and manipulated. The technologies of the network layer are vulnerable depend upon the protocols and the security mechanisms in which they work.

I have analyzed the issues within Bluetooth, Bluetooth Low Energy, Wi-Fi, WiMAX, Z-Wave, ZigBee and LoRa technologies. Some important vulnerabilities of this layer are DoS attacks, User tracking and MITM attacks.

The application layer is the result of close integration between communication technology, computer technology and industry professional which can be able to find applications in many aspects. Acquiring, storing, analysing and processing of data received from the network layer is done in the application layer.

In this layer, Cloud Computing paradigm has been studied. Some of the security issues in application layer include flooding, data stealing problems and tampering.

Moreover, I have analyzed the vulnerabilities of the most common scenarios in the IoT which are Smart Home, Smart Grids, Connected Industry, Connected Health, Connected car and Smart Supply Chain.

Some of the attacks and vulnerabilities in these scenarios include DoS and DDoS attacks, data injection attacks, physical attacks and personal information leakage.

Many of the IoT projects are focused on the study of improvement of security in Connected Industry and Connected car. On the other side, the projects that seek the opportunities that the convergence of the IoT and Blockchain technology are more focused on the Supply Chain, Connected Health and Smart Home environments.

The goals of the thesis have been achieved. I have acquired key information and knowledge through many resources such as articles and research publications that I have used as a guide to analyse the issues and solutions of all the technologies and scenarios. Besides, I obtained important information on projects focused on the opportunities of the combination of IoT and Blockchain technology.

The first aim of the project was to study the vulnerabilities of the technologies within the IoT, but as I gathered more information from different resources I decided to add also the information about the vulnerabilities in the most common IoT scenarios to have more approaches of the threats in these environments and how can be addressed.

Blockchain technology can be the best solution to cover the need for quicker growth of smart connected devices that look for a safe and reliable environment for data store and manage. In this thesis, several solutions have been presented that combine this technology with the IoT. The M2M paradigm plays also an important role in the study of projects related to Blockchain technology, for example Cyber-Physical Systems.

The weaknesses of the Blockchain technology are the slow implementation, the lack of maturity and standards, and also the regulatory problems that depend on the individual policies of each country.

Instead, the strengths are transparency, the absence of intermediaries, and the security that can bring to the IoT.

Many companies are already implementing projects with Blockchain, and if everything goes as well as it is expected, It will be the most important technology in the future for the IoT data protection.

10. Glossary

2FA	2-Factor Authentication
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AES	Advanced Encryption Standard
AMQP	Advanced Message Queue Protocol
AMQP	Advanced Message Queue Protocol
ANN	Artificial Neural Networks
ARIB	Telecommunications Technology Association
ATIS	Alliance for Telecommunications Industry Solutions
BLE	Bluetooth Low Energy
BIoSS	Blockchain Signaling System
CAN	Controller Area Network
CCSA	China Communications Standards Association
CEN	European Committee for Standardization
CoAP	Constrained Application Protocol
CPS	Cyber-Physical Systems
CTS	Clear To Send
DaPP	Decentralized Application
DDoS	Distributed Denial of Service
DKIM	Domain Keys Identified Mail
DLT	Distributed Ledger Technology
DNS	Domain Name System
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
DTLS	Datagram Transport Layer
ECC	Elliptic Curve Cryptography
ECU	Engine control unit
EPR	Electronic Patient Record
ETS	Emissions Trading System
ETSI	The European Telecommunications Standards Institute
FTTX	Fiber to the X
HF	High Frequency
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ICS	Industrial Control System application
IDS	Intrusion Detection System
IEC	The International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEFT	Internet Engineering Task Force
IMAP4	Internet Message Access Protocol 4

IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
Ipsec	Internet Protocol security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISM	Industrial, Scientific and Medical
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU	International Telecommunications Union
KSI	Keyless Signature Infrastructure
LF	Low Frequency
LIN	Local Interconnect Network
LLN	Low-Power and Lossy Networks
M2M	Machine-to-Machine
MAC	Structured Query Language
MAN	Metropolitan Area Network
MIT	Massachusetts Institute of Technology
MITM	Man in the middle atttack
MOST	Media Oriented Systems Transport
MPDU	MAC Protocol Data Unit
MQTT	Message Queue Telemetry Transport
MQTT-SN	Message Queue Telemetry Transport-Sensor Network
NFC	Near Field Communication
NRS	Narrowband Reference Signal
OASIS	Advancing Open Standards for the Information Society
OMA	Open Mobile Alliance
OTA	Over-The-Air
OVN	Open Vote Network
P2P	Point to point
PaaS	Platform as a Service
PAN	Personal Area Network
POP3	Post Office Protocol 3
PoW	Proof of work
PUF	Physical Unclonable Function
QR	Quick Response code
REST	Representational state transfer
RF	Radio frequency
RFID	Radio-frequency identification
RSA	Rivest, Shamir y Adleman
RTS	Request To Send
SaaS	Software as a Service
SDN	Software Defined Networking
SMC	Secure multi-party computation
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol

SPF	Sender Policy Framework
SQL	Structured Query Language
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TTA	Telecommunications Technology Association
TTS	Text-To-Speech
UDP	User Datagram Protocol
UHF	Ultra-High Frequency
USB	Universal Serial Bus
WPA2	Wi-Fi Protected Access 2
WSN	Wireless sensor networks
XML	eXtensible Markup Language
XMPP	Quick UDP Internet Connections
XMSS	eXtended Merkle Signature Scheme

11. Bibliography

[1] F. Mattern and C. Floerkemeier, " From the Internet of Computers to the Internet of Things", ACM Digital Library, From Active Data Management to Event-Based Systems and More,2010, http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf

[2] R. Minerva, A Biru, D. Rotondi, "Towards a definition of the Internet of Things (IoT)", IEEE Xplore Digital Library, 2015 https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[3] A. Shaddad Abdul-Qawy, P. P. J, E. Magesh, T. Srinivasulu "*The Internet of Things (IoT): An Overview", Directory of Open Access Journals,* International Journal of Engineering Research and Applications, V.5, N. 12*,* 12/2015

[4] E.Borgia, *"*The Internet of Things vision: Key features, applications and open issues*",*ScienceDirect,Computer Communications, 10/2014, http://0-www.sciencedirect.com.cataleg.uoc.edu/science/article/pii/S0140366414003168,

[5] J. Holdowsky M. Mahto Michael E. Raynor M. Cotteleer, *"Inside the Internet of Things"* , Deloitte University Press,2015 *https://dupress.deloitte.com/content/dam/dup-us-en/articles/iot-primer-iot-technologies-applications/DUP_1102_InsideTheInternetOfThings.pdf "Inside the Internet of Things"*

[6] D.Mendez, I. Papapanagiotou, B Yang, "Internet of Things: Survey on Security and Privacy", Cornell University Library, 2017, https://arxiv.org/abs/1707.01879

[7] G. Xu, Y.Ding, J. Zhao, L. Hu, X. Fu, "Research on the Internet of Things (IoT)" ProQuest, Sensors & Transducers, Volume 160, Number 12, 12/2013

[8] J. Gubbi, R. Buyya, S.Marusic, M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Science Direct, Future Generation Computer Systems, Volume 29, Issue 7, 2013

[9] *URL* , The TCP/IP protocol, "http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/TCPIPTutorial.pdf ", 5/10/17

[10] *URL*, C. Hoffman, What's the Difference Between TCP and UDP? https://www.howtogeek.com/190014/htg-explains-what-is-the-difference-between-tcp-and-udp/ 8/10/17

[11] *URL*, F.Azzola, IoT protocols behind the next technological revolution https://www.survivingwithandroid.com/2016/08/iot-protocols-list.html 11/10/17

[12] *URL,* Solace, Understanding IoT Protocols – Matching your Requirements to the Right Option, https://solace.com/blog/use-cases/understanding-iot-protocols-matching-requirements-right-option, 11/10/17

[13] S. Cirani, L. Davoli, G. Ferrari, " A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things" IEEE Xplore Digital Library, IEEE Internet of Things Journal, 2014, Volume 1, Number 5
http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/6899579

[14] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Directory of Open Acces Journals , Journal of Electrical and Computer Engineering, 2017, Volume 2017
https://doaj.org/article/5725fd54c29f46e48bd5365d18e22285

[15] T. Salman, "Networking Protocols and Standards for Internet of Things", 2016, https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot.pdf

[16] J. Granjal, E. Monteiro, J. Sá Silva, " Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Xplore Digital Library, IEEE Communications Surveys & Tutorials, 2015, Volume 17, Number 3, http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/7005393

[17] A.Rehman, S. Ur Rehman2, I. Uddin Khan, M. Moiz and S. Hasan, " Security and Privacy Issues in IoT ", ProQuest, International Journal of Communication Networks and Information Security, 12/2016, Volume 8, Number 3,
https://search.proquest.com/docview/1852722486?pq-origsite=summon&accountid=15299

[18] *URL* InetServicesCloud,The Four Internet of Things connectivity models explained http://www.inetservicescloud.com/the-four-internet-of-things-connectivity-models-explained/, 14/10/17

[19] *URL* The Internet of Things, http://netlab.csie.ntut.edu.tw/seminar/year2011/99598001_20111130.pdf, 14/10/17

[20] K. Bernard Rwanshane, "STRUCTURE OF TYPICAL IOT SETUP", Oulu University of Applied Sciences, 2016,http://www.theseus.fi/bitstream/handle/10024/119418/katunzi_bernard.pdf;jsessionid=CC866E70DC2FC96EE5DF6F4D6228F36D?sequence=1

[21] Suchitra C., Vandana C., "Internet of Things and Security Issues", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.1, January-2016, http://www.ijcsmc.com/docs/papers/January2016/V5I1201636.pdf

[22] E. Vasilomanolakis ,J. Daubert, M.Luthra," On the Security and Privacy of Internet of Things Architectures and Systems", ResearchGate, 2015 Conference: INTERNATIONAL WORKSHOP ON SECURE INTERNET OF THINGS (SIOT 2015), https://www.researchgate.net/publication/282075370_On_the_Security_and_Privacy_of_Internet_of_Things_Architectures_and_Systems

[23] Q. Jing, A.V. Vasilakos, J. Wan, J.Lu, D. Qiu, " Security of the Internet of Things: perspectives and challenges", SpringerLink, 2014, Wireless Networks, 11/2014, Volum 20, Número 8, https://0-link-springer-com.cataleg.uoc.edu/article/10.1007%2Fs11276-014-0761-7

[24] R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, " Internet of Things (IoT) Security:Current Status, Challenges and Prospective Measures", ResearchGate, 2016, https://www.researchgate.net/publication/307945826_Internet_of_Things_IoT_Security_Current_Status_Challenges_and_Countermeasures

[25] *URL*, S. Smiley,RFID insider, Active RFID vs Passive RFID: What's the Difference?, https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid 24/10/17

[26] A. Al-Fuqaha, "Internet of Things: A Survey of Enabling Technologies, Protocols, and Applications, IEEE Xplore Digital Library, IEEE Communications Surveys & Tutorials, 2015, Volume 17, Number 4,
http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/7123563/

[27] O.Said and M Masud, "Towards Internet of Things: Survey and Future Vision", 2013,http://cs.brown.edu/courses/cs227/papers/Towards_Internet_of_Things_Survey_and_Fu.pdf

[28] C. Maple, "Security and privacy in the internet of things", Journal of Cyber Policy, Volume 2, Issue 2: The Internet of Things, 2017 ,
http://www.tandfonline.com/doi/full/10.1080/23738871.2017.1366536

[29] W. Rui and W. Jinguo, "Analysis of key technologies in the Internet of things", ResearchGate, 2015 ,
http://download.atlantis-press.com/php/download_paper.php?id=25837790

[30] *URL,* IMPINJ, Types of RFID systems, https://www.impinj.com/about-rfid/types-of-rfid-systems/ 24/10/17

[31] *URL,* S.Smiley, Active RFID vs. Passive RFID: What's the difference?
https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid 24/10/17

[32] R. Want, Near Field Communication, IEEE Xplore Digital Libray,IEEE Pervasive Computing, 2011, Volume 10, Number 3,
http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/5958681/

[33] V. Sharma, "Near Field Communication",
2013, https://www.atlantis-press.com/php/download_paper.php?id=6331

[34] K. Curran, A. Millar, and C. Mc Garvey, “Near field communication,”, International Journal of Electrical and Computer Engineering (IJECE) Vol.2, No.3, June 2012,https://search.proquest.com/docview/1430775906?pq-origsite=summon&accountid=15299

[35] *URL,* M. Rouse, TechTarget Network,
http://searchmobilecomputing.techtarget.com/definition/Bluetooth, 11/11/17

[36] *URL,* Wikipedia, Bluetooth, https://en.wikipedia.org/wiki/Bluetooth 11/11/17

[37] E. Feroo, Bluetooth and WI-FI wireless protocols: A survey and a comparison, IEEE Xplore Digital Library, IEEE Wireless Communications, 2005, Volume 12, Number 1,
http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/1404569/

[38] *URL,* Rs components, IoT protocolos de comunicación
https://www.redeweb.com/ficheros/articulos/p62a65.pdf , 22/11/17

[39] *URL* Efor, Tecnologias de comunicación para IoT,
https://www.efor.es/sites/default/files/tecnologias-de-comunicacioon-para-iot.pdf
22/11/17

[40] *URL* Tutorialspoint,WiMAX-What is WiMAX
https://www.tutorialspoint.com/wimax/what_is_wimax.htm, 23/11/17

[41] *URL* SmartHome, What is Z-Wave?,https://www.smarthome.com/sc-what-is-zwave-home-automation 24/11/17

[42] A. Lewis, Cloud Computing , IEEE Xplore Digital Library, Computer, 2017, Volume 50, Number 5, http://0ieeexplore.ieee.org.cataleg.uoc.edu/document/7924250/

[43] *URL,* K.Bonsor and W. Fenlon, How Stuff workds, How RFID works, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid3.htm 24/11/17

[44] P.Rao, B. B, P. Saluja, "Cloud Computing for Internet of Things & Sensing Based Applications", IEEE Xplore Digital Library, 2012 Sixth International Conference on Sensing Technology (ICST), 2012
//0-ieeexplore.ieee.org.cataleg.uoc.edu/stamp/stamp.jsp?arnumber=6461705

[45] J.Harauz, "Data Security in the World of Cloud Computing", IEEE Xplore Digital Library, COPublished by the IEEE Computer and Reliability So, 2009 http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/5189563/

[46] *URL,* IoT analytics, The 10 most popular Internet of Thinhs applications right now, https://iot-analytics.com/10-internet-of-things-applications/ 24/11/17

[47] *URL* Bitcoinwiki, Satoshi Nakamoto, https://en.bitcoin.it/wiki/Satoshi_Nakamoto 25/11/17

[48] A. Bahga, V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things"Scientific Research, Vol.9 No.10, October 2016, https://www.scirp.org/Journal/PaperInformation.aspx?PaperID=71596

[49] J. Chen, "Flowchain: A Distributed Ledger Designed for Peer-to-Peer IoT Networks and Real-time Data Transactions", 2017, https://flowchain.co/Flowchain-WhitePaper.pdf

[50] M. Conoscenti, A. Vetrò, J. De Martin, "Peer to Peer for Privacy and Decentralization in the Internet of Things", IEEE Xplore Digital Library https://nexa.polito.it/nexacenterfiles/peer_to_peer_for_privacy_and_decentralization_in_iot.pdf , 2017

[51] D. Oana Firica, "BLOCKCHAIN TECHNOLOGY: PROMISES AND REALITIES OF THE YEAR 2017", ProQuest, Calitatea, 10/2017, Volume 18, Number S3, https://search.proquest.com/docview/1938536039?pq-origsite=summon&accountid=15299

[52] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A Margheri, and V. Sassone, "Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments", First Italian Conference on Cybersecurity (ITASEC17), Venice, Ita 2017, http://ceur-ws.org/Vol-1816/paper-15.pdf

[53] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, " Where Is Current Research on Blockchain Technology?A Systematic Review", Plos One, 2016, http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477

[54] G.Zyskind, O. Nathan, A. Sandy Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", IEEE Xplore Digital Library , Security and Privacy Workshops (SPW), 2015 IEEE, http://ieeexplore.ieee.org/document/7163223/

[55] S. Singh, "Blockchain: Future of financial and cyber security", Research Gate, 2016,https://www.researchgate.net/publication/316732822_Blockchain_Future_of_financial_and_cyber_security

[56] *URL* F. Zaninotto, The Blockchain explained to web developers, https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html 29/11/17

[57] *URL* Ethereum, https://www.ethereum.org/ether, 29/11/17

[58] T. Crain, V. Gramoliy, "(Leader/Randomization/Signature)-free Byzantine Consensus for Consortium Blockchains", Cornell University Library, 2017 https://arxiv.org/abs/1702.03068

[59] T. Tuan Anh Dinh, R. Liu, "Untangling Blockchain: A Data Processing View of Blockchain Systems", Cornell University Library, 2017 http://www.comp.nus.edu.sg/~ooibc/blockchainsurvey.pdf

[60] S. Popejoy, "Confidentiality in Private Blockchain", Kadena.io http://kadena.io/docs/Kadena-ConfidentialityWhitepaper-Aug2016.pdf 2016

[61] *URL* Coindesk, How Blockchain Technology works?, https://www.coindesk.com/information/how-does-blockchain-technology-work/, 29/11/17

[62] K. Christidis, "Blockchains and Smart Contracts for the Internet of Things" IEEE Xplore Digital Library, IEEE Access, 2016, Volume 4 http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/7467408/

[63] *URL,* B. Dickson, Crunch network https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/, 1/12/17

[64] *URL, N. Bauerle, Coindesk, What is the difference between BLockchain and a database?* https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database/, 1/12/17

[65] *URL,* P. Huminski,Business Insider, The technology behind bitcoin could revolutionize these 8 industries in the next few years, http://www.businessinsider.com/8-applications-of-blockchain-2017-7, 1/12/17

[66] B. Cresitello-Dittmar, "Application of the Blockchain For Authentication and Verification of Identity" , 2016
http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf

[67] B. Kewell R. Adams G. Parry, "Blockchain for good", Wiley Online Library, Volume 26, Issue 5, September 2017 P. 429-437,
http://onlinelibrary.wiley.com/doi/10.1002/jsc.2143/abstract, 2017

[68] K. Kim, T. Kang, "Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology", 2017,https://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Kim-Kang-blockchain-technology.pdf

[69] Dr. Kazi Zunnurhain,"Vulnerabilities with Internet of Things", 2016 http://worldcomp-proceedings.com/proc/p2016/SAM9719.pdf

[70] A.Mitrokotsa, M. R. Rieback, A. S. Tanenbaum, "Classification of RFID Attacks" , Springer Link, Information Systems Frontiers November 2010, Volume 12, Issue 5 pp 491-505, https://link.springer.com/article/10.1007/s10796-009-9210-z

[71] Q. Xiao, T. Gibbons and H.Lebrun, "RFID Technology, Security Vulnerabilities, and Countermeasures" ,Supply Chain, The Way to Flat Organisation, Book edited by: Yanfang Huo and Fu Jia, ISBN 978-953-7619-35-0, pp. 404, December 2008, I-Tech, Vienna, Austria, http://cdn.intechopen.com/pdfs/6177.pdf

[72] O.El Mouaatamid, M. Lahmer, M. Belkasmi, "Internet of Things Security: Layered classification of attacks and possible Countermeasures", Electronic Journal of Information Technology, 2016,www.revue-eti.net/index.php/eti/article/download/98/pdf

[73] *URL,* CR consumer reports, Tips: Three ways to protect yourself against card skimming,https://www.consumerreports.org/cro/news/2011/05/tips-three-ways-to-protect-yourself-against-card-skimming/index.htm**,** 4/12/17

[74] URL Wikipedia, Side-channel attack, https://en.wikipedia.org/wiki/Side-channel_attack, 3/12/17

[75] H. Gross, M Holbl, D Slamanig, and R. Spreitzer, " Privacy-Aware Authentication in the Internet of Things?",2015, https://eprint.iacr.org/2015/1110

[76] K.Xing , S. Sundhar Rajamadam , M.Rivera ,J. Li, X. Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey", 2005http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.363.8818&rep=rep1&type=pdf

[77] *URL* Incapsula, https://www.incapsula.com/ddos/attack-glossary/ping-icmp-flood.html, 3/12/117

[78] F. Shahzad, M. Pasha, A. Ahmad, "A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 12, December 2016 https://arxiv.org/ftp/arxiv/papers/1702/1702.07136.pdf

[79] *URL*, J. Reeds, Ivoryresearch.com ,A review of a Sybil attack in wireless sensor networks, https://www.ivoryresearch.com/writers/15429-2/, 8/12/17

[80] *URL* Eva Z., How secure is NFC technology?,http://rfid4u.com/how-secure-is-nfc-technology/, 6/12/17

[81] *URL* C. Kirsch, Ten phishing countermeasures to protect your organization, https://blog.rapid7.com/2015/09/11/phishing-countermeasures-to-protect-your-organization/, 6/12/17

[82] *URL* L.V.Oort, Tap Track, NFC relay attacks, https://www.taptrack.com/article/blog/nfc-relay-attacks/ , 4/12/17

[83] *URL,* G.Legg, EETimes, The Bluejacking, Bluesnarfing, Bluebugging Blues: Bluetooth Faces Perception of Vulnerability, https://www.eetimes.com/document.asp?doc_id=1275730, 8/12/17

[84] N. Be-Nazir, I. Minar and M.Tarique, "BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 https://pdfs.semanticscholar.org/8872/521819c79505ac20e5da8dd14f8c41eb3f07.pdf

[85] *URL,* A.Menon, SIMFORM, Common BLE security vulnerabilities in IoT and countermeasures,https://www.simform.com/ble-iot-security-vulnerability-countermeasures/, 8/12/17

[86] *URL,* D. Atow, The challenge of ensuring secure Wi-Fi http://www.techradar.com/news/the-challenge-of-ensuring-secure-wi-fi, 8/12/17

[87] T. Nguyen, "A survey of WiMAX security threats",2009 http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2.pdf

[88] D. Simion, M. Ursuleanu, A. Graur, " An Overview on WiMAX Security Weaknesses/Potential Solutions", 11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, May 17-19, 2012 http://www.dasconference.ro/cd2012/data/papers/B58.pdf

[89] *URL*, Walfram MathWorld, http://mathworld.wolfram.com/Diffie-HellmanProtocol.html, 7/12/17

[90] N.Vidgren, K. Haataja, J. Luis Patino-Andres, J. Jose Ramırez-Sanchis, P.Toivanen "Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned", IEEE Xplore Digital Libray, 2013 46th Hawaii International Conference on System Sciences, 2013 http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/6480466/

[91] O. Olawumi, K.Haataja, M. Asikainen, P.Toivanen, "Three Practical Attacks Against ZigBee Security: Attack Scenario Definitions, Practical Experiments ", Research Gate, Conference: Conference: IEEE 14th International Conference on Hybrid Intelligent Systems (HIS2014), At Kuwai http://ieeexplore.ieee.org/document/7086198/

[92] C. Badenhop , SR. Graham , B.W. Ramsey, B E. Mullins, L. O. Mailloux, "The Z-Wave routing protocol and its security implications", ScienceDirect , Computers & Security,Vol.68,July2017,http://www.sciencedirect.com/science/article/pii/S0167404817300792, 2017

[93] *URL* Wikipedia, Packet drop attack,https://en.wikipedia.org/wiki/Packet_drop_attack, 11/12/17

[94] E. Aras, G. Sankar Ramachandran, P. Lawrence and D. Hughes, "Exploring The Security Vulnerabilities of LoRa", ProQuest,IEEE International Conference on Cybernetics (CYBCONF 2017), https://lirias.kuleuven.be/bitstream/123456789/587540/1/camera_ready.pdf

[95] K. Zunnurhain, "Security Attacks and Solutions in Clouds", 2017, CiteSeerx, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.232.807

[97] C. Stergiou, K. E. Psannis, B. Kim, B.Gupta, "Secure integration of IoT and Cloud Computing", ScienceDirect,Future Generation Computer Systems vol. 78,part 3, January2018,http://0www.sciencedirect.com.cataleg.uoc.edu/science/article/pii/S0167739X1630694X

[98] J. Daubert, A. Wiesmaiera and P. Kikirasa, " A View on Privacy & Trust in IoT",IEEE Conference Publication 2015, https://www.informatik.tudarmstadt.de/fileadmin/user_upload/Group_TK/filesDownload/Published_Papers/joerg15privacytrust.pdf

[99] M. Abdur Razzaq, M. Ali Qureshi, S. Habib Gill, S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017 https://thesai.org/Downloads/Volume8No6/Paper_50-Security_Issues_in_the_Internet_of_Things.pdf

[100] H. Cho, "A study on IoT platform for Security", ProQuest,International Information Institute (Tokyo). Information, 03/2016, Volume 19, Num 3, https://search.proquest.com/docview/1786439237?pq-origsite=summon&accountid=15299

[101] A.Sanjab, W. Saad, I. Guvenc, A.Sarwat, S. Biswas, "Smart Grid Security: Threats, Challenges, and Solutions", Cornell University Library, https://arxiv.org/abs/1606.06992, 2016

[102] Dr. Florian von Baum, "Managing security, safety and privacy in Smart Factories", Based on a Panel Discussion during the Smart Factory Innovation Forum 2014 Held on September 25th, 2014 at TÜV SÜD AG, Munich, Germany

https://www.pinsentmasons.com/dokument/it-security-in-smart-factories-white-paper-april-2015.pdf

[103] G.Martin, P,Martin, C, Hankin, A.Darzi, J. Kinross, "Cybersecurity and healthcare: how safe are we?", ProQuest, British Medical Journal (Online); London Vol. 358, (Jul 6, 2017,https://search.proquest.com/docview/1916616077?pq-origsite=summon

[104] T. Zhang, Fellow, H. Antunes, and S. Aggarwal, " Defending Connected Vehicles Against Malware:Challenges and a Solution Framework", IEEE Xplore, EEE Internet of Things Journal, 2014, Vol 1, Num 1, http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/6720160/

[105] *URL,* H.Kirby, Supply Chain Cyber Attacks, https://www.linkedin.com/pulse/supply-chain-cyber-attacks-what-businesses-need-know-haydon-kirby, 9/12/17

[106] S. Radomirovic," Towards a Model for Security and Privacy in the Internet ofThings",IEEEXplore, 2015,http://www.caad.arch.ethz.ch/noolab/files/external/conferences/IoT2010_proceedings/pdf/WS1/WS1_9.%20seciot2010_submission_10_final_v0.pdf

[107] F. H. Alshammari, " An Efficient Approach for the Security Threats on Data Centers in IOT Environment", Article Published in International Journal of Advanced Computer Science and Applications(ijacsa), Volume 8 Issue 4, 2017. http://thesai.org/Downloads/Volume8No4/Paper_10-An_Efficient_Approach_for_the_Security_Threats.pdf

[108] Elike Hodo, X. Bellekens, A. Hamilton, P. Dubouilh," Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System", Cornell University Library, 2016, https://arxiv.org/abs/1704.02286

[109] D. Ralf Huuck, "IoT: The Internet of Threats and Static Program Analysis Defense" embeddedworld 2015 exhibition and conference, https://ts.data61.csiro.au/publications/nicta_full_text/8517.pdf

[110] *URL*, Red lizard Software, https://en.wikipedia.org/wiki/Red_Lizard_Software, 9/12/17

[111] K. Karolewicz, A. Beben, J. Mongay Batalla,G. Mastorakis and C. Mavromoustakis, "On efficient data storage service for IoT", Wiley Online Library , Vol 27, Issue 3 May/June 2017
,http://onlinelibrary.wiley.com/doi/10.1002/nem.1932/abstract

[112] M. O'Neill, "Insecurity by Design: Today's IoT Device Security Problem" , O'Neill, M. (2016). Insecurity by Design: Today's IoT Device Security Problem. Engineering, 2(1). DOI: 10.1016/J.ENG.2016.01.014
https://pure.qub.ac.uk/portal/files/135497683/Insecurity_by_Design_3A_Today_26rsquo_3Bs_IoT_Device_Security_Problem.pdf

[113] U. Chatterjee, R. Subhra Chajraborty and D. Mukhopadhyay, " A PUF-Based Secure Communication Protocol for IoT" ,ACM Transactions on Embedded Computing Systems (TECS)-Special Issue on Embedded Computing for IoT, Special Issue on Big Data and Regular Papers, Volume 16, Issue 3, 2017, Article No. 67,
https://dl.acm.org/citation.cfm?id=3005715

[114] X.Huang, P. Craig, H. Lin and Z. Yan, "SecIoT: a security framework for the Internet of Things", Security and communication networks, Wiley Online Library, 1 May 2015, http://onlinelibrary.wiley.com/doi/10.1002/sec.1259/abstract

[115] *URL,* Wikipedia, SQLite https://en.wikipedia.org/wiki/SQLite, 9/12/17

[116] C. Niu, K.Zou, Y. Ouyang, G. Tang and Y. Zou, "Security and Privacy Issues of the Internet of Things", ProQuest, Applied Mechanics and Materials, 09/2013, Volume 416-417, https://search.proquest.com/docview/1441882101?pq-origsite=summon&accountid=15299

[117] *URL, Wikipedia, Attack tree, https://en.wikipedia.org/wiki/Attack_tree*

[118] A.Sadeghi, C. Wachsmann, M. Waidner, "Security and Privacy Challenges in Industrial Internet of Things", IEEE Xplore Digital Library, Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE
https://pdfs.semanticscholar.org/474a/4a3d4be882f6a40fe655f4b9ec3cf7dc08e0.pdf,

[119] J.H. Serrano, J.L.Muñoz, A. Bröring, O. Esparza, L. Mikkelsen, W. Schwarzott and O.Leon "On the Road to Secure and Privacy-preserving IoT Ecosystems"

International Workshop on Interoperability and Open-Source Solutions
InterOSS-IoT 2016: Interoperability and Open-Source Solutions for the Internet of Things pp 107-122
http://www.arne-broering.de/inteross-iot-secpriv.pdf

[120] C.Cheng, R. Lu, A. Petzoldt and T. Takagi, IEEE Xplore Digital Library, Securing the Internet of Things in a Quantum World, IEEE Communications Magazine > Volume: 55 Issue: 2
http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/7842421/, 2017

[121] L. Marin, M. P. Pawlowski, A. Jara, Open access Sensors " Optimized ECC Implementation for Secure Communication between Heterogeneous IoT Devices ", MDPI,Sensors (Basel, Switzerland), 2015, Volume 15, Number 9 http://www.mdpi.com/1424-8220/15/9/21478

[122] X.Liu, M. Zhao, S. Li, F. Zhang, W. Trappe, "A Security Framework for the Internet of Things in the Future Internet Architecture" , ProQuest , 01/2017, Volume 9, Number 3 ,
https://search.proquest.com/docview/1952648277?pq-origsite=summon&accountid=15299

[123] P. Wang, "Privacy Preserving Techniques in the Internet of Things", ProQuest Applied Mechanics and Materials, 09/2013, Volume 427-429
https://search.proquest.com/docview/1443260078?pqorigsite=summon&accountid=15299,

[124] S. Tanaka, K. Fujishima, N. Momura, T. Ohashi, M. Tanaka, "IoT System Security Issues and Solution Approaches", Hitachi Review, 2016
http://www.hitachi.com/rev/archive/2016/r2016_08/111/index.html

[125] *URL* D.Bieler,M.Bennet, Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge,https://www.i-scoop.eu/internet-of-things-guide/blockchain-internet-things-big-benefits-expectations-challenges/ ,3/12/17

[126] *URL* B. Dickon, Tech Talks https://bdtechtalks.com/2016/06/09/the-benefits-and-challenges-of-using-blockchain-in-iot-development/ ,3/12/17

[127] *URL* Consultancy.uk, https://www.consultancy.uk/news/13484/blockchain-technology-how-it-works-main-advantages-and-challenges, 3/12/17

[128] *URL* S.Williams, 5 big advantages of Blockchain, and 1 reason to be very worried,https://www.fool.com/investing/2017/12/11/5-big-advantages-of-blockchain-and-1-reason-to-be.aspx, 3/12/17

[129] A. Dorri, S.S. Kanhere, R. Jurdak, " Towards an Optimized BlockChain for IoT ", ACM Digital Library,IoTD'17 Proceedings of the Second International Conference on Internet-of-Things Design and Implementation Pages 173-178, 2017, https://dl.acm.org/citation.cfm?id=3055003

[130] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things", Springer Link, Peer-To-Peer Networking and Applications, 07/2017, Volume 10, Number 4 https://0-link.springer.com.cataleg.uoc.edu/article/10.1007/s12083-016-0456-1

[131] Q.Xia, E.Boateng, A. Smahi, S. Amofa and X. Zhang, " BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments" MDPI, Information, 01/2017, Volume 8, Number 2, http://www.mdpi.com/2078-2489/8/2/44

[132] H. Shafagh, A. Hithnawi, "Towards Blockchain-based Auditable Storage and Sharing of IoT Data", Cornell University Library, https://arxiv.org/pdf/1705.08230.pdf, 2017

[133] B.Lee, J. Hyouk Lee, " Blockchain-based secure firmware updatefor embedded devices in an Internet of Things environment" Springer Link, Published online: 13 September 2016 © Springer Science Business Media New York 2016 https://0-link.springer.com.cataleg.uoc.edu/content/pdf/10.1007%2Fs11227-016-1870-0.pdf

[134] A.Ouaddah, A. A. Elkalam and A. A.O, " FairAccess: a new Blockchain-based access control framework for the Internet of Things", Wiley Online Library Volume 9, Issue 18 December 2016 Pages 5943–5964, http://onlinelibrary.wiley.com/doi/10.1002/sec.1748/full

[135] B. Rodrigues, "Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS)", Semantic Scholar, 2017 https://www.semanticscholar.org/paper/Enabling-a-Cooperative-Multi-domain-DDoS-Defense-b-Rodrigues-Bocek/7f81b5f319b0733d97a834ff90a4cd2006c991f3

[136] G.Zyskind, O.Nathan, A. Pentland," Enigma: Decentralized Computation Platform with Guaranteed Privacy", Cornell University Library, 2015 https://arxiv.org/abs/1506.03471

[137] *URL* Lightning Network, https://en.wikipedia.org/wiki/Lightning_Network, 14/12/17

[138] A. Outchakoucht, H. Es-Samaali, J.P. Leroy, "Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things", Research Gate, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No.7, 2017,

[139] *URL*, Benchmarking, https://en.wikipedia.org/wiki/Benchmarking, 14/12/17

[140] *URL*, Sunfish Project, http://www.sunfishproject.eu/tag/sunfish-project/, 9/12/17

[141] J. H. Park and J, H,Park, " Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions", MDPI, 2017, http://www.mdpi.com/2073-8994/9/8/164

[142] M. O'Dair and Z. Beaven, "The networked record industry: How blockchain technology could transform the record industry" Wiley Online Library, Volume 26, Issue 5 September 2017 Pages 471–480 http://onlinelibrary.wiley.com/doi/10.1002/jsc.2147/abstract, 2017

[143] T.Crain, V. Gramoli, M. Larrea, M. Raynal, "(Leader/Randomization/Signature)-free Byzantine Consensus for nConsortium Blockchains",2017, Cornell University Library, https://arxiv.org/abs/1702.03068

[144] M.A. Rasheed, "White Paper: Blockchain for Wearable Devices", ResearchGate, 2017,https://www.researchgate.net/publication/319130756_White_Paper_Blockchain_for_Wearable_Devices

[145] M.Ruta, F. Scioscia, S. Ieva, G. Capurso, E. D. Sciascio," Semantic Blockchain to Improve Scalability in the Internet of Things", Research Online Publishing, Open Journal of Internet of Things (OJIOT) Volume 3, Issue 1, 2017 https://www.ronpub.com/OJIOT_2017v3i1n05_Ruta.pdf

[146] *URL, Wikipedia, Service-oriented architecture, https://en.wikipedia.org/wiki/Service-oriented_architecture, 10/12/17*

[147] P.K.Sharma, S. Singh, Y.Jeong, J.H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks" IEEE Xplore Digital Library, IEEE Communications Magazine (Volume: 55, Issue: 9, 2017),http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/8030491/

[148] J.Sun, J. Yan, K.Z.K.Zhang, "Blockchain-based sharing services:What blockchain technology can contribute to smart cities", ResearchGate, Sun et al. Financial Innovation(2016),https://www.researchgate.net/publication/311589778_Blockchain-based_sharing_services_What_blockchain_technology_can_contribute_to_smart_citis

[149] P. Ghuli, U. P. Kumar, R. Shettar, " A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices", Research India Publications, Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2449-2456, https://www.ripublication.com/acst17/acstv10n8_22.pdf

[150] M.A. Walker, A. Dubey, A. Laszka and D. C. Schmidt, "PlaTIBART: a Platform for Transactive IoT Blockchain Applications with Repeatable Testing" , Cornell University Library, 2017, https://arxiv.org/abs/1709.09612

[151] Z.Shae, J.T.P. Tsai, " On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine, IEEE Xplore Digital Library, Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/7980138/

[152] S. Mustard, M. Davison, "Will blockchain technology disrupt the ICS world? ", ProQuest,2017,https://search.proquest.com/docview/1976419010?pq-origsite=summon&accountid=15299

[153] L. Cocco, A. Pinna and M. Marchesi, "Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology ",2017,SemanticScholar, ,https://www.semanticscholar.org/paper/Banking-on-Blockchain-Costs-Savings-Thanks-to-the-Cocco-Pinna/f322b14e92abcb30795b9a1c21175077066ff54e,

[154] R. Beck, M. Avital, M. Rossi, J. B. Thatcher, " Blockchain Technology in Business and Information Systems Research", Springer Link, Business & Information Systems Engineering December 2017, Volume 59, Issue 6, pp 381–384 https://link.springer.com/article/10.1007/s12599-017-0505-1, 2017

[155] Y.Lin, J. R. Petway, J. Anthony, H. Mukhtar, S. Liao, C. Chou, Y. Ho, " Blockchain: The Evolutionary Next Step for ICT E-Agriculture", MDPI, 2017http://www.mdpi.com/2076-3298/4/3/50

[156] G. Baxendale, "Can Blockchain revolutionise EPRs?", 2016 http://www.bcs.org/content/conWebDoc/55798

[157] T. F. Heston, "A Blockchain Solution to Gun Control", ProQuest, 2017,https://peerj.com/preprints/3407.pdf

[158] Y. Cai and D. Zhu, " Fraud detections for online businesses: a perspective from blockchain technology", Springer Link, Financial Innovation December 2016 https://link.springer.com/article/10.1186/s40854-016-0039-4

[159] M. Russo, " Why Is Blockchain A Great Career Option For IT Professionals?: The next big thing for job seekers", ProQuest, Talent Acquisition Excellence Essentials 2017,https://search.proquest.com/docview/1953021897?pq-origsite=summon&accountid=15299

[160] S.Yin, J. Bao, Y. Zhang, X Huang, " M2M Security Technology of CPS Based on Blockchains", MDPI, 2017, www.mdpi.com/2073-8994/9/9/193/pdf

[161] *URL*, Wikipedia, Cyber-physical system, https://en.wikipedia.org/wiki/Cyber-physical_system, 10/12/17

[162] B. V. Lier, "Can Cyber-Physical Systems reliably collaborate within a Blockchain", Wiley Online Library, Volume 48, Issue 5,October 2017 Pages 698–711

http://onlinelibrary.wiley.com/doi/10.1111/meta.12275/abstract

[163] W. Lehmacher, J. McWaters, "How Blockchain Can Restore Trust In Trade" ProQuest,2017,https://search.proquest.com/docview/1878303391?pq-origsite=summon&accountid=15299

[164] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, M. Kraft, " Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application", Science Direct, Applied Energy, Volum. 209, January 2018, P 8-19 https://www.sciencedirect.com/science/article/pii/S0306261917314915

[165] G. Wolfond, "A Blockchain Ecosystem for Digital Identity:Improving Service Delivery in Canada's Public and Private Sectors", Technology Innovation Management Review, October 2017 (Volume 7, Issue10)http://www.timreview.ca/sites/default/files/article_PDF/Wolfond_TIMReview_October2017.pdf

[166] P.McCorry, S. F. Shahandashti and F. Hao, " A Smart Contract for Boardroom Voting with Maximum Voter Privacy", 2017, https://eprint.iacr.org/2017/110.pdf

[167] *URL* Wikipedia,Open Vote Network, https://en.wikipedia.org/wiki/Open_vote_network, 15/12/17

[168] K. Korpela, "Digital Supply Chain Transformation toward Blockchain Integration", Research Gate, 2017 https://www.researchgate.net/publication/312218996_Digital_Supply_Chain_Transformation_toward_Blockchain_Integration