HELLENIC REPUBLIC
UNIVERSITY OF MACEDONIA
DEPARTMENT OF APPLIED INFORMATICS

DEMOCRITUS UNIVERSITY OF THRACE
FACULTY OF LAW

INTERDISCIPLINARY POSTGRADUATE PROGRAM

Master of Science in "LAW & INFORMATICS"

CYBERSECURITY IN INTERNET OF THINGS

Thesis of
Athanasios A. Kamaris

Thessaloniki, February 2023

CYBERSECURITY IN INTERNET OF THINGS

Athanasios A. Kamaris

B.Sc. in Informatics & Telecommunications
Faculty of Science, University of Athens, 2015

Bachelor's degree in Law Enforcement
Senior-officers' School, Hellenic Police Academy, 2004

M.Sc. Thesis
submitted as a partial fulfillment of the requirements for

THE DEGREE OF MASTER OF SCIENCE IN "LAW & INFORMATICS"

Supervisor:
Professor Konstantinos E. Psannis

Approved by examining board on …… …………………… 2023

Prof. Konstantinos Psannis	Prof. Maria Vlachopoulou	Prof. Christos Georgiadis
....	....	....

Athanasios A. Kamaris

Abstract

The Internet of Things (IoT), i.e. all Internet-connected devices that surrounding us, is estimated to exceed 25 billion by 2030. As the IoT now occupies a very wide area of our daily lives, security of these devices especially from cyberattacks is becoming a major issue. The research of this thesis will focus on the analysis of cybersecurity issues in the IoT, the threats and security vulnerabilities that arise, the proposed countermeasures and solutions from a cyber-technical point of view, through various cybersecurity frameworks, models and methodologies. After all, due to the extremely wide variety and way of implementation of the hardware and software that is each IoT device carries, it is not possible to establish a default security policy or a single solution for all IoT devices, but it is possible to mitigate and address effectively the majority of cybersecurity issues, by classifying them into categories, analyzing them, and implementing to the IoT ecosystem the necessary countermeasures accordingly.

Keywords and Key phrases

Internet of Things, IoT, IoT domain, IoT taxonomy, IoT asset, IoT architecture, IoT cybersecurity, IoT threat, IoT vulnerability, IoT cybersecurity measures, IoT security models.

Acknowledgements

A great thanks to my professor and to everyone who even indirectly supported me for this thesis. The completion of this study is dedicated to those who contributed me with their impediments and distractions.

Let every obstacle, be the cause and the motive for something greater in our lives…

Table of Contents

Index of Figures

Index of Tables

Acronyms – Abbreviations

AI	Artificial Intelligence
aka	as known as
BoT	Block of Things
CPU	Central Processing Unit
D2D	Device-to-Device
DDoS	Distributed Denial of Service
DL	Deep Learning
DoS	Denial of Service
e.g.	exempli gratia *(latin)*, means “for example”
GPS	Global Positioning System
i.e.	id est *(latin)*, means “that is”, “in other words”
ICT	Information and Communications Technologies
IDS	Intrusion Detection System
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS	Information Systems
IT	Information Technologies
M2M	Machine-to-Machine
MitM	Man in the Middle
ML	Machine Learning
NFC	Near Field Communication
NIC	Network Interface Card
RAM	Random Access Memory
RFID	Radio Frequency Identification
RoT	Root of Trust
SCADA	Supervisory Control and Data Acquisition
SQL	Scripted Query Language
UPnP	Universal Plug-and-Play
WSN	Wireless Sensor Network

1 st Chapter: Introduction

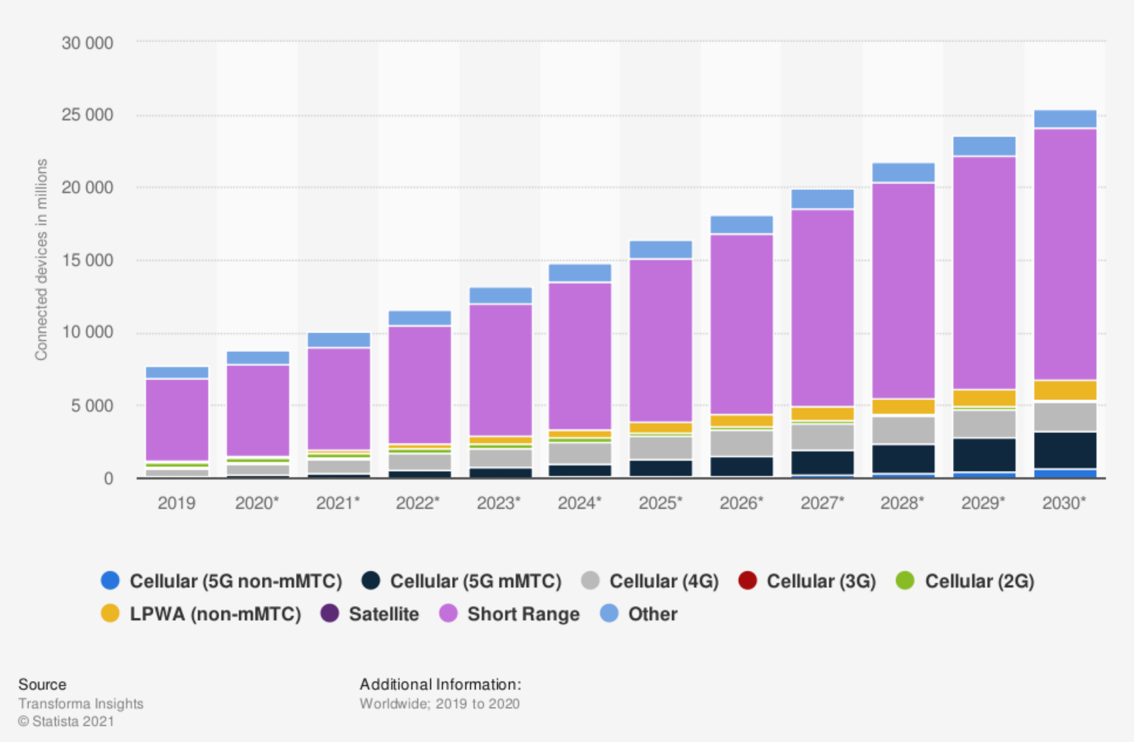
1.1 Issue - Severity - Motivation

In today everyone's life everyday objects that surrounding us, the "*things*", from watches and cameras to home appliances and cars are becoming smarter, more intelligent, interconnected and more interactive both with us and the environment, constructing entire new application areas like Smart Homes, Smart Cars, Smart Public Transportation, Smart Buildings, Smart Hospitals, Smart Airports, Smart Cities, Smart Grids, etc. and all of them form the Internet of Things (IoT) [1].

All these characteristics and the brand-new fascinating features of the "things" around us bring a "revolution" to how life is going to be in the following years, forming a picture that could only be found in science fiction novels and movies.

According to a survey conducted in December 2020 [2] and is shown on **Figure 1-1**, the IoT connected devices across the world on 2019 were 7.74 billion and this number was being forecasted to increase at 11.57 billion on year 2022 and exceed 25 billion by 2030, which is an increase of almost 3 times more connected IoT devices in a decade. By the end of year 2022, though, it was estimated that the online IoT devices were 13.1 billion, a number that exceeded the forecasts. Of course, there are much more installed but not connected directly to the Internet, IoT devices, sensors and actuators, having a total number of almost 42.62 billion [3].

These new interactive features of the "things" make them more invasive to many aspects of our daily lives, due to the colossal amount of information they collect to perform their ultimate purpose of existence, which is not other than to serve us, each one in its way, like from security, convenience, companionship, health, etc. point of view. Further to that, these smart "things" are getting more and more in numbers and are being spread and implemented almost everywhere, in a way that we are not any more being able not to interact with them even if we try hard to avoid them.



Source
Transforma Insights
© Statista 2021

Figure 1-1: The worldwide growth of connected devices through the Internet of Things from 2019 to 2030(*estimation) classified by their communication technology. [2]

Keeping these in mind is quite obvious that despite the huge advantages these "things" provide us, they also track us and affect our lives. While the wide spread of "things" and the information they collect is necessary for the features they offer, misuse of this information and bad-actors' compromise and control of them will have devastating results to our personal lives and ultimately to society. It is needed just one compromised "thing" by a bad actor, and personal information, from a smart in-house security camera for example, can be leaked in the public Internet revealing sensitive personal data to third parties, or give unauthorized malicious access in an entire application area, e.g. a Smart Power Grid, and a whole city can be turned down into darkness for a couple of hours or even overload the power plants and disable them at all.

It is though becoming for us imperative to be protected from any kind of malicious use of the "things" and while these "things" are being interconnected beyond local networks, the Internet is the major source of any kind of malicious activity against the "things".

Thus, Cybersecurity in Internet of Things (IoT) has to be taken very seriously nowadays, as it is becoming a severe security issue against our personal lives and society in general, especially considering that the majority of the sectors which incorporate IoT are critical.

These fascinating, almost sci-fi, features of the IoT and how we will benefit the most from these without risking our prosperity or at least mitigating the risks arising, is the main motivation behind this study.

1.2 Objectives - Goals - Research contribution

This study endeavors both to identify the cybersecurity risks and issues in the IoT, by examining the various threats and vulnerabilities that arise in the IoT world, and accumulate the proposed, by various scholars and authorities, countermeasures and solutions to mitigate them, from a technical point of view and from the point of view of implementing security policies, through and various threat analysis, frameworks, models, methodologies, taxonomy, and classification.

The overall contribution of the research conducted, emphasizes more on cyber risks than the physical risks and aims on concentrating the existing knowledge in this topic, pivoting future researchers to continue from a single basis.

1.3 Study approach

This study was conducted in a four-step approach, by defining the matter at issue with its research objectives, conducting desktop research, analyzing other scholars' work, and producing the final document of the thesis after supervisor professor's validation.

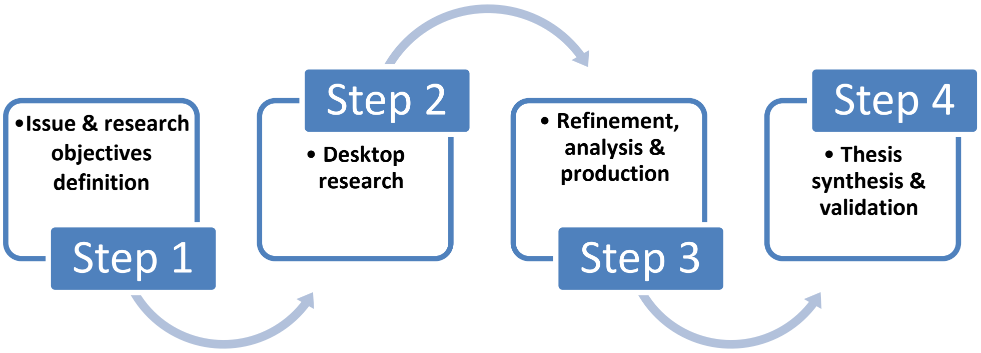

•Issue & research objectives definition
Step 1
Step 2
• Desktop research
• Refinement, analysis & production
Step 3
Step 4
• Thesis synthesis & validation

Figure 1-2: Methodology of this study

- ✓ **Issue & research objectives definition:**

  The matter at issue was defined giving an overall picture about the issue itself, the basic motivation behind the study and the research objectives and goals.

- ✓ **Desktop research** [4]; [5]; [6]**:**

  Existing research scholars' papers, journals, articles, surveys, conference proceedings, online data, various authorities' reports, and data regarding the matter at issue were searched in online scientific databases, relevant institutes and organizations.

- ✓ **Refinement, analysis & production:**

  The literature found to be relevant was more than a hundred (100) of sources, which were refined according to their content, based mainly on their title, abstract and skimming content; the remaining literature was studied, collated, analyzed, and summarized to produce the information needed for this study.

- ✓ **Thesis synthesis & validation:**

  At last, all the information and knowledge yielded from the research analysis was synthesized to this study, which was validated by the supervisor professor to produce the final document of this thesis.

1.4 Key terminology

The following terms will be used in this thesis, and a definition or short explanation for each one is being given:

Backend: In software development, frontend and backend terms describe the division of responsibilities between the user interface (frontend) and the data management (backend) portions of a software application [1].

[1] **Wikipedia** Frontend and backend [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Frontend_and_backend

Cloud: Cloud computing refers to the ability to access computing resources, particularly data storage and processing power, as needed without the need of physical infrastructure existence from the user side [2].

Credentials: In information systems, credentials refer to a user's identification information, typically consisting of a username and a password [3].

Deductive reasoning: Deductive reasoning involves making logical conclusions based on given premises. A deductive inference is considered valid when the conclusion inevitably follows from the premises, meaning that it is not possible for the premises to be true and the conclusion false [4].

Frontend: In software development, frontend and backend terms describe the division of responsibilities between the user interface (frontend) and the data management (backend) portions of a software application [5].

Gateway: A gateway is a networking device or software application used in telecommunication networks to facilitate data transfer between networks. It differs from routers or switches as it uses multiple protocols to link multiple networks and operates on any of the seven layers specified in the OSI (Open Systems Interconnection) model [6].

[2] **Wikipedia** Cloud computing [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Cloud_computing

[3] **Wikipedia** Credential [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Credential

[4] **Wikipedia** Deductive reasoning [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Deductive_reasoning

[5] **Wikipedia** Frontend and backend [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Frontend_and_backend

[6] **Wikipedia** Gateway (telecommunications) [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Gateway_(telecommunications)

Open source: Open source refers to publicly accessible source code that can be modified and distributed freely. Products under open source licensing usually come with the right to use the source code, design documents, and other content [7].

Router: A router is a device in computer networks' infrastructure that directs data packets between different networks, including the Internet [8].

Script kiddie: A script kiddie is an unskilled person who employs scripts or programs written by others, mostly for harmful purposes [9].

1.5 Thesis overview - Structure of document

After the introductory chapter, the study is overviewed as follows:

Chapter 2: Literature review.

The literature selected is being reviewed, after the overall refinement,

Chapter 3: The Internet of Things (IoT).

A light historical review is being made regarding the IoT and its origins, followed by the various IoT definitions and its added value to our lives. Further, the IoT is disassembled to its elements for analysis, and the heterogeneity is getting clearer to the reader. Lastly, the IoT application areas are being described briefly, and the multiple architecture approaches are overviewed.

Chapter 4: Cybersecurity issues in IoT.

Security challenges in IoT are being distinguished according to the different point of views and they are listed and briefly analyzed, taking into account the IS security principles and framework functions. The vulnerabilities that can be spotted to IoT ecosystem are also listed and explained thoroughly, followed by IoT asset taxonomy and categorization. Deriving from these, a listing, and a comprehensive approach of all the threats an IoT ecosystem could need to address is conducted,

[7] **Wikipedia** Open source [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Open_source

[8] **Wikipedia** Router (computing) [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Router_(computing)

[9] **Wikipedia** Script kiddie [Online]. - 01 20, 2023, https://en.wikipedia.org/wiki/Script_kiddie

crossmatching them with other aspects of IoT, in order to better prevent attacks or mitigate their impact.

Chapter 5: Security-issues' countermeasures in IoT.

The security approaches that can be applied to IoT environments are being described, and the one adopted in this thesis is explained. According to this approach the cybersecurity measures are listed, analyzed, classified and crossmatched with the threats that each one mitigates. As an extend to the security measures, various models that counteract to threats are introduced.

Chapter 6: Conclusion.

Conclusions, final thoughts and future work of this study.

Chapter 7: Bibliography – References.

The literature analyzed, used and referred to this study.

2 nd Chapter: Literature review

As introduced in the previous chapter, security in Internet of Things is a major issue that should be addressed effectively, but many drawbacks are being arised in the process.

Desktop research revealed that in the last years an exceptionally long list of documents, reports, articles, journals, papers, etc. has been published, various research have been conducted, scientific knowledge converged with experts' experience in the field, to address security issues in IoT in the most effective way.

In this thesis, the literature that has been selected, after thorough research and refinement, comes from official national or federal authorities, public and private institutes, and organizations, as long as from many individual researchers, plus the most up to date and latest scholars' work was reviewed and analyzed.

Specifically, the key-literature is overviewed in alphabetical order as follows:

- **Abdalla, et al. in 2020** [27] investigate the vulnerabilities of IP cameras as part of IoT and their effect on users' security and privacy.
- **Abdullah, et al. in 2018** [25] explore and identify universal architectural layers in IoT and discuss the security vulnerabilities and concerns in each layer.
- **Ahmed, et al. in 2020** [14] discuss the pros and cons of IoT, highlight architectural issues, vulnerabilities, future concerns about security and privacy, and underline probable measure could be employed IoT to strengthen the security of IoT.
- **Ali, et al. in 2019** [22] explain how privacy is being invaded or violated using insecure IoT devices, what information is yielded in attacks to IoT devices using machine and deep learning techniques, plus recommend solution approaches.
- **Anwar, et al. in 2020** [16] highlight a succinct overview of the security risks, difficulties, and attacks faced by the IoT and its associated applications.
- **Ayed, et al. in 2020** [17] discuss existing IoT attacks and propose Blockchain technology as a solution to IoT security problems aside with its weaknesses, introducing a specific blockchain-based solution called "Block of Things".
- **Bhagyashri A Bhandari, et al. in 2020** [11] provide an examination of security principles, technology-related challenges, and security difficulties, discuss the threats emerging by the concept of "IoT features" and the proposed counter measures to help the researcher to address the security issues for IoT layers.

- **Duangphasuk, et al. in 2020** [15] survey, analyze security problems in IoT in all IoT layers and recommend security solutions for each layer to counteract each type of attack, concluding that authentication is a crucial security property.
- **European Telecommunications Standards Institute (ETSI) 2019** [34] focuses on provisions that all parties, involved in the development and manufacturing of consumer IoT, should take into consideration, and apply respectively in order to secure their IoT products from cyber threats.
- **European Union Agency for Cybersecurity (ENISA) in 2019** [30] associates challenges and recommendations for Industry 4.0 cybersecurity issues with People, Processes and Technologies following an holistic and comprehensive approach.
- **European Union Agency for Cybersecurity (ENISA) in 2019** [7] fosters, after desktop research and experts' interview, cybersecurity in IoT systems and services in Software Development Life Cycle, a key area for applying security measures which can effectively and proactively avoid IoT vulnerabilities in application and services level.
- **European Union Agency for Network and Information Security (ENISA) in 2017** [1] outlines a comprehensive set of cybersecurity recommendations for the Internet of Things (IoT) with a specific emphasis on Critical Information Infrastructures, after desktop research and experts' interviews analysis. In this work IoT critical assets and relevant threats are also being mapped, possible attacks are assessed, and potential practices and measures for security enhancement are identified.
- **Fasila, et al. in 2020** [18] study existing techniques regarding security in IoT networks and conclude that security in IoT systems is strengthened when a blockchain assisted Distributed ABE cryptosystem is being applied.
- **Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) in 2020** [8] focuses mainly on security issues in IoT solutions observed in the field, providing best security practices in order developers to be aware of them and incorporate security measures into their development procedures.

- **IoT Security Foundation (IoTSF) in 2020** [31] released the IoT Security Compliance Framework in order to promote knowledge and best security practices to those parties who specify, make and use IoT products and systems. By following this framework, the stakeholders are guided through a structured process of questing and evidence gathering, ensuring this way that security mechanisms and practices are being implemented in IoT products and systems.
- **James in 2019** [28] identifies the three key cybersecurity aspects, Confidentiality, Authentication, Access control, and proposes via a systematic study an intrusion prevention system methodology for cybersecurity-based attacks at smart home IoT end devices.
- **Jung, et al. in 2020** [10] analyze the security requirements for Machine-to-Machine services, outlines the security necessities for Internet of Things (IoT) devices and presents a secure platform built on the ARM Platform Security Architecture which utilizes ARM TrustZone-based Root of Trust hardware, in order to overcome the development difficulties while embedding PSA security functions.
- **Khursheeed, et al. in 2020** [20] evaluate the review of previous studies on security of IoT other researchers carried out, by measuring the flaws in IoT security.
- **Malche, et al. in 2020** [26] present a study which deals with the two most crucial concerns in the IoT: authentication and authorization. They propose an IoT architecture where authentication process is based on asymmetric key cryptography (public-private security keys).
- **NSFOCUS Inc. in 2019** [32] enumerates the major IoT incidents in 2018 and focuses on the actual exposure of IoT assets on the Internet, aiming on revealing the overall security posture of these assets based on threat intelligence. Further, analyses the vulnerabilities and potential threat for UPnP protocol stack which is majorly used in IoT applications.
- **NSFOCUS Inc. in 2020** [33] enumerates the major IoT incidents in 2019 and updates the data from the previous security report in IoT landscape regarding actual exposure of IoT assets on IPv4 and IPv6 networks. Further, analyses IoT threat sources from the perspective of vulnerability and protocol exploitation, providing a protection solution for IoT devices.

- **Plageras, et al. in 2017** [37] focus on utilizing IoT, Cloud Computing, and Big Data to tackle healthcare sector issues and ensure the security of medical data by involving real-time data collection through wearable sensor devices and cloud server analysis.
- **Plageras, et al. in 2017** [38] discuss advancements in security and interconnectivity for Intelligent Buildings, presenting a patient monitoring system and BMS design with a comparative analysis of its benefits. The authors propose security solutions and use simulations to track network traffic in real time. Future work involves emulating the entire system for implementation.
- **Poonia, et al. in 2018** [19] emphasize the various security aspects and difficulties of systems utilizing the IoT and recommends prospective mitigation strategies from both a technical and management perspective.
- **Prakash, et al. in 2020** [9] propose mainly a security model for IoT and explains how this model can be implemented. The proposed model is considered to address quite effectively threats and attacks in an IoT network based on choosing and applying the most suitable, according to the IoT environment at issue, security algorithms and protocols for IoT security layers.
- **Rajmohan, et al. in 2020** [21] conducted a Systematic Mapping Study researching patterns and architectures for IoT security and privacy by analyzing relevant published papers from other scholars and researchers.
- **Ranjit Patnaik, et al. in 2019** [12] review and discuss various security techniques regarding IoT security and authentication, plus issues and challenges both with some probable solutions about the IoT environment.
- **Ray, et al. in 2020** [24] propose a security model for Smart Homes, featuring a cloud layer, a fog layer, a security application engine, and an interface between the fog and cloud layers with a firewall for enhanced security.
- **Sharma, et al. in 2020** [29] present a blockchain-based security analysis of data generated from IoT devices in order to prevent malicious attacks and intrusion in the IoT network.
- **Srivastava, et al. in 2020** [13] presents, analyzes, and compares various general and hybrid security enhancement techniques for IoT, based on other scholars' work.

- **Statista Inc. in 2020** [2] surveyed the number of IoT connected devices worldwide on 2019 and forecasted this number per year from 2020 to 2030, by communications technology.
- **Stergiou, et al. in 2018** [39] survey the integration of Mobile Cloud Computing and Internet of Things (IoT) with a focus on their security issues and examine the benefits of the integration and highlights the contribution of Cloud Computing to the function of IoT. The security challenges of the integration are also discussed.
- **Stergiou, et al. in 2018** [40] propose a new system for Cloud Computing integrated with Internet of Things to handle Big Data while addressing security and privacy issues, by introducing a security "wall" to eliminate these issues and make Cloud Computing more efficient. The study presents a survey of IoT and Cloud Computing with a focus on their security issues and the challenges of their integration, and aims to provide a more secure and "green" environment for sustainable computing.
- **Stergiou, et al. in 2019** [36] explore the integration of Cloud Computing (CC) and Internet of Things (IoT) technologies with a focus on security issues when handling Big Data, by examining the benefits of combining CC and IoT to ensure secure transmission of Big Data and presenting how CC can improve IoT's operation as a base technology for Big Data systems.
- **Stergiou, et al. in 2021** [41] propose a secure infrastructure for big data management in smart buildings using a 6G wireless network, by combining IoT, cloud computing, and edge computing to create a smart and secure environment. A novel cache decision system (CDS) is also proposed with a cloud and an edge server, providing a safer and efficient environment for data sharing and management, and the proposed solution with related cache scenario systems is compared.
- **Stergiou, et al. in 2023** [42] explore the integration of Cloud Computing and Big Data exported from IoT to achieve a sustainable Digital Twin scenario, by focusing on security and management challenges and proposing a novel security algorithm for the integrated system. The results show the potential of combining the two technologies for better privacy and security services.

- **Wheelus, et al. in 2020** [35] carry out analytics approach to review security risks associated with IoT systems and propose Machine Learning-based solution to characterize and detect IoT attacks.
- **Wustrich, et al. in 2020** [23] propose an extensible IoT threat taxonomy based on the affected architectural IoT layers and the affected fundamental security principles.

3 rd Chapter: The Internet of Things (IoT)

3.1 What is IoT

In 1980's a private research University student at Carnegie Mellon in Pittsburgh, USA, applied a network connectivity feature to a vending machine in order the machine to be able to report its inventory remotely and provide to the users the status and temperature of the drinks at will. This was the first "thing" that was got connected to the network and the idea of the interconnected "things" was arised [17]. Years later, in 1999, Kevin Ashton of Procter and Gamble company introduced the term "Internet of Things" [16] where the "things" could get connected with and be remotely managed [17]. Of course, the notion "Internet" in the term "Internet of Things" implies the capability of being interconnected, and is being used as a generalization without explicitly declaring that each one thing is globally accessible through the Internet as we know it [1].

In the past decade, quite many definitions for the "Internet of Things" term were proposed by the researchers, specialists, and various entities, but there was no unique or fully acceptable definition by the scientific community [17].

Some recent definitions by researchers are:

- *"IoT can be defined as a systematic setup of interrelated computing devices, individuals, connected things, advanced machines, data, and information that are given through unique identification and capable to send information over a system without direct interfering of human"*, by Prakash, et al. (2020, p.771) [9].
- *"The Internet of things (IoT) is scenario, where the physical devices, vehicles (referred to as "connected devices" and "smart devices"), buildings, and other items (those items which don't consider as computer) embedded with internet connectivity, computational power, electronics boards, applications, power unit, sensors, actuators, and control system which enable these things to communicate, generate, collect, exchange and consume data without intervention or negligible intervention of human"*, by Ray, et al. (2020, p.218) [24].

where other definitions provided by technology entities are:

- IEEE Standards Association defines an IoT system as: *"a system of entities (including cyber-physical devices, information resources, and people) that exchange information and interact with the physical world by sensing, processing information, and actuating"*, as referred by Rajmohan, et al. (2020, p.138) [21].
- ENISA (2017, p.12) [1] defines the Internet of Things (IoT) as: *"a cyber-physical ecosystem of interconnected sensors and actuators, which enable decision making"*.

As inferred by the aforementioned definitions the common points are that IoT is a big collection of everyday devices and objects, plus humans and services, which are being connected together with multiple ways, wirelessly or not, using a variety of different protocols, enabling them to interchange information in form of digital data, and interact with people or each other autonomously without or at most with negligible human intervention, having a common objective in the application area they serve. To this extent, IoT is the computing evolution [1], and can be easily considered as the Future Internet [14].

The spectrum of IoT application areas is keep getting wider, as more and more "things" are added to each assortment of this ecosystem, having nowadays numerous domains such as agriculture, healthcare, transportation, manufacturing, logistics, robotics, energy production and distribution, smart cars, smart homes, smart cities, smart grids, wearables, and much much more. Therefore, it is being noticeable that the application areas are ranging from personal to enterprise environments, allowing human beings to interact with their surrounding environment in a holistic way, letting devices to become smarter and perform daily tasks for their convenience [11]. This "device intelligence" is leveraging the power of interconnectivity and computation, exploiting the existing networks and the known Internet [24] along with a continuous and real-time information feeding, decision making and dynamic adaption [1], making all the "things" a symbol of "free flow of information" [20].

Finally, it is worth noting that an IoT ecosystem, enumerating manifold smart devices, may exist and operate in a local or wider isolated environment, without connection to outer digital world [1].

3.2 Advantages of IoT

Owning to the cyber-physical systems that Internet of Things form, quite a few advantages for our lives are emerged.

Despite of many advantages can be enumerated taking into consideration the different aspects of applications, the most common which present importance are the following [11]; [14]:

- ✓ *Security*. The aspect of providing safety to infrastructures from houses to enterprise and public environments, is bundled with interconnected "things" such as cameras, sensors, alarm systems, door locks, etc.
- ✓ *Monitoring*. Except security, simple monitoring ability, such as temperature, humidity, audio, video, etc. of the "things' " surrounding environment is a major added value.
- ✓ *Automation and Control*. The ability to make automated decisions, acting accordingly and autonomously, based on the information they receive from their environment is another major advantage. To this, it is added the ability to be controlled, from a distant location, with no need of human presence in the field of action.
- ✓ *Real-time communication*. Communications between the environment and human beings becomes easy, immediate, accurate, and efficient, plus can be achieved from anywhere geographically. This communication is extended further between both the machines (M2M communication) resulting to much more faster decisions and actions, and humans making them virtually connected at all the time.
- ✓ *Cost-effectiveness*. In the business sector, the physical interventions for various operations, like logistics, asset tracking, inventory control, security, etc., have been lessened dramatically, by automating them, resulting to huge financial benefits.

Of course, as already stated, these are not exhaustively listed, and much more advantages can be included in the aforementioned list, depending on the point of view by which we inspect the IoT ecosystem and its impact to our society and everyday lives.

3.3 Elements of IoT

Decomposing the IoT to its core components, we can analyze a bit deeper which elements comprise an IoT ecosystem, from a “thing” itself to the infrastructure and its services, which is an excellent way to better verge on its bare functions and how physical to cyber world interaction is established.

A “thing” is any physical, but also any virtual, object having the ability to be integrated, be uniquely identified, and communicate in a network assortment of other similar or not objects [17]; [14].

The core function that baptizes an object to a “thing” is the capability of communicating [17], under the concept of information interchange both amongst them and with various services in the cloud [11].

In addition, the “things” may have multiple other capabilities and features, depending on the nature of their function, some of the more common ones are sensing the physical world and actuating respectively in real-time functions [25], capturing, storing, processing and analyzing data capabilities, and many more [1].

The key building block elements of the “***things***” are the *sensors* and the *actuators* [1].

The ***sensors*** are integral hardware, which serve as input to IoT systems, and they can produce information in the form of data from the physical world in one hand, where data is generated by physical, biological, or chemical stimuli, and in the other hand from the digital world such as the network and applications. These data then are being processed immediately or being stored for future use. The basic use for sensors is to monitor their environment, so the most widespread sensors measure ambient conditions like temperature, humidity, light, acceleration, proximity, pressure, sound, rain, wind, motion, amongst many other factors.

On the contrary, ***actuators*** can be considered as the reverse mechanism of a sensor, serving as output to an IoT system. It transforms electrical data to action in the physical or digital world. Actuators may vary according to their operation, and they are responsible for physical movements of a system, for controlling a physical mechanism, for regulating brightness or temperature, etc.

Further to these basic building blocks of the “things”, there is also additional ***fundamental hardware*** that they consist of [20] in order to be functional. This hardware reflects to the usual components of a modern computer-based hardware, such as a microprocessor, volatile memory banks, storage units, power supply, integrated circuits and microcontrollers depending on the function needed in addition, physical ports, networking modules, etc..

The latter, networking modules, make use of plethora ***communication protocols*** and technologies, with the Wi-Fi, Bluetooth/Bluetooth Low Energy (BLE), ZigBee, Near Field Communication (NFC), Radio Frequency Identification (RFID), and the less-known Z-wave, 6LoWPAN for ***short-range radio networks*** [1]; [16], and for ***long-range low-power wide area networks*** the cellular networks such as SigFox, NarrowBand-IoT, LTE-M, LoRaWAN, WiMAX, etc. [20]. Of course, both wireless and wired infrastructure can be used for IoT networking.

The technology used is being selected according to the needs and nature of the IoT ecosystems in particular, but quite often a combination of different communication protocols is implemented, using gateways for seamless interoperability amongst the network systems [1]. These combinations of various network protocols are depended by the type of communications that take place between the “things”, reported as machine-to-machine (M2M) or device-to-device communication (D2D) [29]; [16].

As all the wirelessly connected “things” of an IoT ecosystem together constitute a ***Wireless Sensor Network*** (WSN) [29], they are controlled and administered by smart systems obtaining the gathered by each “thing” ***information***.

This information, which comes in form of processible data, has three basic states:

- ***at rest***, a state when the information is stored in a long-term storage either in the cloud backend services or locally in the devices,
- ***in transit***, when the information travels through the network infrastructure between the IoT elements,
- ***in use***, when the information is being used, processed by a software, or an IoT element.

These states may be interchanging from one to another, having an ultimate purpose which is not other than intelligent decision-making.

Intelligent decision-making in the era of Internet of Things is a key-element in the IoT structure. Decision-making is something that human beings do every millisecond, by analyzing in their brains the information received from their sensory organs, i.e. eyes, ears, nose, tongue, skin, and acting accordingly by their moving organs, i.e. various muscles throughout the human body, like arms, legs, mouth, etc. producing movements, speech and more. These operations are, respectively, the input of information to the processing unit, the human brain, and the output of the processed and analyzed data, which are either just actions towards the environment or a new input feed for new processing cycles. These procedures lead us to make decisions regarding on how we react to specific environmental stimuli that come from the outside world.

Accordingly, an IoT ecosystem, especially whereas actuating is a core function of IoT equipment, has the ability to make its own autonomous decisions, called *intelligent decision-making* as in general it is a replica of the same human procedure. Intelligent decision-making, as conclusively derived, builds up foremostly from the available information. These decisions that IoT ecosystems should face up, may be as straightforward as a mechanism that crosses a limit, or as precocious as machine learning (ML) and deep learning (DL) techniques. Added to that, the output of decision-making will finally transform to some kind of an action and may be used as new input to the same ecosystem, exactly like humans do, as explained above. So, as the beating heart of an IoT ecosystem is the information itself, the need of information management techniques, such as ***data mining***, ***data processing*** and ***data analytics***, of the vast volume of collected and generated data is an important aspect that should be addressed effectively, in order to give meaningful value and produce exploitable results. The analysis and process of the input will take place, depending mostly on the "thing" and its computational power, either remotely, by delegating to another part of the ***IoT infrastructure***, such as another "thing", a ***gateway***, a ***router***, an ***aggregator***, a ***local IoT management device***, a ***fronted*** or ***backend application*** or ***service*** in the ***cloud***, etc. or locally by themselves [1].

The latter feature, the one of locally processing capability of the "things", turns them to something more than just simple input, like the sensors, or output, like the actuators, units. It is very common nowadays to find "things" that can sense, process, communicate and act themselves without the necessity of being online and connected to any backend service or other "things" continuously. For a "thing" to be a such, should have integrated hardware just like a computer does, even this hardware is a low-end one as in the most cases is. This hardware consists of a stand-alone mainly ***power supply*** and circuits such as a processing unit (CPU), memory banks, volatile (RAM) and non-volatile (EEPROM/Flash memory), networking interfaces (NICs), and of course the appropriate capability to run software plus the custom software itself. When a "thing" collates all these hardware and features, is called an ***Embedded System***, and these kinds of "things" are the majority that we use every day, like medical implants, smart watches, smart thermostats, smart web-cameras, smart light bulbs, smart switches, etc. [1]. Below, in **Figure 3-1**, there is a schematic illustration of a "thing" that is an Embedded System.

Of course, as it becomes noticeable by the aforementioned analysis, the elements of IoT are not just physical hardware and devices, but also ***software*** and services. Operating systems, firmware, applications, web-based frontends, backend applications and services, cloud infrastructure services, software for device and network management and usage, are significant to the IoT, as these elements bring to life all the hardware parts of the IoT ecosystem, making it to operate and be intelligent.

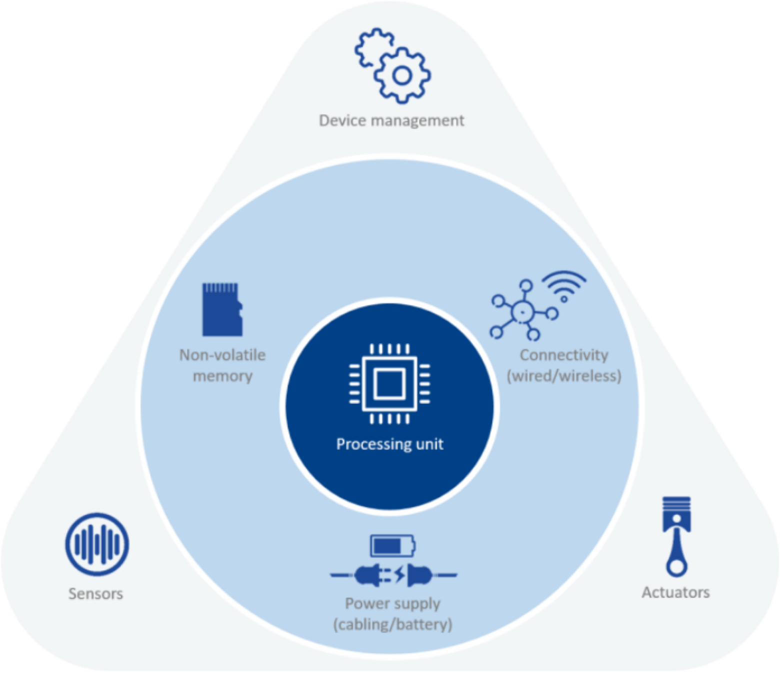


Figure 3-1: Schematic illustration of an IoT embedded system [1]

3.4 Diversity in IoT

Internet of Things is an ecosystem that by its nature counts an immense set of interconnected devices globally, having a huge variety of not only amongst the different purposes of their existence, e.g. smart homes, smart cars, smart wearables, etc., but also amongst the same types of each kind of devices, e.g. cameras, light bulbs, thermostats, etc.

Inspecting closer the IoT, the findings reveal a non-homogeneous ecosystem.

- The *hardware* a "thing" is equipped, integrates different architectures and vary according to its purpose of existence, the features that supports, the cost for its production and the target of consumers' group that is intended to be addressed, whether it is promoted as a cheap low-end smart device or an expensive featured smart device.
- The *communications* of a "thing" for exchanging information with local or distant resources, use different types of networking hardware and various networking protocols that have different capabilities in the domains of efficiency, quality of service, resilience, management, security, which they cannot by default cooperate and exchange information directly and safely.
- The *software* used by the "things" incorporates diverse operating code and applications, for its backend and frontend services, either proprietary or open-source or even custom-made, using services in the cloud from different manufacturers, not-promoting by default interoperability.

As this is the case in a close eye, each manufacturer produces and promotes its smart products while applying its policies and standards, especially in the security field, if any of course, leading to a very fragmented and immature environment.

This wide variety in many sectors in the IoT ecosystem, and the lack of international technical standardization and legal obligation towards the IoT-products' manufacturers, advances the complexity in the ecosystem, generates diversity and promotes heterogeneity in the global IoT environment [1]; [16].

3.5 IoT domains

Internet of Things, as already mentioned is a very wide global ecosystem. Though depending on the sector that the "things" are getting accumulated, various areas of IoT application are formed, the so called *IoT domains*, which due to their intelligence they implement are referred as "*smart*" environments.

In this extend of terms and notions, big IoT sectors are the *Smart Cars*, *Smart Transport*, *Smart Homes*, *Smart Cities*, *Smart Grid*, *Smart Health*, *Smart Supply Chain*, etc.

To understand a little better how IoT technology transforms a "dump" area to an intelligent one, a brief explanation is supplied as follows per IoT sector [16]; [19]:

Smart Cars: Cars nowadays make use of more and more intelligent systems and technologies providing numerous information services to the driver and entertainment services to the passengers. These services make use the information being collected by the outside environment of the car, being processed and used by the various system the car implements. Many, though, car's systems are getting linked to the internet for a better experience from all these services. Some smart-car-systems' examples are automatic ambient lightning and wipers, heads-up-display, various versions of parking assist, real-time traffic-based GPS navigation, automatic car accident assistance, etc.

Smart Transport: It is the evolution of the smart cars in conjunction with other smart domains. Intelligent transportation systems interconnect the smart cars together, with roadside infrastructure and also other means of transportation like buses and railways, providing real-time data exchange amongst them, purposing to automation, increased road safety, lesser traffic congestion lowering significantly the travelling time.

Smart Homes: In homes intelligent devices interacting each other as a unity providing many convenient features for their residents are quite usual than ever. Devices like refrigerators knowing when to automatically order the consumed products, robot vacuum cleaners, TVs, ambient light shutters, automatic locks, artificial lightning, and much more devices and services are integrated to houses, operating as a single interacting entity.

Smart Cities: Cities are comprising by many other smaller intelligent sectors. In a smart city, public transport means, roadside infrastructure, waste disposal facilities and services, urban lightning, buildings, interact each other as a living organism, providing safer and healthier environment, lesser energy footprint, and a better overall living quality for all of the residents.

Smart Grid: Electricity is one of the most important aspects of modern life. Electrical power, though, is being distributed from power plants to the end-users through power lines forming an enormous global power grid. Grids are extremely complex making use of a IoT devices, sensing and acting accordingly, in order the energy to be delivered efficiently and reliably to the grid users. IoT in power grids provide services to the grid, such as resilience to disasters, monitoring the systems and the consumptions, identifying and respond to the faults, etc.

Smart Health: Many people owe their lives to the IoT implementation in the health sector. All these microdevices, which certain group of patients implanted to their bodies, like heart pacemakers, are IoT devices. In the other hand, doctors can monitor, diagnose and even do surgeries remotely and/or with extreme precision providing instant medical services, whenever is required saving time and costs.

Smart Supply Chain: Supply chain is a particularly important domain as unobstructed and on-time delivery of the goods across the globe feeds everybody. Multiple IoT technologies, provide monitoring of the warehouse quantities, tracking the shipments, eliminating the necessary time needed to deliver the goods, etc.

Of course, the smart domains are not exhaustively listed here, as application areas can be theoretically infinite. The aforementioned domains thus, are the most common and important areas where IoT is already implemented in a quite aggressive way.

3.6 IoT Architectures

In order for IoT structure to be organized and efficient, its architecture is categorized to different layers, just like other technologies, networking for example, do.

Scholars and researchers, though, have not concluded to a specific number of layers this architecture consists of, so various layered approaches have been proposed by the scientific community, counting in their majority from *three* to *seven* layers.

The **three-layer** approach consists of the following layers [16]; [11]; [15]; [23]; [14]:

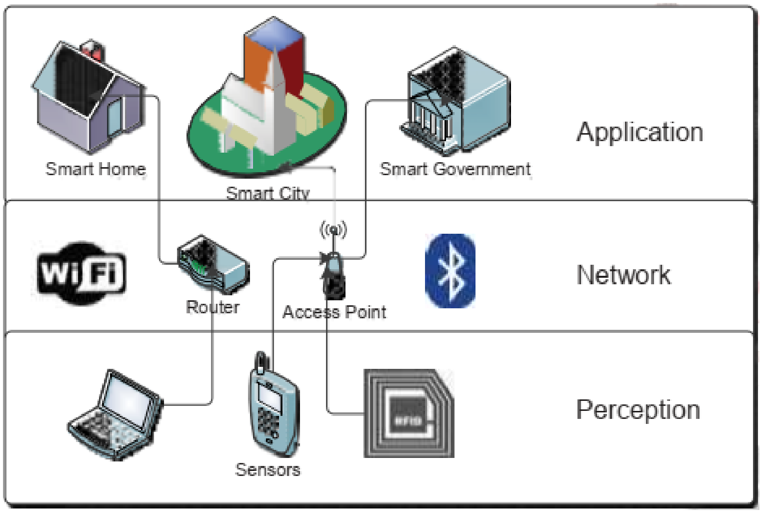


Figure 3-2: The 3 layers of IoT Architecture [11]

The *perception layer* or *cyber-physical layer* [23] or *sensor layer* [11] or *hardware layer* [16] is the lowest in hierarchy layer and consists of the sensors and actuators. The devices in this layer are generally limited in computational power and any kind of resources, performing simple actions without applying heavy algorithms and workflows. The basic feature of this layer is to acquire information from the environment and nearby objects, making use of sensing technologies, such as Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), Global Positioning System (GPS), etc. for collaboration with other “things” if needed, pass the information in form of data to the layers higher in the hierarchy to make decisions, and control objects and mechanisms based on these decisions as the data flows in reverse order down to this layer again.

The *network layer* or *middleware layer* [23] or *transmission layer* [15] is responsible for information flow between the lowest –*perception*– layer, and the highest –*application*– layer, reliably both ways, via data aggregation, filtering, transmitting and routing by applying the appropriate transportation and addressing techniques amongst the IoT ecosystem devices, and specifically the sensors, actuators, local IoT nodes, various switching, routing and Internet gateway devices, cloud computing platforms, using different communication wired and wireless technologies such as, Wi-Fi, ZigBee, Bluetooth, Radio Frequency Identification (RFID), Infrared, Z-wave, 6LoWPAN, SigFox, Near Field Communication (NFC), NarrowBand-IoT, LTE-M, Cellular 4G/5G, LoRaWAN, WiMAX, Optical Fiber (OC) and so on according to the needs and the implementation selected. Lastly, the *network layer* is also responsible for the seamless communication between different manufacturers making use of different or even conflicting networking protocols or technologies [23].

The *application layer* or *service layer* [15] is the last frontier between the devices and the end-users, having as its ultimate purpose to create the anticipated “smart” environment. It is responsible for establishing a connection between them, by providing services requested by them, presenting all the necessary information obtained from the lowest layer, the sensors, via the network layer in specific human-readable formatting for interaction and management. It is this layer’s responsibility to guarantee for Confidentiality, Integrity, and Authenticity of the aggregated data from the whole IoT ecosystem that it represents, by utilizing complex algorithms and workflows. To achieve these, it is equipped with plenty of resources, by far much more than the lowest level of sensors.

Being said these, it is worth to note that the aforementioned three layers are not always all implemented to every IoT device. This means that an IoT device may only be a part of the *perception* and *network layers*, a sensor for example, another may only be a part of the *network* and *application layers* due to the absence of the need for environmental interaction, having just the purpose for collecting data and making decisions. However, it is obvious that on both occasions the *network layer* is always a part of every IoT device, as the need of communicating is fundamental by definition in Internet of Things [23].

Given the fact that the three-layer approach is the most concise IoT architecture for the majority of the scientific community, adding more layers to the architecture particularize further specific areas of each of the three above-described layers or extending the basic approach to include more areas in higher or lower levels.

Therefore, the **four-layer** approach divides, in a way of speaking, the *application layer*; particularly a *management layer* is added between the *network* and *application layers*, so this architecture runs as follows [12]; [8]; [25]; [17]:

The *perception* or *sensor layer*, and the *network layer* are responsible for everything as in the three-layer approach.

Basically, the same is valid for the *application layer* except the various management procedures that take place before delivering the data to the end user for interaction. This is translated into that *application layer* in this architecture approach is responsible only for the end-user software, the web and mobile applications for example, and its backend services, such as data analytics in the highest level, API services, big data analytics, machine learning (ML) and artificial intelligence (AI) modelling, data processing and storage, etc. [8].

The intermediate *management* or *service management* or *middleware layer* has the job of autonomous device management in the concept of provisioning, monitoring, updating, controlling, applying security measures to the IoT devices.

Summing up, the hierarchy in this approach is in accordance with the next figure.

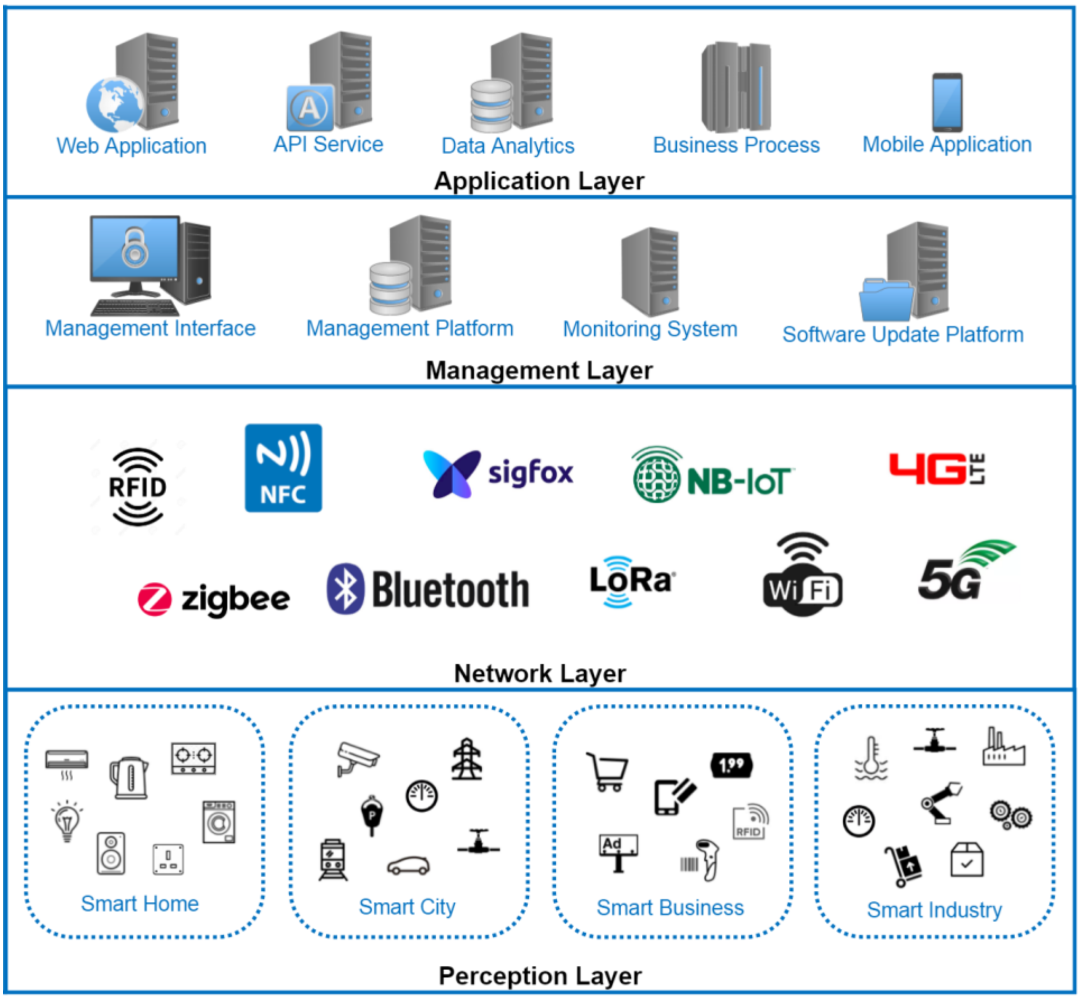


Figure 3-3: IoT 4-layered Architecture Model [8]

However, some scholars distinguish the responsibility of data processing, analytics and storage in the cloud, out of the *application layer*, as they accept to be a part of this *middleware/management layer*.

The **five-layer** approach is adding an extra layer above the four-layer hierarchy called the *business layer* [20]. This layer is out of the relatively close scope of a single IoT ecosystem, taking into account the bigger picture of the IoT environment a business may have. Such approach aggregates the application layers, managing and controlling this way the whole IoT system, including the manifold applications that may exist, business models, users' privacy, holistically, as a single one.

This hierarchy structure imprints to the figure comes next.

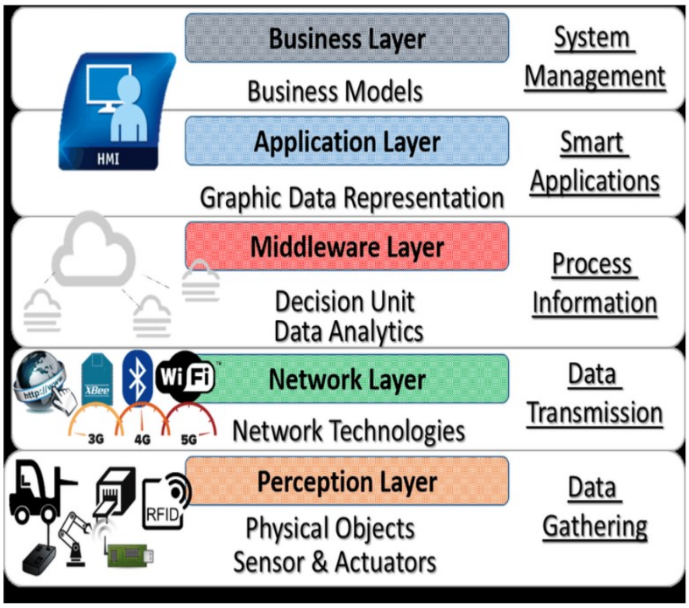


Figure 3-4: 5-layered IoT Architecture [20]

The **six-layer** approach is not very common but is noted as some researchers refer it. In this approach a lower level, below the *perception level* is included, named the *coding layer* [9].

The **seven-layer** approach is the last approach, and it is adopted not only by scholars but also from leading companies, like Cisco.

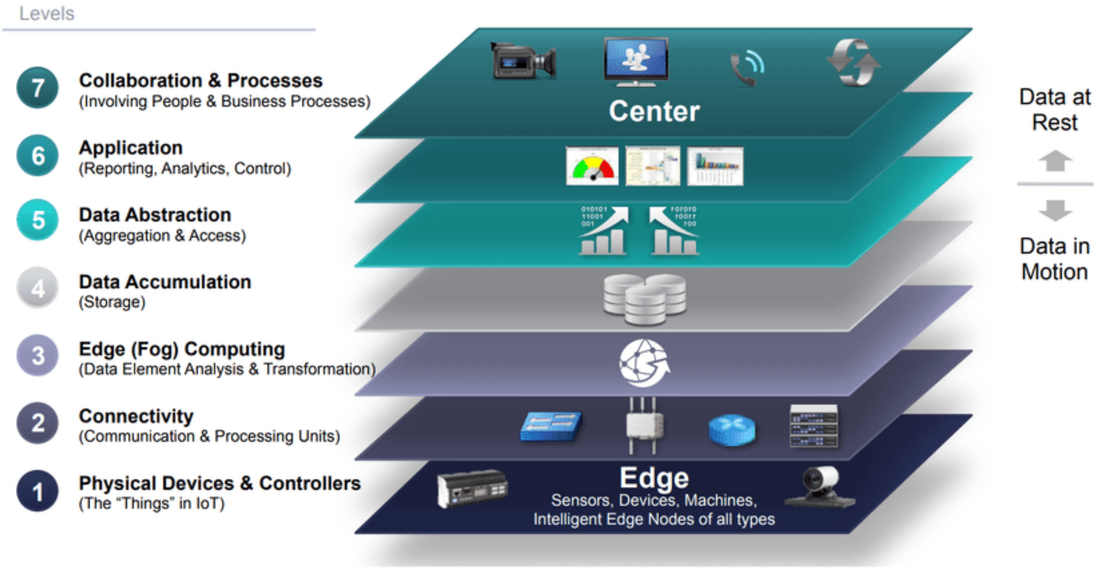

Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge (Fog) Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types
Data at Rest
Data in Motion

Figure 3-5: Cisco's 7-layered IoT reference model [43]

In this approach, the lowest layer, layer one, is the *physical devices and controllers' layer* or *edge layer*, which is the same with the *perception layer* of the other architecture approaches.

The next upper layer, layer two, is the *connectivity layer*, representing all the hardware and protocols that should be used to achieve connection and communication amongst IoT devices. In this layer, switching, routing, network level security is taking place to assure reliability in the data transportation, coupling the physical with the logical technologies.

Third, is the *edge/fog computing layer* where data handling, accompanied with end-to-end security mechanisms like encryption, is applied, plus other data processing functions, such as filtering, scrubbing, protocol conversion, low-latency decisions, etc., is done if needed.

The fourth layer, named *data accumulation* or *storage layer*, puts data from motion to rest. This happens by storing in long term storage units for optimization or querying. The main purpose of this layer is to serve as an intermediate of incoming to outgoing traffic of information.

The fifth layer is the *data abstraction layer*. Quality and completeness assurance functions are implemented in the procedure, such as data manipulating through aggregation, comparison and processing, resulting in more straightforward, performance-enhanced traffic for the next layer.

The *application layer* also exists in this architecture, forming the sixth layer, having the same semantics and functions as the other architectures explained thoroughly earlier.

Lastly, the seventh layer, known as *collaboration and processes layer*, can be compared to the *business layer* reported in the five-layered approach above. Specifically, in this layer human interaction takes place with the whole IoT system and all the lower layers generate value for the business.

Concluding, all the aforementioned IoT architecture approaches are almost the same examining every single layer from bottom up either they are more general and concise, or more particular and extensive. Of course, some architectures consider a more extended approach in order to include some aspects out of the hardcore scope of the fundamental three-layered architecture.

4 th Chapter: Cybersecurity issues in IoT

4.1 Security challenges in IoT

Internet of Things has considerably entered deep in our lives. Every item surrounding us, each device gains intelligence, becomes a "thing" and gets access to the networked systems, where data flow continually. Billions of "things" collect, manipulate, and transmit tremendous volume of information all over the internet, becoming at the same time target for adversaries and eventually the source of intrusion or interference to "closed" information systems, jeopardizing security of data, systems, privacy, etc. [1].

Therefore, security is the primary issue that should be addressed reliably and with maturity. Failure succeeding to do that, will lead users to drop trust to IoT devices and services, as data is compromised or devices malfunction especially in critical IoT infrastructures, and eventually will outweigh their benefits [21]. Of course, this is not as simple as it may sound, generating this way manifold security challenges regarding the use and implementation of IoT.

Security challenges in IoT are not something new. Many of them are inherited from networking technologies, though new challenges have arised by the new features that IoT apply, and while considering the rapid expansion of the "things" in the world the risks are getting multiplied exponentially.

Having this in mind, these security challenges can be divided in two main categories, the one from the *technological* point-of-view, and the other from the *cybersecurity* point-of-view [11].

The *technological* challenges arise because of the same nature of IoT ecosystem which is characterized by heterogeneity and ubiquity.

In the other hand, *cybersecurity* challenges come from the principles that should be obligated to apply in order to strengthen the security of the IoT network.

The three security principles *Confidentiality*, *Integrity*, and *Authenticity*, known as the "***CIA triad***", is applied in any information management system. Further to these three security principles, the security framework that controls access to information system (IS) resources and is combined closely with IS cybersecurity, is mostly known as the "***AAA security framework***", which stands for *Authentication*, *Authorization*, *Accounting*. So, the IoT infrastructure, as it is an Information System, is not an exception and is covered under the umbrella of the aforementioned principles and security framework functions [23].

Explaining in a concise and laconic way each principle in CIA triad and security function in AAA framework, the definitions have as follows:

- ✓ *Confidentiality*: Is fulfilled when the information is disclosed only to entities that have the appropriate authority to access it.
- ✓ *Integrity*: Is fulfilled when the information is maintained to a known state without any kind of modifications, by unauthorized entities.
- ✓ *Availability*: Is fulfilled when the information is always available when requested.
- ✓ *Authentication*: Is the function that verifies whether an entity is the one which claims to be. The function assures trustworthiness making use of identities, such as credentialing.
- ✓ *Authorization*: Is the function that controls whether an entity has the proper rights to access the information or the resources requested. The function assures proper level of trustworthiness making use of access lists.
- ✓ *Accounting*: Is the function that tracks the audit trails of actions, removing the option of plausible deniability for the entities.

At this point, it is worth mentioning that except the CIA triad, some scholars proposed an extension to the security principles, which is known as "***IAS octave***" [15]; [35]. The IAS octave, which stands for *Information Assurance and Security octave*, supplements the CIA triad, in a manner of speaking as the AAA security framework does, being different to the concepts of *Authentication* and *Authorization*, which are changed to one concept of *"Trustworthiness"*, the concept of *"Accountability"*, which is the same as the *Accounting*, to the concepts of *"Auditability"*, *"Privacy"* and *"Non-repudiation"*, which are being added:

- ➢ The concept of *Auditability* is the ability of a system to monitor and verify all actions taking places in it.
- ➢ The concept of *Privacy* ensures that the information is managed only by these entities that have the authority to do so.
- ➢ The concept of *Non-repudiation* is the ability of a system to ensure that no one can deny an action that had already took place.

Though, the IAS octave and its concepts will not be considered further in this thesis.

So, the key-security challenges in IoT are data manipulation in such way that CIA triad and AAA security framework are fulfilled for the point-of-views mentioned before, thus both *technological* and *cybersecurity*. Deriving from this, the key-security challenges could be broken down particularly to the following [20]; [9]; [25]; [16]; [22]; [1].

- *Data integrity*: there is a need for correct, consistent, and complete data to the whole IoT ecosystem, guaranteeing that information is not altered or lost from exogenous factors.
- *Data confidentiality*: the secrecy of information that flows or gets stored to the system from prying eyes, is almost unified with security itself, as there is an ultimate need for non-disclosure to the wrong recipients.
- *Privacy issues*: evaluating the deep penetration of IoT devices in everybody's life and collecting extremely huge amounts of sensitive, mainly, information about individuals, it is a major issue on how this information is manipulated into the system, as any leak comprises a severe danger to people even in the physical world.
- *Data availability*; as the flow of information is extremely important for the IoT ecosystem to be operational, any issue to the accessibility to this information would be devastating for the entire IoT network.
- *Authorization* and *authentication*: effective access control in the IoT ecosystem both externally, from the users or third-party entities, and internally, between the nodes of the same ecosystem themselves, is very important in order to be determined whether a resource can be acquired by the requesting party, and access be granted accordingly at the right level of clearance.
- *Communication security*: data transmission over the network, especially when this refers to Internet transmission e.g. the cloud, where other local security measures are absent, is a paramount challenge as the information flows down the road to the destination by its own and anyone can intercept it with malicious intents.
- *Common framework*: The lack of unified principles, guidelines, policies, laws, standardization for the IoT has bad impact to the homogeneity,

interoperability, and security, as every manufacturer follows its practices according to their maturity, convenience, benefit, profit, ethics, etc. both in hardware and software implementation in their IoT devices.

- *Security updates and patches*: the ability of every IoT device manufacturer to address vulnerabilities that have been detected through software patching by producing firmware updates, but also the immediate way to deploy them rapidly is another major issue that compromises the security.

4.2 IoT Vulnerabilities

The term "vulnerability" is defined as a hole in a systemic asset that someone could exploit for his advantage. This hole is a backdoor, a way, an entrance, for entering somewhere without having the legal rights to do it and in many cases without the owner's knowledge that this is possible to happen. This action is better described as invasion or intrusion to assets, gaining access to victim's systems, either hardware or software or even procedures. In other words, if vulnerabilities would not exist, no system would be in danger and no security measures would have to be taken.

In today's digitized environment where intelligent devices have been occupying in a cataclysmic manner our physical world, and individuals and objects interact with each other more and more, an entire new field of play for cybercriminals has been unfolding ahead.

Unfortunately, cybercriminals are seeking constantly and with great meticulousness the gaps that manufacturers or developers left unintentionally in their products, or even the mistakes in the adopted procedures regarding the security of their products, which both can expose open doors to enter easily in that product and gain full access not only to the product itself but also to the entire hosting ecosystem. The bad actors need just a single vulnerability to exploit, and they are able to intrude illegally and perform their malicious intends, affecting adversely the compromised system and all the interconnected devices.

Obviously, the aforementioned term of "devices" can interchangeably be used with the term "things" when the vulnerabilities are examined in the scope of Internet of Things.

Examining these vulnerabilities, it is important to pay attention to the collegiality of IoT, which means that the “things” in IoT cannot be approached solitarily but as an entity of consolidated singularities.

Various studies had been made by researchers to identify the root causes for exploiting IoT systems and confront the pitfalls of the IoT design. The studies revealed the generic and the more particular issues that lead to vulnerable spots [1]; [9]; [35].

By analyzing the latter, the most generic vulnerability is the ***extremely large attack surface***. Billions of “things” exist in the world, so malicious users have a vast space of victim-devices to extend their search and practice their penetrating skills, with increased odds to reveal multiple security gaps giving them the coveted unauthorized access.

In addition, the “things” are very tempting targets due to the gigantic volume of them ***spread widely in global scale***, characteristic that can lead in creating quite easy massive international armies of zombie device-soldiers to perpetrate further attacks. Furthermore, the mass deployment of the IoT in critical infrastructures gives many more reasons to attack them due to their value in our society, such as power grids, water supply networks, defense systems, airports, etc., having mostly huge impact to economies and to the effectiveness of the enemy parties in cases of warfare.

The IoT is rather a ***complex ecosystem*** than an homogenous one, involving heterogenous assets, such as individuals, devices, gateways, services, networks, all of these with diverse design, operation and implementation to the environment, and deployment inside the networked ecosystem, adding high-influence drawbacks in both IoT hardware and software, which consequently generate severe problems, affecting negatively the whole IoT map.

The “things” are everywhere, especially when they come in form of embedded systems, which are considered completely stand-alone, autonomous devices, being connected directly to the cloud via internet. It is very common such kind of devices to be found in harsh environments, adding to the vulnerability stack of severe problems to confront. So, contradicting the traditional hardware equipment, which is generally located behind firewalls inside secure data centers having physical security, segregated access, and guards, quite many IoT devices are installed in remote unprotected places, without tamper-resistant packaging, being available for in-person tampering to assailants due to their ***weak physical security***.

Devices in Internet of Things are often very small in size in order to fit everywhere, they are also very dedicated-purpose, meaning that are manufactured for very specific tasks and have to be as much simple as necessary to be effective [35]. In addition, manufacturers produce them having in mind mostly the affordable cost for their consumers and their profit, consequently then "things" tend to have a lot of constraints both in their hardware and software.

Hardware limitations are always in the fore [10]; [20]. IoT products are usually not attached to the power grid, as they are often a kind of mobile devices, and its necessary electrical power comes from battery packs embedded in these devices. To this extend, the limited power availability has to be counterbalanced with low-power consumption components, such as low clock-rate CPUs and peripherals, limiting the processing power to levels that cannot support computationally costly algorithms for cryptographic services. Additionally, memory has its own limitations in the "things' " hardware. Since they are not equipped with roomy memory banks, capacity after subtracting their operating system's memory consumption cannot support simultaneously running software needing plenty of free volatile memory to utilize such as cryptographic algorithms, allowing just the main-purpose functions to operate. Extending the term "memory" it is also an issue to address the lack of abundant non-volatile memory which is usually referred to as storage. No matter what kind of storage type is available to these low-end devices, it is always a big issue that should be considered from its point-of-view, since their storage capacity would never compete the conventional information systems' capabilities in terms of storage availability to store locally huge quantities of data. This adverse phenomenon is getting more problematic when storage in such devices is not extensible somehow, either by adding more or replacing the existing memory, making these devices obsolete.

Another constraint is the, corresponding to hardware, ***software limitations*** [20]; [14]. There are various matters to address when it comes to software vulnerabilities, as gaps in the software development are manifold both from the side of the software itself, and from the procedures side that may or may not be followed with veneration. From a generic perspective the first drawback is the operating system of the IoT devices itself that comes in light, slim-line versions, in accordance with the available hardware slim-line resources, lacking significantly in security features and components. Aligning to this, it is worth mentioning the ***insufficient security configurability***, which limits the system to specific security settings and eventually becoming inadequate to protect sufficiently against the newly emerged threats.

Stepping forward and more particularly in the software limitations design, a lot of flaws can be identified while inspecting IoT systems. The IoT market is a booming economy, having lots of pressure in delivering products as soon as possible, not leaving time for beta testing or excessive software design techniques, while this poorly-written applications are imposing serious constraints in using security techniques or implementing privacy by design procedures, leaving products with ***insecure software***.

Moving a bit further from insecure programming, the ***lack in updates and security patches*** leave serious open holes in IoT devices that anyone can exploit. Even a novice script-kiddie, someone without deep knowledge in systems' penetration techniques, or in heavy various languages' programming, or in networks' functions and security, would be able take advantage of these open holes, which are serving as well-known backdoors to the global security community, and infiltrate to the system with ease just by following the already published guidelines for exploiting the outdated software. Such common paradigms are the running operating system itself or the web interfaces of devices functioning like the interacting frontend with users. However, updating and patching IoT devices from manufacturers' perspective is not a straightforward and easy task to accomplish even if updates and patches are developed, rather it is a very challenging one, due to poor updating mechanisms implemented by default in the products, the extremely wide range of involved products having significant differences into their code and the costly operations needed for these updating procedures.

In the concept of the insecure software, there are other services in the IoT ecosystem the end-devices use to fulfill their existence. These services can be found in the mobile frontends which are always a companion to the intelligent "things". Though, these end-user applications are another security flaw to the whole IoT design as they impose a super weak entry point for attackers, due to the full access to the device that has been always granted previously and possibly this fronted application can be considered as a single point of failure, whether multiple "things" are attached with full-access rights to that ***insecure mobile interface***.

In the same way, an attacker may achieve an unauthorized entry to ***insecure cloud services interface*** of an IoT ecosystem, hosting a huge number of "things", which is a severe vulnerability. Taking access of the cloud services by a bad actor can easily lead in losing not only single devices but also the control of the entire IoT network. The devastating consequences of course are extended further while all the information collected by the "things" are getting consolidated in this compromised cloud service, being available to the intruders.

The latter, reveals another vulnerability may exist in IoT ecosystems, regarding ***privacy concerns***. Unfortunately, many of the "things" collect more information than that they need, or in case that this further information is actually mandatory for some reasons, it is still not being protected properly in the event of data thefts or leaks anyhow.

Except hardware and software limitations of the "things", the ***network-based limitations*** can also be identified as a major source of vulnerabilities [9]; [20]; [14]. All the "things" fundamentally have to be connected to each other and to the entire IoT ecosystem, in order to operate and provide their added-value. This connectivity is mandatory but is accompanied with several risks due to the vulnerability of the networks. The flow of data between the devices are as much secure as the network link is. Whether the link is compromised, the whole system is at stake. The lack of ***transport encryption and integrity verification*** amongst the IoT nodes, which means that data is in human-readable format during their transmission, and no checks for altering them is applied, intensifies the risk of data compromise especially when ***insufficient authentication or authorization*** credentialling is applied both to the end-nodes and to the intermediate network devices. Of course, the risk increases when the medium utilized for networking is not wired, but wireless, which is easier to scan and retrieve the flowing "in the air" information in form on transmitting data chunks within the wireless medium channel. So, the wireless communications, are more susceptible to cyber assaults in contradiction with wired installations where physical security to the network medium, the wire line, is used to be applied.

Beyond the aforementioned vulnerabilities which refer to a more tangible point-of-view, aka the implementation of hardware and software in the IoT devices, vulnerabilities are also emerging through procedures.

The major issue regarding this matter is the excessive ***fragmentation of standards and regulations*** which performs as a catalyst to adverse effects of any other tangible vulnerability. It is already referred earlier that no specific regulations or laws have been implemented yet for IoT devices, regarding the minimum specifications and the standards that “things” ought to meet in order to provide a minimum accepted level of security. This shortcoming is a quite big issue in the IoT world, regardless of the provider, and is pretty hard to overcome due to the contradicting interests and viewpoints of the parties and stakeholders being involved. Without having any regulated framework for IoT in any aspect of “things’ ” lifecycle, major security vulnerabilities will always be emerged in one way or another. Of course, here can be added the ***absence of expertise*** of people who must have the suitable skillset to identify, propose, develop and in any way implement cybersecurity regulations and techniques to this novel domain of IoT which is making its first serious steps of its life.

Analyzing a little broader, and maybe more generic in a way of speaking, the vulnerabilities of IoT devices arise when securing every single layer in the reference model in IoT architecture, fails for some reason [16]; [35]. It is needed just one security gap in any layer of any implemented architecture approach to break the chain of the CIA triad and the IoT ecosystem is compromised. Needless to say, that more security gaps in each layer or in more layers simultaneously, add disproportionally adverse effects and risk of a security incident. In this context, vulnerabilities in the IoT systems have significant variability according to their position in the architecture layer, despite of the reference model approach –three-layered, four-layered, etc.– that is being used.

The following Table lists the above analyzed vulnerabilities, that can be found in IoT ecosystems in the most cases. The listing though, as imprinted below, is neither hierarchized anyhow, nor following any kind of precedence.

IoT VULNERABILITIES		
Extremely large attack surface Spread widely in global scale Complex ecosystem Weak physical security Hardware limitations Software limitations	Insufficient security configurability Insecure software Lack in updates and security patches Insecure mobile interface Insecure cloud services interface Privacy concerns	Network-based limitations Transport encryption and integrity verification Insufficient authentication or authorization Fragmentation of standards and regulations Absence of expertise

Table 4-1: List of the most common IoT vulnerabilities

4.3 IoT asset taxonomy

Scanning the IoT ecosystem for its security challenges and vulnerabilities, is not enough to address the threats that are arising. It is necessary to decompose the IoT ecosystem to its elements –as already done earlier in *Chapter 3*– which have been identified by the researchers, scholars, and experts in this field, having significant key-roles. These elements are the IoT *assets* which, being prone to threats, have to be analyzed regarding their criticality against an IoT system.

The aforementioned IoT assets can be grouped into eight more generic categories for the ease of further study in the scope of their exposure to threats [1].

The grouping has as follows:

ASSET GROUPS							
IoT devices	**Other IoT ecosystem devices**	**Commu-nications**	**IoT Infra-structure**	**IoT Platform & Backend**	**Intelligent decision making**	**Applica-tions & Services**	**Informa-tion**
IoT ELEMENTS (ASSETS)							
Fundamental hardware Sensors Actuators Software	Aggregators Local IoT management devices Embedded systems	Short-range radio networks Long range low power wide area networks Protocols	Routers Gateways Power supplies	Web-based services Cloud infrastructure services	Data mining Data processing	Data analytics Device and network management Device usage	Information at rest Information in transit Information in use

Table 4-2: IoT asset taxonomy

Despite all these IoT assets play significant roles in IoT ecosystem, there is an hierarchy regarding how critical for the “health” of the ecosystem each asset is. This means that not every single IoT asset has the same severity to the system when it is under the impact of an arised threat.

This significance is referred as *IoT asset criticality*, and when security in IoT is implemented, the assets should be prioritized according to their importance classification; from crucial to low or not important.

To this extent, researchers and experts found that the topmost crucial IoT asset is the *sensors* of the ecosystem, followed by the *device and network management* system, which are risking the most, the good and secure operation of the entire IoT system.

The following chart reflects the importance of the assets in a percentage factor:

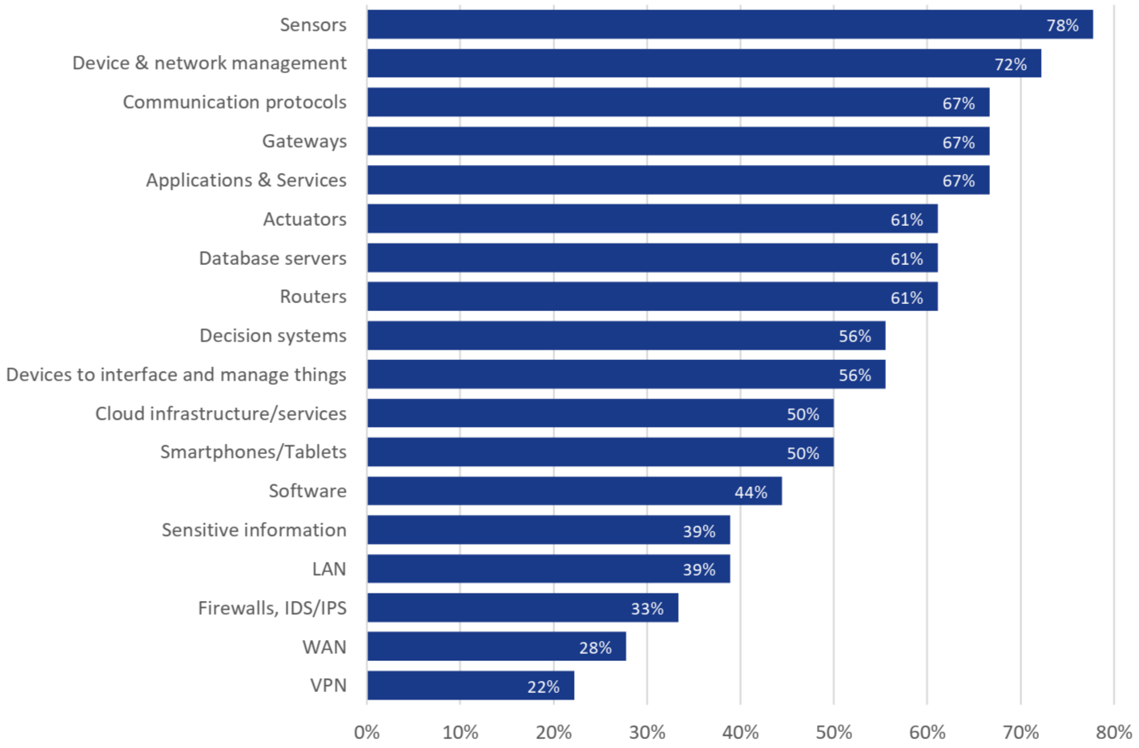


Figure 4-1: IoT assets' criticality [1]

4.4 IoT Threats

While vulnerabilities are holes, gaps in the security of a system, ***threats*** are processes that intensify the possibility of the occurrence of an adverse incident. This kind of processes could be actions of vulnerabilities' exploitation, meaning that a weakness to the system –the vulnerability– exposes this system to malicious actions – the threats– of a bad actor –the adversary–.

Internet of Things is included in the above term "systems", and of course cannot escape from the threats that will inevitably appear and shall be addressed.

The main concerns, threats generate, are the impact may have to humans' privacy, security and overall safety in the physical world, factors that can be jeopardized by attacks in IoT deployments, especially while gaining access to a single IoT device can lead to large-scale attacks and can serve as a means of attack against various critical infrastructures, in accordance with the extreme penetration of IoT in a wide spectrum across the facilities and activities [25]; [1].

Analyzing a little more meticulously the *threats* an IoT ecosystem may come, they can be enlisted, in alphabetical order, as follows:

- *Brute force attack*: This type of attack is quite simple, as the attacker attempts to infiltrate to the system, frontend or backend of a node, just by entering exhaustively all of the possible credentials' combinations. Of course, the attempts start by entering the most usual-used or the factory-default credentials, as users tend to apply guessable passwords or not changing the default ones [35].
- *Calibration Parameters Tampering attack*: While sensors and actuators are preconfigured via calibration in order to provide accurate measurements or movements respectively, in this attack an adversary miscalibrates these components by readjusting their configuration parameters to falsify the measurements sensors provide, and how the actuators interact with their environment [23].
- *Cryptanalysis attack*: Despite the great effort and significant amount of processing power may be needed, an adversary may attempt to decipher encrypted communications, using cryptanalytic techniques, in order to gain unauthorized access to an IoT system, especially in cases where obsolete encryption methods are still being used [23].
- *Data leakage*: Revealed data by any means, intentionally or not, to not authorized third parties is a potential great risk, depending of the kind of the information that is leaked. In cases where these data is considered as sensitive, either due to privacy matters, or security matters, the significance of the leakage is becoming a very important issue to address [1].
- *Device destruction / sabotage*: Attack incidents caused by human actions such as theft, bomb attacks, vandalism, etc. lead to device unavailability, due to destruction or sabotage of the IoT devices, which in many cases could also lead to various malfunction of the whole IoT ecosystem, e.g. incomplete measurements if the sabotage refers to some kind of IoT

sensors. In these cases the attacker does not require any previous understanding regarding the IoT system to unleash his mean [1]; [15].

- *DoS / DDoS attack*: DDoS stands for Distributed Denial of Service, and is the offspring of the DoS attack, where the attack was deployed just from one source than multiple as Distributed term states. More specifically, DoS and DDoS attacks are the attacks with ultimate purpose to usurp a system's or infrastructure resources, from one or multiple attack origins respectively, leading the attacked system or network to a halt or crashed state, becoming unavailable for servicing legitimate requests of authorized users, due to capacity overload which is being produced by flooding the system/network with erroneous or dummy requests excessing the maximum amount of traffic that is able to handle normally [1]; [14]; [35]; [15]; [23]; [13]. Examples of IoT (D)DoS attacks are: *Mass Node Authentication attack*, where a large number of dummy authentication requests is required by the IoT system [15], *ACK Flooding attack*, which is an attack that target the network infrastructure itself by distributing false acknowledgement requests to neighboring network devices [15], *Hello-flood attack*, where a hello-message request is broadcasted to all nodes producing exaggerate network delay and consuming the power of nodes [15], *Sleep Deprivation attack*, where a battery-powered device is prevented maliciously to enter into energy-saving mode in order to drain all of its power reserve and power off becoming unavailable [15]; [23].
- *Environmental disaster*: If the danger to the "things" or the IoT infrastructure is referred to the narrow scale of the IoT deployment environment, like interference of adjacent objects, the threat is considered rather environmental than natural [1].
- *Exploit Kits*: Special code designed to exploit a known weakness in a system to gain unauthorized high-level access [1].
- *Software malfunction*: Like hardware, malfunction could also occur in applications and services, which are one of the core elements of the IoT infrastructure, as it is that component which gives intelligence to

"things". Any software outage, could break down the entire ecosystem [1].

- *Hardware malfunction*: A threat with significant impact in IoT infrastructure is the failure of the IoT devices themselves, plus each device component necessary for seamless operation of the IoT ecosystem, such as the network devices, the end devices, etc. [1].
- *Fake node*: Counterfeit devices are altered with original ones in the ecosystem, in order not to be easily distinguishable from other devices. These fraudulent devices make use of their backdoors to either input fake data into the network, destroying this way the communications infrastructure by breaking legal information transmission, or give access to bad actors in the ICT system and conduct further attacks [1]; [15].
- *Identity theft*: While "things" amass enormous quantities of data, it is easy for an intruder to exploit the information contained in this data to impersonate another device or person, stealing in a way of speaking their identity [14].
- *Jamming*: This kind of attack can be considered a DoS attack variation. The main concept behind this attack is to prevent communication between devices, by creating radio/signal interference mostly in wireless settlements, leading to degradation of the network channel making the communication extremely slow or impossible [35]; [15]; [23]; [12].
- *Services' support outage*: When an IoT component stops working, supporting services will take action by removing the malfunctioning component from the network, repairing it, or replacing it. Unavailability of the supporting services would lead to IoT ecosystem break down for a long time or even eternally [1].
- *Machine learning attacks*: A more sophisticated type of attacks which uses machine learning (ML) techniques. This type of attacks provides the power of artificial intelligence (AI) in the hands of the adversaries giving them an obvious advantage to the known security techniques being already implemented in the IoT systems. Some examples of ML attacks are: *Model attack*, where information itself or patterns of information can be yielded from ML models, just from observing the communication

channel between entities, even if the data is encrypted or anonymized, *Membership inference attack*, where the type of an IoT device being used can be identified in order known weaknesses to be exploited, *De-anonymization / Re-identification attack*, where by tracking certain activity for patterns, a user or device can be identified amongst others even without declaring explicitly its identification details [22].

- *Malicious Code Injection Attack*: A quite common hacking technique where malevolent code is injected to the nodes or the backend supporting software systems such as databases [15]. One of the most well-known attacks of this kind is *SQL injection attack*. SQL stands for Scripted Query Language and is a programming language used in database management systems for programming and administration. In this type of attack malicious code is implemented in SQL commands targeting on high-privileged access gain to systems or degrading the contents of the databases that IoT uses [35]. Another well-known attack of this kind is the *Buffer overflow attack* in which the attacker injects into the volatile memory, e.g. RAM, of the device malformed inputs, that will overflow a fixed-size segment of the memory, leading to gain privileged access to the system or produce a system crash [15].
- *Malware*: Any kind of software code designed to perform without being detected unwanted and unauthorized actions that is off the scope of knowledge of the user, with purpose to interfere or disrupt the normal operation of a system or steal data and information. In order this to succeed, the software needs to be granted with proper high-level access to the victim's information system. Common malicious software of this kind are worms, viruses, trojans, etc.. Its impact to the whole system is considered high [1]; [35]; [15].
- *Man in the Middle*: MitM, as the abbreviation is, is a real-time eavesdropping attack, where an adversary intrudes into the communication of two or more parties-victims, either users or systems, relaying their communication stream through him. This way the adversary drops, alters, or generate new data, generally in form of messages, for his advantage, giving however the impression to the parties

that they exchange information directly. It can be considered as an advanced version of the spoofing attacks [1]; [14]; [15].

- *Information alteration*: Attacks that target the information itself between devices purposing to manipulate it accordingly, to create disorder or attain financial benefits, while devices are remain unaffected [1].
- *Natural disaster*: As all physical objects around are susceptible to natural conditions, their prosperity is very dependent to extreme weather and physical phenomena, such as fire, floods, earthquakes, winds, etc. that could literally destroy the "things" in a very physical manner [1].
- *Network Disruption*: Whether communications fail, by accident or not, the IoT network collapses and is not able to fulfill its purpose of existence. This threat, despite it is not originated from inside the network but from exogenous factors, like power failures, cabling deterioration, etc., could be such important ranging from high to critical, considering the criticality of the network segment and total time until recovery [1].
- *Node tampering*: The attackers could physically seize the node, either an end device or an intermediate, such as a gateway, whether it is exposed in the environment. This threat could lead to other threats as could be the source of attacks to the entire IoT ecosystem, or the source of information leakage [1]; [15].
- *Phishing*: It is considered as social engineering and is a way of exploiting human errors. As humans are prone to errors by accident, this type of attack targets human-victim tricking in order to disclose confidential information, mostly credentials, and ultimately gain illegal access to system without hacking it [15]; [23].
- *Privacy compromise*: Attacks targeting users' privacy through data leaks or by exposing the private network data to not authorized third party personnel [1]; [15].
- *Replay attack*: The adversary captures a legitimate transmission and retransmits it later as a proof that he is the legitimate node in order to manipulate target's response maliciously by impersonating a legitimate sender. To unleash this kind of attack there is no need of extensive

knowledge or mapping the network, as it is sufficient to record and replay the captured message [1]; [15]; [23].

- *Reverse engineering*: This type of attack targets both the hardware and the software, in order by deductive reasoning to accomplish the discovery of flaws and weaknesses to the systems and eventually exploit them possibly unleashing other type of attack. Simply put, reverse engineering is a way to understand how the system works, going backwards and without having any prior knowledge about it, except the output of the system itself [35].
- *SCADA Attack*: SCADA stands for Supervisory Control and Data Acquisition*,* which is a control system architecture for industrial use, where IoT systems are implemented to ensure real-time automation. Generally, SCADA systems include many and various sensors that monitor manifold machinery and device-outputs, in order to control a variety of actuators, such as motors, pumps, valves, etc. In this kind of attacks the adversary takes control of a key device that acts as supervisor to other devices and send erroneous data to the system and the actuators in order to damage or bring to halt the entire system, by operating out of its factory-specified limits. A very well-known attack of this kind was the "Stuxnet worm" that brought out of order various systems of Iranian nuclear plants [14]; [23].
- *Session hijacking*: The adversaries add fake nodes to act as legitimate ones in purpose of stealing the transmitting data in the connection, altering them, or deleting them, so the destination nodes receive modified, erroneous or incomplete information [1].
- *Sinkhole attack*: This type of attack is a classic network targeting attack that exploits the used routing protocol. The compromised node attracts, by sending forged routing information to nearby nodes, a huge amount of network traffic offering a very attractive, according to the routing protocol link, e.g. promising very low latency. This way all the network packets are passing through the compromised node, like water in a sinkhole, capturing their data and deciding next what to do with them.

Extra energy consumption to the nodes due to this kind of attack may result in Denial of Service [15]; [23].

- *Sniffing attack*: The adversary who has intruded to the network listens to the traffic between nodes and intercepts various type of information, giving special attention to the sensible one, like usernames, passwords node identification and configuration, content of files, and anything else that is being transmitted. This type of attack is very common to wireless networking due to shared medium of transmission, the air [1]; [15].
- *Software vulnerabilities*: Flaws and defects in software due to programming bugs produced by developers unintentionally are very common. Weak default password, errors in default configuration, lack of advanced options in software configuration are unavoidable as code development does not follow any kind of standardization, giving acting space for exploit-kits' usage [1]; [15].
- *Spoofing*: This is an attack where infiltration to an IoT system is intended, by means of disguise to an ostensibly legitimate message sender. The spoofing sender, uses data, credentials or other information, pretending validity of them in purpose of gaining unauthorized access to the system [35]; [15].
- *Sybil attack*: This attack is a kind of identity theft but from device point of view. In this case the malicious node claims the identities of other devices in the network, and impersonating them tries to influence the decision-making tasks of the network nodes. This type of attack has also the adverse effect of reducing the effectiveness of the fault tolerant schemes of the ecosystem, and a potentially Denial of Service due to extra energy consumption of the legitimate devices [15]; [23].
- *Targeted attacks*: Extremely particular attacks designed from scratch for a very specific target, launched for long-term period, and carried out in multiple stages in order to avoid detection and to extract sensitive data or control the system as much as possible. Impact of this threat is rated as medium [1].

4.4.1 IoT Attack surface

The term “attack surface” refers to the domain or space, logical or physical, of the party being the target of an attack. In other words, the attack surface is that set of possible targets of attacks in a narrower or wider scope of a domain.

The main purpose of examining the attack surface is to explore the security threats and categorize them by giving more attention in order to better understand what the motive of the attacker is, how the attack takes place and is being deployed, what are the vulnerabilities being exploited, what systems may be compromised, and what information may get affected, leaked, etc. The categorization in attack surfaces unifies the manifold different attacks into attack groups, or summarizes broader domains of attacks to more concise ones, for better manipulation in research, management, and threat mitigation. Nevertheless, attack surfaces have not default categories but can be wider or narrower, logical or physical.

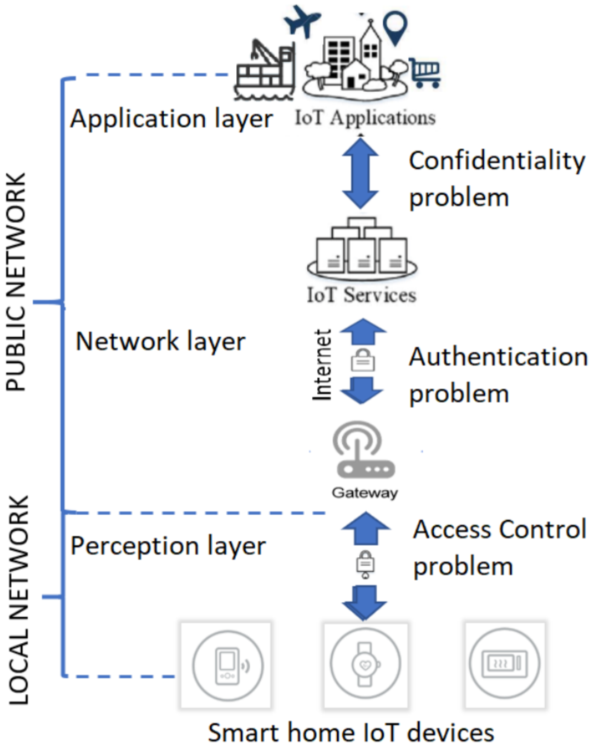


Figure 4-2: The attack surface, and the cybersecurity issues across various IoT layers [28]

Separation of attack surfaces examples can be according to the domain, i.e. smart home, smart car, etc., according to the type of attack source, i.e. local or public network (as shown in the above figure), according to the architecture layer, i.e. perception or communications layer, according to specific spots in the IoT ecosystem, i.e. web applications, etc. [28].

4.4.2 Threat taxonomy in IoT

By analyzing the "attack surface" of the IoT ecosystems a threat taxonomy into categories could be applied with an ultimate purpose to better prevent attacks or mitigate the impact of them.

Multiple categorization approaches can be implemented to the taxonomy of threats in IoT. However, the topmost seven types of categorizations can be distinguished amongst:

1. **Level of access needed** to the asset, having the categories of *Logical / Remote*, *Physical*, and *hybrid* [23].
   - *Logical / Remote* threats are the kind of threats whose existence depends solely to the ability of networking, and without being connected to a network these threats would never emerge. The source of the threats comes from the cyber world and from distance without the need of physical contact with the device.
   - *Physical* threats' existence, in the other hand, depends on everything else than networking dangers, can arise mostly in the physical world, as the need of physical contact with the device is necessary.
   - *Hybrid* threats are the threats that depending on the source of the danger can arise from either logical / remote or physical access level, meaning that could come from both the cyber and the physical world.

   Below is in table format a summarized view of IoT threat categorization based on the level of access needed to the IoT system *(Mind that the traits of each threat or category can also be identified and cross-matched by the color-coding to the tables in chapters 4 and 5, overall)*:

LEVEL OF ACCESS NEEDED		
LOGICAL / REMOTE	**HYBRID**	**PHYSICAL**
THREATS PER CATEGORY		
Brute force attack	Data leakage	Device destruction / sabotage
Calibration Parameters Tampering attack	Identity theft	Environmental Disaster
Cryptanalysis attack		Software malfunction
DoS / DDoS		Hardware malfunction
Exploit Kits		Services’ support outage
Fake node		Natural Disaster
Jamming		Network Disruption
Machine learning attacks		Node tampering
Malicious Code Injection Attack		
Malware		
Man in the middle		
Information alteration		
Phishing		
Privacy compromise		
Replay attack		
Reverse engineering		
SCADA Attack		
Session hijacking		
Sinkhole attack		
Sniffing attack		
Software vulnerabilities		
Spoofing		
Sybil attack		
Targeted attacks		

Table 4-3: Categorization of IoT threats based on the level of the access needed

2. **Source of threat**, having the categories of *Malevolent activity / Misuse*, *Interception / Eavesdropping*, *Malfunctions / Failures*, *IT assets' Destruction*, *Outages*, *Disasters*, *Physical attacks* [1].
    - *Malevolent activity / Misuse* threats are those which their source comes from the intentions of the attacker to abuse a system in a more generic grouping point of view.
    - *Interception / Eavesdropping* threats are those attacks that target more specifically the transmitted information through the networks.
    - *Malfunctions / Failures*, are threats that arise from something that is not working as intended to be, either intentionally or unintentionally.
    - *IT assets' Destruction* threats refer to the adverse effect that emerge when IT assets of an IoT ecosystem are damaged, disclosed to unauthorized parties, get lost or stolen.
    - *Physical attack* threats are anthropogenic attacks to the IoT devices in a physical way.
    - *Outages'* threats are those that are connected with unavailability of IoT resources.
    - *Disasters'* threats are derived from not easily predictable conditions of the IoT physical environment.

    Below is in table format a summarized view of IoT threat categorization based on the source of the threat. The tables following, are color-coded for easy cross-matching:

SOURCE OF THREAT						
Malevolent activity / Misuse	**Interception / Eavesdropping**	**Malfunctions / Failures**	**IT assets' Destruction**	**Physical attacks**	**Outages**	**Disasters**
THREATS PER CATEGORY						
Brute force attack Calibration Parameters Tampering attack DoS / DDoS Exploit Kits Fake node Jamming Malicious Code Injection Attack Malware Information alteration Phishing Privacy compromise Reverse engineering SCADA Attack Sybil attack Targeted attacks	Cryptanalysis attack Machine learning attacks Man in the middle Replay attack Session hijacking Sinkhole attack Sniffing attack Spoofing	Software vulnerabilities	Data leakage Identity theft	Device destruction / sabotage Node tampering	Software malfunction Hardware malfunction Services' support outage Network Disruption	Environmental Disaster Natural Disaster

Table 4-4: Categorization of IoT threats based on source

It is worth mentioning that another grouping can be formed conclusively, as the *source of the threat* categories can be combined and grouped together in their total with the corresponding *level of access to the asset needed* categories, forming the following table of groups:

LEVEL OF ACCESS NEEDED TO THE ASSET						
LOGICAL / REMOTE			HYBRID	PHYSICAL		
SOURCE OF THREAT CATEGORY						
Malevolent activity / Misuse	Interception / Eavesdropping	Malfunctions / Failures	IT assets' Destruction	Physical attacks	Outages	Disasters

Table 4-5: Grouping of source of threats' categories based on needed level of access to the asset.

3. **Way the threat is unleashed**, having the categories of *passive* or *active* attacks, and sometimes the attacks can be unleashed *both* ways [23]. This type of categorization takes into consideration only the kind of threats that are man-made, expressing the specific intention of a perpetrator to attack an IoT system, excluding those threats that cannot be considered as "attacks". The excluded threats are those sourced by the categories of *Outages* (Network Disruption, Hardware malfunction, Software malfunction, Services' support outage) and *Disasters* (Natural Disaster, Environmental Disaster), as already mentioned above.
   - In *passive* attacks the attackers are just observers and will not interact with or influence anyhow the attacked system. In this kind of attacks the information is collected passively from the IoT environment by the adversary.
   - *Active* attacks, in the contrary, need effort from the attackers' side either to gain access to an IoT system, or to extract the information from it. In this attack cases the attackers interact with the system and the system is influenced by them.
   - In some cases, the attacks are a conjunction of *both* passive and active attacks, depending on the way the threat is unleashed.

Below is in table format a summarized view of IoT threat categorization based on the way the threat is unleashed against an IoT system:

WAY OF THE THREAT IS UNLEASHED		
ACTIVE ATTACK	BOTH WAYS	PASSIVE ATTACK
THREATS PER CATEGORY		
Brute force attack Calibration Parameters Tampering attack DoS / DDoS Exploit Kits Fake node Jamming Malicious Code Injection Attack Malware Man in the middle Information alteration Replay attack Reverse engineering SCADA Attack Session hijacking Spoofing Sybil attack	Data leakage Privacy compromise Software vulnerabilities Targeted attacks	Cryptanalysis attack Device destruction / sabotage Identity theft Machine learning attacks Node tampering Phishing Sinkhole attack Sniffing attack

Table 4-6: Categorization of IoT threats based on the way the threat is unleashed against an IoT system

4. **Violated security goals**, having the categories [23] of the CIA triad:

- *Confidentiality*,
- *Integrity*,
- *Availability*,

and the AAA security framework:

- *Authenticity,*
- *Authorization,*
- *Accounting*.

This type of categorization enlists the threats against security goals in IoT ecosystems that are or can be violated by each specified threat. Though, a threat may violate more than one security goal.

Below is in table format a summarized view of IoT threat categorization based on the violated security goals:

SECURITY GOALS VIOLATION					
Confidentiality	**Integrity**	**Availability**	**Authenticity**	**Authorization**	**Accounting**
THREATS PER CATEGORY (multiple per category)					
Cryptanalysis attack Data leakage Exploit Kits Machine learning attacks Malware Privacy compromise Reverse engineering Session hijacking Sniffing attack Software vulnerabilities Targeted attacks	Calibration Parameters Tampering attack Environmental Disaster Malware Man in the middle Information alteration Natural Disaster Node tampering Reverse engineering Session hijacking Sinkhole attack Software vulnerabilities Targeted attacks	Device destruction / sabotage DoS / DDoS Environmental Disaster Fake node Hardware malfunction Jamming Malware Natural Disaster Network Disruption Reverse engineering SCADA Attack Services' support outage Sinkhole attack Software malfunction Software vulnerabilities Targeted attacks	Brute force attack Exploit Kits Identity theft Phishing Replay attack Reverse engineering Software vulnerabilities Spoofing Sybil attack Targeted attacks	Exploit Kits Fake node Malicious Code Injection Attack Malware Node tampering Reverse engineering Software vulnerabilities Targeted attacks	Reverse engineering Software vulnerabilities Targeted attacks

Table 4-7: Categorization of IoT threats based on the violated security goals

5. **Layers of IoT architecture** affected by each threat [35]; [23]. The categorization in this kind of threat taxonomy could be manifold due to various IoT architecture approaches that exist, starting from the 3-layered one until the 7-layered one, as already analyzed thoroughly in the previous chapter.

   In order to keep it as simpler as it gets, the IoT architecture approach that will be adopted to this categorization here, is the 3-layered one, having the categories of:

   - *Perception layer* or *cyber-physical layer*,
   - *Network layer* or *middleware layer*,
   - *Application layer* or *service layer*

   Below is in table format a summarized view of IoT threat categorization based on the layer of the IoT architecture that is being affected:

AFFECTED IoT ARCHITECTURE LAYER		
Perception layer / Cyber-physical layer	**Network layer / Middleware layer**	**Application layer / Service layer**
THREATS PER CATEGORY (multiple per category)		
Calibration Parameters Tampering attack Device destruction / sabotage DoS / DDoS Environmental Disaster Fake node Hardware malfunction Jamming Natural Disaster Network Disruption Node tampering Replay attack Reverse engineering SCADA Attack	Brute force attack Cryptanalysis attack Data leakage DoS / DDoS Exploit Kits Identity theft Information alteration Jamming Machine learning attacks Malicious Code Injection Attack Malware Man in the middle Privacy compromise Reverse engineering	Brute force attack Cryptanalysis attack Data leakage DoS / DDoS Exploit Kits Malicious Code Injection Attack Malware Phishing Privacy compromise Reverse engineering Services' support outage Sniffing attack Software malfunction Software vulnerabilities

AFFECTED IoT ARCHITECTURE LAYER		
Perception layer / Cyber-physical layer	**Network layer / Middleware layer**	**Application layer / Service layer**
THREATS PER CATEGORY (multiple per category)		
Services’ support outage Sniffing attack Spoofing Targeted attacks	Services’ support outage Session hijacking Sinkhole attack Sniffing attack Spoofing Sybil attack Targeted attacks	Targeted attacks

Table 4-8: Categorization of IoT threats based on affected IoT architecture layer (3-layered approach)

6. **IoT asset groups affected** by each threat [1]. As the IoT assets, explained analytically before, play significant role to the functions and the health of the IoT ecosystem, a cross-matching between each IoT asset group and the threats that affect it, is presented below in a summarized view table format:

AFFECTED IoT ASSET GROUP							
IoT devices	**Other IoT ecosystem devices**	**Communications**	**IoT Infrastructure**	**IoT Platform & Backend**	**Intelligent decision making**	**Applications & Services**	**Information**
THREATS THAT AFFECT EACH ASSET GROUP (multiple per category)							
Calibration Parameters Tampering attack Data leakage Device destruction / sabotage DoS / DDoS Exploit Kits Fake node	Data leakage Device destruction / sabotage DoS / DDoS Environmental Disaster Exploit Kits Fake node Identity theft	Jamming Man in the middle Network Disruption Node tampering Services’ support outage	Device destruction / sabotage DoS / DDoS Environmental Disaster Exploit Kits Fake node Jamming	Data leakage Device destruction / sabotage DoS / DDoS Environmental Disaster Information alteration	Calibration Parameters Tampering attack Identity theft Replay attack SCADA Attack Services’ support outage	Brute force attack Malicious Code Injection Attack Reverse engineering Services’ support outage Software vulnerabilities	Calibration Parameters Tampering attack Cryptanalysis attack Data leakage Information alteration Machine learning attacks

AFFECTED IoT ASSET GROUP							
IoT devices	**Other IoT ecosystem devices**	**Communications**	**IoT Infrastructure**	**IoT Platform & Backend**	**Intelligent decision making**	**Applications & Services**	**Information**
THREATS THAT AFFECT EACH ASSET GROUP (multiple per category)							
Hardware malfunction Information alteration Machine learning attacks Malware Man in the middle Natural Disaster Node tampering Privacy compromise Replay attack Reverse engineering Services' support outage Session hijacking Sniffing attack Software malfunction Software vulnerabilities Sybil attack	Information alteration Malware Natural Disaster Privacy compromise Reverse engineering SCADA Attack Services' support outage Software malfunction Software vulnerabilities Spoofing Sybil attack	Session hijacking Sinkhole attack Sniffing attack Spoofing	Machine learning attacks Natural Disaster Network Disruption Services' support outage Sinkhole attack Software vulnerabilities Sybil attack Targeted attacks	Machine learning attacks Malware Natural Disaster Privacy compromise Reverse engineering Services' support outage Software malfunction Software vulnerabilities Targeted attacks	Sniffing attack		Man in the middle Phishing Privacy compromise Replay attack SCADA Attack Services' support outage Session hijacking Sinkhole attack Sniffing attack Spoofing Targeted attacks

Table 4-9: Affected IoT asset group per threat

7. **IoT domains**, having categories of various IoT application areas, such as *Smart Cars, Smart Transport, Smart Homes, Smart Cities, Smart Grid, Smart Health, Smart Supply Chain*, etc.

   Since these categories are not exhaustively listed, and each category is an area of a smaller entire IoT ecosystem which includes a plethora of IoT assets, it is futile to list and enumerate specific threats per domain as almost all threats can be arised in every domain under certain circumstances.

   Though, in a more generic way, the major threats that possibly can be spotted are noted, excluding the physical ones, as follows:

   - ***Smart Cars***: Cars' systems are susceptible to *Software-vulnerabilities'* exploitation which may lead to serious car accidents.
   - ***Smart Transport***: The major threats of transportation systems are *Denial of Service*, which will bring to a halt all public transportation services of an area.
   - ***Smart Homes***: As in our homes we live our lives in a private manner, the major threat is the *Privacy compromise*, in case of a smart home compromise by a bad actor.
   - ***Smart Cities***: Like smart transport, a smart city offers plenty of other smart services to the civilians, a collapse of it, would have severe and broad impact, so the most serious threat is the *Denial of Service.*
   - ***Smart Grid***: An extremely important sector is the energy domain. A breakdown of its normal operation will be critical; thus *Denial of Service* is the basic threat here, too.
   - ***Smart Health***: The most important aspect to this kind of IoT devices and services is to operate accurately when requested, as human lives depend on that, making the *Calibration Parameters Tampering* attack to be at the top of the threats for Smart Health systems.
   - ***Smart Supply Chain***: The topmost threat can be considered the *Privacy compromise* when information for both the identities of the parties involved, and the content of the shipment is revealed without authorization to third parties.

5 th Chapter: Security issues' countermeasures in IoT

5.1 Horizontal versus Vertical security approach in IoT environment

IoT environments, are usually studied regarding the domain of the application. Consequently, IoT is referred preferably to Smart areas, as it is most common to everyday use of IoT devices and services. Smart homes, Smart cars, Smart transport, etc. are domains humans interact the most, rather than single devices themselves, and this is because a Smart system provides a more convenient and complete experience to its human users.

As this is the case, and taking into account both the threats that emerge in each IoT domain and the security measures which must be implemented, a very specific to the domains' IoT assets risk assessment should be carried out with the corresponding attack scenarios, and mitigation techniques should be applied according to every different IoT application area, based on every different attack, against to every IoT asset.

This procedure is the only feasible way to address the hazards of an IoT ecosystem and apply security measures due to the variable criticality and the different threats that emerge when the IoT environment changes from domain to domain. This security approach is called *vertical*, because it is aligned to a specific IoT ecosystem, analyzing it either top-down, or bottom-up. Of course, this approach is more particular when a specific ecosystem should be examined and security measures are applied explicitly to this IoT system design; it is considered more accurate, thus better [1].

Conversely, an holistic approach, takes into account every IoT asset, from IoT devices, to networks, communications, software, information management, services, to all these different IoT elements, without considering the use scenario and the IoT domain. This kind of security approach is called *horizontal*, and is much more complex due to the aforementioned use scenario differentiality [1].

However, the vertical approach is not, obviously, a finite procedure, as application areas are theoretically infinite, concluding that it cannot be used as a baseline to build an holistic security framework for all IoT ecosystems, not even to stand-alone IoT elements.

Therefore, in this thesis an horizontal approach of the security measures will be followed, providing the best approach to a more generic way of mitigating the risk of the threats in all IoT environments, building up a minimum security baseline framework, on which a vertical approach in each IoT domain could act as a security supplement in particular.

5.2 Cybersecurity measures and classification

Internet of Things in terms of security is extremely challenging than traditional information systems or network infrastructures. Big amount of IoT nodes, large attack surface, colossal heterogeneity, lack of standards, all of these and much more important issues increase the exposure to internal and external threats and consequently the probability to adversaries' attacks.

Despite IoT-devices' vendors may apply fundamental security mechanisms, these are practically not quite effective, due to the complexity, to the computational power needed, and for quite a few more reasons.

As the IoT domains, i.e. Smart homes, Smart cars, Smart cities, etc., are manifold areas of concern which each one of them need particular security approach, an holistic security-measures' landscape setting is therefore the basis for further standardized actions to be taken.

So, in the following security-measures' build up, it will be summed up, as much as possible, detailed lists of globally applicable cybersecurity measures to IoT ecosystems, aiming in mitigating threats, vulnerabilities, and the risks which arise in the context of the cyber world; all of them identified, in this thesis, to affect the IoT ecosystems.

Of course, every cybersecurity measure serves in applying the fundamental security principles, the *CIA triad*, and the *AAA security framework* across the IoT ecosystem [21].

The *cybersecurity measures*, denoted henceforth with the acronym *"**CybSecM**"*, are various security controls that can be implemented in IoT ecosystems to mitigate or prevent threats. These cybersecurity measures are listed as follows [1]; [34]; [8]; [16]:

CybSecM.01: Root of Trust (RoT), which is an entity in a cryptographic system that all parts can always trust, should be a hardened hardware module.

CybSecM.02: Incorporating hardware with built-in security features can enhance the device's protection and integrity. This can encompass specialized security chips or coprocessors that incorporate security at the transistor level and are integrated into the processor. These features can provide trusted storage of device identity, authentication means, key protection during storage and use, and prevent unauthorized access to security-sensitive code. Additionally, functional security can protect against local and physical attacks.

CybSecM.03: The foundation of trust must be established in the initial startup process before any trust can be placed in other software or programs that run on the system.

CybSecM.04: Ensure the integrity of code by digitally signing it, and implement additional security measures, such as secure execution monitoring and runtime protection, to prevent any malicious attempts to alter the code after it has been loaded on the device.

CybSecM.05: Restrict loading procedure of software and files in the operating system, by implementing procedures for authentication, to prevent unauthorized access.

CybSecM.06: The code shall be reduced to the bare minimum required for device functioning.

CybSecM.07: Implement a recovery process that allows the system to revert to a state that has been verified as secure, in the event of a security breach or unsuccessful upgrade.

CybSecM.08: Employ trust-based protocols and trust management techniques to establish and maintain trust relationships within the system.

CybSecM.09: Implement a secure-by-default approach, where all relevant security features are enabled, and any unnecessary or vulnerable functionalities are disabled by default.

CybSecM.10: Implement unique and robust default passphrases that are device-specific and difficult to crack, as part of the system's security measures.

CybSecM.11: Ensure compliance with data protection regulations by collecting and processing personal data in a fair and lawful manner, and obtaining explicit consent from the data subject before any collection or processing of their personal information.

CybSecM.12: Ensure that personal data is employed for the specific reasons for which it was obtained, and that any additional usage is consistent with the original purpose, and that the data subjects are fully informed of the intended processing of their information.

CybSecM.13: Practice data minimization, by limiting the amount of data collected and stored to the minimum necessary.

CybSecM.14: Ensure compliance with EU General Data Protection Regulation (GDPR) by all IoT stakeholders, to protect personal data and privacy.

CybSecM.15: Implement data subject rights such as right to information, access, erasure, data portability, rectification, objection to processing, restriction of processing, and the right not to be evaluated on the basis of automated processing, allowing users of IoT products and services to exercise their rights under GDPR.

CybSecM.16: Implement fail-safe mechanisms and design for resilience, to avoid the risk of system disruption causing unacceptable injury or physical harm.

CybSecM.17: Include self-diagnostic and self-repairing functions to restore the system in case of failure, malfunction or a compromised state.

CybSecM.18: Implement offline functionality, to ensure that essential features continue to operate in case of communication loss, and maintain a log of negative impacts resulting from compromised devices or cloud-based systems.

CybSecM.19: Implement secure Over-The-Air (OTA) update mechanism for device software/firmware, configuration, and applications through secure update server, secure transmission, absence of sensitive data, digital signature by authorized trust entity, encryption and digital signature, signing certificate and signing certificate chain, validation by the device prior to initiation of the update process.

CybSecM.20: The manufacturer or service provider must inform the consumer that an update is required for the device.

CybSecM.21: Software components must be updated in a timely manner when updates are available.

CybSecM.22: The manufacturer or service provider must publish a policy for the device's end-of-life that outlines the minimum duration for which the device will receive software updates and the rationale behind the length of the support period. This policy must be readily accessible and clearly understandable for the consumer.

CybSecM.23: The need for each update must be unambiguously conveyed to the end user, and the update process must be easy to implement. Software security updates should be supplied in a proactive manner, such as via automatic updates, to address security vulnerabilities before they can be taken advantage of.

CybSecM.24: Ensure backward compatibility of firmware updates by maintaining user-defined preferences, security, and privacy settings, and providing notification to the user before modifying them during automatic firmware updates.

CybSecM.25: For devices that are unable to receive software updates, the product should be designed in a way that it can be isolated and the hardware can be replaced.

CybSecM.26: Develop device-specific authentication and authorization schemes, in alignment with the system-level threats.

CybSecM.27: Device software shall not contain any credentials that are hard-coded and unchangeable.

CybSecM.28: Require the change of default usernames and passwords during the initial configuration, and ensure that null, weak, blank or universal factory default passwords are not permitted.

CybSecM.29: Passwords should expire and a policy for regularly changing passwords should be in place.

CybSecM.30: Implement using strong passwords or personal identification numbers (PINs) as authentication methods, and incorporating two-factor authentication (2FA) or multi-factor authentication (MFA) into the system, using one-time passwords (OTPs), biometrics, etc., in addition to certificates.

CybSecM.31: Use salting, hashing and/or encryption for authentication credentials.

CybSecM.32: Implement protection, such as account lockout mechanisms, against "brute force" attacks and other malevolent login attempts, including safeguarding keys stored on devices.

CybSecM.33: Measures such as CAPTCHA should be in place to prevent denial of service attacks on account lockout mechanisms.

CybSecM.34: Develop robust password recovery or reset mechanism, both for login credentials and key-management, which does not reveal information indicating a valid account.

CybSecM.35: Role-based access control should be implemented in environments with multiple users.

CybSecM.36: Adhere to the Principle of least privilege (POLP) to restrict the actions permitted for a specific system, which means that applications have to operate at the lowest privilege level possible.

CybSecM.37: An option for changing privileged account usernames should be provided.

CybSecM.38: Create a design for the device firmware that separates privileged code, processes, and data from those that don't need access to them. In addition, hardware isolation should be established to prevent unauthorized access to security-sensitive code.

CybSecM.39: Web applications should be tested to ensure it is not vulnerable to common web application vulnerabilities.

CybSecM.40: Web session timeout should be enabled.

CybSecM.41: A web application firewall should be in place to safeguard the web application.

CybSecM.42: To access the API service, authentication should be required first.

CybSecM.43: The API service should only process requests that have been authenticated.

CybSecM.44: The API service should have a session timeout feature enabled to prevent unauthorized access.

CybSecM.45: All input data should be validated before being processed by the API service to prevent malicious inputs.

CybSecM.46: The API service should use encryption to secure the transmitted data to and from the service.

CybSecM.47: The API service should have a valid TLS server certificate signed by a trusted certificate authority to provide a secure connection and to confirm the authenticity of the service to the clients.

CybSecM.48: The API service should incorporate rate limiting to decrease the speed of volumetric attack attempts and prevent unauthorized access.

CybSecM.49: The API service should be protected by a web application firewall to prevent unauthorized access and malicious activities.

CybSecM.50: Sensitive data should be stored in secure storage facilities on the mobile device to protect personal data, user credentials and cryptographic keys.

CybSecM.51: The mobile application should use mobile-specific authentication methods like facial recognition or fingerprint to secure the collected and stored data.

CybSecM.52: The mobile application should use encryption when communicating with backend cloud applications or IoT devices to secure the transmitted data.

CybSecM.53: Implement access controls to ensure data integrity and confidentiality and enforce defined security policies for authorized subjects.

CybSecM.54: Implement context-sensitive security and privacy measures that represent various degrees of significance.

CybSecM.55: Implement tamper protection and detection mechanisms that do not rely on network connectivity for detection and reaction.

CybSecM.56: Design the device to be tamper-proof, encrypt data storage medium at rest and make it hard to remove.

CybSecM.57: Limit the device to have only essential physical external ports (such as USB) needed for its function, secure test/debug modes, and restrict physical ports to only trusted connections to prevent malicious access.

CybSecM.58: Implement the appropriate use of cryptography to safeguard the confidentiality, authenticity and integrity of any data and information in transit and at rest, by selecting standard and robust encryption algorithms, strong keys and disabling insecure protocols.

CybSecM.59: Ensure secure management of cryptographic keys.

CybSecM.60: Design devices to support lightweight encryption and security techniques.

CybSecM.61: Implement key management methods that can adapt to changing needs.

CybSecM.62: Ensure the security of information in transit on networks or at rest in the IoT application or in the Cloud, by protecting its confidentiality (privacy), integrity, availability, and authenticity.

CybSecM.63: Data stored and transmitted on the cloud should be protected using encryption.

CybSecM.64: For IoT solutions that process highly sensitive data, a FIPS 140-2 certified cryptographic module such as a Hardware Security Module should be used to secure encryption keys for added security assurance.

CybSecM.65: Implement standardized security protocols, such as TLS, for communication encryption.

CybSecM.66: Ensure that credentials are kept confidential and not revealed in network communications.

CybSecM.67: Ensure data authenticity through signing captured and stored data to facilitate secure and reliable transfer of data from sender to recipient.

CybSecM.68: Implement thorough verification for all received data and interconnections, by discovering, identifying, and authenticating connected devices before establishing trust and maintaining their integrity for reliable solutions and services.

CybSecM.69: Each device should have a unique identifier for identification.

CybSecM.70: Each device should be able to be tracked on the device management platform.

CybSecM.71: The device management platform should allow for checking the device model and firmware version.

CybSecM.72: When an anomaly with the integrity of the device is detected, it should be isolated from the device management platform.

CybSecM.73: Design IoT devices to restrict by default communication.

CybSecM.74: Implement intentional connections and prevent unauthorized connections at all levels of the protocols.

CybSecM.75: Restrict access to specific ports and/or network connections, providing selective connectivity.

CybSecM.76: Control network traffic with bandwidth limiting in order to mitigate the possibility of automated attacks.

CybSecM.77: Isolate potential security breaches by dividing network components.

CybSecM.78: Develop protocols to ensure that a single device compromise does not affect the entire system.

CybSecM.79: Avoid using the same secret key across an entire product line to prevent exposing the whole product line if one device is compromised.

CybSecM.80: Limit access to only necessary ports.

CybSecM.81: Establish DDoS-resistant and load-balancing infrastructure.

CybSecM.82: Ensure user sessions are fully encrypted from device to backend services and prevent vulnerabilities to XSS, CSRF, SQL injection, etc.

CybSecM.83: Incorporate security considerations in error message design.

CybSecM.84: Verify the safety of input data prior to use through input validation, and filter output data.

CybSecM.85: Implement a logging system that records key security-related events such as user authentication, account management, access rights changes, security rule modifications, and system performance. These logs should be stored securely and retrievable through authenticated connections.

CybSecM.86: Regularly monitor the device for malware and integrity issues.

CybSecM.87: Regularly evaluate the effectiveness of security controls through audits and reviews, and conduct penetration testing at least twice a year.

CybSecM.88: Establish a system for handling reports of vulnerabilities. Companies that offer internet-connected devices and services are required to have a publicly accessible means for reporting potential vulnerabilities as part of their vulnerability disclosure policy. These reported issues must be addressed in a prompt manner. Furthermore, companies must consistently assess and correct any security weaknesses in their products and services, both those they manufacture and those they provide as a service, as part of their overall product security strategy.

However, a classification of cybersecurity measures could lead to easier application to IoT elements, leaving space for uniting these measures to separate groups [1].

So, the aforementioned *cybersecurity measures* can be grouped into *security considerations* which are the generic security areas that those measures cover. The following table maps each one cybersecurity measure to a security consideration. These mappings are the major ones, meaning that some measures could be mapped to more than one security consideration group.

SECURITY CONSIDERATIONS	CYBERSECURITY MEASURES
Access Control - Physical and Environmental security	CybSecM.53, CybSecM.54, CybSecM.55, CybSecM.56, CybSecM.57
Application Programming Interface (API) Security	CybSecM.42, CybSecM.43, CybSecM.44, CybSecM.45, CybSecM.46, CybSecM.47, CybSecM.48, CybSecM.49
Authentication Security	CybSecM.26, CybSecM.28, CybSecM.29, CybSecM.30, CybSecM.31, CybSecM.32, CybSecM.33, CybSecM.34, CybSecM.35, CybSecM.37
Authorization Security	CybSecM.36, CybSecM.38
Cloud Data Security	CybSecM.62, CybSecM.63, CybSecM.64
Cryptography	CybSecM.58, CybSecM.59, CybSecM.60, CybSecM.61
Data protection and compliance	CybSecM.11, CybSecM.12, CybSecM.13, CybSecM.14, CybSecM.15
Device Management	CybSecM.69, CybSecM.70, CybSecM.71, CybSecM.72
Hardware security	CybSecM.01, CybSecM.02
Logging	CybSecM.85
Mobile Application Security	CybSecM.50, CybSecM.51, CybSecM.52
Monitoring and Auditing	CybSecM.86, CybSecM.87, CybSecM.88

SECURITY CONSIDERATIONS	CYBERSECURITY MEASURES
Secure and trusted communications	CybSecM.65, CybSecM.66, CybSecM.67, CybSecM.68, CybSecM.73, CybSecM.74, CybSecM.75, CybSecM.76
Secure input and output handling	CybSecM.84
Secure Interfaces and network services	CybSecM.77, CybSecM.78, CybSecM.79, CybSecM.80, CybSecM.81, CybSecM.82, CybSecM.83
Secure Software / Firmware updates	CybSecM.06, CybSecM.19, CybSecM.20, CybSecM.21, CybSecM.22, CybSecM.23, CybSecM.24, CybSecM.25, CybSecM.27
Strong default security and privacy	CybSecM.09, CybSecM.10
System safety and reliability	CybSecM.16, CybSecM.17, CybSecM.18
Trust and Integrity Management	CybSecM.03, CybSecM.04, CybSecM.05, CybSecM.07, CybSecM.08
Web Application Security	CybSecM.39, CybSecM.40, CybSecM.41

Table 5-1: Grouping of cybersecurity measures to security considerations.

These mappings can give a quick reference about which measures have to be applied to an IoT ecosystem according to the security area that is needed to be protected. Nevertheless, to secure an IoT ecosystem all of them should be taken into consideration, and further a more vertical security approach should be examined per IoT domain, as already said before.

Though, cybersecurity measures are implemented to the IoT ecosystem to address or mitigate, to the most effective way, the threats emerging from vulnerabilities.

The following table provides a crossmatching between the *cybersecurity measures* and the *source of threats* analyzed in the previous chapter, giving a quick overview of the counter measures for each threat category, meaning that each threat can be dealt with the corresponding counter measures [1]; [15]:

SOURCE OF THREATS CATEGORY	COUNTER MEASURES
Malevolent activity / Misuse	CybSecM.03, CybSecM.04, CybSecM.05, CybSecM.06, CybSecM.07, CybSecM.08, CybSecM.09, CybSecM.10, CybSecM.11, CybSecM.12, CybSecM.14, CybSecM.15, CybSecM.19, CybSecM.20, CybSecM.21, CybSecM.22, CybSecM.25, CybSecM.26, CybSecM.27, CybSecM.28, CybSecM.29, CybSecM.30, CybSecM.31, CybSecM.32, CybSecM.33, CybSecM.34, CybSecM.35, CybSecM.36, CybSecM.37, CybSecM.38, CybSecM.39, CybSecM.40, CybSecM.41, CybSecM.42, CybSecM.43, CybSecM.44,

SOURCE OF THREATS CATEGORY	COUNTER MEASURES
	CybSecM.45, CybSecM.46, CybSecM.47, CybSecM.48, CybSecM.49, CybSecM.50, CybSecM.51, CybSecM.52, CybSecM.53, CybSecM.54, CybSecM.55, CybSecM.56, CybSecM.58, CybSecM.59, CybSecM.60, CybSecM.61, CybSecM.62, CybSecM.67, CybSecM.68, CybSecM.69, CybSecM.70, CybSecM.71, CybSecM.72, CybSecM.73, CybSecM.74, CybSecM.75, CybSecM.76, CybSecM.81, CybSecM.82, CybSecM.83, CybSecM.84, CybSecM.87, CybSecM.88
Interception / Eavesdropping	CybSecM.04, CybSecM.05, CybSecM.06, CybSecM.07, CybSecM.08, CybSecM.19, CybSecM.20, CybSecM.26, CybSecM.27, CybSecM.28, CybSecM.29, CybSecM.30, CybSecM.31, CybSecM.32, CybSecM.33, CybSecM.34, CybSecM.35, CybSecM.36, CybSecM.37, CybSecM.38, CybSecM.39, CybSecM.42, CybSecM.43, CybSecM.44, CybSecM.45, CybSecM.46, CybSecM.47, CybSecM.48, CybSecM.49, CybSecM.50, CybSecM.52, CybSecM.53, CybSecM.54, CybSecM.57, CybSecM.58, CybSecM.59, CybSecM.60, CybSecM.61, CybSecM.62, CybSecM.63, CybSecM.64, CybSecM.65, CybSecM.66, CybSecM.67, CybSecM.68, CybSecM.69, CybSecM.70, CybSecM.71, CybSecM.72, CybSecM.73, CybSecM.74, CybSecM.75, CybSecM.76, CybSecM.77, CybSecM.78, CybSecM.79, CybSecM.80, CybSecM.88
Malfunctions / Failures	CybSecM.03, CybSecM.09, CybSecM.10, CybSecM.16, CybSecM.17, CybSecM.18, CybSecM.19, CybSecM.20, CybSecM.21, CybSecM.22, CybSecM.23, CybSecM.24, CybSecM.25, CybSecM.26, CybSecM.27, CybSecM.28, CybSecM.29, CybSecM.30, CybSecM.31, CybSecM.32, CybSecM.33, CybSecM.34, CybSecM.35, CybSecM.36, CybSecM.37, CybSecM.38, CybSecM.39, CybSecM.48, CybSecM.53, CybSecM.54, CybSecM.57, CybSecM.61, CybSecM.62, CybSecM.68, CybSecM.72, CybSecM.80, CybSecM.84, CybSecM.88
IT assets' Destruction	CybSecM.11, CybSecM.12, CybSecM.13, CybSecM.14, CybSecM.15, CybSecM.25, CybSecM.50, CybSecM.54, CybSecM.63, CybSecM.64, CybSecM.65, CybSecM.66, CybSecM.70, CybSecM.85, CybSecM.86, CybSecM.87, CybSecM.88
Physical attacks	CybSecM.01, CybSecM.02, CybSecM.53, CybSecM.55, CybSecM.56, CybSecM.57
Outages	CybSecM.01, CybSecM.02, CybSecM.03, CybSecM.05, CybSecM.07, CybSecM.09, CybSecM.10, CybSecM.16, CybSecM.17, CybSecM.18, CybSecM.19, CybSecM.21, CybSecM.22, CybSecM.23, CybSecM.24, CybSecM.33, CybSecM.81
Disasters	CybSecM.01, CybSecM.02, CybSecM.16

Table 5-2: Overview of the counter measures for each threat category.

As it is obvious, the measures assigned to each threat overlap in some cases, indicating that certain controls may be effective against multiple types of security threats.

This is being even more descriptive in the following table, where its contents are derived by the previous one. So, each counter measure is being cross matched one by one with all the threats that it mitigates.

COUNTER MEASURES	MITIGATING THREATS
CybSecM.01	Node tampering, Device destruction / sabotage, Network Disruption, Hardware malfunction, Software malfunction, Services' support outage
CybSecM.02	Node tampering, Device destruction / sabotage, Network Disruption, Hardware malfunction, Software malfunction, Services' support outage
CybSecM.03	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.04	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.05	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.06	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.07	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.08	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration

COUNTER MEASURES	MITIGATING THREATS
CybSecM.09	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.10	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.11	Data leakage, Identity theft
CybSecM.12	Data leakage, Identity theft
CybSecM.13	Data leakage, Identity theft
CybSecM.14	Data leakage, Identity theft
CybSecM.15	Data leakage, Identity theft
CybSecM.16	Software vulnerabilities
CybSecM.17	Software vulnerabilities
CybSecM.18	Software vulnerabilities
CybSecM.19	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.20	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.21	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.22	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.23	Software vulnerabilities

COUNTER MEASURES	MITIGATING THREATS
CybSecM.24	Software vulnerabilities
CybSecM.25	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities, Data leakage, Identity theft
CybSecM.26	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.27	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.28	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.29	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.30	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.31	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities

COUNTER MEASURES	MITIGATING THREATS
CybSecM.32	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.33	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.34	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.35	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.36	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.37	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.38	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities

COUNTER MEASURES	MITIGATING THREATS
CybSecM.39	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.40	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.41	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.42	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.43	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.44	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.45	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.46	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.47	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration

COUNTER MEASURES	MITIGATING THREATS
CybSecM.48	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.49	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.50	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Data leakage, Identity theft
CybSecM.51	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.52	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.53	Node tampering, Device destruction / sabotage, Software vulnerabilities, Network Disruption, Hardware malfunction, Software malfunction, Services' support outage
CybSecM.54	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Software vulnerabilities, Data leakage, Identity theft
CybSecM.55	Node tampering, Device destruction / sabotage
CybSecM.56	Node tampering, Device destruction / sabotage
CybSecM.57	Node tampering, Device destruction / sabotage, Software vulnerabilities, Network Disruption, Hardware malfunction, Software malfunction, Services' support outage
CybSecM.58	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities

COUNTER MEASURES	MITIGATING THREATS
CybSecM.59	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.60	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.61	Software vulnerabilities, Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.62	Software vulnerabilities, Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.63	Data leakage, Identity theft
CybSecM.64	Data leakage, Identity theft
CybSecM.65	Data leakage, Identity theft
CybSecM.66	Data leakage, Identity theft
CybSecM.67	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.68	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities

COUNTER MEASURES	MITIGATING THREATS
CybSecM.69	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.70	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities, Data leakage, Identity theft
CybSecM.71	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.72	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.73	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.74	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.75	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities

COUNTER MEASURES	MITIGATING THREATS
CybSecM.76	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.77	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks
CybSecM.78	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks
CybSecM.79	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks
CybSecM.80	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Software vulnerabilities
CybSecM.81	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.82	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.83	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration
CybSecM.84	Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities
CybSecM.85	Data leakage, Identity theft
CybSecM.86	Data leakage, Identity theft
CybSecM.87	Data leakage, Identity theft, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration

COUNTER MEASURES	MITIGATING THREATS
CybSecM.88	Man in the middle, Sniffing attack, Session hijacking, Replay attack, Spoofing, Sinkhole attack, Cryptanalysis attack, Machine learning attacks, Malware, Exploit Kits, Malicious Code Injection Attack, DoS / DDoS, Jamming, Brute force attack, Reverse engineering, Phishing, Sybil attack, SCADA Attack, Calibration Parameters Tampering attack, Targeted attacks, Fake node, Privacy compromise, Information alteration, Software vulnerabilities, Data leakage, Identity theft

Table 5-3: Crossmatching of the counter measures and their mitigating threats.

However, despite all the above mentioned cybersecurity measures are intended to revert all, or at least the majority of the emerging risks that threats generate, none of them is enough, if due care will be not applied in the early stages of IoT ecosystem development.

Thus, ensuring robust security capabilities requires making informed decisions during the design and implementation phase, commonly referred to as "***security by design***". [31]

Security by design is emphasized throughout the entire lifecycle of Internet of Things devices. This approach ensures that products are constructed using the latest secure development techniques, thorough security testing has been conducted, and that developers are committed to update their software to mitigate any newly discovered vulnerabilities or threats [1].

Overall, *security by design* is a proactive approach that can help organizations to better protect their assets and reduce the risk of cyber-attacks.

5.3 Models for IoT security

While IoT security is a crucial aspect of modern technology, many scholars and scientists proposed the use of various models in order to ensure IoT security. The use of models can help identify potential vulnerabilities and predict potential attacks. These models can be used to design and implement security protocols, as well as to monitor and detect any security breaches. Some well-known models for IoT security include intrusion detection systems, access control models, and threat intelligence models. Overall, the use of models for IoT security can greatly enhance the protection of connected devices and networks and help to mitigate the risks associated with IoT technology.

Though, more state-of-the-art models were proposed as well.

Utilizing *patterns* to guide security throughout the development process is one of these kinds of models, and from a security engineering perspective is considered a best practice. Security patterns are constructed using universally recognized security knowledge and expertise that are not specific to any particular domain. These patterns are general in nature, allowing for reuse, and serve as a proven solution for addressing design problems. They should not be considered as a finished implementation but rather as a strategy or template to solve problems that can be applied in various contexts.

Another model supports the utilization of *Blockchain technology*. Blockchain technology is a decentralized ledger technology capable of documenting any type of information, including confidential information. It has been proposed as a solution for improving security in the IoT by connecting and tracking devices in the same network scope or even worldwide, and allowing manufacturers to secure their devices without the need for investing in new standards. A specific solution, called "*Block of Things*" (BoT) offers a decentralized IoT platform that authenticates and manages the exchange of data amongst devices within a private network. BoT is composed of a confidential, decentralized blockchain with duplicates stored in every device. To authenticate users, a private blockchain called for example "Authenblock" has to be used, where devices are registered and a hash is generated that encompasses the device's name, distinctive identification number, and the entities with whom the device is permitted to exchange information. Despite its advantages, the blockchain model is not flawless and has some drawbacks such as scalability issues, the power and processing time required for coding algorithms, and storage limitations. [17].

The use of *cryptographic algorithms*, scoping to provide security, comes from some other model, while these algorithms should be lightweight as a result of the constrained resources on IoT devices. Lightweight ciphers have been introduced to provide data confidentiality, but authentication mechanisms may also be required to provide privacy. However, some drawbacks to certain encryption methods still exist, such as the attribute revocation and key escrow problem. In conjunction to the use of lightweight encryption, the use of blockchain technology is proposed as a solution to provide a secure distributed environment for IoT. By incorporating *Attribute-Based*

Encryption (ABE) techniques in IoT security, multiple security objectives can be achieved, and utilizing a decentralized IoT infrastructure can eliminate the challenges encountered with a centralized approach, making use of blockchain technology as an effective solution for providing a secure distributed environment for IoT [18].

Another proposed model is a *three-stage security system* that focuses on security layers, security protocols, and database servers. The primary objective of the model is to select and implement appropriate security protocols and algorithms to detect problems and protect the system from unwanted situations. The first stage involves maintaining security requirements of the IoT security layer, such as access control, privacy, confidentiality, integrity, availability, authorization, and authentication. The second stage involves selecting the most appropriate communication protocols for the perception layer, which is IEEE 802.11, and the network layer, which is 6LowPAN, which encapsulates IPV6. The third stage involves using the SMQTT protocol for the application layer. The SMQTT protocol includes four primary steps: setup, encryption, publishing, and decryption.

Lastly, a variety of models are employed to ensure secure communication in Wireless Sensor Networks (WSNs) and the Internet of Things. These models can be grouped into several research categories [20], including:

A. *Centralized Approaches*. Security measures that are centralized and pre-configured with shared keys from all entities are considered practical for limited sensor resources. However, the key issue is the lack of flexibility in key management.

B. *Intrusion Detection Systems* (IDS). The use of data collection and passive analysis to monitor and analyze data from users, networks, and services is an effective means for network administration and prompt identification of vulnerabilities.

C. *Rule-Based Approaches*. This methodology involves designing IDS based on an event processing model.

D. *Distributed Detection Based Approach*. In this approach, the algorithm is used to detect anomalous behavior in the node by predicting light energy. The cluster leader is accountable for predicting the energy consumption of all clusters in the cluster. An attack can be detected by discrepancies between the anticipated energy and actual energy consumption; however, this method can only identify gray attacks and flooding.

E. *Requirements for Provisional Measures*. Immediate action is required once a problem is detected, such as isolating the incident site, protecting against further attacks, and reducing damage.

Concluding, there are numerous models proposed, from various perspectives, which provide added-value to the cybersecurity measures that IoT ecosystems have to implement, which is impossible to enumerate them all. Thus, a concise summary to a couple of these models without further analysis has been introduced above.

6 th Chapter: Conclusion

6.1 Sum-up and final thoughts

The Internet of Things is a focal point of our daily lives, more than ever. The world around us includes dozens of "things", tiny, small, or bigger. They provide us with plenty of features, including many types of physical security, environment monitoring, automation and control, real-time communication, cost-effectiveness, etc. in various areas, such as in transportation, houses, cities, energy distribution sector, healthcare, supply chain, etc. This is how our modern life is, without realizing anymore that we already co-exist with them, or that we are directly, even exclusively, dependent on them, except when some "thing" stops fulfilling its purpose usually due to some malfunction. But the worst is not this malfunction. People are in a really bad position when their security is anyhow compromised, especially in terms of their physical security as well as their privacy, data security, financial security, etc.

However, worst case scenarios include large scale security issues, especially in critical infrastructures where the hundreds of thousands of "things" that exist interconnected with them, multiply the possibility of severe risks due to the extremely large attack surface, which means much more available vulnerabilities for adversaries to exploit, while the criticality and impact in any such case increases exponentially.

As it naturally follows, security is very important in the Internet of Things and especially in the scope of protection against cyber threats. For this purpose, in a rapidly developing era for the world of the Internet of Things, it is required to define security frameworks for the good, seamless and safe operation of "things" to all directions.

This thesis dealt with exactly these issues and the ways to mitigate them, based on the scientific research of other scholars, reports and studies of various agencies and organizations around the world, by collecting this material, analyzing it, combining the knowledge obtained and the proposals mentioned in it, and coming to the following summing up conclusions:

- ❖ IoT ecosystems, are types of Information System infrastructures, which are covered under the umbrella of the **CIA triad principles** and the **AAA security framework functions**, meaning that they can be fully protected by incorporating somehow the concepts of Confidentiality, Integrity, Authenticity, Authentication, Authorization, and Accounting.

- The exposed vulnerabilities of IoT elements, which cybercriminals could exploit, should be always identified promptly and analyzed by the cybersecurity specialists, paying attention both to the **collegiality of IoT**, which means that "things' " security in IoT cannot be approached solitarily but as an entity of consolidated singularities, and to **the root causes** for exploiting IoT systems, confronting this way the pitfalls of the IoT design that lead to vulnerable spots' existence.
- To address effectively the vulnerabilities, an IoT ecosystem has to be decomposed firstly to its significant key-role elements, which are the **IoT assets** that are being prone to threats, thus have to be analyzed regarding their criticality against the IoT system. For the ease of further study in the scope of their exposure to threats, these assets it is better to be grouped into more generic asset categories.
- To apply cybersecurity measures in IoT ecosystem **threat identification** is mandatory, as long as the examination of its **attack surface** and a categorization of it, which unifies the manifold different attacks into attack groups, or summarizes broader domains of attacks to more concise ones, for better manipulation in research, management, threat and impact mitigation. This gives a **threat taxonomy** based on: a) the level of access need to each asset, b) the source of each threat, c) the way the threat is unleashed, d) the violated security goals, e) the layers of IoT architecture affected by each threat, f) the IoT asset groups affected by each threat, and g) the IoT domain/area.
- Given the extreme heterogeneity of the IoT world, an holistic approach to the issue for the creation of one or even more unified security frameworks is not possible, due to great IoT environment diverse which negatively affects the integration of a single way of threat mitigation. Though, the basic conditions, principles, directions, controls and measures can be determined, which, if they do not eliminate the threats from the outset, will at least limit both the threats, and the consequences in the event of an attack. This leads to an **horizontal approach** regarding the IoT cybersecurity. Thus, globally, applicable to IoT ecosystems, cybersecurity measures can be implemented to mitigate or totally prevent

threats, by enforcing the aforementioned fundamental security principles of the CIA triad, and the AAA security framework across the IoT ecosystem.

- The cybersecurity measures can be **grouped** in order to give easier implementation to IoT ecosystems, according to the security area that needs to be protected, the source of threat that needs to be addressed, or conversely by each countermeasure, knowing the mitigated threats that can address itself.
- The cybersecurity measures have to be combined, and be implemented as many as possible in order to revert all, or at least the majority of the emerging risks that threats generate. However, due care should be applied in the early stages of IoT ecosystem development, implementing **security by design**.
- State-of-the-art **models for IoT security**, such as security design pattern, blockchain utilization, cryptographic algorithms use, etc. developed by scholars and specialists provide added-value to the cybersecurity measures, and can be implemented in parallel to enhance the protection of the IoT ecosystem from cybersecurity risks.

6.2 Added value and Future work

Hoping for providing an added value to the field of cybersecurity in the Internet of Things, this study was based on meticulous secondary-desktop research, which is proven to give high-accuracy results due to knowledge extraction from a broader domain of work made by other researchers, either on-the-field, or based on a secondary level too.

Therefore, the produced result of this work could be characterized as a "conclusion of the conclusions", thus a more complete and condensed provision of knowledge and proposals to the scientific community, making the content of this thesis a point of reference, a baseline, both for the use and implementation of the proposed measures directly by any stakeholder, as well as for any future research and study by IoT cybersecurity researchers.

Regarding the future extensions of this work, since the approach taken in this study is horizontal, holistic, so as to be applicable to all elements and processes of the IoT without discrimination providing the fundamental protection and cybersecurity, further research can be done following the vertical approach for each IoT area or domain, i.e. by field of application, smart domain, deepening and specializing in specific cybersecurity measures and procedures, in order to complement the aforementioned countermeasures and controls, achieving the maximum possible protection.

Further future work may also be done, in other than the technical types of security measures covered in this study, such as Policies and Guidelines that must be considered during device development, and Organizational measures aimed at the business and workforce that the organization itself must implement.

7 th Chapter: Bibliography – References

[1] European Union Agency for Network and Information Security (ENISA), "Baseline Security Recommendations for IoT (in the context of Critical Information Infrastructures)," EU Publications, Heraklion, Greece, 2017 [https://op.europa.eu/s/oz0X - https://doi.org/10.2824/03228].

[2] Statista Inc., "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by communications technology," Transforma Insights, December 2020 [https://www.statista.com/statistics/1194688/iot-connected-devices-communications-technology]. [Online]. [Accessed 14 05 2021].

[3] Techjury.net, "How Many IoT Devices Are There in 2023? [All You Need To Know]," 12 01 2023. [Online]. Available: https://techjury.net/blog/how-many-iot-devices-are-there/. [Accessed 12 01 2023].

[4] R. M. Church, "The Effective Use of Secondary Data," *Learning and Motivation,* vol. 33, no. 1, pp. 32-45, 02 2002 [https://doi.org/10.1006/lmot.2001.1098].

[5] Wikipedia, "Secondary research," 2023. [Online]. Available: https://en.wikipedia.org/wiki/Secondary_research. [Accessed 20 01 2023].

[6] Victorian Goverment Directory, "Desktop research," 29 04 2020. [Online]. Available: https://www.vic.gov.au/desktop-research. [Accessed 01 12 2022].

[7] European Union Agency for Cybersecurity (ENISA), "Good Practices for Security if IoT: Secure Software Development Lifecycle," EU Publications, Athens, Greece, 2019 [https://op.europa.eu/s/oz0Y - https://doi.org/10.2824/742784].

[8] Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), "IoT Security Best Practice Guidelines," Hong Kong Productivity Council (HKPC), 14 January 2020 [https://www.hkcert.org/c/document_library/get_file?uuid=cc040767-fa07-4c87-aaa9-cdf46d4b92c6&groupId=16]. [Online]. [Accessed 18 December 2020].

[9] C. Prakash and R. K. Saini, "A Model on IoT Security Method and Protocols for IoT Security Layers," in *Mobile Radio Communications and 5G Networks*, 2020 [https://doi.org/10.1007/978-981-15-7130-5_63].

[10] J. Jung, J. Cho and B. Lee, "A Secure Platform for IoT Devices based on ARM Platform Security Architecture," IEEE, 2020 [https://doi.org/10.1109/imcom48794.2020.9001713].

[11] Bhagyashri A Bhandari and Jareena N Shaikh, "A Survey on IoT related Security Issues, Challenges And their Solutions," vol. 06, no. 01, 2020 [https://doi.org/10.35291/2454-9150.2020.0317].

[12] Ranjit Patnaik, Neelamadhab Padhy and K. Srujan Raju, "A Systematic Survey on IoT Security Issues, Vulnerability and Open Challenges," in *Intelligent System Design*, India, 2019 [https://doi.org/10.1007/978-981-15-5400-1_68].

[13] S. Srivastava and S. Prakash, "An Analysis of Various IoT Security Techniques: A Review," in *8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida India, 2020 [https://doi.org/10.1109/icrito48877.2020.9198027].

[14] E. Ahmed, A. Islam, M. Ashraf, A. I. Chowdhury and M. M. Rahman, "Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider," in *11th ICCCNT 2020*, Kharagpur, 2020 [https://doi.org/10.1109/icccnt49239.2020.9225283].

[15] S. Duangphasuk, P. Duangphasuk and C. Thammarat, "Review of Internet of Things (IoT): Security Issue and Solution," in *17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, 2020 [https://doi.org/10.1109/ecti-con49241.2020.9157904].

[16] R. W. Anwar, A. Zainal, T. Abdullah and S. Iqbal, "Security Threats and Challenges to IoT and its Applications: A Review," in *Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2020 [https://doi.org/10.1109/fmec49853.2020.9144832].

[17] A. B. Ayed, P. Taveras and T. BenYounes, "Blockchain and IoT: A Proposed Security Framework," in *17th International Conference on Information Technology–New Generations (ITNG 2020)*, 2020 [https://doi.org/10.1007/978-3-030-43020-7_17].

[18] K. Fasila and M. Sheena, "Blockchain based Protocols for IoT Security using ABE Cryptosystems," in *International Conference on Communication and Signal Processing*, India, 2020 [https://doi.org/10.1109/iccsp48568.2020.9182247].

[19] A. S. Poonia, C. Banerjee, A. Banerjee and S. Sharma, "Security Issues in Internet of Things (IoT)-Enabled Systems: Problem and Prospects," in *Soft Computing: Theories and Applications*, 2018 [https://doi.org/10.1007/978-981-15-0751-9_130].

[20] F. Khursheeed, M. Sami-Ud-din, I. A. Sumra and M. Safder, "A Review of Security Machanism in Internet of Things (IoT)," 2020 [https://doi.org/10.1109/icacs47775.2020.9055949].

[21] T. Rajmohan, P. H. Nguyen and N. Ferry, "A Systematic Mapping of Patterns and Architectures for IoT Security," in *5th International Conference on Internet of Things, Big Data and Security*, 2020 [https://doi.org/10.5220/0009583001380149].

[22] H. Y. Ali and W. El-Medany, "IoT Security: A review of Cybersecurity Architecture and Layers," in *2nd Smart Cities Symposium*, Bahrain, 2019 [https://doi.org/10.1049/cp.2019.0191].

[23] L. Wustrich, M.-O. Pahl and S. Liebald, "Towards an Extensible IoT Security Taxonomy," 2020 [https://doi.org/10.1109/iscc50000.2020.9219584].

[24] A. K. Ray and A. Bagwari, "IoT based Smart home : Security Aspects and security architecture," in *9th IEEE International Conference on Communication Systems and Network Technologies*, 2020 [https://doi.org/10.1109/csnt48778.2020.9115737].

[25] A. Abdullah, H. Kaur and R. Biswas, "Universal Layers of IoT Architecture and Its Security Analysis," in *Advances in Intelligent Systems and Computing*, 2018 [https://doi.org/10.1007/978-981-13-9330-3_30].

[26] T. Malche, P. Maheshwary and R. Kumar, "Secret Key based Sensor Node Security in the Internet of Things (IoT)," in *Fifth International Conference on Communication and Electronics Systems (ICCES)*, 2020 [https://doi.org/10.1109/icces48766.2020.9138078].

[27] P. A. Abdalla and C. Varol, "Testing IoT Security: The Case Study of an IP Camera," 2020 [https://doi.org/10.1109/isdfs49300.2020.9116392].

[28] F. James, "IoT Cybersecurity based Smart Home Intrusion Prevention System," in *3rd Cyber Security in Networking Conference (CSNet)*, 2019 [https://doi.org/10.1109/csnet47905.2019.9108938].

[29] R. K. Sharma and R. S. Pippal, "Malicious Attack and Intrusion Prevention in IoT Network using Blockchain based Security Analysis," in *12th International Conference on Computational Intelligence and Communication Networks*, 2020 [https://doi.org/10.1109/cicn49253.2020.9242610].

[30] European Union Agency for Cybersecurity (ENISA), "Industry 4.0 Cybersecurity: Challenges & Recommendations," EU Publications, Athens, Greece, 2019 [https://op.europa.eu/s/oz01 - https://www.doi.org/10.2824/143986].

[31] IoT Security Foundation (IoTSF), "IoT Security Compliance Framework (version 2.1)," IoTSF, 2020 [https://www.iotsecurityfoundation.org/wp-content/uploads/2020/05/IoTSF-IoT-Security-Compliance-Framework-Questionnaire-Release-2.1.zip].

[32] NSFOCUS Inc., "Annual IoT Security Report 2018," NSFOCUS Inc., USA, 2019 [https://nsfocusglobal.com/2018-annual-iot-security-report].

[33] NSFOCUS Inc., "Annual IoT Security Report 2019," NSFOCUS Inc., USA, 2020 [https://nsfocusglobal.com/2019-annual-iot-securityreport].

[34] European Telecommunications Standards Institute (ETSI), "Cyber Security for Consumer Internet of Things," ETSI, France, 2019 [https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf].

[35] C. Wheelus and X. Zhu, "IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework," pp. 259-285, 19 October 2020 [https://doi.org/10.3390/iot1020016].

[36] C. Stergiou, A. P. Plageras, K. E. Psannis and B. B. Gupta, "Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications*, Springer, 2019 [https://link.springer.com/chapter/10.1007/978-3-030-22277-2_21].

[37] A. P. Plageras, C. Stergiou, K. E. Psannis, G. Kokkonis, Y. Ishibashi, B.-G. Kim and B. Gupta, "Efficient Large-Scale Medical Data (eHealth Big Data) Analytics in Internet of Things," in *19th IEEE International Conference on Business Informatics (CBI'17), International Workshop on the Internet of Things and Smart Services (ITSS2017)*, Thessaloniki Greece, 2017 [https://doi.org/10.1109/CBI.2017.3].

[38] A. P. Plageras, C. Stergiou, K. E. Psannis, B.-G. Kim, B. Grupta and Y. Ishibashi, "Solutions for Inter-connectivity and Security in a Smart Hospital Building," in *15th IEEE International Conference on Industrial Informatics (INDIN 2017)*, Emden, Germany, 2017 [https://doi.org/10.1109/INDIN.2017.8104766].

[39] C. Stergiou, K. E. Psannis, B.-G. Kim and B. Gupta, "Secure integration of IoT and Cloud Computing," *Future Generation Computer Systems,* vol. 78, no. 3, pp. 964-975, January 2018 [https://doi.org/10.1016/j.future.2016.11.031].

[40] C. Stergiou, K. E. Psannis, B. Gupta and Y. Ishibashi, "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT," *Sustainable Computing, Informatics and Systems,* vol. 19, pp. 174-184, September 2018 [https://doi.org/10.1016/j.suscom.2018.06.003].

[41] C. L. Stergiou, K. E. Psannis and B. B. Gupta, "IoT-based Big Data secure management in the Fog over a 6G Wireless Network," *IEEE Internet of Things Journal,* vol. 8, no. 7, pp. 5164-5171, April 2021 [https://doi.org/10.1109/JIOT.2020.3033131].

[42] C. L. Stergiou, E. Bompoli and K. E. Psannis, "Security & privacy issues in IoT-based Big Data Cloud systems in a Digital Twin scenario," *MDPI, Applied Sciences,* vol. 13, no. 2, January 2023 [https://doi.org/10.3390/app13020758].

[43] S. Millar, "IoT Security Challenges and Mitigations: An Introduction," 2021 [https://www.researchgate.net/publication/357417180_IoT_Security_Challenges_and_Mitigations_An_Introduction].

[44] European Union Agency for Cybersecurity (ENISA), "Internet of Thing (IoT)," [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot. [Accessed 01 04 2021].