ESCUELA POLITÉCNICA NACIONAL

THESIS

For the award of the degree of

DOCTOR OF PHILOSOPHY IN INFORMATICS

Resolution RPC-SO-43-No.501-2014 of the Consejo de Educación Superior

Presented by

Roberto Omar Andrade Paredes

Thesis supervised by **Dr. Sang Guun Yoo Professor of the Escuela Politécnica Nacional (EPN).**

Analysis of IoT device´s factors affecting on the security risks in IoT systems

Oral examination by the following committee:

Cecilia Paredes, Ph.D.
Escuela Politécnica Nacional (EPN)

Luis Urquiza, Ph.D.
Escuela Politécnica Nacional (EPN)

Miguel Flores, Ph.D.
Escuela Politécnica Nacional (EPN)

Rebeca Estrada, Ph.D.
Escuela Superior Politécnica Litoral (ESPOL)

Manuel Sánchez Rubio, Ph.D.
Universidad de Alcalá, Universidad Internacional de La Rioja (UNIR)

DECLARATION

I hereby declare under oath that I am the author of this work, which has not previously been presented for obtaining any academic degree or professional qualification. I also declare that I have consulted the bibliographic references included in this document.

Through this declaration, I transfer my intellectual property rights corresponding to this thesis, to the Escuela Politécnica Nacional, as established by the Intellectual Property Law of Ecuador, its Regulations and the current institutional norms.

I declare that this work is based on the following articles of my authorship (as main author or co-author) related to the title of this thesis:

Journals

SJR Q1
R. O. Andrade, S. G. Yoo, L. Tello-Oquendo and I. Ortiz-Garcés, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities," in *IEEE Access*, vol. 8, pp. 228922-228941, 2020, doi: 10.1109/ACCESS.2020.3046442.

SJR Q2
Roberto O Andrade, Sang Guun Yoo, Cognitive security: A comprehensive study of cognitive science in cybersecurity, Journal of Information Security and Applications, Volume 48, 2019, 102352, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2019.06.008.

SJR Q3

- Andrade, R.O.; Yoo, S.G.; Ortiz-Garces, I.; Barriga, J. Security Risk Analysis in IoT Systems through Factor Identification over IoT Devices. *Appl. Sci.* 2022, *12*, 2976. https://doi.org/10.3390/app12062976

- Andrade, R.O.; Yoo, S.G. A Comprehensive Study of the Use of LoRa in the Development of Smart Cities. *Appl. Sci.* 2019, *9*, 4753. https://doi.org/10.3390/app9224753

I also declare that I have acknowledged the collaboration of third parties, and the contribution made by other published or unpublished material.

Roberto Omar Andrade Paredes

CERTIFICATION

I certify that Roberto Omar Andrade Paredes has carried out his/her research under my supervision. To the best of my knowledge, the contributions of this work are novel.

Sang Guun Yoo, Phd.
ADVISOR

DEDICATION

To my parents, although they could not be with me throughout all this process, were undoubtedly the catalysts for my interest in learning and contributing to the development of society.

To my beautiful wife to believe in me and push me through the academic and research world. Many of her contributions are directly and indirectly in this manuscript although she is not expert in cybersecurity field, without her ideas, hours, and patience, I would not have been able to develop this research.

To the Escuela Politécnica Nacional for gave me the opportunity to take a new step in my professional life, through of each one of its members, teachers, colleagues, students, and administrative staff, who have contributed to me in different ways in this research.

ACKNOWLEDGMENTS

To PhD. Sang Guun Yoo, for his guidance and knowledge, which allowed the development of each stage of this research.

To PhD. Cecilia Paredes, PhD. Rebeca Estrada, PhD. Luis Urquiza, PhD. Miguel Flores, and PhD. Manuel Sánchez Rubio for their time and guidance to define the structure of the different chapters of this manuscript.

To each one of the colleagues and friends who took the time to review this manuscript and listen to me about it, which allowed improved this manuscript in different ways.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

RESUMEN

Organizaciones, ciudades y países han optado por implementar procesos de transformación digital mediante la inclusión de tecnologías emergentes como: Cloud Computing, BigData, IoT e Inteligencia Artificial para mejorar la efectividad de sus operaciones, y manteniendo un consumo adecuado de recursos renovables y no renovables. Sin embargo, estas tecnologías han abierto la posibilidad de enfrentar amenazas de ciberseguridad que podrían tener un impacto económico, social y ambiental negativo. Particularmente, IoT ha sido el foco de esta investigación, debido a sus características inherentes que han permitido su adopción en múltiples áreas como salud, educación, transporte, energía, entre otras. Aunque la adopción del concepto "inteligente" se ha implementado en un número cada vez mayor de dispositivos en todo el mundo, también están los riesgos de seguridad, que han sido de interés para la investigación en los últimos años.

Uno de los aspectos importantes desde la perspectiva de la seguridad relacionada con IoT, es que, según algunas investigaciones, las metodologías de análisis de riesgos, que son el primer paso para establecer cualquier estrategia de seguridad, necesitan adaptarse a las particularidades de IoT. Si bien se han presentado varias propuestas, estas difieren de los parámetros utilizados para evaluar el riesgo, y en algunos casos no se especifica el motivo de su selección. En este sentido, el objetivo de esta investigación es establecer los factores de riesgo de los dispositivos IoT que pueden ser considerados en el análisis de riesgos de seguridad, a través de una revisión sistemática de literatura, experimentación y juicios de expertos, enmarcados dentro de una metodología de investigación DRM de 4 fases. Los resultados presentan siete factores de riesgo relevantes en IoT, que han sido modelados matemáticamente y utilizados en una metodología de riesgo basada en un análisis de decisión multicriterio para obtener un valor de riesgo agregado.

ABSTRACT

Organizations, cities and countries have chosen to implement digital transformation processes through the inclusion of emerging technologies such as: Cloud Computing, BigData, IoT and Artificial Intelligence to improve the effectiveness of their operations, and maintaining adequate consumption of renewable and non-renewable resources. However, these technologies have opened the possibility of facing cybersecurity threats that could have a negative economic, social and environmental impact. Particularly, IoT has been the focus of this research, due to its inherent characteristics which have allowed its adoption in multiple area such as health, education, transportation, energy, among others. Although the adoption of the "smart" concept has been deployed into an increasing number of devices worldwide, there are also the security risks, which have been of research interest in recent years.

One of the important aspects from the security perspective related to IoT, is that, according to some researches, risk analysis methodologies, which are the first step in establishing any security strategy, need to be adapted to the particularities of IoT. Although several proposals have been presented, these differ from the parameters used to assess the risk, and in some cases the reason for their selection is not specified. In this sense, the aim of this research is to establish the risk factors of IoT devices that can be considered in security risk analysis, through a systematic literature review, experimentation and expert judgments, framed within a 4-phases DRM research methodology. The results present seven relevant risk factors in IoT, which have been modeled mathematically and used in a risk methodology based on a multi-criteria decision analysis to obtain an aggregate risk value.

PROLOGUE

Different verticals such as health, energy, transportation, agriculture, government, among others, have adopted digital transformation processes to improve the efficiency of their strategic processes by optimizing the use of their resources. In this adoption, organizations, cities and countries have incorporated emerging technologies such as Bigdata, Cloud, Artificial Intelligence, Internet of Things (IoT), which has promoted the incorporation of "Smart" concepts in different verticals.

However, these technologies also bring new challenges from a security perspective, cloud architectures are managed by third parties, artificial intelligence algorithms can be manipulated, Bigdata architectures can be attacked, and IoT devices can be used as pivot to generate different attacks not only on information technology (IT) infrastructures but also on operational technologies (OT) that were traditionally isolated from the Internet.

Although the security of emergent technologies has been the focus of research in recent years, IoT is one that presents for us greater interest due to its inherent characteristics such as heterogeneity of components and technologies, physical location in unprotected places, limited hardware and software resources for the incorporation of security controls, interconnectivity between many IoT devices, and interaction between IT and OT.

Although, CLOUD, Bigdata and artificial intelligence algorithms have seen important improvements in cybersecurity, especially because they are more mature in time and have the support of strong technology companies that have looked at a business niche through them. IoT is still a growing technology and its characteristics allow the developed by large companies but also by entrepreneurs without greater technical knowledge, this makes that some cybersecurity gaps in IoT domains.

In this sense, the contribution of this research poses three specific objectives:

1. Identify the most relevant factors that allow defining the security risk level of an IoT device.
2. Evaluate the relationship between the factors related to the IoT device's risk level.
3. Establish a methodology to calculate an approximate value of the security risk level of an IoT device.

Through the analysis of these three objectives using a scientific process based in the research methodology DRM that proposes four phases: research clarification, descriptive study I, prescriptive study and descriptive study II, in which different research methods are

used as a systematic literature review, empirical data analysis and experimentation, our intention is contribute to organizations, cities, entrepreneurs, students and professionals, with the knowledge about the aspects of management and operation of cybersecurity in IoT systems.

CHAPTER 1

1. INTRODUCTION AND SCIENTIFIC CONTRIBUTION

The increasing use of Internet of Things (IoT) devices in different domains such as health, education, transportation, energy, among others, has contributed to the digital transformation as well as the inclusion of the “smart” concept [1]. However, the inherent characteristics of IoT devices such as the lack of security in their design, limited hardware resources for security mechanisms, installation in non-traditional places, use of heterogeneous technologies, have expanded the attack surface within organizations [2]. From a security perspective, the way to face this problem is to establish adequate security controls, which are defined based on a risk analysis that includes processes such as an asset inventory, vulnerability discovery, threat identification and prioritization of safeguards [3-4].

Although, the problem could be addressed in a simple way through the selection and application of available risk analysis methodologies, several researchers have mentioned that while these methodologies can work well for traditional IT systems that are more static and deterministic, they are nor suitable for IoT scenarios. As a consequence, risk analysis methodologies need to be adapted to the IoT-based scenarios [5].

The main problem arises because, even though IoT devices are like traditional computing systems with memory, processor and network connections, their interconnection and interoperability with other IoT devices, IT (Information Technologies) and OT (Operational Technologies) systems results in the creation of systems more complex, dynamic, and non-deterministic than traditional IT [6-7]. So, specific factors related to IoT must be taken into consideration when performing the risk assessment. In this context, the purpose of this research focuses on analysing the characteristics of IoT devices, and identifying the most relevant factors that could affect the security risk of such systems.

The content of this work is organized as follows: Chapter 2 shows a theorical background related with IoT applications, security of IoT devices and risk analysis methodologies. Additionality, it shows the research design used to address the identification of IoT device´s factors affecting on the security risks in IoT systems. Chapter 3 covers the two initial phases of the research methodology: research clarification and descriptive study I, which are focus on identify the possible IoT device´s factors affecting on the security risks in IoT systems.

Then, Chapter 4 covers the last two phases of research methodology: Prescriptive Study (Results) and Descriptive Study II, focus on validate the IoT device´s factors selected to development risk analysis of IoT solutions. Finally, Chapter 5 presents the conclusions and future work.

1.1 Background

Digital transformation has been used by organizations, cities, and countries as a mechanism to improve efficiency in their strategic and operational processes. An element of the digital transformation has been the incorporation of "smart" concepts in different domains, such as smart health, smart agriculture, smart home, smart cities, among others [8-9]. Achieving these smart features from a technological perspective has been possible thanks to the support of solutions based on cloud computing, artificial intelligence, IoT and big data [10]. However, the incorporation of such technologies introduces new security risks. For this reason, digital transformation must consider the security management as a transversal axis in their strategic, tactical, and operational processes [11]. Aspects related to these security risks have been of interest to many researchers around the world, but attacks on IoT have been of special interest in recent times due to its worldwide growth and its intrinsic characteristics.

1.2 Context

To manage the cyber security of organizations (it means companies, cities or countries), it is necessary to deliver protection from the perspective of the security triad (i.e., confidentiality, availability and integrity). To establish this protection, several strategies, methodologies, and techniques have been defined, such as the principles of zero-trust, risk analysis, security verification.

First context: Zero-trust principle for IoT

The zero-trust principle establishes in first instance a minimum of security requirements that one device must be accomplish in order to access into the organizational network, considering that such a device has also a low security level [12]. Then, the new device should demonstrate that it fulfils organization’s security requirements before accessing its network. Since for a device is practically impossible

to have a 100 percent of security level, the zero-trust principle only establishes a establishes a minimum value of security level based on security controls or mechanisms of security, which opens the probability of attacks.

Regarding IoT devices, applying zero-trust entails some challenges due to their intrinsic characteristics such as: heterogeneity of devices and protocols, lack of security in design, limited hardware resources, location in non-traditional places, and particularities in interconnectivity, interoperability and scalability. So, IoT device generates an opportunity to develop security attacks when it will be included into the organizational network. Under the principle of zero-trust, we could establish a minimum value of security that the IoT device should have to be incorporated into the network and under this precept arise the following question: **Which factors of IoT device should be considered to define an adequate security level to produce a low cyber risk?**

Second context: Risk analysis for IoT systems

In reference [11], three aspects that could affect the application of traditional risk assessment methodologies to IoT systems are mentionated:

1. The high variability in the scalability of IoT systems due to the inclusion of new devices and systems.
2. The dynamism and temporality of IoT connections. IoT devices could be coupled for performing some specify task.
3. The heterogeneity of IoT devices, type of actors, systems and networks.

Similarly, NISTIR 8288 identifies three main aspects that may affect additionally to the management of cybersecurity and privacy risks for IoT devices if we compare with conventional IT devices [13].

1. Interoperability, many IoT devices interact with the physical world in ways conventional IT devices usually do not.
2. High volume of IoT devices, interacting with physical components. Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.
3. Privacy capabilities, the availability, efficiency and effectiveness of cybersecurity controls are often different in IoT devices, compared to conventional IT devices.

Likewise, [14] mentions that IoT devices could affect cybersecurity and privacy risk in a different way as opposed to traditional IT systems:

1. The volume of IoT devices increase the spectrum of vulnerabilities and many of them are harder to detect when they are online.
2. The impact of multiple compromised devices connected to the Internet may be higher than having a single vulnerable device.

In this context, reference [14] suggests that organizations need reconsider the use of traditional risk management. In fact, [5] it is mentioned that traditional risk assessment approaches are unsuitable for IoT. All these arguments generate the following question: **Which IoT device´s factors should risk assessment methodologies take into account?**

Third context: Security Verification for IoT systems.

The security verification process implies validating that the security level is appropriate to the risks faced by users of a system. NIST IR 8259, ETSI EN 303 645 and ISA/IEC 62443-4-1 demands manufacturers to cover the "most common risks" faced by their customers. The Internet of Things Security Verification Standard (ISVS) proposal by OWASP establishes a set of security verification requirements based on three security level (L1, L2 and L3). Each level contains a set of requirements mapped to security-sensitive capabilities and features.

1. Level 1: no sensitive information is being stored on the device.
2. Level 2: some form of sensitive information is stored on the device.
3. Level 3: highly sensitive information is stored on the device may end up un fraud if the device is compromised.

The first security verification of ISVS is to “verify that the IoT system is developed with the level of security (L1, L2, or L3) applicable to the product's capabilities and risks posed in its deployed environment.” At this point, the key is identifying the IoT devices’ security level (L1, L2 or L3), which brings forward the following question: **Which factors of IoT device could be used to define a risk’s profile?**

1.3 Motivation and Purposes

The three contexts described above emphasize the lack of a risk assessment approach adapted to the characteristics of IoT systems. Hence, the importance of defining risk factors related to the cyber-risk on IoT devices is needed for the following activities:

- Defining IoT risk methodologies.

- Proposing IoT security level assessment methodologies.

- Developing zero trust exploitation for IoT.

- Increasing the security level in IoT solutions.

Thus, our main research question is: **What are the factors of an IoT device that affect the security risk level of a IoT system?**

The answer to this question could be addressed from the understanding of the intrinsic characteristics of IoT devices and their direct or indirect relationships with the susceptibility to be a victim of attack, the severity of the attack and the level of impact or damage. However, IoT devices also have other aspects such as the high level of interconnectivity not only between IoT devices, also with traditional information systems (IT) and operational systems (OT). Additionality, another aspect related to the challenge of categorizing devices by its security risk level is their relationship with sensitive information. For instance, IoT devices could have associated, in their basic functions, the real-time monitoring of physical or behavioural parameters of people. So, using IoT attacks, an adversary could obtain sensitive information without the need to directly contact the user.

Currently, there are various frameworks for IoT security, but they do not consider a strong approach for the analysis of the factors of IoT devices that affect the overall risk of the IoT systems that they belong to. Consequently, there is a clear gap between theoretical models and real implementations.

The purpose of this work is identifying possible factors which could contribute to the risk level of IoT devices. This categorization of factors can be used for a risk analysis methodology, security verification process, zero-trust strategies or secure development of IoT systems. In this context, this thesis has three main objectives:

1. To identify the most relevant factors that allow defining the security risk level of an IoT device.

2. To evaluate the relationship between the factors related with IoT device risk level.

3. To establish a methodology to calculate an approximate value of the security risk level of an IoT device.

1.4 Thesis Outline

The content of this work is organized as follows: Chapter 2 shows a theorical background related with IoT applications, security of IoT devices and risk analysis methodologies. Additionality, it shows the research design used to address the identification of IoT device´s factors affecting on the security risks in IoT systems. Chapter 3 covers the two initial phases of the research methodology: research clarification and descriptive study I, which are focus on identify the possible IoT device´s factors affecting on the security risks in IoT systems. Then, Chapter 4 covers the last two phases of research methodology: Prescriptive Study (Results) and Descriptive Study II, focus on validate the IoT device´s factors selected to development risk analysis of IoT solutions. Finally, Chapter 5 presents the conclusions and future work. (See Figure 1.1)

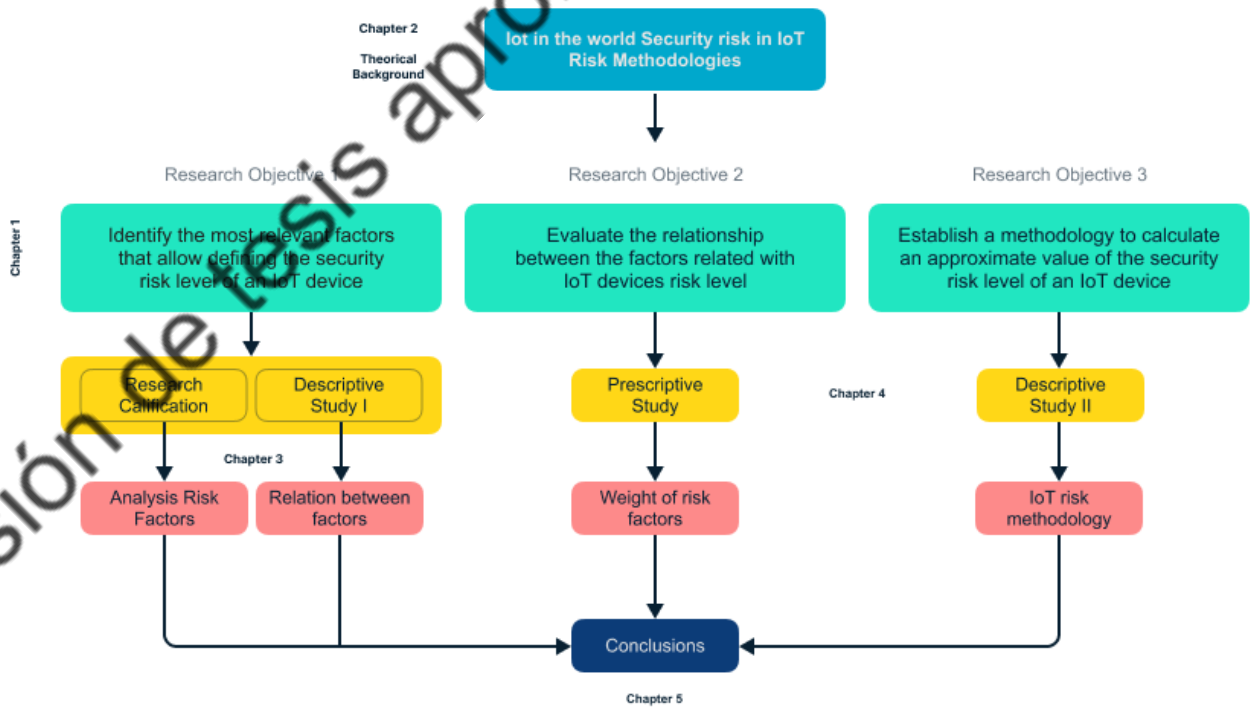


Figure 1.1 Thesis outline

1.5 Scientific Contribution

Emerging technologies such as Cloud computing, IoT, Bigdata and Machine Learning have generated attention at an academic and industrial level for their contribution to digital transformation processes. The study "An Exploratory Study of Cognitive Sciences Applied to Cybersecurity" developed as part of this research allowed us to identify that IoT technologies are of great interest due to their accelerated growth since they are being incorporated in different sectors such as health, transport, energy, among others. According to Forbes data, the estimation of IoT devices is approximately 50 billion by the year 2030 [15], and significant growth is established in different sectors. However, from the cybersecurity perspective, also addressed in the study, the same line of IoT technology, both in the academic and industrial fields, has generated interest in analyzing different aspects that cause security problems, such as: heterogeneity of technologies or devices used in IoT, the lack of security in design, or the lack of computational resources in IoT devices to define security mechanisms. In this context of cybersecurity in relation to IoT devices, this work interested to know four relevant points of IoT systems:

Emerging technologies such as Cloud Computing, IoT, Big Data and Machine Learning have generated attention at an academic and industrial level due to their contribution to the digital transformation processes. The study "An Exploratory Study of Cognitive Sciences Applied to Cybersecurity" developed as part of this research allowed us to identify that IoT technologies are of great interest due to their accelerated growth in different sectors such as health, transport, energy, among others. This is because solutions in these areas have been developed which seek to incorporate "smart" concept and data collection processes in the objects that make up their organizational systems. According to Forbes, the estimated number of IoT devices will be of approximately 50 billion by the year 2030 [15], with a significant growth in different sectors. However, from the perspective of cybersecurity, also addressed in the study, the same line of IoT technology, both in the academic and industrial fields, has generated interest in analyzing different aspects that cause security problems such as: heterogeneity of technologies or devices used in IoT, the lack of security in their design, or the lack of computational resources in IoT devices to incorporate security mechanisms (why not talking a bit of fog computing here? – you may be asked about it as a solution to delegate security controls to other systems

and not the IoT systems themselves). In the context of IoT-related cybersecurity, it is of our interest to unveil four relevant points:

1. The importance of IoT systems today.
2. The fundamentals of the IoT system.
3. Security aspects that affect IoT systems.
4. The impact of security attacks on IoT systems.

Figure 1.2 presents the relationship between our research question, our main research objectives, and these new secondary research objectives, which are addressed through the scientific contribution made in this research work. Regarding the first point, as mentioned above, IoT systems have become an important enabler in decision-making processes and digital transformation in organizations. The study "A comprehensive study of the use of LoRa in the development of smart cities [16]", carried out as part of this research, allowed us to make visible that IoT systems are being used in different verticals such as city management and parking, health, traffic management, home, agriculture sectors. The study "Cybersecurity, sustainability, and resilience capabilities of a smart city [17]" which is part of this research allowed us to understand that, in the case of cities, the inclusion of IoT has allowed the establishment of management models for the use of renewable and non-renewable resources based on data, to achieve the sustainable development goals, set in the 2030 Agenda of the United Nations. The use of IoT allows an abstraction of the values present in physical elements of the city to digital values that can be analyzed by the different methodologies of data analysis and statistical processes for establishing a situational context. However, one of the characteristics that has made IoT solutions so popular is their ability to be applied in different scenarios, giving the generation of concepts such as smart health, smart grid, smart traffic management, and smart homes. As we mentioned before, although many of these solutions focus on digital transformation processes that can be established to improve the effectiveness of operations in organizations or cities, it is also important to consider that IoT has been considered as an enabler to improve processes related with the quality of life and health of people. The studies "A comprehensive study of IOT for Alzheimer's disease" and "Methodology for designing AAL-IOT solutions for older adults [18]", Allowed us to make visible the importance of IoT in the treatment of diseases such as Alzheimer's and the development of assisted living environments for people with limited abilities or older adults who have physical degradation due to the normal aging process.

These studies allowed us to take into consideration that IoT solutions have an important contribution to the process of management of cities and organizations. So, IoT solutions can have a direct impact on the axes of the economic, environmental, social, and human. IoT solutions have been very well received due to their ability to be applied in different scenarios, due to that there are certain patterns that are common or fundamental when developing an IoT solution. The study, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities [19]", allowed us to understand that there are different IoT models; one of the most used one is the one proposed by ITU in its reference ITU-Y2060 “Overview of Internet of things [20]”. The model proposes a scheme based on layers called: Device, Network, Service and Application. The problem from a cybersecurity perspective is that each of these layers are susceptible to attack. In the book called "Cybersecurity Risk of IoT on Smart Cities [21]", an analysis of the different attacks on the different layers of the IoT model has been developed, being able to determine that is necessary to establish cybersecurity strategies that comprehensively cover the entire IoT layers to have an effective solution. A proposal based on this context was proposed in the study "Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation [22]", in which is analyzed the existing vulnerabilities in an IoT system against security controls proposed by CIS with the purpose of perform a hardening of IoT devices prior to putting them into production. This study emphasizes the need to develop a risk analysis in the IoT system to evaluate the effectiveness of the hardening process. However, some authors have established that traditional risk analysis methodologies used in IT systems do not cover all aspects of IoT systems. A literature review carried about risk in IoT systems in this research shows the criteria issued by [7], who indicates that IoT systems require short evaluation periods and consider aspects of the heterogeneity of components of IoT systems. In [23] et .al, also mentions that it is necessary to adapt methodologies and consider new factors in IoT systems such as the number of IoT devices, ports used, and interoperability between layers. Along the same lines, [5] et. al proposes that IoT methodologies consider quantitative assessments. To corroborate about the mentioned in the aforementioned investigations, we contributed with an undergraduate thesis on the implementation of a web solution for IoT risk analysis in Smart homes based on MAGERIT. The selection of MAGERIT was based on the fact that despite being obsolete, it remains as one of the widely used methodologies to evaluate IT systems at an international level and has a qualitative and quantitative evaluation. When applying MAGERIT for the evaluation of a Smart home, we found some limitations such as: i) there is no catalog for IoT devices, ii) an economic impact assessment is not handled, and iii) having to

register all the assets, dependencies and vulnerabilities, the process is too long, and it is difficult to carry them out in short periods.

However, several of the IoT security risk analysis proposals are very relevant in their contribution but use different input parameters to assess the security risk, which does not allow for a standardized guide and in many of them cases, the proposals do not mention the origin of the parameters considered. Based on this context, in the study "Security Risk Analysis in IoT Systems through Factor Identification over IoT Devices" an analysis of the factors of IoT devices that contribute to security risk was carried out based on security proposals in IoT for establish a macro categorization of input and output factors for risk analysis in IoT systems. Finally, to obtain a quantitative risk value, in the study "Factors on risk analysis for IoT system [24]", a mathematical model was proposed to evaluate the risk based on the input and output categorizations obtained through the factor analysis process. In Table 1, a description of the scientific contributions presented in journals is presented, while in Table 2 the contributions made in conferences are presented. Table 3 shows the contributions made in books and book chapters. Table 4 presents degree theses directed in relation to security in IoT. Finally, Table 5 presents the contribution of the contributions to the objectives of this research.

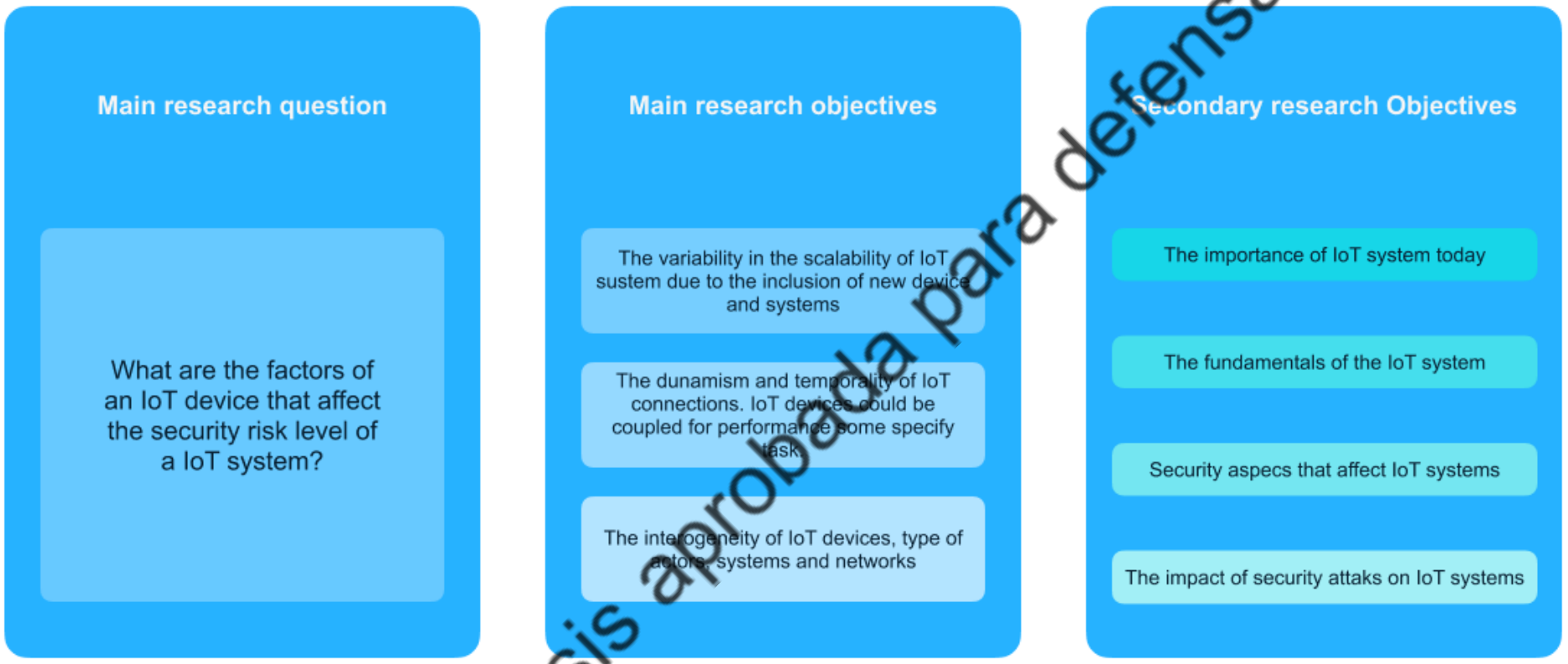


Figure 1.2 Relation among research question, objectives research, and scientific contributions.

Table 1.1 Scientific contributions in journals.

Manuscript	Journal	Authors	Editorial	Year	Indexación	DOI
Smart parking: A Literature Review from the Technological Perspective [25]	Applied Science	Barriga, J.J.; Sulca, J.; León, J.L.; Ulloa, A.; Portero, D.; Andrade, R.; Yoo, S.G.	MDPI	2019	Q2	https://doi.org/10.3390/app9214569
A Comprehensive Study of the Use of LoRa in the Development of Smart Cities [16].	Applied Science	Andrade, R.O.; Yoo, S.G.	MDPI	2019	Q2	https://doi.org/10.3390/app9224753
A Comprehensive Study of the IoT Cybersecurity in Smart Cities [19].	IEEE Access	R. O. Andrade, S. G. Yoo, L. Tello-Oquendo and I. Ortiz-Garcés	IEEE	2020	Q1	doi: 10.1109/ACCESS.2020.3046442
Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation [22].	Applied Sciences	Echeverría, A.; Cevallos, C.; Ortiz-Garces, I.; Andrade, R.O.	MDPI	2021	Q2	https://doi.org/10.3390/app11073260
Cognitive security: A comprehensive study of cognitive science in cybersecurity [26].	Journal of Information Security and Applications	Roberto O Andrade, Sang Guun Yoo,	Elsevier	2019	Q1	https://doi.org/10.1016/j.jisa.2019.06.008.
Security Risk Analysis in IoT Systems through Factor Identification over IoT Devices [24].	Applied Sciences	Andrade, R.O.; Yoo, S.G.; Ortiz-Garces, I.; Barriga, J.	MDPI	2022	Q2	https://doi.org/10.3390/app12062976

Table 1.2 Scientific contribution in conferences

Paper	Conference	Authors	Editorial	Year	Indexación	DOI
A comprehensive study of IOT for Alzheimer's disease [18].	Multi Conference on Computer Science and Information Systems	Andrade, R. O., Yoo, S. G., & Cazares, M. F	MCSS	2019	Scopus	https://doi.org/10.33965/eh2019_201910l021
Cybersecurity Attacks on Smart Home During Covid-19 Pandemic [27].	2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability	R. O. Andrade, I. Ortiz-Garcés and M. Cazares,	IEEE Xplorer	2020	Scopus	doi: 10.1109/WorldS450073.2020.9210363.

Table 1.3 Scientific contribution on books and chapter book

Chapter	Book	Authors	Editorial	Year	DOI
Cybersecurity Risk of IoT on Smart Cities [21].	Cybersecurity Risk of IoT on Smart Cities.	Roberto O. Andrade, Luis Tello-Oquendo, Iván Ortiz.	Springer	2021	https://doi.org/10.1007/978-3-030-88524-3
Cybersecurity, sustainability, and resilience capabilities of a smart city [17].	Smart Cities and the SDGs,	Roberto O. Andrade, Sang Guun Yoo, Luis Tello-Oquendo, Iván Ortiz	Elsevier	2021	https://doi.org/10.1016/B978-0-323-85151-0.00012-9.

Table 1.4 Engineering thesis related with IoT systems.

Thesis	Authors	Year
Web application development for risk analysis in smart homes with IoT ecosystems	Arevalo Proaño Alex, Parco Gualpa Marco.	2021
Security analysis in smart home based on the OWASP ASVS methodology on a real case study.	Chancusing Chancusing Jairo, Guasamba Lucero Jefferson.	2021

1.6 Summary and Implications

The scientific contributions as part of the research work have focused on the analysis of four relevant points: 1). The importance of IoT systems today: These systems have become a key element of digital transformation processes in different verticals such as: health, education, transportation, energy, waste management, among others. 2). The fundamentals of the IoT system: The constitution of these IoT systems in the different verticals have certain fundamental aspects, such as: construction under a layered approach i.e., physical layer elements allow interaction with the physical medium in order to obtain data and perform abstraction when digital world, network layer elements allow the interconnection between different technologies and communication protocols, and application elements allow the integration between the user and the IoT systems. 3). Security aspects that affect IoT systems: Each of the elements of the different layers of the IoT systems can present vulnerabilities that make them susceptible to security attacks, and their interconnection between IoT devices and IT and OT systems expand the attack surface. 4.) The impact of security attacks on IoT systems: The interdependence among IoT, IT and OT systems could allow attacks on IoT systems to have the necessary scalability to effect on the economic, social and environmental axes of organizations, and even cities and countries.

These four points allows the development of risk analysis methodologies that can consider the characteristics of IoT systems, to identify more clearly the factors of risk of cybersecurity that could affected IoT systems. Additionally, the knowledge generated has served to contribute to the development of standards and regulations on IoT cybersecurity topics, such as: Smart city Planning and Technical Guide" of IEEE P2784. "This guide will provide a framework that outlines technologies and the processes for planning the evolution of a smart city. Smart Cities and related solutions require technology standards and a cohesive process planning framework for the use of the internet of things to ensure interoperable, agile, and scalable solutions that can be implemented and maintained in a sustainable manner", and the Framework for IoT cyber risk of International Telecommunications Union (ITU), describes the elements of an IoT system and analyzes the contribution of each one to the total value of cyber risk in a smart city environment.

Table 1.5 Contribution of scientific manuscripts to address research objectives

Secondary Research objectives	Manuscripts	Main findings	Main conclusions
Importance of IoT	• Cybersecurity, sustainability, and resilience capabilities of a smart city • Smart parking: A literature review from the technological perspective • A comprehensive study of IOT for Alzheimer's disease	• IoT is applicable in different verticals such as: smart city, traffic, health, among others. • • IoT is applicable for processes of obtaining data from environment variables and process automation	IoT supports organizations in the execution of three axes: • Economy • Ambient • Social
Establish the fundamentals of the IoT system	A comprehensive study of the use of LoRa in the development of smart cities	• IoT is used together with different technologies, such as Bluetooth, Wi-Fi, LoRa, NB-IoT, which allows IoT solutions to have coverage ranges from a few meters to hundreds of km. • • Layer-based IoT model. One layer encompasses the physical characteristics of IoT devices. Other layer encompasses the communication characteristics used by IoT devices. Finally, a layer that covers the way of interacting between the user and the IoT system. • • IoT devices can be developed on arduino, raspbery. Solutions can be developed in-house or in specialized companies. Computing resources may be limited, due to energy provisioning through batteries.	• Layer-based architecture of IoT systems. • Interconnection of IoT systems with IT and OT systems. • Dynamic systems in number of devices, interconnection and data flow. • Heterogeneity. (Both in types of devices, protocols and technologies). • Limited computational resources on IoT devices. • Lack of security in the design of some IoT solutions.
Establish the security aspects that affect IoT systems	• A comprehensive study of the IoT cybersecurity in smart cities • Cybersecurity model based on hardening for secure internet of things implementation.	• The different layers of an IoT system can be attacked. • There are specific attack vectors for each layer of the IoT model.	• Attacks can affect IoT systems. • IoT systems can be compromised at any of their layers (physical, network and application)

		• Vulnerabilities can occur at the physical level, at the communication level, at the application level in IoT devices.	
Define the impact of security attacks	• Cybersecurity attacks on Smart Home during Covid-19 pandemic • Smart home • Cybersecurity Risks of IoT on Smart Cities	• Attacks from IoT systems can escalate to other interconnected IT and OT systems. • The attack of IoT systems can affect economic, environmental and social aspects of organizations.	• Attacks on IoT systems could reach other IT and OT systems. • Impact on economic, social and environmental aspects.
Mechanisms to assess cybersecurity	• Cognitive security: A comprehensive study of cognitive science in cybersecurity. • Development of web application for risk assessment in smart homes with IoT ecosystems	• Various methodologies to assess security risk, mostly focused on traditional IT systems. • Identification of the need for a methodology that adapts to IoT systems.	• Need to adapt risk methodologies to IoT systems. • Need to identify factors that can be used in risk analysis methodologies

CHAPTER 2

2. THEORICAL BACKGROUND AND RESEARCH DESIGN

This chapter begins with a description of the use of IoT devices in the different verticals (section 2.1) and then analysis the problems of cybersecurity in IoT solutions (section 2.2). Section 2.3 highlights the implications for the application of risk analysis to assess cybersecurity in IoT systems. Section 2.4 details the methodology used in the study to identify the factors of security risk associated with IoT devices and discusses how each phase of methodology support the objectives in this research. Finally, section 2.5 discusses the ethical considerations of the research and its potential problems and limitations.

2.1 IoT devices in the world

The number of IoT devices is expected to grow devices is expected to grow to between 25 and 30 billion by 2022 [1]. Gartner indicates that in the automotive sector alone, IoT is growing by 21% [1]. The automotive sector alone shows a 21% increase in the number of IoT devices by 2020 compared to 2019; this represents a 5,000 million increase by 2020 compared to 2019; this represents 5.1 billion more endpoints worldwide [28]. However, IoT solutions have driven economic growth, and contributed to social, environmental, and commercial aspects. According to the World Economic Forum, IoT projects have contributed to all 17 Sustainable Development Goals -SDGs [29]. This hyperconnectivity and the continuous availability of IoT solutions enable the development of smart cities, but also the IoT solutions enable the development of smart cities, but also increase cyber threats and attacks [30]. An analysis of Forbes of security events shows that cyber-attacks on IoT devices increased by about 300% [31]. According to [31], the development of IoT solutions raised issues of privacy and security. Some of the cyber-attacks that can occur in a smart city are:

1. Control of traffic lights: attackers can manage the city's traffic lights attackers can manage the city's traffic lights causing accidents; traffic lights have become susceptible to attacks due to wireless networks [32].
2. Attacks against intelligent vehicles: attackers can inject false routes or simulate other vehicles in the environment to provoke collisions [33].
3. Power grid collapse: attackers can provoke power failure in the city [34].
4. Water supply: attackers can modify the levels of chemical additives in water and cause public health problems [35].

5. Surveillance cameras: attackers can spy on people and access personal data [36].

2.2 IoT security

Security challenges in IoT systems are due to vulnerabilities in any layer of the IoT architecture. In addition, an IoT node (device, gateway, server) depends on other IoT nodes. Therefore, vulnerabilities of an IoT node could allow the amplification of an attack through a cascading process. From a security point of view, the inclusion of IoT systems expands the attack surface in the city due to the number of IoT nodes installed, the interconnection with multiple networks, and several multiple networks, and various vulnerabilities in each IoT layer. The attack surface is based on four elements:

1. Channel: includes protocols, transmission channels (media), and input/output ports
2. Attack: includes all types of attacks against critical assets.
3. Data: includes data at different stages: rest and transmission; storage or processing.
4. Method: includes the methods and techniques used to carry out the attacks.

The characteristics of IoT systems, such as heterogeneity and lack of security in design, introduce new challenges in the cybersecurity perspective [37]. For example, modelling attack surfaces in the city could be challenging due to the number of installed IoT nodes and the interconnection with multiple networks and the possibility of several vulnerabilities in each layer of the smart city architecture information model [38]. To better understand the surface attacks in IoT systems, the following subsections describe each security features of each layer.

IoT security attacks to physical layer

Physical security focuses on physical access to IoT components (device fog/cloud platform, or application). The goal of an attacker is to gain access to take control of power, memory, firmware, and processing capabilities. Once the attacker is inside the IoT component, sensitive key material, passwords, configuration data, and other sensitive parameters could be obtained. Attackers take advantage of the locations where the IoT devices are located and use JTAG or UART to gain access to them or steal SD cards if they do not have tamper control mechanisms (automatic memory

erase test box). For example, an attacker could tamper with an eMMC flash chip and, via a standard SD card reader, retrieve the firmware, operating system, and software used for IoT devices, and then through the UART pins, access the command prompt with the ability to execute commands [39].

JTAG and UART are the hardware access point for the debugging process. Through these, the attacker can access the contents of memory, registers and flow instructions. Debugging processes are useful during the development and test stages but will be disabled in the production stage to prevent attackers from gaining access to the root shell. However, an attacker could also weld Transmission (TX) and JTAG and UART receive (RX) pins to gain access. Therefore, IoT devices located in open-air outdoor locations should use tampering-resistant enclosures. Vulnerabilities related to IoT device firmware are like those of computers or network devices. With access to the firmware, an attacker can look for vulnerabilities and modify the device.

This can be achieved by downloading the firmware, modifying it and reloading it into the device with a backdoor or other new vulnerability [12]. Sensors in IoT devices can also be attacked. In general, attackers focus on injecting fake patterns into the sensors to alter the information used for decision making or processing [40]. Some attacks on sensors include the following:

1. Information leakage, sensors can be exploited to obtain sensitive data. Techniques such as eavesdropping or keystroke jamming.
2. Malicious information, patterns and commands, an attacker could use malicious information to change the behaviour of the systems. By attacking sensors, the attacker could also use it to create additional communication channels.
3. Fake sensor data injection, an attacker introduces fake sensors to inject fake data to modify IoT system behaviour or information provided to decision makers.
4. RFID/NFC attacks; attackers gain access to physical spaces through the drawbacks of RFID/NFC systems. Some techniques are RFID/NFC spoofing, RFID/NFC cloning, RFID/NFC, unauthorized RFID/NFC access.

Some technique attacks on physical layer are shown in Table 2.1.

Table 2.1 Cyber-attack to physical layer

Technique	Description
Tampering	Attacker modify IoT devices trough JTAG o UART interfaces
Eavesdropping	Unauthorized real-time interception of a private communication
Jamming	A *jamming* attack is an attack in which an attacker transfers interfering signals on a wireless network intentionally.
Denial of Service	A cyber-attack on a specific server or network; the purpose of DDoS is to disrupt the normal operation by flooding the targeted network resources such as IoT devices

IoT Communication layer

The IoT communication layer is responsible for transporting data between devices, gateways, fog, cloud and applications. The IoT attack surface at the communication layer could include vulnerabilities in the following elements:

1. The sensor networks.
2. The IoT gateway.
3. The enterprise computer network.

TCP/UDP protocols is vulnerable to port scanning. Threat actors perform scan the ports of target devices to discover what services are available. The port scanners can provide very detailed information about the services running in the network, and then these services may be vulnerable to exploitation by threat actors. Network services such as Telnet and other undesirable applications should not be run on IoT devices. The attacker could also hide port numbers. Therefore, any IoT node should be evaluated to identify the communication protocols enabled on it by default and which listening ports are open [41].

Table 2.2 Cyber-attack to communication layer

Technique	Description
Sinkhole	Compromised node tries to attack network traffic by advertise its fake routing update
Wormhole	Attacker records packets at one location in the network, then tunnelling to another location
Blackhole	Attacker become parent over an active area to attract packets
Flooding	Malicious node in IoT consumes the network resources like bandwidth and nodes processing capabilities.

IoT Application layer

Data in motion can be intercepted, damaged or altered. Therefore, data storage must be secure, and applications must be tested to ensure that no data leaks occur. Data processing occurs on the gateway, fog or cloud components; short cryptography could expose sensitive data. Data presentations should be made in a secure be made in a secure environment and prevent unauthorized users from accessing the information. However, attackers could use shilling attacks to introduce "shilling profiles" to alter ratings to affect the recommendation in decision support systems, or recommender systems [42]. Mobile applications provide threat actors with access to and control of mobile devices. Insecure authentication of app sessions does not provide the process to identified users when necessary. Session management and authentication can be authentication can be implemented incorrectly; this allows the attacker to discover keys and passwords or to impersonate users. Mobile applications use features built into the platforms such as TouchID Keychain and Android intents, but these options can also be attacked [43]. The misused or misconfigured of security controls could be compromised the access to the IoT device and other applications. Attackers can execute commands in the interpreter to gain unauthorized access to data without authorization. An injection attack typically performs SQL or NoSQL queries in an application. Application programming interfaces (APIs) and web applications can expose sensitive data. OWASP defines a top ten list of attacks on web applications [43]: 1) Injection, 2) Broken Authentication, 3) Sensitive Data Exposure, 4) XML External Entities (XXE), 5) Broken Access Control, 6) Security

Misconfigurations, 7) Cross-Site Scripting (XSS), 8) Insecure Deserialization, 9) Using Components with Known Vulnerabilities and 10) Insufficient Logging and Monitoring. Some techniques for attacks in application layer are shown in Table 2.3.

Table 2.3 Cyber-attack to application layer

Technique	Description
Broken authentication	Attackers are able to compromise passwords, keys or session tokens, user account information, and other details to assume user identities.
Unauthorized access	A person gains logical or physical access without permission to a network, system, application, data, or other resource
Injection	Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program.
Malware	Malicious node in IoT consumes the network resources like bandwidth and nodes processing capabilities.

2.3 Risk analysis on IoT systems

Several risk assessment methodologies are available for information systems but specific risk methodologies for the IoT area is now in development phase. Today, there are common traditional risk methodologies for evaluating IoT systems, in Table 2.4 we show an overview of the most relevant aspects of them.

Table 2.4 Methodologies for risk analysis

Methodologies	Focus on	Strengthen	Weakness
NIST	Security controls	Guidelines to execute security controls according risk assessment.	Needs work with other standards to address compliance
ISO	Compliance of security controls	Analyses of information security risks according to specific criteria.	Coordination and integration to member to update the standard.
MAGERIT	Assets values	Assessments of critical assets, and the threats and risk mitigations that could degrade them.	It requires time for identification of critical assets.
TARA	Attacks	Define a list of possible attacks.	It does not quantify risk impact

However, in [5] mentioned that current risk assessment methods fail in IoT ecosystems due to the following aspects:

1. Short periods of assessment: Risk methodologies are generally not focused on being carried out in short periods of time. However, since the IoT ecosystem changes continuously because of the incorporation of new devices daily, it is necessary the assessment of risks in a short period of time.
2. Limited knowledge on IoT systems: Most risk assessments are focused on traditional systems and do not consider inherent factors of IoT devices.
3. Connections to other systems: IoT devices connect to other systems or technologies such as cloud computing, big data and traditional systems. This situation expands the attack surface of IoT ecosystems.
4. Failure to consider asset as an attack platform: IoT devices can be used to carry out attacks, if the devices lack of minimum security aspects, they could expand the possibility of new attacks.

In [16] it is proposed that the following parameters should be considered to assess the security risk in IoT systems: Type of network (nwt), Type of protocol (prt), Heterogeneous system involved (het), Device security (des) and Type of impact on the CIA (cia). Based on these criteria the risk impact of a device would be given by the equation:

$$w(d) = \frac{1}{5}[nwt(d) + prt(d) + het(d) + des(d) + cia(d)] \qquad \text{Equation 2.1}$$

While the risk probability would be given by the weight of past attacks (pat), the weight of the IoT layer with more attacks (lyr), the weight of the sector where the IoT solution is applied (scr) and the risk factor of the device according to its use (drf). Based on these criteria, the risk probability of a device would be given by the equation:

$$S(d) = \frac{1}{4}[pat(d) + lyr(d) + scr(d) + drf(d)] \qquad \text{Equation 2.2}$$

Finally, the proposal presented by [16] evaluates risk (Rs) as a function of impact by probability, denoted as the product of w(d) times S(d). The exploitation of this proposal is interesting because it includes characteristic aspects of IoT solutions such as the application sector and the layered architecture in IoT. The proposal covers in

a general way the components without making more detail about the threats, attacks or vulnerabilities of IoT systems, allowing to establish the weights for the risk calculation. Additionally, a method could be included to reduce subjectivity when considering the weights of each component.

In [44] defines cybersecurity performance algorithm as: Ef is the Efficiency. Where, Dev is the number of devices connected to the network; Sor is the number of sensors; Svs is the number of services and processes; Int is the number of interfaces; Met is the number of reports, indicators or metrics; Dat is the number of data structures; Scf is the number of smart contract functions; Prot is the number of protocols or standards adopted.

$$Ef = 100 - \left(\frac{\sqrt{Dev \cdot Sor}}{\sqrt{Dat \cdot Scf}} \cdot \frac{Svs + Int + Met}{5\,\pi + Pot}\right) \quad \text{Equation 2.3}$$

The proposal by [44] considers the characteristics of IoT systems from the perspective of the large numbers of devices, sensors and processes. The proposal addresses the security aspects of IoT in a general approach without going into detail on how the CIA aspects are affected by the different threats. The proposal considers all IoT devices equally, this could limit the process of selection of security controls to reduce the risk because there is not detail about the type of information in IoT device or the criticality of IoT device for application related with health or energy.

In [45] the evaluation of the risk is based on layered approach focus on four stages: a) Measuring threats to the layers; (b) Processes/procedures for data security in the layers; (c) Third parties and human factors affecting the security of the layers; and (d) Criticality of the layers and the scale of the attack surface. The model proposes a qualitative risk assessment based on three criticality scales: low, medium and high. In [34], also mentions the importance of considering in the risk assessment the heterogeneous systems participating in the IoT system and the attacks on the different layers of the IoT systems. The proposal does not address in detail how to establish the values of the components that allow to have a more precise or objective risk value.

In [46] a Risk Management Strategy Reference Model (IoTSRM2) is based on six domains: Asset management, Business environment, Governance, Risk assessment, Risk management strategy, Supply Chain Risk Management. Inside the domains include aspect such as: Hardware inventory, Software inventory, Dependencies and critical functions, Critical service resilience, Security related policies, Structures and

responsibilities, Regulatory requirements, Governance and risk management plans, Vulnerability discovery, Threat identification, Risk analysis, and Risk responses. The framework establishes a set of security criteria that could be applied to improve the security level of IoT systems based on the analysis of 25 international security frameworks. A possible drawback of the proposal is that it does not present a detailed operational process to development each of the security criteria proposed in the framework.

In [47] a risk assessment on IoT devices using scores between 0 and 1 for subcomponents of five different attack categories on an IoT device (Physical, Network, Mobile, Web, unknown Risk). In [47] defines the risk ri for each category based on the normalizing the sum of each of the subcomponents ci and dividing by the value of S which is the total possible score of all the subcomponents of an attack category.

$$ri = \frac{1}{S}\sum_{i=1}^{n} ci \qquad \text{Equation 2.4}$$

The proposal by [48] is focused on attacks on the three layers of the IoT model, although [48] separates mobile and web they are part of the application layer; this separation would allow to have more detail of the risk because they are components with a different dynamic with the user, but at the time of establishing a risk weight to the layer, this value would be doubled. Another possible limitation of the proposal is that it only considers a limited number of attacks that may exist in IoT. Also, the weighting of subcomponents depends directly on the experience and subjectivity of the evaluator. A relevant aspect of the proposal is considering a percentage of the weight of risk to unknown factors that might not be easily visualized by the evaluator.

Based on the analysis of the proposed risk methodologies for IoT systems, we conclude that they are focused on various aspects of IoT such as: heterogeneous devices and networks, vulnerabilities and attacks on physical, communication and application layers of the IoT architecture, and the application domain of the IoT system or the number of IoT devices (maybe for better understanding, would it not be better to refer to them as nodes?). However, there is not a clear detail about why these factors have been selected or the weight of these factors to the total risk evaluation.

On the other hand, risk assessment methodologies such as MAGERIT, TARA, OCTAVE, among others, have the strength in the amount of documentation for their

use. These methodologies present a detail of formulas, tools, or methodologies to define the values of the components that are used in the risk assessment process. However, as mentioned by some of the authors cited in this section, traditional methodologies do not cover all aspects of IoT systems that are related to risk, so there is a gap that still needs to be addressed by these methodologies or by new proposals to have a more effective, practical, and repeatable risk analysis process.

2.4 Research Design

This section describes the methodology used in this work which is the Design Research Methodology (DRM). DRM was used to achieve the following objectives:

1. Identify the most relevant factors that allow defining the security risk level of an IoT device.
2. Evaluate the relationship between the factors related with the IoT device's risk level.
3. Establish a methodology to calculate an approximate value of the security risk level of an IoT device.

2.4.1 Methodology and Research Design to study of risk factors in IoT systems

According to [49], the design research methodology is defined as an approach and a set of supporting methods and guidelines to be used as a framework to address the research. In this sense, Blessing [49], proposes a Design Research Methodology (DRM), that links the research questions together and provides support to address these in a systematic way. The DRM is based on four stages: i) Research clarification which is used to create an overview of the main factors based on the basic mean of a System Literature Review, ii) Descriptive Study I based on an empirical analysis which is used to define and understand the main factors associated with the security risk in IoT devices, iii) Prescriptive study which is based on experiments, tests and focus group to support the relation between the factors, and iv) Descriptive Study II which is based on an empirical analysis to evaluate the contribution of factors to risk value. Figure 2.1 shows how each of the phases of the DRM methodology contributes to generating the main outcomes that will allow the fulfillment of the research objectives of this work. Figure 2.1 also presents the basic means to generate the main outcomes using DRM.

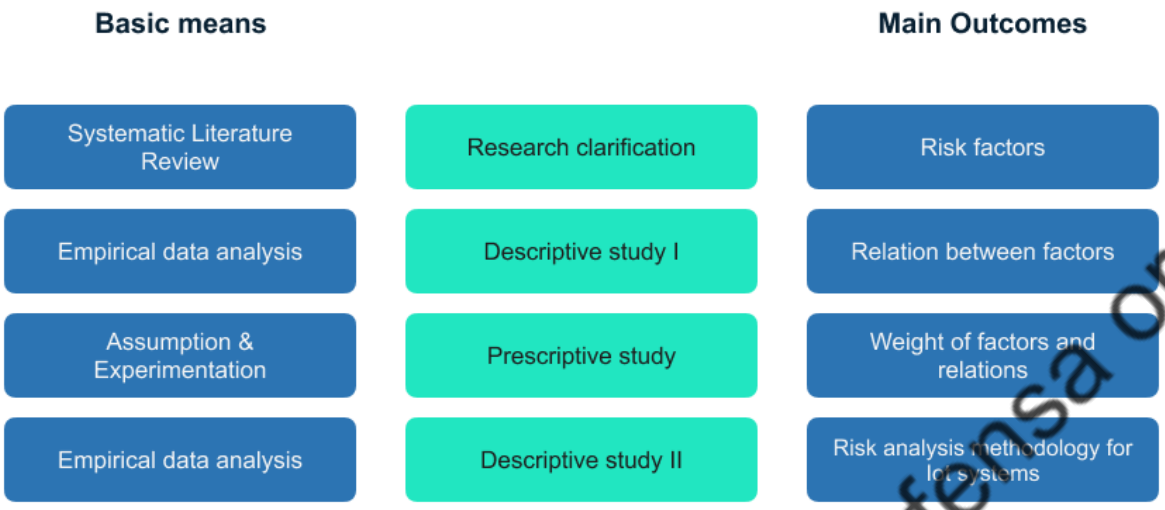


Figure 2.1 DRM methodology used to identify factors of IoT devices that affect the risk level of IoT systems.

The first phase i.e., research clarification has the objective of establishing an understanding the risk factors of IoT systems that could deliver possible negative impact in a security attack. The objective of this phase is reached through a systematic review of the literature that will allow obtaining risk factors in IoT systems.

The second phase of the DRM i.e., descriptive study I seeks to obtain the relationship between the previously established risk factors as the main outcome. For reaching this objective an empirical data analysis is performed.

The main outcome of the third phase of the DRM e.g., Prescriptive study is to define the weight of the risk factors as well as the relationships that may exist between these factors. For this phase, the basic means based on the approach of assumptions and simulations are used.

Finally, the fourth phase of DRM i.e., Descriptive Study II has as its main outcome the establishment of a risk analysis methodology based on the determined risk factors. For this phase, the basic mean based on the use of empirical analysis is used.

2.5 Ethics and limitations of the research

This research is based on the application of the scientific method to identify the risk factors associated with IoT devices that can increase the probability of a security risk in IoT systems. The DRM methodology has been selected based on an analysis of research methodologies that allowed us, from theoretical support and

experimentation, to obtain results for a practical application in a real scenario. However, it is important to mention that since there are different IoT scenarios in different verticals, it is difficult to consider all these scenarios in the present research. Additionally, in Ecuador at the time of developing this research, there is still very little development of IoT solutions or Smart systems, which has made an analysis with real scenarios difficult. This research has been developed under the principles of research ethics, and the different authors who have participated in its development have been recognized, as well as the due citation of the work considered by third parties.

CHAPTER 3

3. RESEARCH CLARIFICATION AND DESCRIPTIVE STUDY I

This chapter cover the first and second phases of the DRM. The first phase is focus on the generation of a prior knowledge related with security risk methodologies and the need to include some characteristic of IoT systems such as attacks on different layers of the IoT architecture, the attack surface, and heterogeneity of IoT devices (Section 3.1). The second phase of DRM takes a deeper analysis of the different factors of IoT devices that could be affected the security of an overall IoT system. (Section 3.2).

3.1 Research clarification

3.1.1 Systematic literature review.

To identify the IoT device´s factors affecting on the security risks in IoT systems, we developed a literature review process (SLR) based on PRISMA methodology [50]. PRISMA methodology is based on four stages: identification, screening, eligibility analysis and inclusion. The identification stage includes different steps such as: selection, study selection, inclusion and exclusion criteria, manual search and elimination of duplicates. The screening stage consists of reviewing titles and abstracts. The eligibility analysis stage performs the reading of full texts of the selected articles. Finally, the inclusion stage consists of data extraction.

The selected works were those focus on the analysis of security aspects such as attacks, vulnerabilities, security controls in the context of IoT. At this stage, the works related to proposals of risk analysis in IoT systems have not been considered to avoid bias in the process of identifying risk factors in IoT devices.

Stage 1. Identification

Study selection: the selection of studies was based on a systematic review following the Prisma Guidelines [50]. The following databases were used: Springer, Scopus, IEEE, Association for Computing Machinery (ACM), Web of Science and Science Direct. These databases were chosen because they are the most relevant sources of information for Computer Science. The range of the publications covers from 2016 to 2021.

Inclusion and exclusion criteria: the inclusion criteria were: (i) manuscripts published by peer-reviewed academic sources; and (ii) manuscripts that analyzing the factors that allow security attacks on IoT systems. On the other hand, exclusion criteria included: (i) manuscripts that even though included technical aspects do not take into consideration the factor that enabled the security attack. The research strings used were:

- "(IoT OR Internet of thing)" AND "(Security attacks OR cybersecurity attacks)"
- "(IoT OR Internet of thing)" AND "(Security risk OR cybersecurity risk)"
- "(IoT OR Internet of thing)" AND "(Threats OR vulnerabilities)"

From the search string, we found 1607 papers. Figure 3.1 indicates the searched papers distributed on conferences, journals, series, chapters and books.

Publication types	
CONF	807
Journal Article	559
SER	215
CHAP	23
BOOK	3

Figure 3.1 Publication types based on Systematic Literature Review

An overview of the topics covered on the papers are show in the cloud word in the Figure 3.2.

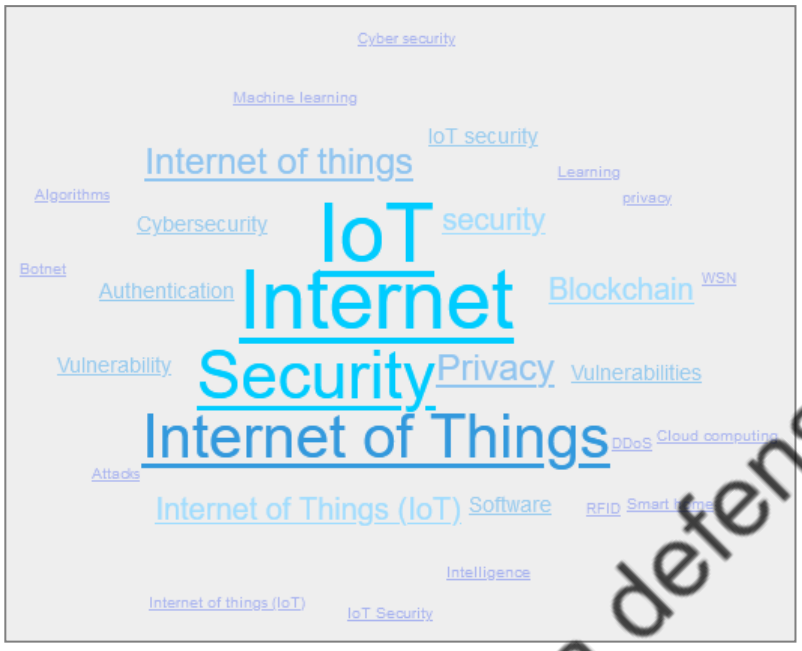


Figure 3.2 Screenshot of Rayyan related about topics in SLR.

Duplicates were eliminated through a manual review of the collected documents. In this process, 23 duplicates were eliminated.

Stage 2. Screening

The screening process was based on the review of titles and abstracts of the papers using the web application Rayyan, which was created for the systematic review process by MIT. The web application allows reviewers to view the titles and abstracts of the collected articles, maintaining a blinded review process. The papers that did not meet the inclusion criteria in the title or abstract were excluded at this stage of the study (See, Figures 3.3 and 3.4).

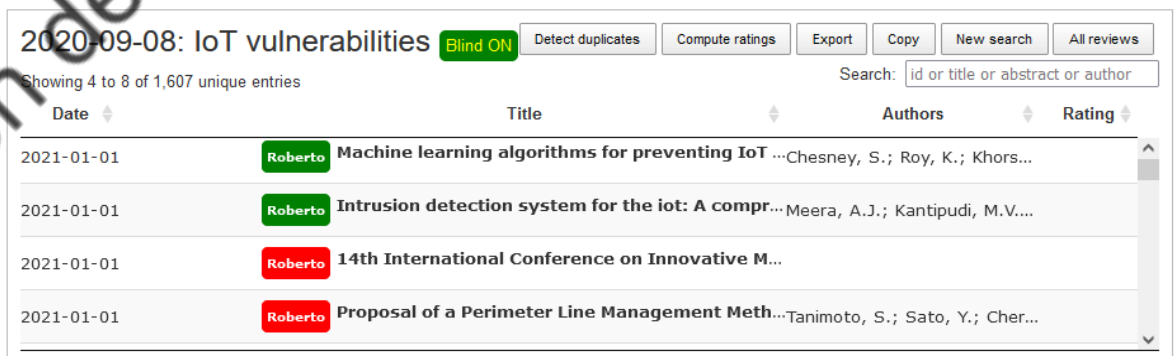


Figure 3.3 Screenshot of inclusion and exclusion of papers based on abstract review.

Inclusion decisions	—
Undecided	0
Maybe	0
Included	370
Excluded	1237

Figure 3.4 Number of articles include and excluded for screening process.

Stage 3. Eligibility analysis

A full text review of each one of 370 papers was made and those that presented detail on the operation of the security attacks, factors used by attacks and impact that they produced were considered for further review. After this step, 55 articles were selected for quality analysis, how is show in the Figure 3.5.

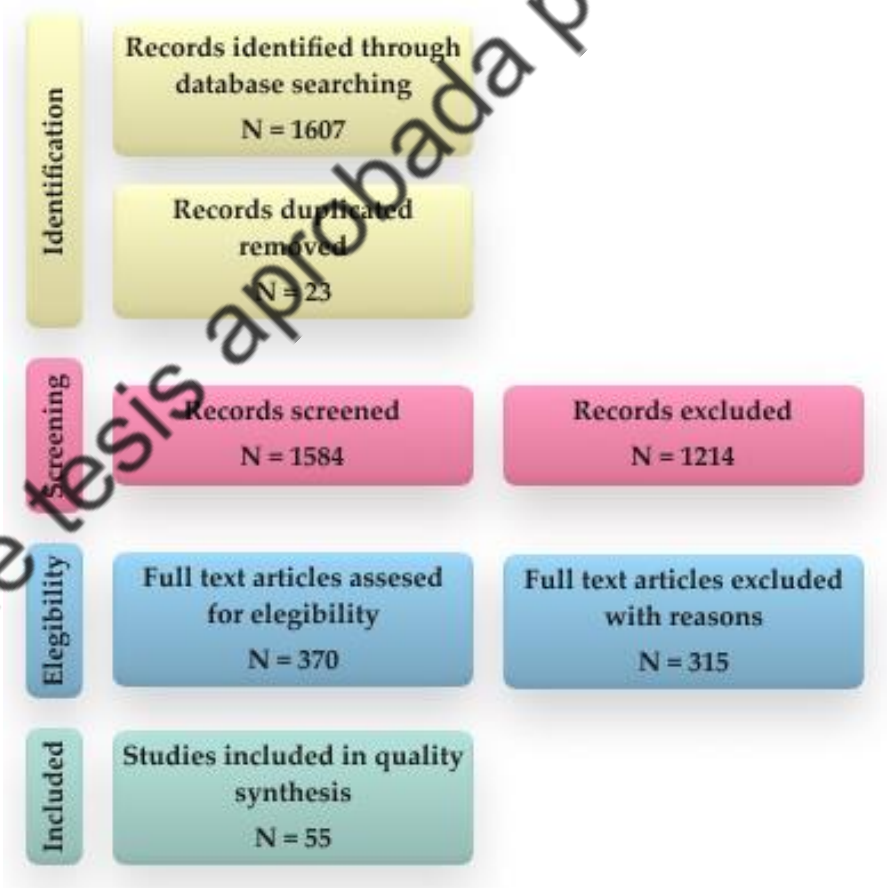


Figure 3.5 Prisma methodology used for the SLR.

Stage 4. Inclusion. Data extraction.

For this stage, we have developed a qualitive analysis using ATLAS TI version 9. Figure 3.6 shows a screenshot of the Atlas TI including the 55 selected articles. The documents were numbered automatically by Atlas IT labeling them with the letter D followed by a sequential number.

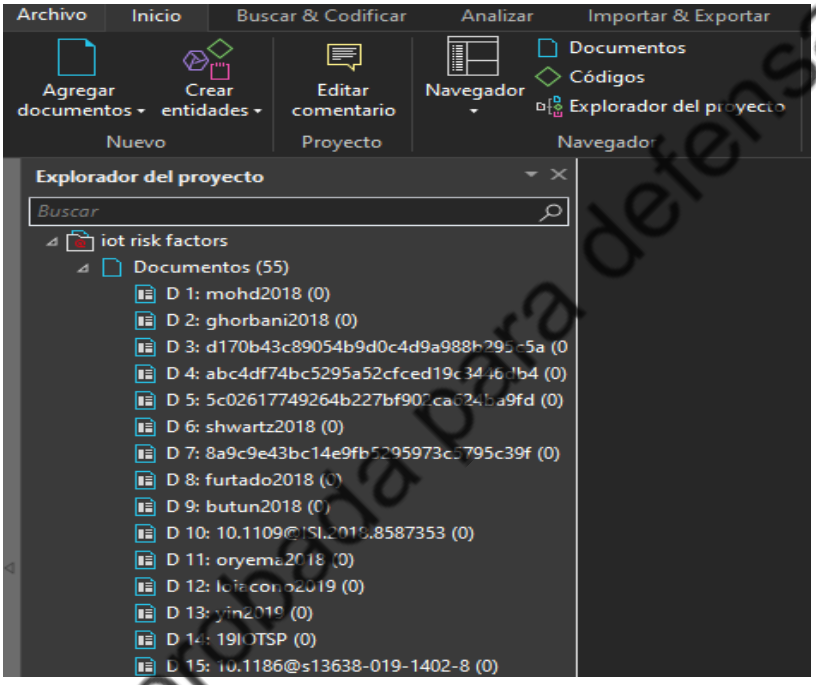


Figure 3.6 Screenshot for ATLAS TI with the 55 papers selected for data extraction.

To obtain an overview of these documents a new word cloud was generated using Atlas TI which is presented in the Figure 3.7.

Figure 3.7 Cloud of words generated in ATLAS TI based in the 55 papers for data extraction.

During the qualitative analysis, 11 codes have been defined in Atlas TI associated to possible factors (see Figure 3.8):

- Application domain, related to the verticals in which IoT systems have been implemented.
- Attack Surface, related to the entry and exit points that can be used to perform attacks.
- Interdependency, related to the relationship of the IoT system with other IT/OT/IoT systems that could increase the severity of the attack.
- Scalability, related to the coverage area that can be affected by the propagation of the attack.
- Severity, related to the damage value that can be caused by the attack.
- Susceptibility, related to the predisposition to catch the effects of an attack.
- Type of attack, related to the attack vector, technique or methodology,
- Type of device, related to the type of IoT device.

- Type of information, related to the type of information that is processed, stored or transmitted by the device.
- Uncertainty, related to unknown factors that could affect the security of IoT systems.
- Vulnerabilities, related to weaknesses that IoT systems may have and may increase the possibility of being affected by an attack.

Figure 3.8 Manual codes generated from the qualitative analysis using ATLAS TI.

Using the option Concurrence-Table on ATLAS TI, we have analyzed the relationship between the codes. We found a relation between the code “Severity” and the code “Type of attack”. Also, we can observe the relation between the code "Type of attack" with "Severity" and with the code "Vulnerabilities". We can also observe the relation between the code "Vulnerabilities" with the code "Type of attack". Finally, we can observe that the attack surface is associated with elements such as network size (number of nodes or devices), interfaces and links, and security elements of the IoT system components (see, Figure 3.9).

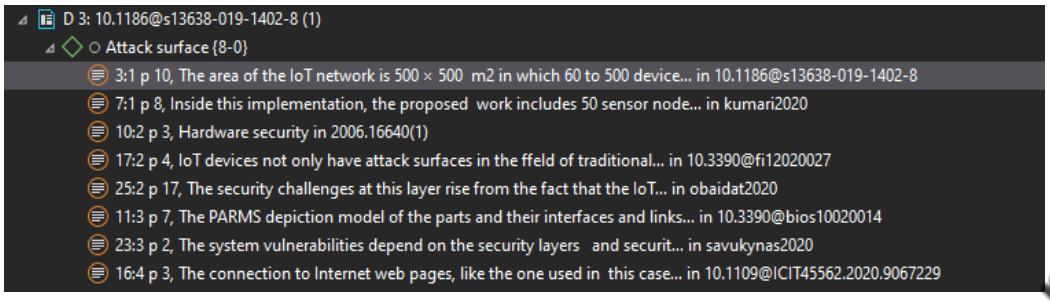


Figure 3.9 Elements of IoT attack surface based on qualitative analysis.

Table 3.1 shows the density values generated during the qualitative analysis for each code. For the security analysis processes, we can define three groups: First group of factors with values upper 5, second group of factors with values between 3 to 5, and finally third group of factors with values lower than 3.

Table 3.1 Density of codes related with risk factors using ATLAS TI

Factors	Density
Application domain	4
Attack surface	8
Interdependency	7
Scalability	4
Severity	5
Susceptibility	2
Type of attack	10
Type of device	3
Type of information	1
Uncertainty	0
Vulnerabilities	17

The first group of factors with greater relevance are the type of vulnerabilities (density =17), followed by the type of attack (density =10), then the attack surface (density =8) and finally interdependence (density =7). Second group have the factors: severity (density =5), followed by scalability (density =4), then application domain (density =4) and finally device type (density =3). The third group with the lowest

relevance values corresponds to the factors: type of information (density =1), followed by uncertainty or unknown factors (density =0).

3.1.2 Initial reference model.

Based on the eleven factors identified in the literature review, we analyse if them were covered in the previous work on IoT risks (See Table 3.2).

The proposal [23] evaluates the attack surface and interdependence on the parameters: Type of network (nwt), Type of protocol (prt), Heterogeneous system involved (het), but does not consider in detail the contributions of vulnerabilities and attack types. The Kandasamy proposal evaluates the severity in the Type of impact on the CIA (cia) parameter and the type of device in the Device security (des) parameter, but it does not consider the scalability and application domain factors. Reference [44] defines the attack surface in the parameters Dev (number of devices connected to the network, Sor (number of sensors), Svs (number of services and processes), Int (number of interfaces), and Prot (number of protocols or standards). However, the proposal does not detail the factors related with the impact of the cyberattack and their related factors such as type attacks, vulnerabilities, scalability.

Table 3.2 Factors considered in the proposals of IoT risk analysis.

Factors\Proposals	Kandasamy [23]	Toapanta [44]	Aydos [45]	Popescus [46]	Levitsky [47]
Application domain	Not covered	Not covered	Not covered	Not covered	Not covered
Attack surface	Covered	Covered	Covered	Covered	Covered
Interdependency	Covered	Covered	Not covered	Not covered	Not covered
Scalability	Not covered	Not covered	Not covered	Not covered	Not covered
Severity	Covered	Not covered	Not covered	Not covered	Covered
Susceptibility	Not covered	Not covered	Not covered	Not covered	Not covered
Type of attack	Not covered	Not covered	Covered	Covered	Covered

Type of device	Covered	Not covered	Not covered	Not covered	Not covered
Type of information	Not covered	Not covered	Not covered	Not covered	Not covered
Uncertainty	Not covered	Not covered	Not covered	Not covered	Covered
Vulnerabilities	Not covered	Not covered	Not covered	Covered	Not covered

The proposal [45] covers the attack surface based on risk assessment of threat processes/procedures for data security and criticality of attack surface layers. However, the proposal does not address vulnerabilities, attack types and impacts in detail. The proposal [46] covers the factors of vulnerability, attack surfaces, and types of attack. However, the proposal does not perform an analysis about how the calculation could be done in detail. Finally, the proposal [47] does not cover the vulnerabilities, and scalability in detail. However, the surface attack and type attacks are considered in the process of the evaluation of subcomponent scores for each of the attack categories.

The analyzed risk analysis proposals do not cover all the factors established in the literature review that could be associated with cyber-attacks and their impact. However, these proposals are effective in the contexts defined by the authors and could be taken as a basis for risk analysis in other contexts with IoT systems. Taking into consideration of the inclusion of other factors could support the increase in their effectiveness and accuracy of risk analysis methodologies.

Based on the literature review, an initial reference model for risk analysis is proposed (see Figure 3.10). The model considers as the main component the ***application domain*** e.g. health, education, transportation, energy, which **uses *IoT devices*** for its digital transformation processes. Several IoT devices can be used in the domain to **increase** the ***interdependency*** between IoT devices and IT and OT systems to increase the functionalities of IoT system. The interdependency also **increases** the ***attack surface*** and the ***scalability*** of attacks to other systems. Attacks can **use** the ***vulnerabilities*** and ***susceptibilities*** of IoT devices to enhance their effectiveness. Attacks can also **use** the large attack surface and scalability to create greater impact (***severity***) in their attack. The IoT device could be of different ***types*** and it **manages** different ***information*** according to its functionality in the application domain.

The proposed model considers the risk factors identified in the systematic literature review and possible relation among them. The relevance of the factors has been established based on the number of times (density) in which we identified the factor in the qualitative analysis. In this point, it is important to consider a possible bias because the papers analyzed could be focused on considering a specific factor from a perspective of the interest of analysis and publication by researches, rather than the fundament of that factor is relevant for the success of an attack and its implications on the impact on IoT systems. This could be the case of the factor vulnerability, which had the highest density in qualitative analyses.

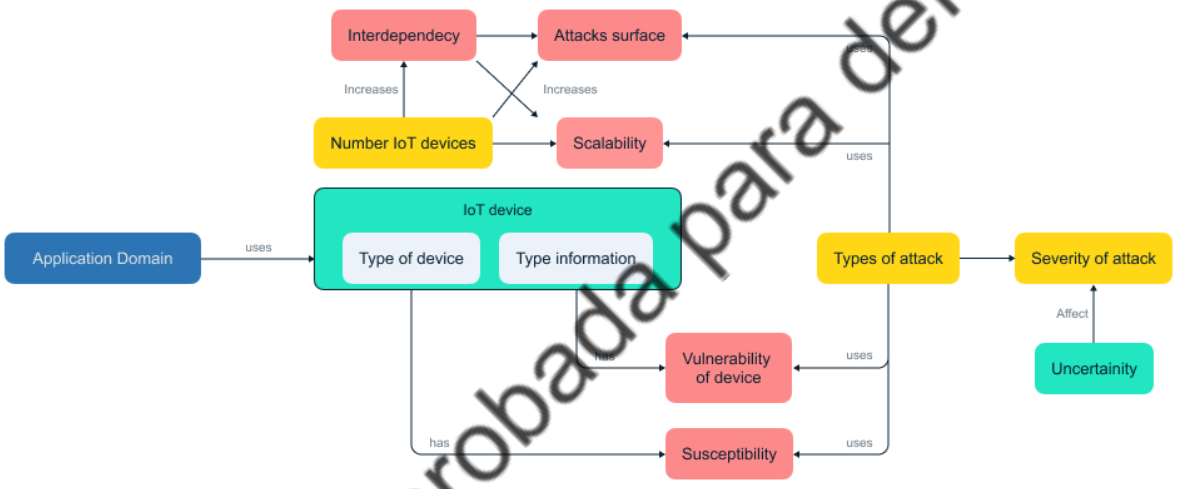


Figure 3.10 Initial reference model for risk analysis in IoT systems based on IoT device factors.

Based on the developed systematic literature review, we can highlight the following findings:

- A detail of the relation between factors has not been found. The main emphasis is the relation between cyber attacks and the vulnerabilities.
- Factors associated with uncertainty are not considered in the analysis of cyber attacks
- The dependency of IoT with other OT and IoT systems is mentioned, although their degree of relation among them and the possible impact of IoT attack to other systems are not detailed.
- The attack surface can exceed hundreds of devices or nodes, but there is not a detail about the impact or scalability of cyber attacks if a high percentage of nodes are affected.

- The relation between continuous attacks is not addressed. There is not a detail if one success attack could allow a second attack.

At this point, it would be interesting to know if the aforementioned factors are relevant to evaluate risk on IoT systems and if there is a relation among these factors.

3.2 Descriptive study I (Analysis)

This chapter comprises the second phase of the proposed research methodology i.e., "Descriptive Study I", in which an empirical analysis is carried out to define a general understanding of the main factors associated with the security risk in IoT devices. Based on the research clarification, we can identify the following possible factors that could affect the risk level of IoT devices (we have categorized the possible factors as hypotheses denoted by the letter H):

H1. Interdependency (inter-domain, inter-device).

H2. Application domain (agriculture, health, traffic).

H3. Type of information (sensitive, personal) of the IoT device.

H4. Type of IoT device (enterprise, home).

H5. Attack surface of the IoT device.

H6. Severity of the attack on the IoT device.

H7. Vulnerabilities of the IoT device.

H8. Level of scalability of the IoT attack (cascade effect).

H9. Level of susceptibility to specific attacks.

H10. Types of attacks

H11. Not known factors (Lack of knowledge, random).

Based on the qualitative analysis on research clarification, we can consider grouping the 11 factors into three major constructs: Severity, Susceptibility and Risk behaviors. In other words, the risk value will be given by the susceptibility of the systems to be attacked, the severity of the damage caused by cyber-attacks and the behavior of the attack in relation to the risk aspects (for example, if the effect of the

attack is temporary, if the scalability of the attack can cover a considerable area of nodes or systems or if there are unknown events such as the attacker deciding to interrupt the attack). So, we can define research items show in the Table 3.3, to guide our research to define the relation among factors. We are coding the research items to represent the values for the weight of the factors and the relation among them.

Table 3.3 Research items and codes to address the hypothesis (risk factors).

Construct	Hypothesis (risk factors)	Code	Research Items
Severity	H6. Application domain	S-A	Cyberattacks on IoT systems could affect to economic, social or environmental domains.
		S-A-P	Cyberattacks to IoT systems could be target to IoT solutions on health, energy, traffic, agriculture.
	H4. Interdependency	S-I-Sys	Cyberattacks to IoT systems could be affected to other IoT, IT and OT systems.
		S-I-nd	The growth of number of IoT devices could increase the probability of cyberattacks
	H7. Level of scalability	S-Scl	Cyberattacks on IoT systems could generate shock on markets or risk systemic events.
	H9. Level of susceptibility	S-Sc	Security configurations on IoT devices depends of domains or pillars where IoT devices will be used.
Susceptibility	H4. Interdependency	Sc-I-Sys	Interdependency of IoT device with other IoT, IT, and OT systems could increase the probability to attack IoT systems and cause bigger damage.
	H4. Attack surface	Sc-As-nd	The growth on the number of IoT devices could increase the susceptibility to suffer cyberattacks on organizations due to the large surface attack.
	H1. Vulnerabilities	Sc-V	Vulnerabilities on IoT devices could increase the probability of cyber-attacks to IoT systems
	H9. Level of susceptibility	Sc-Ta	IoT devices are susceptible to specific type of cyberattacks
	H2. Types of attacks	Sc-Ta2	Previous attack allows the execution of new attacks.
	H2. Types of attacks	Sc-Ta-L	Attacks could be executed on different layers.

	H8. Type of IoT device	Sc-Td	Security configurations on IoT device could increase the susceptibility to be attacked.
Risk behaviors	H5. Severity	Rb-Sv-Ta	Cyberattacks could generate degradation in the operation of IoT devices
	H5. Severity	Rb-Sv-Sr	Cyberattacks could affect to CIA on IoT systems.
	H7. Level of scalability	Rb-Scl	Cyberattacks could be scaled from one layer of IoT system to other one.
	H11. Factors not known	Rb-U-f	The frequency of cyberattacks could increase the successful of them.
	H11. Factors not known	Rb-U-Tp	Short times on the propagation of cyberattacks could increase the damage of cyberattacks.
	H7. Level of scalability	Rb-Scl-L	Cyberattack could affect different layers of IoT systems increase the surface of damage.

3.2.1 Instruments

The development of this phase is based in the development experiments due to that are instruments that allow produce immediate results in order to test behaviours in the object of research (IoT device), determine variables (factors) and identified relations between them.

Experiment Setup 1.

The Figure 3.11 shows a simulation of an IoT system of a smart home solution implemented using Phyton libraries. The lights are connected to the organizational network through a hub which allows the communication with IT devices such as computers, smartphones and voice assistants by connecting the hub with the router (gateway). The smart home solution has two voice assistants based on cloud services to control the lights.

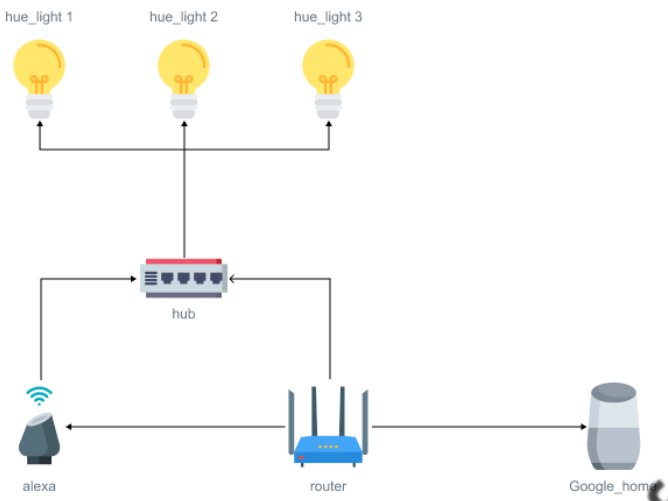


Figure 3.11 Simulated smart home scenario using Bayesian networks.

Experiment Setup 2.

We simulate a smart city with IoT nodes representing a smart home (SH), smart grid (SG), smart agriculture system (SA) and smart traffic management system (ST), how is shown in Figure 3.12. The scenario was simulated using a Bayesian network implemented in the software called Bayesian Server. The probabilities based on expert judgment are show in the Table 3.4.

Table 3.4 Simulated smart home scenario.

BD	AI	Cloud	IoT	ECO-F	ECO-T	ENV-F	ENV-T	SO-F	SO-T
False	False	False	False	0.571	0.429	0.6	0.4	0.615	0.385
False	False	False	True	0.606	0.394	0.645	0.355	0.385	0.615
False	False	True	False	0.612	0.388	0.675	0.325	0.604	0.396
False	False	True	True	0.392	0.618	0.452	0.548	0.404	0.596
False	True	False	False	0.459	0.541	0.429	0.481	0.444	0.556

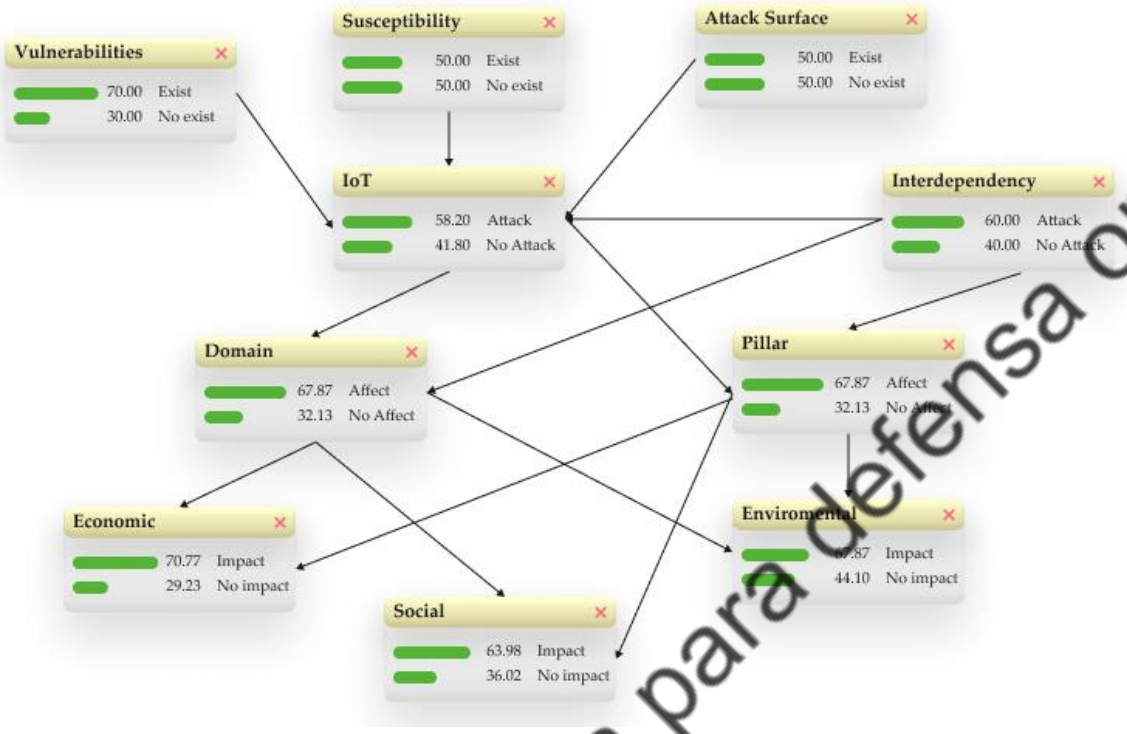


Figure 3.12 Simulation of the relation and probability of attacks to smart city.

Experiment Setup 3.

The simulated scenario is based on smart home attacks. The scenario is based on the work proposed by Dr.Mariam Wajdi Ibrahim, who simulated smart home attacks based on JKind and Graphviz [51]. The work shows that if an attacker could execute a specific attack for instance phishing, then the attacker could have the capability to execute DoS attacks. We replicated this scenario and added Bayesian probabilities. So, we can show that a type of attack can also have a relationship with other attacks which can generate a greater impact. Figure 3.13 shows a graph of the attacks, in which the following behavior can be visualized.

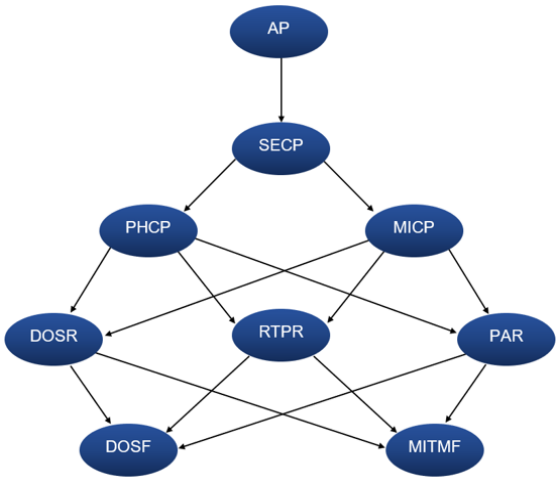


Figure 3.13 Simulated environment to smart home attacks.

Experiment Setup 4.

We propose a prototype to check the possible vulnerabilities in embedded systems based on Arduino Mega 2560 and Raspberry Pi 3B+. Figure 3.14 indicates the diagram and the elements used in the architecture. In the sensing (perception) layer, the following sensors were used: temperature, humidity, gas, and ultrasound. In the communication layer, a Raspberry pi 3B+, an Arduino Mega 2560 and a modem were used. In the application layer, we used applications to visualize the data delivered by the sensors.

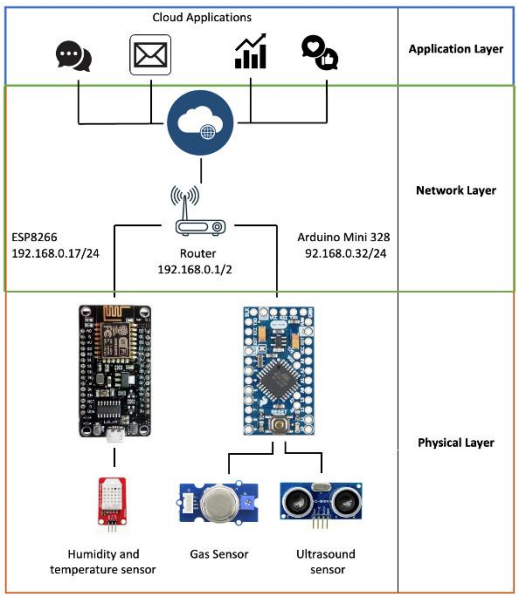


Figure 3.14 IoT application based on Raspberry and Arduino

Experiment Setup 5.

A smart home prototype has been developed by configuring the following devices: three Alexa devices, a Google home device, a WEMO switch, a fire tv and three lights Phillips (see Figure 3.15). The voice assistants allow us to perform the turn on and off of the lights and smart tv which are connected to the home's Wi-Fi network. The lights use ZigBee technology for communication with a hub which is connected to the home wireless router via network cable. The WEMO switch allows the switching on and off of electronic devices executing the commands delivered by voice assistants or mobile devices, The switch is connected to the home network using Wi-Fi. Finally, the fire tv device is connected to the home network using Wi-Fi. All devices are configured to be accessed by the virtual assistants from their management platform allowing them to send commands to control the status. Figure 3.16 shows communication messages between devices.

Figure 3.15 Smart home prototype.

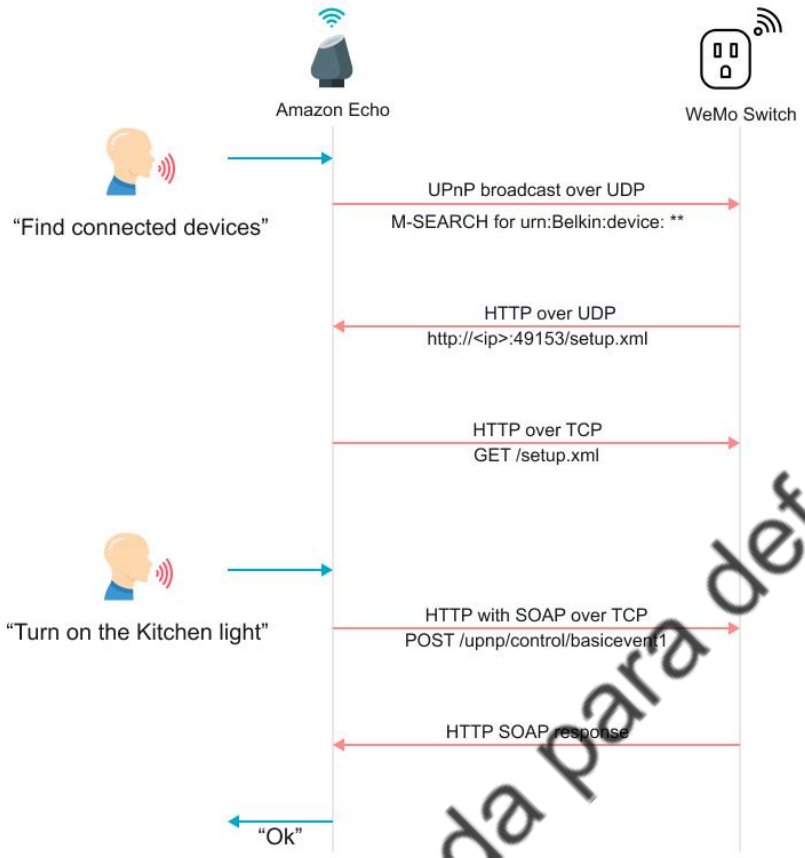


Figure 3.16 Smart home communication messages.

3.2.2 Procedure and Timeline

The experiments have been developed during the time period between 2018 and 2021. The experiments have not been carried in the same physical space due to restrictions in the access to laboratories due to the Covid-19 pandemic. Students and professors from different universities (EPN, UDLA) have contribute to the development of the experiments under the same supervision.

3.2.3 Analysis of the risk factors

To test these hypotheses and answer the research items, we development the experiments described in the instruments section to understand the risk factors such as: vulnerabilities, attack surface, impact on confidentiality, data integrity and availability, and types of attacks on the context of IoT systems.

Interdependency (inter-domain, inter-device).

Based on the result of experiment 1, from a security perspective, the interconnection allows the attack to two different systems at the same time, the attack to IT system (computers, printers, smartphones) and the IoT system (smart lights,

smart locks, voice assistants). If an attacker decides to attack a node of the IT system such as the router, the attacker could later attack any of the lights in the smart home. Also, it could be a scenario in the opposite direction where an attacker decides to attack a virtual assistant and then attack an IT system node. To illustrate the interdomain relation with the probability of attack, we have used the proposed simulation using a Bayesian network. The selection of a Bayesian network has been done based on the fact that we have a stochastic process where we have no prior knowledge of attacks. The simulation was performed in the Google collaborate platform using phyton. We have defined the IoT nodes as R = router, G = google home, A = Alexa, H = Hub, L (1,2,3) = Lights, and assigned an attack probability how is shown in the Table 3.5 which are based on expert judgment, where T = True (when attack exists) and F = False (when attack does not exist).

Table 3.5 Conditional probability table (CPT) for IoT attacks

Devices	Conditional probability value
P(R=T) **P(R=F)**	0.65 0.35
P(G=T|R=T) **P(G=F|R=T)** **P(G=T|R=F)** **P(G=F|R=F)**	0.75 0.25 0.20 0.80
P(A=T|R=T) **P(A=F|R=T)** **P(A=T|R=F)** **P(A=F|R=F)**	0.82 0.18 0.3 0.7
P(H=T|R=T,A=T), P(H=F|R=T,A=T) **P(H=T|R=T,A=F), P(H=F|R=T,A=F)** **P(H=T|R=F,A=T), P(H=F|R=F,A=T)** **P(H=T|R=F,A=F), P(H=F|R=F,A=F)**	0.9, 0.1 0.7, 0.3 0.8, 0.2 0, 1
P(L1=T|H=T) **P(L1=F|H=T)** **P(L1=T|H=F)** **P(L1=F|H=F)**	0.95 0.05 0 1
P(L2=T|H=T) **P(L2=F|H=T)** **P(L2=T|H=F)** **P(L2=F|H=F)**	0.95 0.05 0 1
P(L3=T|H=T) **P(L3=F|H=T)** **P(L3=T|H=F)** **P(L3=F|H=F)**	0.95 0.05 0 1

The equation 3.1 shows the probability of an attack on an Alexa device. The attack to Alexa device depends of the attack to the router on the first place. In this case, we

are not considering attacks coming from Alexa cloud services. The probability of attack to Alexa device from the route is 63.8%.

$$P(A = T) = \quad P(A = T|R = T) \cdot P(R = T) + P(A = T|R = F) \cdot P(R = F)$$

$$P(A = T) = \quad 0.82 \cdot 0.65 + 0.3 \cdot 0.35$$

$$P(A = T) = \quad 0.638$$

Equation 3.1. Probability of attack to Alexa

We can observe that there is a higher probability of an attack to an Alexa device if the router is previously attacked, even if these two devices do not have a direct physical connection; an attack is possible due to the **cybernetic** and **geographical** dependence. Now, we can go one step further, In the Figure 3.17, we can see the probabilities of attacks to different nodes based on values established on CPT, the attacker could also attack directly from the router to any of the lights with a probability of 61.3%, but if the attacker has access to the Alexa device (see code 3.1), the attacker could perform an attack to any light with a probability of 83.93% (see Figure 3.18).

```
0|router|attack,no_attack
0=attack|0.65000
0=no_attack|0.35000
---------------------->
1|google_home|attack,no_attack
1=attack|0.55750
1=no_attack|0.44250
---------------------->
3|hub|attack,no_attack
3=attack|0.64560
3=no_attack|0.35440
---------------------->
4|hue_light1|attack,no_attack
4=attack|0.61332
4=no_attack|0.38668
---------------------->
5|hue_light2|attack,no_attack
5=attack|0.61332
5=no_attack|0.38668
---------------------->
6|hue_light3|attack,no_attack
6=attack|0.61332
6=no_attack|0.38668
---------------------->
2|alexa|attack,no_attack
2=attack|0.63800
2=no_attack|0.36200
---------------------->
```

Figure 3.17 Probabilities of attack to Alexa device.

```
# convert the BBN to a join tree
join_tree = InferenceController.apply(bbn)

# insert an evidence attack of alexa
ev = EvidenceBuilder().with_node(join_tree.get
_bbn_node_by_name('alexa')).with_evidence('att
ack', 1.0).build()
```

Code 3.1 Probabilities of attack to IoT devices based on Bayesian model.

The probability of attack on IoT devices (lights) from another IoT device (alexa) is possible because there is a **functional** dependency that requires connection between these devices.

```
0|router|attack,no_attack
0=attack|0.83542
0=no_attack|0.16458
---------------------->
1|google_home|attack,no_attack
1=attack|0.65948
1=no_attack|0.34052
---------------------->
3|hub|attack,no_attack
3=attack|0.88354
3=no_attack|0.11646
---------------------->
4|hue_light1|attack,no_attack
4=attack|0.83937
4=no_attack|0.16063
---------------------->
5|hue_light2|attack,no_attack
5=attack|0.83937
5=no_attack|0.16063
---------------------->
6|hue_light3|attack,no_attack
6=attack|0.83937
6=no_attack|0.16063
---------------------->
2|alexa|attack,no_attack
2=attack|1.00000
2=no_attack|0.00000
---------------------->
```

Figure 3.18 Probabilities of attack to IoT devices based on evidence of attack to Alexa.

Now, we will analyze a larger scenario based on experiment 2. In the case of a smart city, we have IoT nodes representing a smart home (SH), smart grid (SG), smart agriculture system (SA) and smart traffic system (ST). In this scenario, our previously

attacked smart home has a 47.80% of probability of attack and there is a 37.5% of probability of affecting economic, social or environmental aspects of a city (see Figure 6.2). Focused on a deeper analysis, we can observe that in our simulated scenario, the Bigdata, Cloud, AI and IoT resources, are the same for smart homes (SH), smart grids (SG), smart traffic (ST) and smart agriculture (SA) infrastructures: this is called **downstream dependency**. Also, SH, SG, ST and SA have **logical interdependencies,** although there is not a physical connection among them. They are connected through of Bigdata, Cloud, AI and IoT resources. Ideally, from a security point of view, although the same pool of resources is used, there should be a logical segmentation between SH. SA, ST and SG domains. And this would be the point of interest to evaluate in service provider during risk assessment.

IoT-based solutions are made up of a set of interconnected IoT devices that allow the exchange of information to perform a given action. In this analysis, we can assume that there is an interdomain relationship (IT system, IoT system, OT system) for the probability of success of an attack and so is the damage coverage. At this point, to model the Bayesian network for evaluating the relation intra/inter domain, we need to establish of the following values:

- The a priori attack probability weights that allow us to calculate the conditional probabilities.
- The weight of the correlation among IT/OT/IoT systems and the economic, social or environmental impact value.
- These values could be based on expert judgment or through simulations.

Application domain (agriculture, health, traffic).

IoT solutions are developed based on the needs and functionalities of each domain: agriculture, health, traffic, healthcare, energy, among others as is show in Figure 3.19. From a security perspective, each domain has certain factors that can influence the level of risk an IoT device brings. For instance, in the case of smart parking, IoT solutions can be designed based on the use of floor sensors that can be located in open spaces, which increases the susceptibility to attacks at the physical layer level.

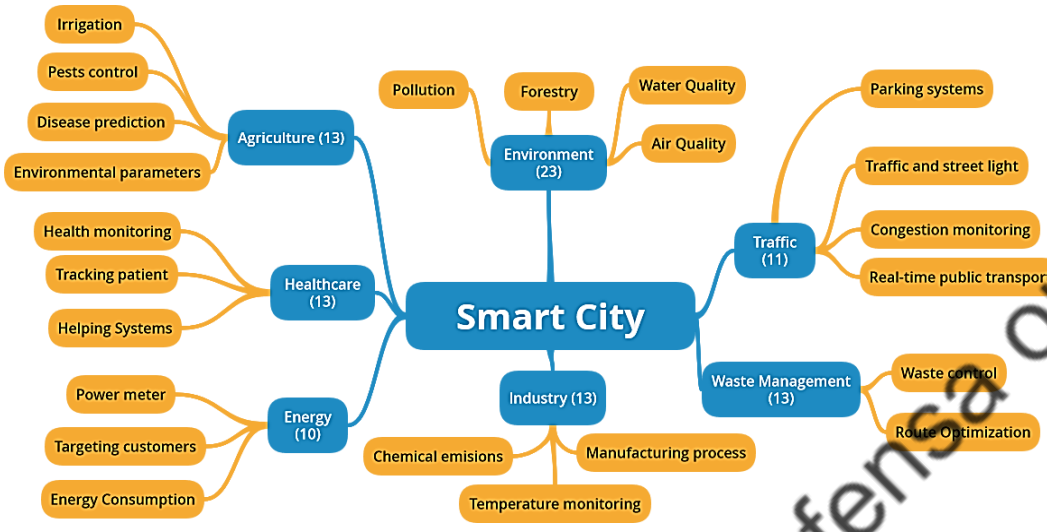


Figure 3.19 Application of IoT on smart city domains.

Type of information (sensitive, personal) of the IoT device.

In the case of solutions focused on healthcare, the type of information is more of the kind “sensitive”, with information of the person, health status, medicines, among others, while in the case of waste management systems, the type of information may be less relevant. The experiment 5, which includes two Alexa devices, a Google home device, three hue lights and a WeMo electrical switch has the objective of testing the environment to obtain sensitive information such as credit card data or personally identifiable identification. For this test, we have used Wireshark and performed a data capture inside the network. Alexa had credit card data and Hue had information about the name of the light and its status (on/off). It was possible to identify the data coming from the IoT devices such as IP, identification, MAC addresses, but both Alexa and Hue used encryption. Although the type of information managed by Alexa and Hue differs, the security level of Hue is relatively good compared to Alexa because it has encryption and authentication mechanisms. The type of information managed by a device does not define the security level of the device but it defines a motivational factor for an attack. In this sense, two aspects to consider are:

- The type of information of a device could generate a level of attraction to the attacker, which increases the probability of device for being attacked.
- It is relevant to evaluate the risk considering the security mechanism implemented in the device which protects the information.

Type of IoT device (enterprise, home).

One factor that has driven the growth of IoT is that users can develop their own IoT devices by using embedded devices such as Arduino or Raspberry. For the test scenario, we have used an Alexa hub and an Alexa device implemented on a Raspberry Pi. The functionalities of the two devices are similar; the voice responses work properly and there is the level of encryption with Amazon cloud. It could be inferred that the security of the Raspberry-based IoT device has an adequate level of security in its application and communication layer. However, the problem is presented in the security at the device level, the Raspberry (with its default configuration in its operating system) has open ports such as 23 (Telnet), 22 (SSH) 80 (http), 443 (https) and 5960 (VNC). Additionally, the device maintains the default credentials created at the time of installation. These two aspects increase the probability of a successful attack on the Alexa device built in a home environment.

Under this context, a group of students from the Escuela Politécnica Nacional taking the course “Optative Professional III” were asked to develop an automation solution using Raspberry Pi, having as results that 90% of the solutions had default credentials and the closing of unused ports was not performed. The solutions developed have not considered the principles of security in design, generating that the products developed under a home-made approach did not comply with an adequate level of security compared to the products delivered from the commercial approach.

At this point, it could be inferred that the solution requires hardening process of the Raspberry Pi device to improve its security level. So, the problem there is not the Raspberry device or the design of the home solution, is more focus on the use of security mechanisms in the devices.

Security requirements of IoT device

Security requirements for IoT devices are aboard by two relevant proposals:

- Security classes proposed by The Internet Engineering Task Force (*IETF*) in the RFC 7228.
- Security levels proposed by OWASP in the ISVS methodology.

Table 3.6 shows five compliance classes of IoT device that have been defined based on security requirements. Class 0 considers a low impact to the confidentiality, integrity and availability. Class 1 considers that the impact may occur, and it has a major impact on integrity and availability. Class 2 considers a significant impact to the availability. Class 3 focuses on sensitive data protection. Finally, Class 4 considers a critical impact to confidentiality, integrity and availability.

Table 3.6 Types of compliance class for IoT devices based in CIA.

Compliance Classes	Description
Class 0	An imperceptible impact could happen in the IoT system
Class 1	The impact that could occur on the IoT systems is limited
Class 2	Besides to class 1, the IoT system withstands significant impacts to availability.
Class 3	Besides to class 2, the IoT system protect sensitive data
Class 4	Besides to class 3, data compromise and loss of control of control the impact of critical IoT system

The proposal created by OWASP is based on the following security levels:

Level 1. The goal of level one requirements is to provide protection against attacks that target software only, i.e., attacks that do not involve physical access to the device. Level one requirements aim to provide a security baseline for connected devices where physical compromise of the device does not result in high security impact.

Level 2. The goal of level two requirements is to provide protection against attacks that go beyond software and that target the hardware of the device. Devices that adhere to level two requirements are devices where compromise of the device should be avoided.

Level 3. The goal of level three requirements is to provide requirements for devices where compromise should be avoided at all costs. Devices where there is highly sensitive information stored on the device or where compromise of the device can result in fraud.

Related to the OWASP proposal, the following concerns are raised in the ISVS methodology development group:

- The level L1, L2, L3 could be subjective depending on the internal risk practices and criteria of acceptation of mitigation.

- The evaluation of the security of a product to determine if it is a level L1, L2 or L3 device should be based on capabilities of the product.
- The evaluation of security should be based on the products but considering the production environment.
- A categorization of devices should be established based on their area of application e.g. medicine, energy, among others.
- The L1, L2 or L3 levels should be adjusted to NIST IR 8259, IEC 62443-4-1 and EN 303 645 recommendations.

Under this context, both proposals classes and levels are based on the type of information and the application domain of the IoT device.

Attack surface of the IoT device.

In IoT systems, the attack surface can be extended to the different layers of the IoT model, for example, based on the proposal of three IoT layers: perception, network and application. Each layer has protocols, technologies and topologies that can be exploited by attackers. For instance, the perception layer includes sensors that allow the abstraction of physical variables to digital values. In some cases, the sensors can be in spaces outside the organization such as streets for smart traffic or open spaces such as crop fields in the case of smart agriculture, this location can make IoT devices more susceptible to physical attacks, where the attacker can gain JTAG or UART access to the device and perform different types of attacks such as information stealing or man-in-the-middle attacks.

Attack surface modeling is based on the analysis of the possible entry and exit points of a system that can be exploited by an attacker and is generally defined based on three elements: data, channel, and method. Establishing an IoT attack surface model can be challenging due to the heterogeneity of devices, technologies and protocols used. Additionally, the interconnectivity of IoT solutions creates an environment with multiple entry and exit points that can be complex and time consuming to evaluate the levels of risk. In our case, we have defined the modeling of the IoT attack surface based on the security requirements that should be accomplished at each IoT layer to maintain an adequate level of security risk for experiment 4 (see Table 3.7).

Table 3.7 Attack surface of IoT based on security-layer approach.

Layer	Process	Type
Physical	Secure and centralize records	Data
	Encrypted communication protocols	Channel
	Strong and secure passwords	Method
	Last stable firmware or operating system version	Method
Communication	Monitoring of communication protocols	Method
	Ports used in a range different for the known ports	Channel
	Protocols used have encryption	Channel
	Separate wireless network	Channel
Application	Safe coding practices	Method
	Explicit error checking for all internal development software	Method
	Adquired software support	Method
	Up-to-date and trusted third-party component	Channel
	Encryption of tested and standarized algortihms	Method
	Personnel trained in secure software development	Method
	Static and dynamic code analysis	Channel
	Separate production and non-production systems	Method
	Web application firewall	Channel

The non-compliance of security requirements could expand the attack surface. For example, IoT devices that use ports outside the range of known ports could affect the selection of security controls, because we do not know how a normal pattern for theses ports. This opens and increase the IoT surface attack to the possibility of receiving attacks these ports if the appropriate security mechanisms are not put in place.

We have used a distribution of kali Linux to detect possible open ports used by default. Executing the command nmap -sV “ip address”, we have founded the following open ports in Raspberry PI: 22 (SSH), 80 (http) and 5900 (VNC) and the port 80 (http) in Arduino. In this point, we can observe that our IoT devices are using port with no encryption channel by default as is shown int he Figure 3.20.

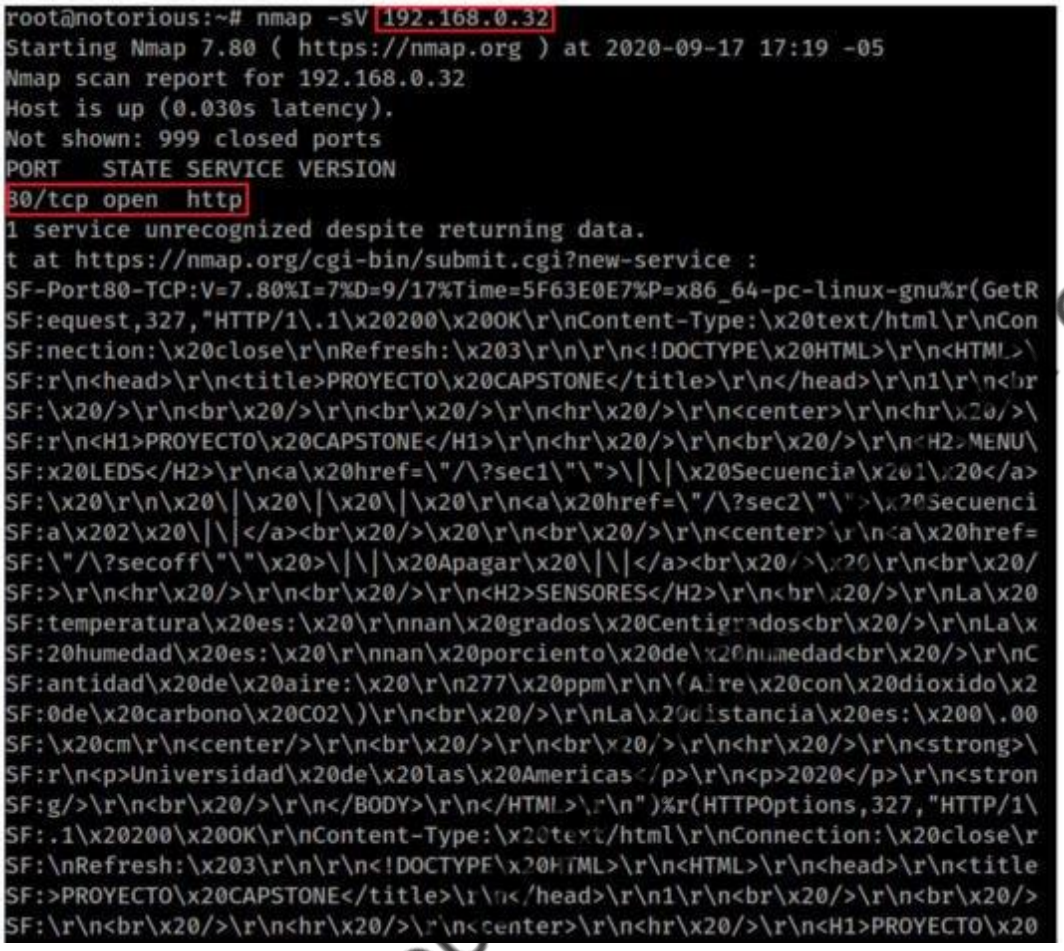


Figure 3.20 Scanning of open ports on raspberry using Kali Linux.

Then, we have used the Nessus tool to detect vulnerabilities associated with the open port 80 (http) and we founded the following vulnerabilities, as shown in Table 3.8.

Table 3.8 Vulnerabilities detected using Nessus tool.

IP	CVE	CVSS	Risk	Port Protocol	Vulnerability
192.168.0.17	CVE-2019-5798	9.8	Critical	80 TCP	phpMyAdmin 4x < 4.8.5
	CVE-2019-11768	9.8	Critical	80 TCP	phpMyAdmin 4x < 4.8.6
	CVE-2019-9517	9.1	Critical	80 TCP	Apache 2.4 x >2.4.41
	CVE-2019-5504	8.8	High	80 TCP	phpMyAdmin 4x < 5.0.1
	CVE-2019-0220	7.8	High	80 TCP	Apache 2.4 x >2.4.39
	CVE-2019-12616	6.5	Medium	80 TCP	phpMyAdmin 4x < 4.9.0

We can observe that, in our prototype, there are vulnerabilities in communication layer and application layer. We have not considered the device layer vulnerabilities in our experiment since we have taken in consideration that there is not a tampering enclosure attack to UART or JTAG ports. Under the above context, the attack surface of an IoT system will be constructed based on the contribution of each of the three layers of the IoT model.

Severity of attacks on IoT devices.

The cyber attack can affect three security components: confidentiality, integrity and availability. We could evaluate the severity of the attack in relation to the degree of affectation of these components. Each cyber-attack can affect the integrity, availability and confidentiality components in different values. The severity value would be calculated considering the impact values produced by each attack. Additionally, cyber attacks generate a level of impact to each layer of the IoT system as is shown in the Table 3.9.

Table 3.9 Impact Score for IoT layers.

Layer	Step	Probability	Compliance Class Score	Risk
Perception	1	4	5	9
	2	4	5	9
	3	4	5	9
	4	0	1	1
Network	5	2	5	7
	6	4	5	9
	7	3	4	7
	8	4	4	8
Application	9	4	5	9
	10	4	5	9
	11	0	1	1
	12	0	1	1
	13	4	5	9

Taking into consideration that it is not possible to determine all the possible effects, an approximate value could be established. Another perspective to evaluate the severity of attacks could be focused on the social, economic and environmental domains. So, the severity of the attack can be considered on two axes:

- Over the infrastructure that supports the IoT solution.
- Over the economic, social and environmental domains supported by the IoT solution.

Values of level of affectation could be determined based on expert judgment.

Vulnerabilities of the IoT system.

IoT devices present vulnerabilities that can be exploited for the execution of attacks. To assess the criticality of vulnerabilities, there are several databases such as the ones developed by CERT and NIST (NVD), which provide a mechanism to establish a weight of vulnerabilities. Common vulnerability scoring system (CVSS) in its current version 3 is one of the most widely used to establish the weight of vulnerability in a device and it can be used also for IoT systems. Based on the experiment 4, we have developed a vulnerability scan of IoT device which is found in Table 3.10.

Table 3.10 Vulnerabilities found using CVSS.

IP	CVE	CVSS	Risk	Port Protocol	Vulnerability
192.168.0.17	CVE-2019-5798	9.8	Critical	80 TCP	phpMyAdmin 4x < 4.8.5
	CVE-2019-11768	9.8	Critical	80 TCP	phpMyAdmin 4x < 4.8.6
	CVE-2019-9517	9.1	Critical	80 TCP	Apache 2.4 x >2.4.41
	CVE-2019-5504	8.8	High	80 TCP	phpMyAdmin 4x < 5.0.1
	CVE-2019-0220	7.8	High	80 TCP	Apache 2.4 x >2.4.39
	CVE-2019-12616	6.5	Medium	80 TCP	phpMyAdmin 4x < 4.9.0

As mentioned, IoT devices are composed of layers, and in each of them there are vulnerabilities that increase the susceptibility of attack. There can be many vulnerabilities in an IoT device, so a good practice is to consider those that have the greatest influence on the system. An alternative is to rely on proposals such as the OWASP one which establishes a top ten of IoT vulnerabilities (see Table 3.11).

Table 3.11 Vulnerabilities in IoT based in OWASP top-ten

OWASP IoT Top 10 vulnerabilities	Compliance Class Score	Probability	Risk Result
Weak, guessable, or hardcoded password	5	4	9
Insecure network services	3	4	7
Insecure ecosystem interfaces	5	3	8
Lack of secure update mechanism	1	1	2
Use of insecure or outdated components	4	3	7
Insufficient privacy protection	5	3	8
Insure data transfer and storage	3	3	6
Lack of device management	5	1	6
Insecure default settings	5	4	9
Lack of physical hardening	5	3	8

Level of scalability of the attack (cascade effect).

Based on the experimentation of scenario 1, the attack on a smart home node (for example to Alexa) would allow attacker to execute an attack to second or third node (for example the lights). A similar scenario occurs in experiment 2. The attack on a smart grid node could allow a second attack on a smart traffic node. This aspect of scalability, that is present in IoT systems, can allow that an attacked to a node continue with an attack to other interconnected nodes, generating a cascade effect. If the number of nodes is high the attack could generate a systemic risk with the capability of leaving critical infrastructures of the cities inoperative and generate a high economic impact (financial shock). The scenario of experimentation 3 proposes that if an attack is executed on an IoT node, for example phishing, a second attack could be executed from it, for example man-in-the-middle (MITM), and the event could produce a third attack for example Denial of Service (DoS). In this context, there is a scalability in the number of attacks that could be executed after the success of a first attack.

Level of susceptibility to specific attacks.

The susceptibility of attacks depends on the existing vulnerabilities and the techniques used by the attackers. We can observe from the experiments that IoT devices can be victims of different types of attacks such as DoS, MITM, ransomware and even could be used as a pivot for make attacks such as DDoS or phishing.

Type of attacks to IoT devices

Based on the experiment 2 using Bayesian networks, we have performed a correlation analysis of data about ransomware and DDoS attacks against the impact on economic and social aspects (See Figure 3.21). The values show a strong relation of attacks with their impacts.

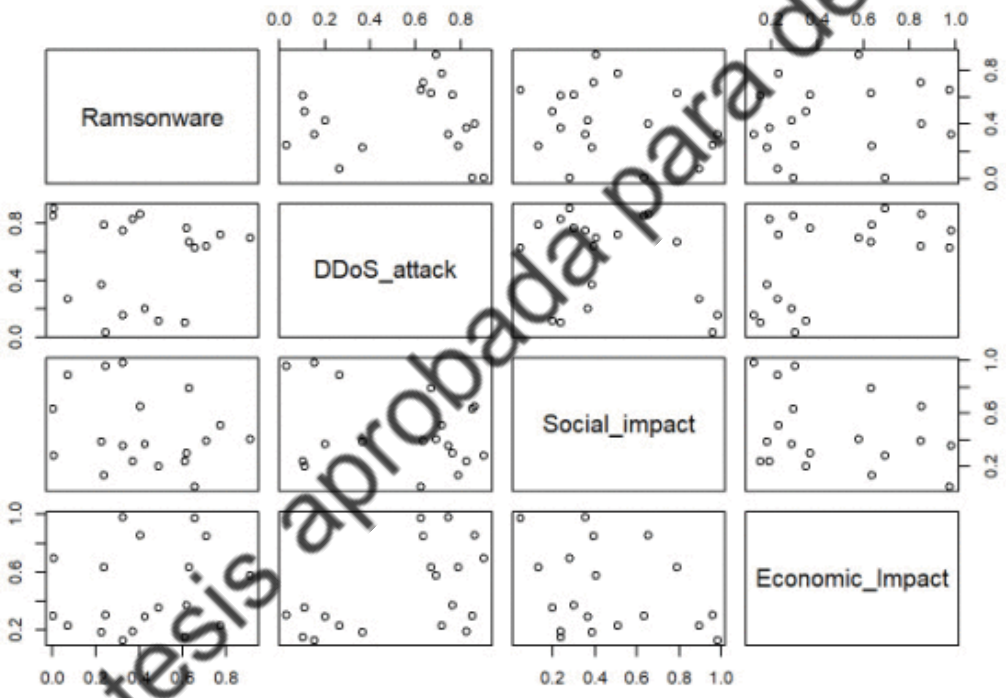


Figure 3.21 Correlation of cyber attacks based on Bayesian simulation.

Based in the analysis of a real scenario, occurred to American oil pipeline system, in which the company agreed to a payment of 75 bitcoins valued at USD$5M due to ransomware attack, because several citizens could not get fuel for two days, generating long queues of vehicles at gas stations, we can see the impact on economic and social aspects of a cyber attacks. Under this context, we can make two conjectures:

- Relationship of the attack with social, economic, environmental impacts.
- Relationship of the attack with other attacks.

Not known Factors (Lack of knowledge, random).

Uncertainty is a relevant factor in security risk assessment processes. There can be uncertainty about the type of attack, the time in which the attack will be taken place, the duration of the attack and the target of the attack (random uncertainty). From a game theory perspective, security management is an imperfect game, i.e., there is no complete information about the adversary (lack of knowledge).

3.3 Summary and Implications

Based on the results of experimentation, Table 3.12 was created which show the research items that could be validate with the proposals experiments and based in these findings a new model of the factors of risk of IoT devices that includes economic, social and environmental aspects, and the relationships between the application domains and pillars, and IT/OT systems is show in the Figure 3.22.

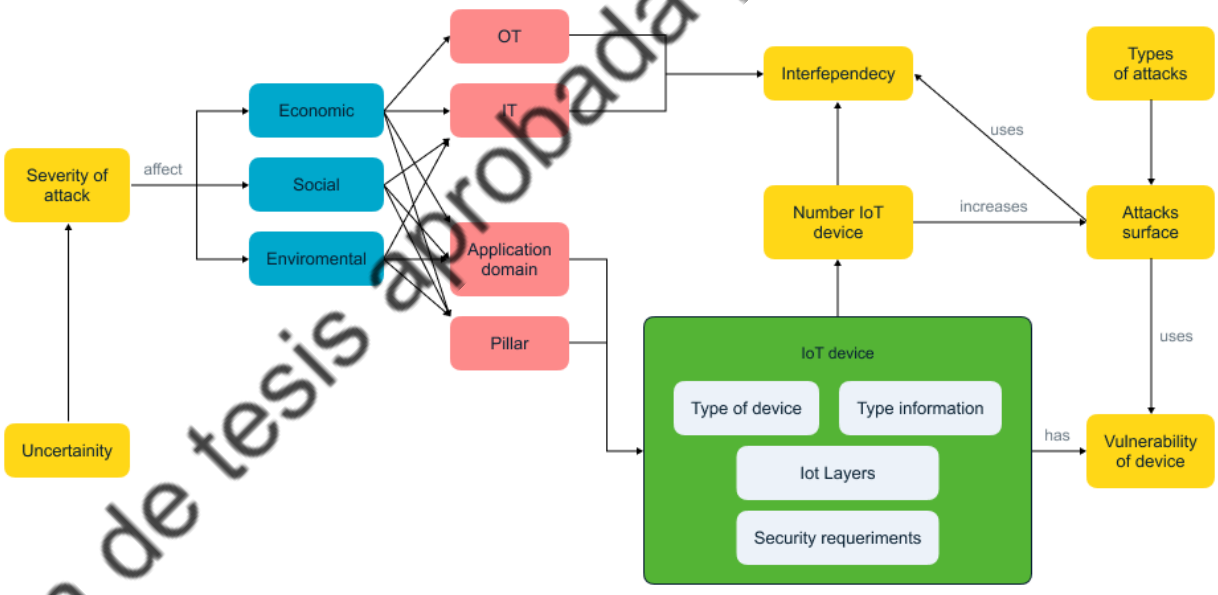


Figure 3.22 Proposal of IoT security risk components based on Descriptive Study I.

Table 3.12 Verifiable means for research items.

Research Items	Verifiable means	Relation
Cyber attacks on IoT systems could affect to economic, social, or environmental domains.	Experiment 1 Experiment 2	S-A
Cyber attacks to IoT systems could be target to IoT solutions on health, energy, traffic, agriculture.	Experiment 1 Experiment 2	S-A-P
Cyber attacks to IoT systems could be affected to other IoT, IT and OT systems.	Experiment 1	S-I-Sys
The growth of number of IoT devices could increase the probability of cyberattacks	Experiment 1	S-I-nd
Cyber attacks on IoT systems could generate shock on markets or risk systemic events.	No verifiable	S-Scl
Security configurations on IoT devices depends on domains or pillars where IoT devices will be used.	Experiment 1 Experiment 3	S-Sc
Interdependency of IoT device with other IoT, IT, and OT systems could increase the probability to attack IoT systems and cause bigger damage.	Experiment 3 Experiment 4 Experiment 5	Sc-I-Sys
The growth on the number of IoT devices could increase the susceptibility to suffer cyberattacks on organizations due to the large surface attack.	No verifiable	Sc-As-nd
Vulnerabilities on IoT devices could increase the probability of cyber attacks to IoT systems	Experiment 4 Experiment 5	Sc-V
IoT devices are susceptible to specific type of cyberattacks	Experiment 1 Experiment 3	Sc-Ta
Previous attack allows the execution of new attacks.	Experiment 3	Sc-Ta2
Attacks could be executed on different layers.	Experiment 4	Sc-Ta-L
Security configurations on IoT device could increase the susceptibility to be attacked.	Experiment 4 Experiment 5	Sc-Td
Cyber attacks could generate degradation in the operation of IoT devices	No verifiable	Rb-Sv-Ta
Cyber attacks could affect to CIA on IoT systems.	Experiment 3 Experiment 4 Experiment 5	Rb-Sv-Sr

Cyber attacks could be scaled from one layer of IoT system to other one.	Experiment 4	Rb-Scl
The frequency of cyberattacks could increase the successful of them.	No verifiable	Rb-U-f
Short times on the propagation of cyber attacks could increase the damage of cyberattacks	No verifiable	Rb-U-Tp
Cyber attack could affect different layers of IoT systems increase the surface of damage.	Experiment 1 Experiment 2 Experiment 3	Rb-Scl-L

CHAPTER 4

4. PRESCRIPTIVE STUDY AND DESCRIPTIVE STUDY II

This chapter is based on the third and four phases of DRM, that comprises the prescriptive study for establishing a support to the understanding generated in the previous phases. The prescriptive study uses instruments such as experiments and judgements of experts to address the assumptions related with the security risks factor on IoT devices (Section 4.1).

4.1 Prescriptive study

The Figure 4.1 shows the status of DRM and how judgements of experts and experiments are used to demonstrate the hypothesis to get a methodology for security risk analysis in the IoT context.

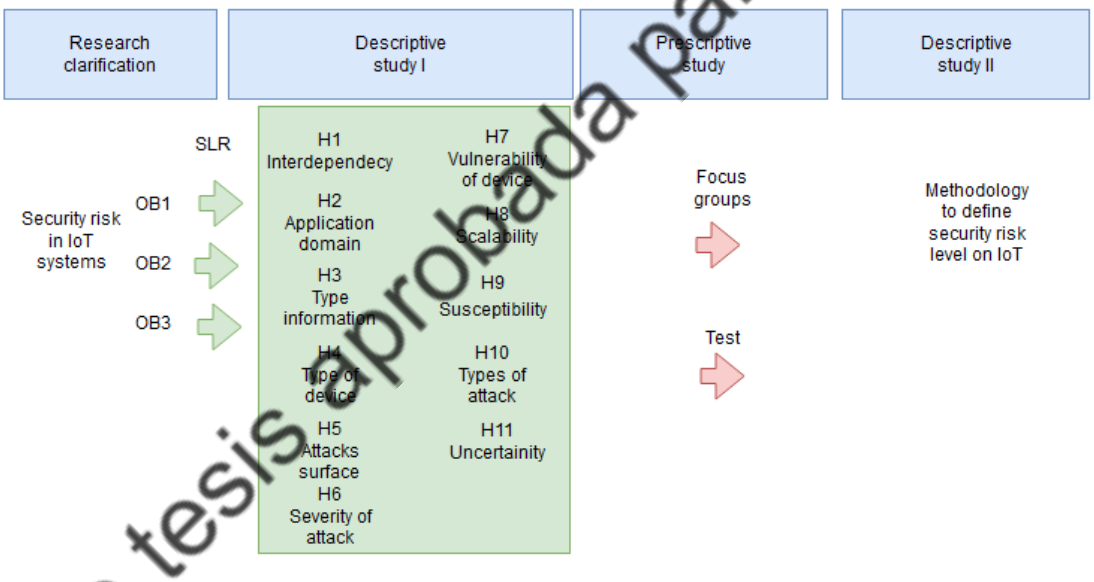


Figure 4.1 DRM status for prescriptive study.

To develop the judgments of experts, we have generated a set of assumptions that will be consulted to a group of experts for their opinion if they think that such assumptions are relevant in the risk assessment process. For the experimentation phase we have proposed to analyze one of the risk analysis methodologies to identify how the proposals assumptions are addressed for the risk methodology. We have selected MAGERIT for the experiment based on the following aspects:

- It is a methodology widely used in different countries to assess security risk.

- It is specifically focused on the security of information and technological systems.
- It includes items related to vulnerabilities, threats and assets for risk assessment, making it a technically complete methodology for security risk analysis.
- There are guides on the use of the methodology.

On the basis of risk factors of IoT devices from the Descriptive Study I, we have identified the following assumptions related with the relation of the proposed factors on IoT systems.

Assumption 1

The risk value will depend on the probability of that the threats can be capitalized in IoT systems but also related to the type of systems such as IT and OT. The probability of impact of the threat will be in function of the contribution of the probability of its occurrence in each of the aforementioned systems.

Assumption 2

The values of risk, severity and probability will depend on the level of dependence and interdependence among IT, OT and IoT systems.

Assumption 3

The risk and severity values will depend on the relationship of the IT, IoT and OT systems with the social, economic, and environmental pillars that are supported by the IoT solutions.

Assumption 4

The risk value will depend on the type of information in the IoT device, its physical location and the application that the IoT solution is supporting.

Assumption 5

The risk value will depend on the security controls that are put in place to protect the information of the IoT device.

Assumption 6

The risk value will depend on the type of the attacks on the social, economic and environmental pillars supported by the IoT solution.

Assumption 7

The risk value will depend on the number of attacks on IoT systems and the relationship these attacks may have to improving their effectiveness.

Assumption 8

The risk value will depend on the value of surface attack and vulnerability score of the IoT system.

To evaluate these assumptions, we have developed a survey based on 10-point scale using Google Forms, where the research items and assumptions were the 27 questions of the survey. The details of all questions is presented in the Annex 1. The goal was to get the opinion of minimum 10 experts in the field of cybersecurity to build the weight of factors and their relations. We obtained 13 responses from security experts. About this point, we expected to get more security experts for the survey but some of them mentioned that they did not have knowledge in the field of IoT security and denied their participation in the survey- This is not a complete limitation for the study because our expectation were get the minimum of 10 security experts to build a matrix of 10X 270 for the use of PCA (Principal Component Analysis) and MCDA (Multicriteria Decision Analysis) to continue our analysis; both types of analysis are used for the evaluation of factors on risk assessment in different fields such as aeronautic or cloud computing [52]. The size of our data is small, and the correlation matrix is a Not Positive Definite Matrix; this could be a limitation in the case of using PCC or SEM (Structural Equation Models) for future works. From the data obtained, we have performed a Principal Component Analysis (PCA) using the software SPSS (see Figure 4.2). The PCA is used for exploratory analysis; for this reason, the number of factors for extraction is 27 which is equals to the number of questions of the survey.

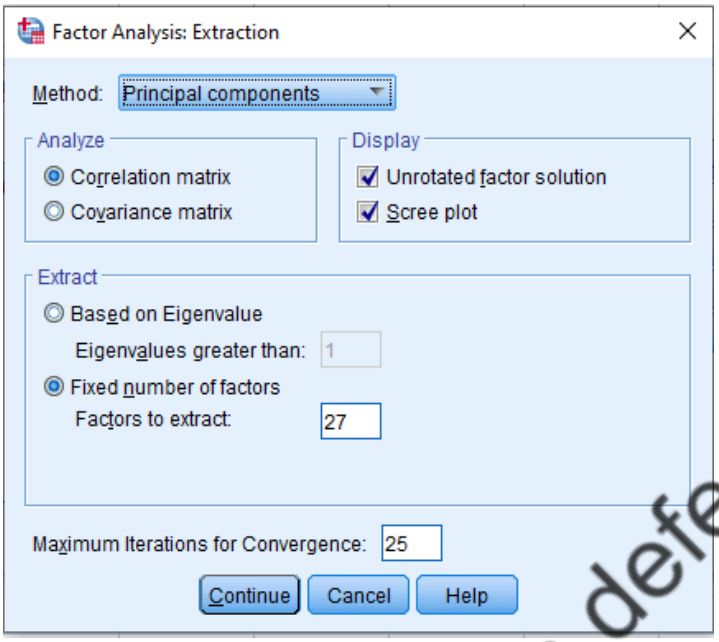


Figure 4.2 Setup of factorial analysis in the SPSS to extract principal components.

Analyzing the graph of sedimentation in Figure 4.3, which was created by SPSS from our data, the number of relevant factors is equal to seven. This mean that there are seven theorical constructs which accumulated the total of variance of our questions, in our case research items and assumptions.

Table 4.1 was obtained from SPSS and it shows the variance for the seven main components. Since the contribution of variance of components 8 to 27 is poor, they are not considered for the rest of our analysis. The first construct explains the 54 percent of the variance, the second contributes with the 12.39% of the variance, the third contributes 11.92% of the variance, the fourth contributes 7.18% and so on, how it is shown in Figure 4.4.

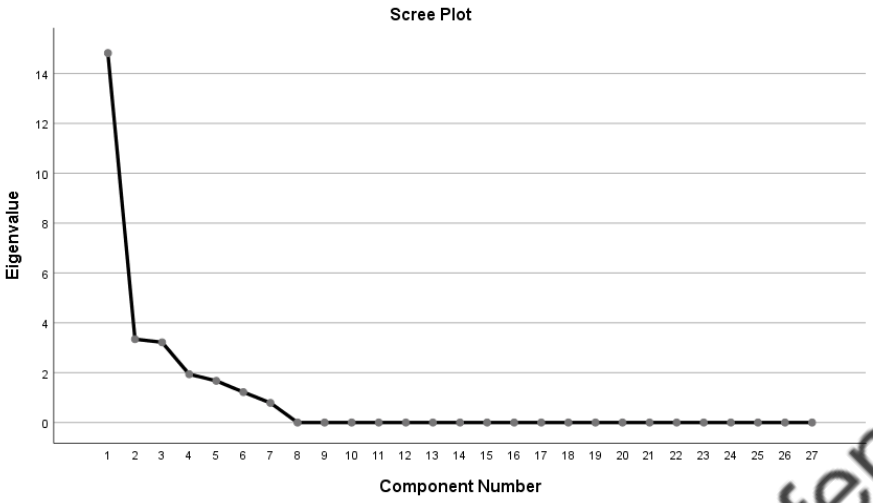


Figure 4.3 Setup of factorial analysis in the SPSS to extract principal components.

Table 4.1 Variance distributed in components (constructs) obtained using SPSS.

Total Variance Explained - Initial Eigenvalues			**Extraction Sums of Squared Loadings**		
Component	Total	Of Variance	Cumulative %	Total	% of Variance
1	14,822	54,895	54,895	14,822	54,895
2	3,344	12,385	67,280	3,344	12,385
3	3,218	11,918	79,197	3,218	11,918
4	1,938	7,178	86,375	1,938	7,178
5	1,671	6,190	92,565	1,671	6,190
6	1,219	4,516	97,081	1,219	4,516
7	,788	2,919	100,000	,788	2,919
8	1,321E-15	4,892E-15	100,000	1,321E-15	4,892E-15
9	1,228E-15	4,547E-15	100,000	1,228E-15	4,547E-15

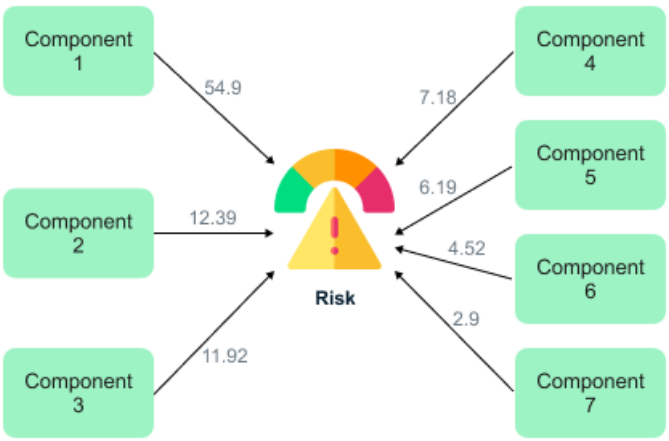


Figure 4.4 Setup of factorial analysis in the SPSS to extract principal components.

Based on the analysis of the seven theorical constructs through of the matrix de components of SPSS with the factors, we have obtained the following results:

Component 1 (54.90% of weight): Organization

- Effect on economic, social, environmental domains.
- Number of IoT devices.
- Effect of shock on the market.
- Security configurations of IoT devices.
- Vulnerabilities of IoT devices.

Component 2 (12.39% of weight): Scalability

- Effect of the relation between IT/OT/IoT systems.
- Number of IoT devices increase the probability of attack.
- Previous attacks allow new attacks.
- Short times to propagate attacks.
- Attacks from one layer to other layers of IoT system.

Component 3 (11.92% of weight): Attack Surface

- IoT devices number increase attack surface.
- Attacks could be on different IoT layers.
- Attacks could be on different domains.

Component 4 (7.18% of weight): Severity

- Effect on CIA.
- Impact depends on type of attack.
- Vulnerabilities in IoT devices.

Component 5 (6.19% of weight): Susceptibility

- IoT devices could be susceptible to attacks.
- Attacks could be on different IoT layers.
- Frequency of attacks.
- Attacks could be on different domains.
- Short time between attacks.
- Interdependency with other IT/OT/IoT systems increases the severity of attacks.

Component 6 (4.52% of weight): Interdependency

- Attacks could be on different domains.
- Interdependency with other IT/OT/IoT systems increases the severity of attacks.
- Attacks could be on different IoT layers.
- Security configurations of IoT devices.
- Frequency of attacks.
- Attack surface.

Component 7 (2.9% of weight): Uncertainty

- Security configurations of IoT devices.
- Number of IoT devices.
- Interdependency with other IT/OT/IoT systems increases the severity of attacks

Validation of results of judgement of experts.

To corroborate the obtained results, we have carried three additional processes:

1) We have used PCA to analyze the factors, which is a widely used technique in exploratory factor analysis to evaluate linker scale data in surveys. Based on the type of data, the use of categorical PCA or non-linear PCA was used. In the SPSS tool it is called CATPCA and is based on Holmals' proposal for analysis of categorical values. Figure 4.5 shows the component number obtained using CATPCA, the number is like get previously with PCA. Figure 4.6 shows a screenshot for SPSS with the weight contributions of components. Figure 4.7 shows a screenshot for SPSS with the percentage of variance of each component.

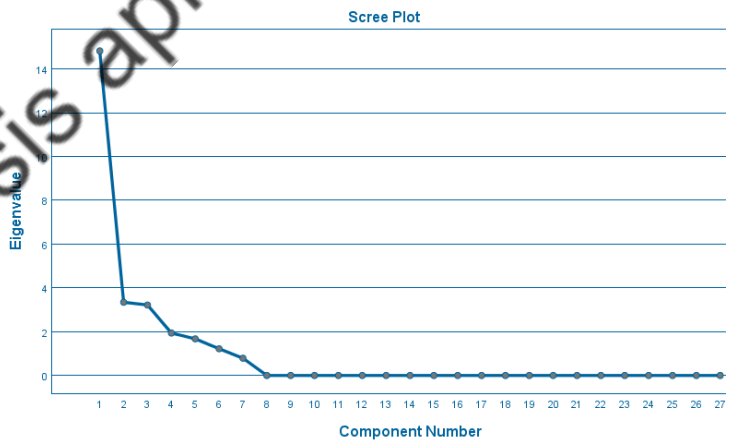


Figure 4.5 Screenshot for component numbers using CATPCA.

	Component					
	1	2	3	4	5	6
Theriskvaluewilldependontheprobabilitythatthreatscanc	,977					
Theriskseverityandprobabilityvalueswilldependonthelev	,958					
Thevalueoftheriskwilldependonthesecuritycontrolsinpl	,935					
Riskandseverityvalueswilldependontherelationshipofl T	,923					
Thevalueoftheriskwilldependonthetypeofinformationin	,917					
CyberattacksonIoTsystemscouldaffecttoeconomicsocialor	,915					
Cyberattackcouldaffectdifferentlayersofl oTsystemsincreas	,892					
IoTdevicesaresusceptibletospecifictypeofcyberattacks	,850				,426	
Thevalueoftheriskwilldependonthenumberofattacksonlo	,840				-,498	
Securityconfigurationsonl oTdevicecouldincreasethesuscept	,835		-,353			
Thevalueoftheriskwilldependonthevalueofthesurfaceat	,827				-,470	
Cyberattackscouldbescaledfromonelayerofl oTsystemtooth	,790	,430			-,361	
Thegrowthofnumberofl oTdevicescouldincreasetheprobabili	,735		,545			-,325
Thefrequencyofcyberattackscouldincreasethesuccessfuloft	,732		-,519		,311	
CyberattacksonIoTsystemscouldaffecttoeconomicsocialor_A	,732		,498		,361	
Securityconfigurationsonl oTdevicesdependsofdomainsorpil	,714					,301
CyberattacksonIoTsystemscouldgenerateshockonmarketsorr	,713	,377	,379			
VulnerabilitiesonIoTdevicescouldincreasetheprobabilityof	,709	-,356	,409		-,354	
Thevalueoftheriskwilldependonthetypeofattacksonthe	,670			,841		
InterdependencyofIoTdevicewithotherIoTITandOTsystems	,661		-,454			,522
Previousattackallowstheexecutionofnewattacks		,942				
CyberattackstoIoTsystemscouldbeaffectedtootherIoTITa		,789		-,519		
Thegrowthonthenumberofl oTdevicescouldincreasethesusce	,400	,736				
Shorttimesonthepropagationofcyberattackscouldincreaseth	,373	,591	-,500	,418		
Cyberattackscouldgeneratedegradationintheoperationofl oT	,648		-,671			
Attackscouldbeexecutedondifferentlayers	,621		,636		,376	
CyberattackscouldaffecttoCIAonIoTsystems	,314		,474	,794		

Figure 4.6 Screenshot from SPSS, with the weights associated with the questions to components (risk factors).

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	14,822	54,895	54,895	14,822	54,895	54,895
2	3,344	12,385	67,280	3,344	12,385	67,280
3	3,218	11,918	79,197	3,218	11,918	79,197
4	1,938	7,178	86,375	1,938	7,178	86,375
5	1,671	6,190	92,565	1,671	6,190	92,565
6	1,219	4,516	97,081	1,219	4,516	97,081
7	,788	2,919	100,000			
8	1,321E-15	4,892E-15	100,000			

Figure 4.7 Screenshot from SPSS with percentage of variance of each component.

2) We development a correlational analysis of the questions. For this process each question was consider as a variable. The result obtained for correlational analysis is show in the Figure 4.8 and Figure 4.9. We can observe the number of dimensions and relation between factors, is similar to result obtained with PCA or CATPCA. (Anexo 2 shows more detail for correlation analysis)

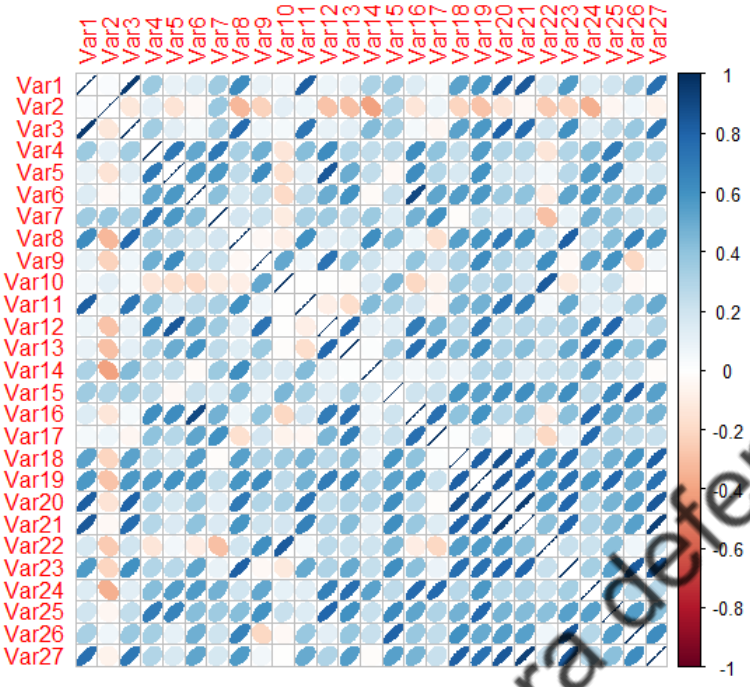


Figure 4.8 Correlation between the questions of survey. The questions were considered as variables for the correlation analysis.

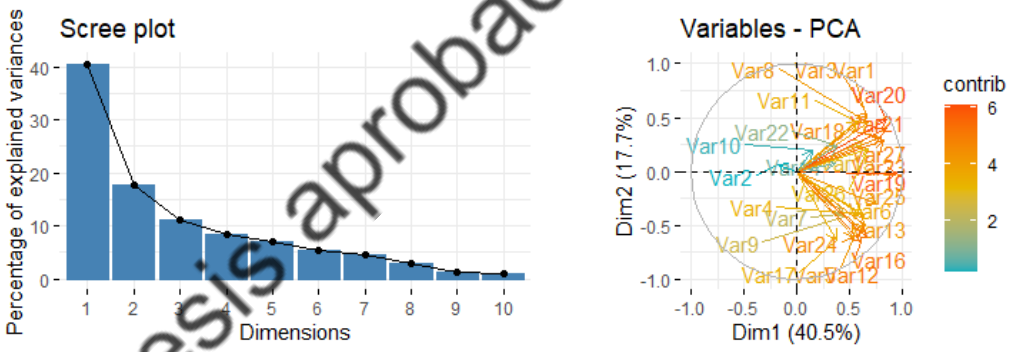


Figure 4.9 Number of components using correlational analysis. Comparative against PCA.

3) Finally, the survey was address to extra number of specialists in fields related with information technology (70 participants. The results are similar to get previously, and it doesn´t change the previous analysis.

These three processes corroborate the results obtained about seven components (factors), which consolidate the major contributions to evaluate the security risk in IoT context.

The results did not change the proposals risk factors related with IoT devices. All factors which were represented in the questions of survey have relations with one of the seven constructs. However, the results impulse a change in our primary proposal of theorical constructs about risk in IoT. In first instance we define three constructs Severity, Susceptibility and Risk behaviors and in this point, we define seven constructs: Domain and Pillars, Risk Behaviors, Attack surface, Severity, Susceptibility, Interdependency and Other factors

In relation to the eleven factors proposed in this study, for four of the factors (vulnerability, type of attack, type of information and type of device) it was not possible to establish indicators from the PCA. However, these factors are considered as inputs to other factors. For example, vulnerability is included in the factors: application, attack surface and severity.

4.1.1 IoT risk analysis framework

Based on the results of desciptive study, we proposes in the Figure 4.10 a risk analysis framework based on six domains:

1. Organization domain. The domain covers the organizational aspects of the organization (city, campus, enterprise, home) where IoT systems is implemented. The domain includes the evaluation of the security configurations according to polices or regulations related with cybersecurity in the different sector such as energy, traffic, health, home. The domain includes the analyze of the possible vulnerabilities that could affect the compliance of the policies or regulations of cybersecurity This domain comprises three components:

- Pillars: represents the social, environmental, and economic contexts that encompass IoT systems.

- Application domains: Represents the application domains that are covered by the IoT system such as: agriculture, health, traffic.

- Systems: Includes the IT/OT/IoT systems that support the development of the IoT system to support the pillars and domains.

2. Dependency/interdependency domain: Include the upstream, downstream, functional, geographic or cyber dependencies that exist between IoT, OT and IT systems.

3. Attack surface domain: Include the natural hazards (earthquakes, floods), human (cyber-attacks) or failures (configuration errors, system malfunctions) that may affect the operation of IoT systems. It includes the analyze of attacks that may occur in the layers of the IoT system.

4.Susceptibility domain: This domain includes the analyze of factor that could be more vulnerable to IoT device to attacks.

5. Severity domain: This domain includes the analyze of impact to CIA, trazability and authenticity of IoT devices.

6. Scalability domain: This domain analyzes the factors that may affect the value at risk, including:

- Impact: represents the value of damage that an IoT system may suffer due to threats.

- Probability: represents the occurrence that a threat may occur.

- Propagation time: represents the time it takes for a threat to propagate and cause medium or high damage.

- Propagation coverage: represents the area of compromise (IT, IoT, OT systems) due to a threat.

6. Uncertainty domain: This domain coverages the address of unknow factors that could contribute to security risk in spatial and temporal axis.

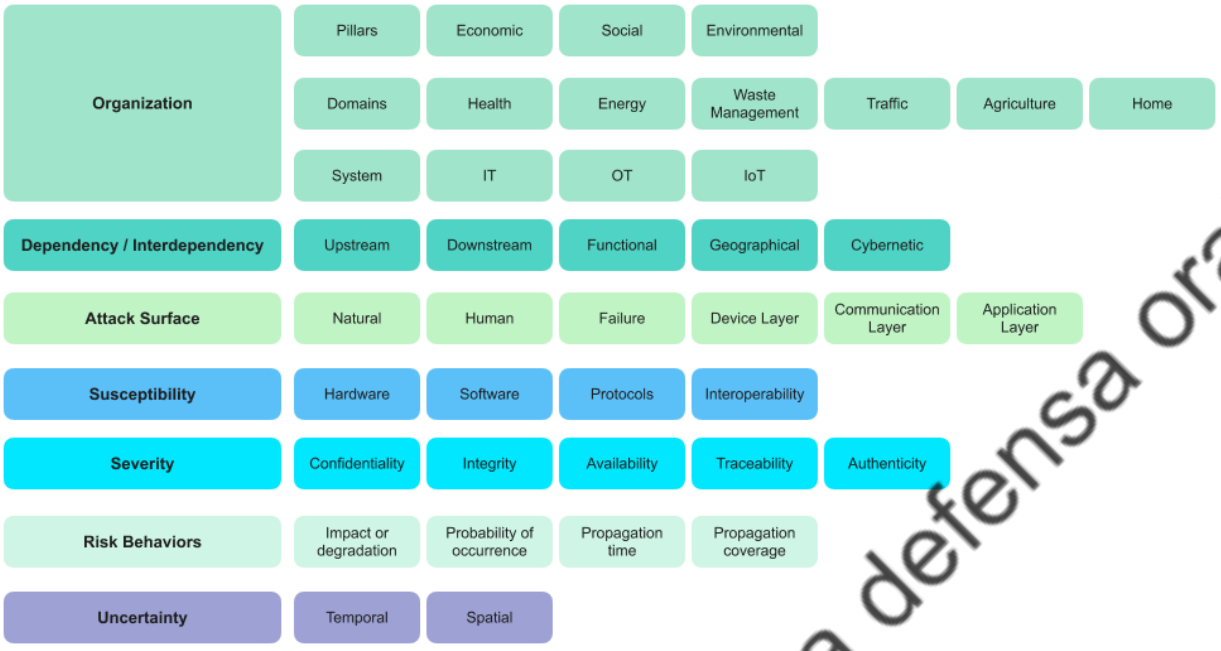


Figure 4.10 Framework proposed based on IoT security risk factors.

4.2 Descriptive Study II

This section is based on the fourth phase of the proposed research methodology that comprises the descriptive study II and it has the objective of establishing a methodology to evaluate the security risk in IoT systems. The descriptive study II uses empirical analysis based on the insights of the previous phases of DRM. The chapter describes the application of the methodology to develop a mathematical model based on the risk factors of IoT devices. Finally, the risk factors are used in multicriteria decision analysis (MCD) to get an aggregated risk value.

4.2.1 Risk calculation in IoT systems.

Once we have derived the seven macro-categories of factors associated with IoT risk, we have focused on understanding how these factors relate to and contribute to the value of risk. For this purpose, we propose a model based on the identified categories of factors. Based on the concept of risk, which is the probability of success of a given threat and its impact on strategic objectives, we can use the equation 4.1.

$$R = Pt \cdot I \qquad \text{Equation 4.1}$$

Where, R represents the risk value, Pt the probability of a threat and I the probability of Impact. The modeling strategy is presented in the Figure 4.11 and comprises three elements, establishing the input elements, the output elements and the methodology that allows the interaction between the inputs and outputs.

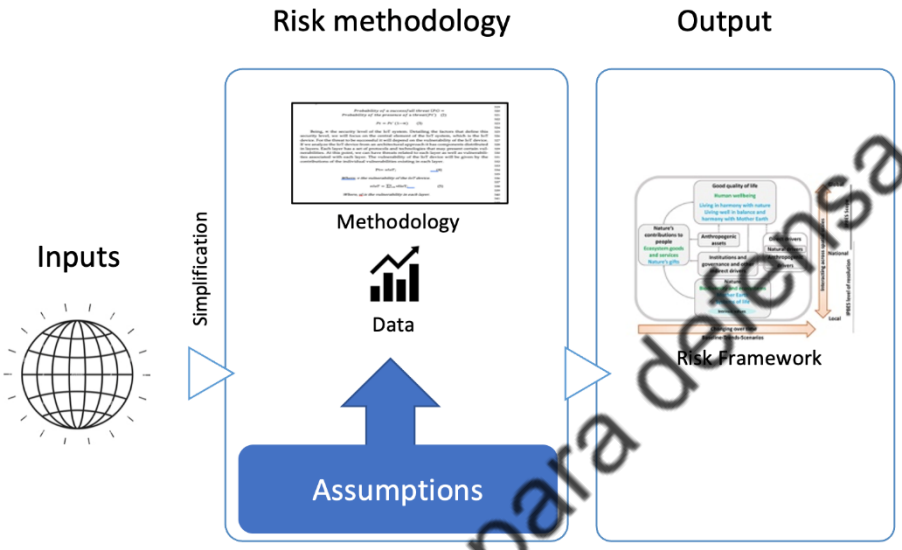


Figure 4.11 Strategy for modelling security risk in IoT.

Input elements

Analyzing the first component of risk, the probability of success of a threat, in the context of IoT systems, as well as computational systems, is the possibility of the presence of threats. The presence of a threat induces a certain value of security risk. However, whether this threat can generate an impact will depend on different factors such as: the vulnerability of the attacked device that can be exploited by this threat, the security levels of the device and the entire IoT system, and the effectiveness of the tools and techniques used by the attacker. In other words, although the presence of the threat already generates a possible risk value, the probability of its success is based on the security levels of the IoT system, for which will give us a more accurate value. So, we will initially propose the value of the probability of success of a threat as the probability of its presence in the IoT system, but the final value of the probability of success will be conditioned by the level of security of the system.

$$Probability\ of\ a\ successfull\ threat\ (Pt) = Probability\ of\ the\ presence\ of\ \text{a}\ threat(Pt') \quad \text{Equation 4.2}$$

$$Pt = Pt'(1-\delta) \quad \text{Equation 4.3}$$

Being, δ the security level of the IoT system. Detailing the factors that define this security level, we will focus on the central element of the IoT system, which is the IoT device. For the threat to be successful it will depend on the vulnerability of the IoT device. If we analyze the IoT device from an architectural approach it has components distributed in layers. Each layer has a set of protocols and technologies that may incorporate certain vulnerabilities. At this point, we can have threats related to each layer as well as vulnerabilities associated with each layer. The vulnerability of the IoT device will be given by the contributions of the individual vulnerabilities existing in each layer.

$$Pt = vIoT \qquad \text{Equation 4.4}$$

$$vIoT = \sum_{l=0}^{n} vlIoT \qquad \text{Equation 4.5}$$

An interesting aspect of IoT is its adaptability to be used in different verticals. We can find in the literature that IoT is used to develop Smart homes, Smart health, Smart grid, Smart cities, among others. This aspect of IoT could have an important implication from the security aspect, because an IoT device based on a certain hardware and software used for agriculture could be modified and used for vehicle control. This adaptability is what has made IoT so popular, and devices such as Raspberry Pis and Arduinos have been widely used to develop Smart solutions. In this perspective, it is worth asking questions, such as: is the required level of security of a device different for an agricultural environment than for a vehicular control environment? And what is the factor that determines the level of security to be applied in each vertical? Regarding these questions, two proposals are the one presented by CIS concerning the definition of a set of classes that represent a security value of the IoT device based on confidentiality, integrity, and availability. On Table 4.2, we present the information of the classes. A second proposal is the one proposed by OWASP in the ASVS methodology for IoT systems in which the security level is established by levels L1, L2 and L3 according to the criticality of the vertical.

Table 4.2 Compliance classes for IoT systems [14].

Compliance Classes	Description	Confidentiality	Integrity	Availability	Score
Class 0	And in president impact could happen in the IoT system	Low	Low	Low	11
Class 1	The impact that could occur in the IoT system is limited	Low	Medium	Medium	22
Class 2	Besides the class one the IoT system withstands significant impact to availability	Medium	Medium	High	33
Class 3	Besides to class two, the IoT system protect sensitive data	High	Medium	High	44
Class 4	Besides the class three, data compromise and loss of control have a critical impact on the IoT system.	High	High	High	55

Additionally, in relation to the influence of the vertical, the susceptibility of the device to be attacked is related with where the IoT device is used. A device may also have certain vulnerabilities, for example a physical vulnerability, thus by not having a case that protects it from an attacker being able to connect directly to a port JTAG. If the IoT device is used in a Smart home, this vulnerability may not be very relevant, but if the device is in a Smart traffic solution, in which the device is in a street, the vulnerability has a greater relevance. The susceptibility of the device will be influenced by the characteristics of the vertical where it is used.

From a practical point of view, the susceptibility would increase the vulnerability value of the device by a factor determined by the characteristics of the vertical domain, where the IoT solution is implemented.

$$vIoT = \beta\, vIoT' \qquad \text{Equation 4.6}$$

Where, vIoT represents the vulnerability value as a function of a Beta. β represents the susceptibility value. Finally, vIoT' is the vulnerability value without considering the susceptibility. The Beta value is obtained as a function from the relationship of the domain and the specific vulnerability in each layer. For instance,

Table 4.3 shows the selection of β for three scenarios. Another aspect related to the security level is the attack surface. The attack surface of a system is constituted by the elements that allow the possibility of an attack: input and output interfaces, data, methods and channels, and attacks. From security perspective, each IoT device is a possible entry point for an attack, and if a device has more vulnerabilities, the probability of a successful attack is high; so, an increase in the number of IoT devices would increase the attack surface and the probability of the threat's success. Where, γ represents the interdependency between systems, $vIoT$ the vulnerabilities of IoT devices and n represents the number of IoT devices.

$$As = \gamma \cdot nvIoT \qquad \text{Equation 4.7}$$

Table 4.3 Relation of susceptibility β among vulnerability and domain of application of IoT systems [15].

Vertical domain	Physical vulnerability	Network vulnerability	Application vulnerability	Beta
Smart home	Within the boundaries of a house or building. Generally, few meters of geographic area.	Network topology generally is of type star. Network topology is small. Few devices in the network.	Applications on mobile devices, especially smartphones.	Low
Smart health	Within the boundaries of building or medical campus. Coverage of geographic area of meters or kilometers.	Network topology could be extended-star type. The size of network is medium. Network could contain hundreds of devices.	Applications on mobile devices (smartphones and tablets.)	Medium
Smart traffic	Within the boundaries of city. Geographic coverage in kilometers.	Mesh type network topology. Large network	Applications on computer devices (information systems).	High

Other entry points for attacks in the IoT context are the interdependencies with other IoT systems and with IT and OT systems. The number of these dependencies modifies the attack surface. Gamma represents the number of connections between IoT devices.

$$\gamma = \frac{n-1}{n} \qquad \text{Equation 4.8}$$

At this point, the proposal is to mention that the level of security of the IoT solution will be related to the level of assurance of the attack surface, in other words, the higher the level of security, the smaller the attack surface.

$$As = \gamma \cdot \left(\beta \cdot \sum_{l=0}^{n} vlIoT \right) \quad \text{Equation 4.9}$$

$$As = \frac{n-1}{n} \cdot n \cdot \left(\beta \cdot \sum_{l=0}^{n} vlIoT \right) \quad \text{Equation 4.10}$$

When replacing in Equation 8.3 the value $\delta = \frac{1}{As}$, with the values for equation 10, we have the following equation:

$$R = Pt \left(1 - \frac{1}{\frac{n-1}{n} \cdot n(\beta \cdot \sum_{l=o}^{n} vlIoT)} \right) \quad \text{Equation 4.11}$$

Analyzing the final proposed formula, reducing the number of IoT devices although it could be feasible through a process of resource optimization may not always be practical. Considering that if more IoT devices are used it could improve the process of sensorization and therefore the data acquisition for decision-making process. So, the number of links between devices would also not be possible to reduce under the same justification.

At this point the two remaining factors would be the Beta value representing susceptibility and vIoT representing vulnerability. This last factor is more intrinsic to the IoT device and could be addressed by a hardening process. The susceptibility which is more an extrinsic element of the device and depends mostly on the conditions of its environment, could be addressed by the implementation of a set of policies, is controlled based on best practices related to each vertical domain. The process of hardening and best practices could be carried out based on security controls such as those proposed by the Center for Internet Security (CIS).

Output elements

To address output elements, we propose the following questions: i) What would be the indicators to assess systemic risk? ii) What would be acceptable values of security risk before having a systemic type of condition? We take as a basis what was presented by the Bank of England in July of 2018 regarding systemic risk thresholds [53]. In Figure 4.12, the graph “a” shows the impact tolerance threshold as a function of aggregating impact as a function of time. The threshold includes a systemic buffer

capacity. The graph “b” shows that using an incident response the shock could be absorbed within of the threshold. Finally, graph “c” shows that if the event exceeds the established tolerance threshold a systemic event could occur, and even more a second disruption event B may occur in ∝ time.

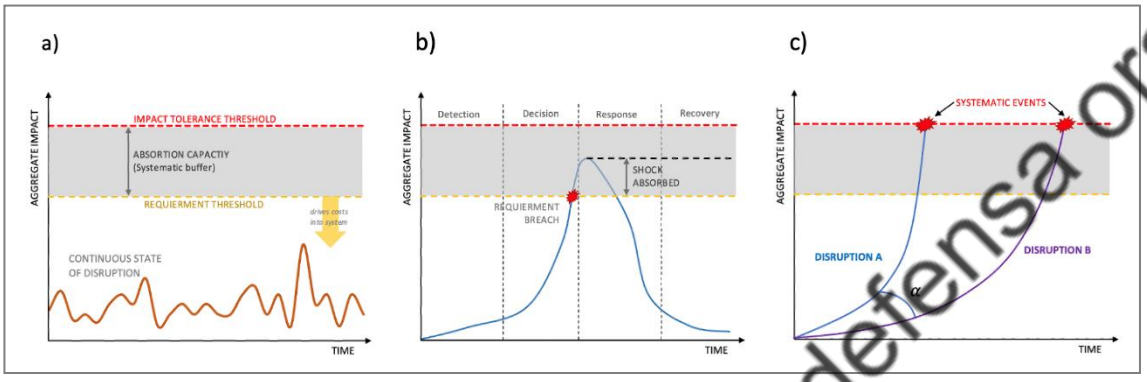


Figure 4.12 Three charts illustrate the concept of impact tolerance and absorptive capacity (A), a shock being absorbed (B), and disruptions with different rates of impact amplification (C). (Source: WEF [7]).

Return from our first risk equation we have the modified equation in which we have included the security level.

$$R = Pt(1-\delta) \cdot I \qquad \text{Equation 4.12}$$

The second component of the equation 4.12, is the level of impact to strategic objectives of the organization due to a cyber attack to the IoT system. For example, an IoT system is used to develop a Smart Health to improve the effectiveness in the processes of measuring the physical conditions of patients, so the impact could be associated with the theft of sensitive patient information, with the manipulation of medical information or with the unavailability of patient’s data. If the IoT system is used to develop Smart traffic, the impact could be reflected in the unavailability of signaling, which can produce traffic jams and generate an economic impact related to the monetary loss of people who cannot move to their jobs or in a social approach to the stress generated in drivers. In this context, we can establish that the impact must be evaluated in strategic axes such as: economic, social, and environmental perspectives (See Table 4.4).

Table 4.4 Possible impact to economic, social and environmental domains due to attacks in IoT systems [16].

Vertical/Domain	Economic	Social	Environmental
Smart city	Potential loss of high economic revenues due to non-operation of city services.	Loss of credibility of public services	Possibility of certain attacks affecting services related with waste management that could affect the environment.
Smart health	Possible high economic losses due to possible legal claims.	Possibility of loss of lives	Possibility of certain attacks affecting waste management
Smart home	Possible low economic losses	Low impact.	Low impact.
Smart grid	Potential high economic losses due to lack of energy for the organization's operations.	Possibility of generating a feeling of chaos, insecurity, or stress in people due to the lack of electric power.	Possibility of certain attacks affecting waste management or environmental control processes in organizations due to lack of energy.
Smart traffic	Possible low to medium economic losses due to delays of people to their jobs.	Possibility of generating anxiety and exhaustion in drivers.	Possibility of increased pollution due to vehicular congestion.

The economic, social, and environmental impact has been of great interest in the research field given its relevance. In this work the scope is to focus on the economic domain given its importance in the security budget management. The budget factor is important and as we mentioned before to improve the security level of the IoT system it is necessary to establish some controls and best practices that directly or indirectly require a monetary value for its implementation.

Economic models try to predict the future level of some key economic variables. These models seek to identify relationships between the movements of one set of economic variables (independent variables) and those of an economic variable of interest (dependent variable) for using in tactical decision making. For instance, an economist may attempt to predict the impact on inflation given information about changing GDP and unemployment levels. These models are classified under the general category of forecasting models. Still other economic models, such as stochastic variable term structure models, are built specifically to determine the price of complex financial derivatives and insurance contracts with embedded options. Some research has contributed to the evaluation of the economic impact by using VAR to estimate possible losses. Some researches, not specifically in the field of security, consider expected loss or also called Conditional Value-at-risk (CVAR),

instead of VAR, since they consider that the latter, by not considering the information of the tails in the distribution, does not allow a more accurate estimation of losses.

As discussed, from a mathematical standpoint, the above variables can be combined with a stochastic model. This stochastic model represents better the cyber value-at-risk, and its output is the probability on any given day to lose a certain amount of money. The assessment of economic impact starts from the need for considering the value of the assets. So, an important task is correctly determining the critical assets. In the case of IoT systems, an alternative to identify the critical assets would be look for those that contribute to obtain gains. To exemplify our proposition, we will analyze a smart parking solution which receives a total of 100 cars per hour, with a billing value of $10 dollars per hour. If the system remains inoperative for three hours due to security attacks, we will have certain losses. When considering the critical assets for loss assessment, the asset would be the smart parking while the IoT devices would be components of the solution, but not the main asset. One aspect of certain IoT solutions is that the IoT devices used can have values that range from between 60 to 100 dollars, so their replacement would not have a high economic impact. This economic aspect of IoT devices is just one of the factors that has enabled the huge growth and inclusion of IoT devices. In this case the value of loss (Impact) will be given by the probability of occurrence of the threat for the estimated value of loss in dollars for the organization, not for IoT devices. We define a lower and upper values of monetary loss and define a probability of loss in this range. Additionality, we establish a probability value where these losses could occur. For example. The probability of occurrence of a DoS attack is 20% and the probability of having losses between 25000 and 50,000 dollars is 90%. We calculate the value Vr that corresponds to economic loss.

$$I = Pt \cdot Vr \qquad \text{Equation 4.13}$$

Where, I represent the impact, Vr represents the possible loss in terms of money. In this case, Vr would be obtained by the means of the CVAR application. It is through the CVAR application that we could define a threat portfolio capable of obtaining monetary losses for every single one of the existing threats.

Methodology

The third component of the generic model is the risk assessment methodology. Although we have defined a mathematical expression for the risk itself as a function of the probability of success, which also depends on the existence of the threat and the security level of the IoT system, and the conditions of scalability and its impact measured in economic losses. Also, is necessary select a risk model to make projections. Some risk models are frequency/severity model, loss-ratio model, or natural catastrophes model.

The methodology for security risk assessment in IoT systems could be defined in the relation between inputs (risk factors) and the output (impact). However, in the context of cyber security, is not always feasible to have enough data to establish a decision-making process. Additionally, being the IoT environment a complex and dynamic system, this aspect related with the lack of data can be a big problem to establish a decision-making process. An alternative is defining a set of actual or hypothetical tests to probe system behavior under unusual conditions and then estimated the response of the system to via conditional probabilities and beliefs (see Figure 4.13).

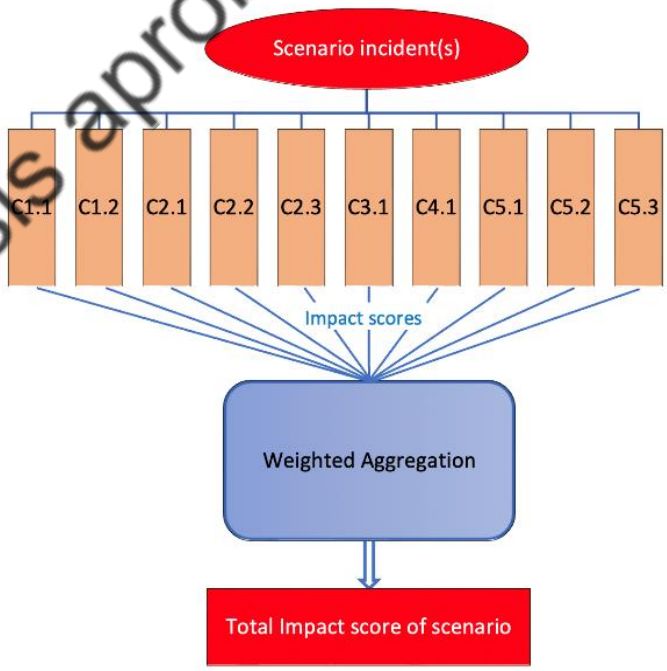


Figure 4.13 Scheme of an actual or hypothetical test, targeted to probe the system's response to a hypothetical but possible scenario.

We have proposed a Bayesian network consisting of the following factors: vulnerability, susceptibility, attack-surface, and interdependency. These factors shine a light on the possible impact on the economic, social, and environmental domain. We have selected the Bayesian network because it allows us to work in data-poor environments with the presence of uncertainty. Additionally, it allows us to incorporate evidence that can update the state of the output variables allowing us to capture the dynamics of IoT systems (See, Figure 4.14 and Figure 4.15).

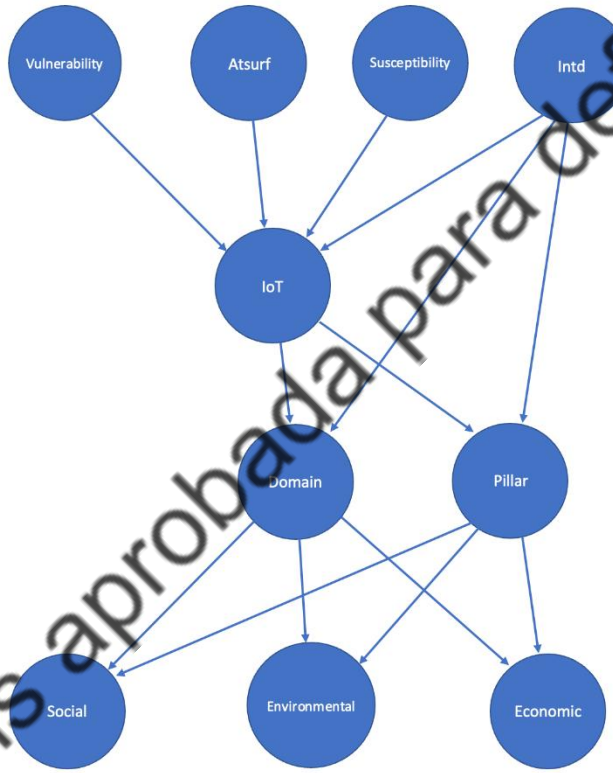


Figure 4.14 Bayesian network model based on IoT security risk factors

Figure 4.14 shows a Bayesian network consisting of various factors (organization, susceptibility, severity, attack-surface, and interdependency) that have potential to impact the economic, social, and environmental domains. In this case, the component "scalability" and the component "uncertainty" are modeled based on the behavior of the Bayesian network.

```
# P(V=T), P(V=F)
vulnerability = BbnNode(Variable(0, 'vulnerability', ['attack', 'no_attack']), [0.65, 0.35])

# P(S=T), P(S=F)
susceptibility = BbnNode(Variable(1, 'susceptibility', ['attack', 'no_attack']), [0.65, 0.35])

# P(N=T), P(N=F)
Atsurf = BbnNode(Variable(2, 'Atsurf', ['attack', 'no_attack']), [0.65, 0.35])

# P(I=T|V=T,N=T,S=T,Sy=T), P(I=F|V=T,N=T,S=T,Sy=T),
# P(I=T|V=T,N=T,S=T,Sy=F), P(I=F|V=T,N=T,S=T,Sy=F),
# P(I=T|V=T,N=T,S=F,Sy=T), P(I=F|V=T,N=T,S=F,Sy=T),
# P(I=T|V=T,N=T,S=F,Sy=F), P(I=F|V=T,N=T,S=F,Sy=F),
# P(I=T|V=T,N=F,S=T,Sy=T), P(I=F|V=T,N=F,S=T,Sy=T),
```

Figure 4.15 This is a figure. Schemes follow the same formatting.

Monitoring of outputs

Finally, the fourth component for the assessment of IoT risk is output monitoring. Based on the BN, we have obtained the results presented on Table 4.5.

Table 4.5 Values for Bayesian network simulation for input factors.

IoT factors (Input variables)				Impact (Output variables)		
Severity	**Risk Behaviors**	**Attack Surface**	**Interdependency**	**Economic**	**Social**	**Environmental**
100%	50%	50%	60%	73.12%	66.04%	57.66%
100%	100%	50%	60%	76.56%	69.08%	60.26%
100%	100%	100%	60%	77.91%	70.25%	61.26%
100%	100%	100%	100%	86.05%	77.15%	67.28%
70%	100%	50%	60%	73.40%	66.30%	57.88%
70%	50%	50%	100%	84.86%	76.22%	66.43%

Having the percentage of possible impact, we are interested in obtaining the resulting economic value from the security attack. For which we are initially interested in seeing if the simulated output data could be adjusted to a financial risk Having the percentage of possible impact, we are interested in obtaining the losses from the economic perspective caused by the security attack. For which we are initially interested in seeing if the simulated output data could be adjusted to a financial risk calculation model to verify if it can fit a normal distribution as the one used by economic models like VAR. There are some ways to estimate whether a variable has a normal distribution or not. We rely mostly on the shape of the frequency polygons. Now we are going to introduce a more formal test of normality. Our null hypothesis in the Shapiro-Wilks test is that the distribution from Bayesian network is a normal

distribution. We choose a significant level of 0.05, and our alternative hypothesis that the distribution is not normal. We observe that the variables vulnerability, susceptibility, attack-surface, interdependency, do not follow a normal distribution, since in all four cases the probability value (p) is less than our chosen level (0.05), so we reject the null hypothesis. On the other hand, we observe that the variables related to impact follow a normal distribution, since in all three cases the probability value (p) is greater than our chosen level (0.05), concluding that the null hypothesis shall not be rejected. The correlations among variables are shown in the Figure 4.16.

Additionally, we can observe evidence that the correlations are positive in all cases, but the interdependence variable has a high correlation close to 1, which implies a higher contribution to a social, economic, and environmental impact.

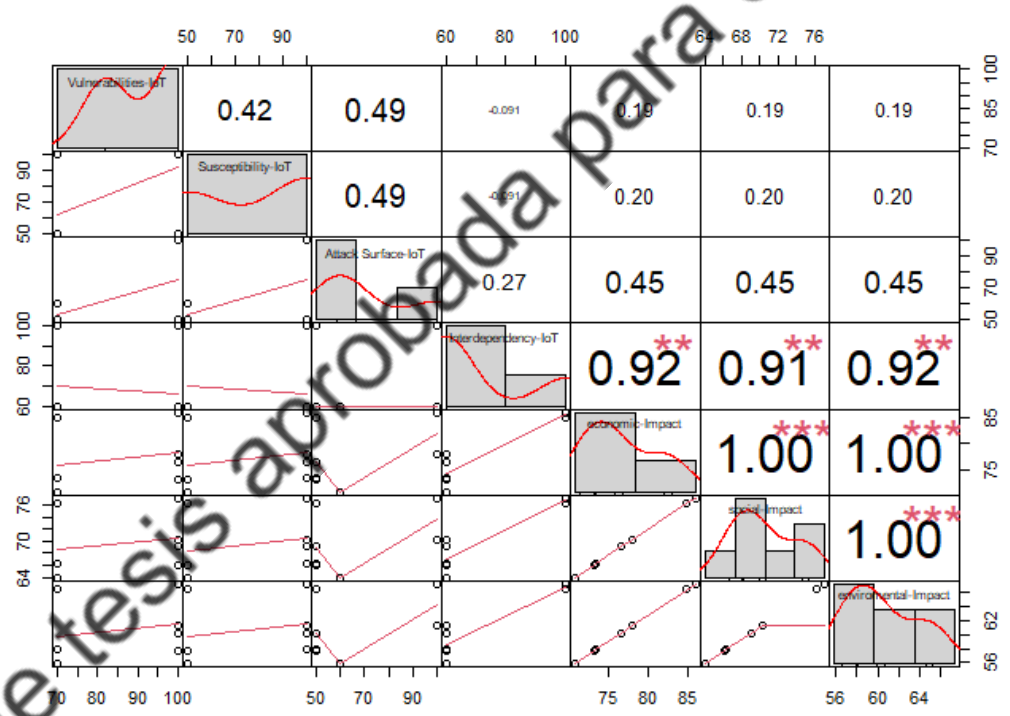
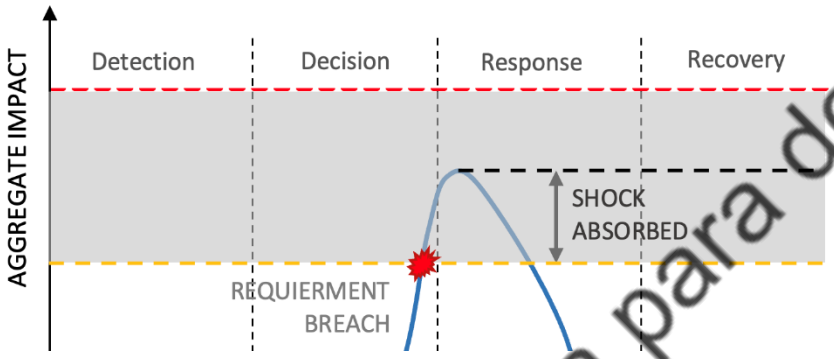


Figure 4.16 Correlation of a set of variables indicating that the null hypothesis shall not be rejected since financial risk calculation model follows the normal distribution.

Then, we can establish a quantitative value of the economic impact based on the normal distribution and the absorption capacity relates to the response that the organization could provide in the case of an incident of security. An organization could use a capital or an insurance value to be able to detect if this value exceeds the threshold defined by the organization. The absorption capacity depends of each organization. A risk value 1 is equivalent to a value of 10% of the range defined for

the absorption capacity or that the value is 10% above the threshold value set by the organization to absorb the impact of security attacks. A risk value of 2 is equivalent to a value of 20% of the range defined for the absorption capacity, a risk value of 3 is equivalent to a value of 30% of the range defined for the absorption capacity and so on accordingly with the rest of the values. A best practice would be to set this threshold value between 70% to 80%, this represents a risk value of 7 and 8 respectively. A risk value of 9 and 10 would mean that the organization exceed the absorptive capacity threshold and generate a systemic event (see Figure 4.17).



Risk value	Percentage
1	10% -20%
2	20% - 30%
3	30% - 40%
4	40% - 50%
5	50% - 60%
6	60% - 70%
7	70% - 80%
8	80% - 90%

Figure 4.17 The percentage in the range absorption capacity relates directly to the risk value and is related to the response given in the event of the security incident.

Table 4.6 presents the risk value as a function of the impact values obtained from the simulations of Bayesian network and the evaluation of normal distribution related with the capacity of absorption.

Table 4.6 Risk level according to economic impact.

Economic-Impact	Risk Level
70,77	7
73,12	7
76,56	7
77,91	7
86,05	8
73,40	7
84,86	8

Following, an example of the risk calculation according to our proposed methodology. We estimate the minimum and maximum values of losses according to a risk portfolio in Table 4.7 and the indicators for estimating the cost of economic security in Table 4.8

Table 4.7 Hypothetical cost for attacks to IoT systems

Attack	Lower	Upper
DoS	15000	45000
Eavesdropping	2000	7500
Privilege Escalation Attack	10000	80000

Table 4.8 Indicator for estimating cost of economic security.

Indicator for estimating cost of economic security	
Damage to smart infrastructure	A DoS attack can affect the IoT infrastructure related to vehicle detection devices, generating 10 hours of inoperability to the parking lot.
Economic Loss	There are financial losses due to an estimated parking flow of 100 cars per hour. Since the inoperability is set to 10 hours with a parking price at 10 dollars. The final loss cost is approximately $10000 USD
Social damage	A social impact is inevitable for the unavailability of parking lots generate stress and latency in people's lives. In this case we estimate that at least half (500) of the owners had an hour delay, taking into consideration 20 dollars an hour, the total loss would be one of $10000.
Environmental damage	The inoperability of parking lots implies that cars will have to circulate throughout the zone generating more contamination to the atmosphere than usual. For simplicity, let's suppose that the environmental damage is of $5000.

Based on the information presented in the proposed Bayesian network, if the probability of having vulnerabilities is 100%, the attack surface is hackable, the interdependence allows an attack, and susceptibility exists, all in a 100%. We would have in the worst case of 86.05% of probability of economic impact, which represent un risk level of 8, and the economic loss value from the analysis of normal distribution built with the values of Table 4.6, Table 4.7 and Table 4.8, is close to $30.000 USD. In this case, we are still inside the range for the capacity of absorption of the shock. But we are very close to the umbral of a systemic event. Additionality, we are not considering the fact of a possible second event in the tetha period, as shown in Figure 4.18, which is associated with the time between attacks.

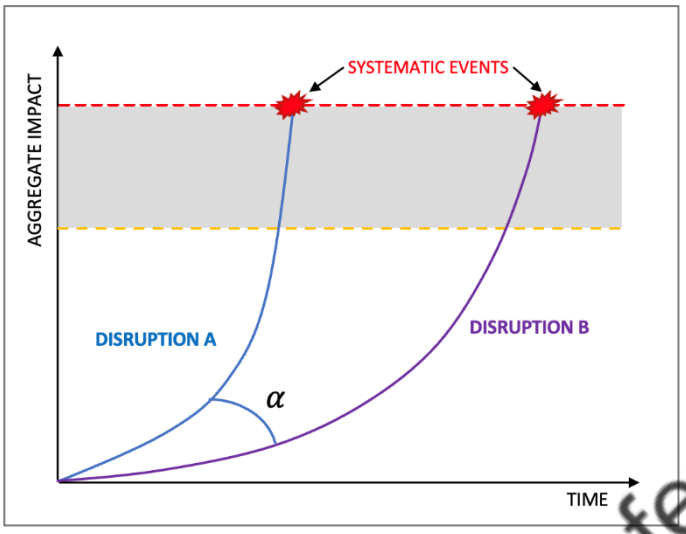


Figure 4.18 Disruptions with different rates of impact amplification

4.3 Multicriteria analysis of IoT security risk factors

Depending on the proposed model, we can see that the categories of defined factors allow us to calculate a risk value. We have defined a set of factors that correspond to input elements (Domain and Pillars, Susceptibility, Attack Surface, Interdependency) while the "Severity" factor corresponds to output elements. While the Risk Behaviors, and Uncertainty factors are associated with the behaviors or dynamics that the model presents.

Focusing on the methodology of the model that allows the link between inputs and outputs, we can establish that a relationship based on weights between factors is handled and that the contribution of the different criteria that make up each factor allows us to have an added value of risk. It would be possible to use the indicators determined in the factorial analysis corresponding to each factor and develop in greater detail the risk methodology and therefore the weights that determine the risk value to have a more approximate value. To address this need we plan to take advantage of the strengths of Multi criteria Decision Analysis (MCDA).

Based on the findings established in the prescriptive analysis, this section delivers the establishment of a proposal on the definition of the relationship between the different factors to obtain a value of risk. Multi-Criteria Decision-Making Method (MCDM) or Multi-Criteria Decision Analysis (MCDA) provides the possibility to evaluate factors to decide which alternative is most suitable. For this reason, MCDM has been used in several fields to evaluate specific aspects. For instance, Siksnelyte et al. [48] propose the assessment of renewable energy technologies in a Household

using MCDA. Vermersch et al. [54] applied MCDA to evaluate the benefit-risk of Cladribine for Patients with Relapsing-remitting Multiple Sclerosis. Ruggeri et al. [55] propose the usage of MCDA to evaluate Health Technologies during the COVID-19 pandemic.

MCDA has been used to develop models for assessing cybersecurity levels. For instance, reference [56] proposes using MCDA with the Preference Ranking Organization Method for Enriched Evaluation (PROMETHEE) II method to select the best to worst alternatives to demonstrate the highest priority criterion for the implementation of personal data security. On the other hand, Zenonas et al. [57] propose using an MCDA hybrid approach to model risk assessment for critical infrastructures. In this proposal, the weights are related to the impact of the threats on critical infrastructures, and they are established for experts using a 10-based Likert-type scale. The impact of threats is classified into six sub-criteria: Loss availability, Loss confidentiality, Loss integrity, Direct loss, Indirect loss, Criticality, and the weight rating was: 1-Low probability, 2-Medium probability, 3-High probability, and 4 Very High probability. A fuzzy technique is used to deal with the criteria for experts. In the same vein, Gaiin et al. [58] propose a decision-analysis-based approach quantity threat vulnerability and consequences through a set of alternatives designed to assess the overall utility of cybersecurity moment. The model proposes ranking the countermeasures using sensitivity analysis to assess the impact of uncertainty results. Finally, a survey development by Umm-e-Habiba [59] about MCDA mentions that the principal strength of MCDA is its capability to resolve:

Several criteria contribute to the total cyber security risk value to assess security risk in IoT systems. These criteria are related to the following factors: Organization, Risk behaviors, Susceptibility, Vulnerability, Attack surface, Interdependency, and Uncertainty. As the final objective of the risk assessment is focused on obtaining a single value based on the evaluation of these different criteria, a multi-criteria analysis method was chosen to address the security risk assessment in IoT systems.

An MCDM tries to find a solution for one or more criteria based on the following main phases [60]:

- Formulate the problem based on identifying the goal, alternatives, and criteria,
- Evaluate the alternatives concerning the criteria,
- Find the importance of the criteria,

- Synthesis the data collected in the previous phases to find a solution,
- Check the reliability and validity of the outcome.

A graphical representation of how the MCDA assesses the risk assessment in IoT systems using the seven factors described above is illustrated in Figure 4.19.

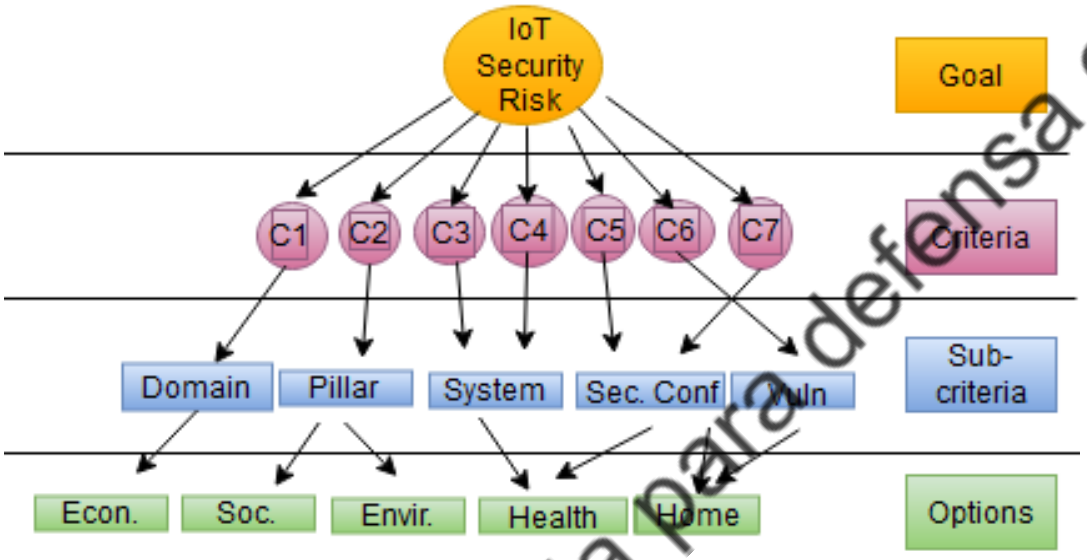


Figure 4.19 Proposal MCDA to evaluate security risk in IoT systems.

Issues on the selection of weights in MCDA for security risk in IoT systems

Once the MCDA structure is defined, the next step is to define the weights of each element of the model. The weights can be established depending on the evaluated IoT systems; they could be modified in each evaluation based on decision-maker criteria or expert's judgment assessment.

The first aspect about the contribution of an expert's judgment is that they tend to value subjectivity based on their expertise. Many MCDA approaches try to use techniques to reduce this kind of subjectivity. For instance, they are using fuzzy techniques.

In this same line, a second aspect to consider concerning the expert's judgments in IoT environments is that IoT solutions are used on different verticals such as health, energy, traffic, among others, and even if the expert has experience in the security field for contributing to the definition of the weights, this selection can be affected by the specific experience of the expert in a particular vertical. To clarify this point, if a security expert in IoT systems in hospitals assesses the security in IoT systems in SCADA systems, the expert could have limited knowledge regarding security threats and behaviors in these kinds of systems. In this context, it is possible to consider that

the weight given by an expert on a specific vertical domain in which the IoT system is evaluated will assign an additional value to its contribution.

A third aspect is the historical data of attacks on IoT systems. Although it is possible to have samples of attacks on IoT systems, the dynamic characteristics of IoT may limit the accuracy of using them in the decision-making process, since that is likely that the path of attack could be changed due to the addition or removal of IoT devices to the network. This lack of data could be a constraint in the process to select weights by the expert because they do not have enough information to decide.

A third aspect is the historical data of attacks on IoT systems. Although it is possible to have samples of attacks on IoT systems, the dynamic characteristics of IoT may limit the accuracy of using them in the decision-making process, since that is likely that the path of attack could be changed due to the addition or removal of IoT devices to the network. This lack of data could be a constraint in the process to select weights by the expert because they do not have enough information to decide.

Finally, the fourth aspect in IoT systems is that they represent a complex and dynamic system. This characteristic increases a set of uncertainties related to security aspects such as the effectiveness of the attack, or the probability of the existence of vulnerabilities. These uncertainties could induce a possible bias in the expert's decision. An overview of the issues, in the process of selection of weights by experts, are the following (see Figure 4.20):

1. Discrepancy in expert judgments due to the subjectivity of each expert.
2. Level of experience in the vertical where the IoT solution is used.
3. Limited data on previous attack patterns due to the dynamic characteristics of IoT.
4. Uncertainty due to the complexity and dynamics of IoT systems.

Figure 4.20 Considerations in the process of selection of weights in IoT security.

Methods to reduce the issues for selection of weights.

To reduce the subjectivity that experts could have when establishing the weights in the MCDA elements for IoT security risk assessment, we have chosen in this study to use the weight selection method based on the analysis of alternatives.

The method consists of posing a set of alternatives to the experts and asking them to quantify the best and worst alternatives on a scale. In our case, the alternatives are related to the values of the seven factors of IoT devices that are considered to assess the level of risk.

An additional method to improve objectivity, about selecting weights based on alternatives, is the Best Worst Method (BWM) proposed by [61], which performs a pairwise comparison-based between the best and worst alternative to define the value of the weight. In this point, it is important to mention that in scenarios where security attributes are evaluated to define a risk value, it is common to use probabilistic values to represent these attributes [62]. For instance, the success of an attack is represented through a probabilistic value based on the likelihood that the attack could be done without restrictions. The use of probabilistic values is since there is limited data to validate a certain attack at one specific time in the field of cybersecurity, and most of the results are post-mortem. To clarify this point, if we use MCDA in the educational environment, and we have the grades of the students in the last four academic periods, it is possible that we can have a degree of certainty about a specific student who has outstanding grades and predict that she/he will have in the next period similar. However, in the cybersecurity context, we cannot mention with a high degree of certainty that if a system or IoT device has not been attacked in the last two years, it will have similar behavior in the next year, and they will not be attacked. So, occurrence and a level of uncertainty about security events in the cybersecurity

environment are probable. Under this premise, the security risk assessment in IoT systems corresponds to a probabilistic scenario, an adaptation of the BWM method could be selected for probabilistic environments. The Bayesian Best Worst Method (BBWM) proposed by [61], including Bayesian algorithms to the BWM method, allows its adaptation in scenarios where the weights can be of the probabilistic type, as is the case of security events.

The Bayesian Best Worst Method considers the following steps:

1. Determine the criteria to be evaluated.
2. Develop survey.
3. Calculate the weights by the experts.
4. Determine the best to worst criteria.
5. Compare the best criteria with other criteria.
6. Compare other criteria with the worst criteria.
7. Take the two values as input for BWM in a probabilistic environment.

For the second aspect related to the experience level, additional weight can be considered if the expert has experience in the vertical in which the IoT system is being evaluated. And for the third aspect, related to the limitation of data about security attributes available to experts for establishing the weights, the use of probabilistic values can be defined. In this sense, we consider creating alternatives using Bayesian networks (BN). BN has the characteristic of being useful in contexts with limited data and uncertainty. There have been some contributions in this line. In [62], attack graphs are proposed to represent all the vulnerabilities and possible attack paths. Then capture the environment factors using Bayesian network models. In [63], a fuzzy probability Bayesian network (FPBN) approach is presented for dynamic risk assessment. In this sense, we propose build a Bayesian network defining as nodes the factors of IoT devices that contribute to the security risk (vulnerability, interdependency, attack surface), and the economic, social, and environmental domains that could have been impacted in the case of an attack to IoT systems. An important aspect of the Bayesian network is the consideration of joint relationships, which allows us to consider the value of a given factor and analyze the relationship between factors. This aspect is important in the IoT environment where there is a high degree of interconnectivity between IoT devices and IT/OT systems. The BN allows the establishment of performance indices in the IoT context to evaluate the values of the node and its relationship and how they could affect the entire IoT system.

Finally, for the fourth aspect related to the degree of uncertainty, we propose to continue using Bayesian. At the moment, we have considered the use of Bayesian

within the processes of generation of alternatives and for the selection of weights, but it is advisable to address the uncertainty in a more direct way previous to the calculation of the final risk value. So, we can include techniques for sensitivity analysis such as Moris [64], Sobol [65], or Bayesian algorithms [62], the last one used in this study to maintain the line of the use of Bayesian networks. We incorporated additional methods to improve the objectivity of MCDA in the methodology to evaluate IoT security risk in the Figure 4.21. The initial MCDA methodology analyzed included four phases: i) establishing the objective, ii) defining the criteria, iii) generating the decision matrix, and iv) determining the risk value. The proposal of MCDA that considers probabilistic environments and management of uncertainty in IoT environments include eight phases. This approach allows MCDA to be more objective than the initial proposal [66]. The phases for the proposal MCDA methodology are the following:

1. Define the objective of the evaluation.
2. Establish criteria set
3. Determine performance indices
4. Obtaining criteria and sub-criteria weights with BBMW
5. Performing consistency analysis
6. Performing sensitivity analysis
7. Creating decision matrix
8. Determining risk level

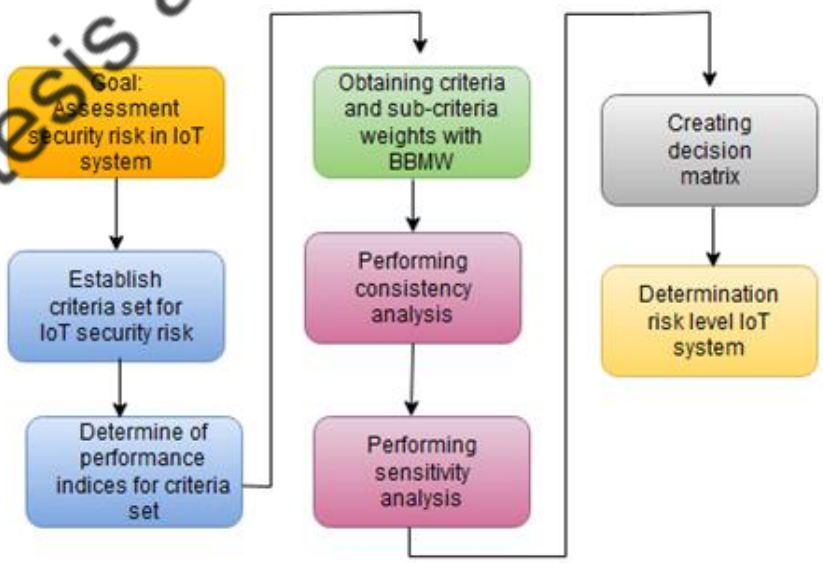


Figure 4.21 MCDA proposal to evaluate IoT security risk using alternatives and sensitivity analysis.

Following the MCDA development process, we have the primary objective: the security risk assessment of IoT systems. The criteria for assessing the security risk of the selected IoT systems are Severity, Scalability, Attack Surface, Interdependency. Based on these criteria, we define a performance index focused on the security level of the economic, social, and environmental strategic axes (organization). In our case, we expect to have values exceeding 70%, representing an adequate level of safety. Performance indices are the alternatives to be considered by MCDA. We have used simulations based on Bayesian networks to create the performance indices. The values of the experts were used to model the network obtaining the values in Table 4.9. We have defined a score of the alternatives based on the best-expected security level. Analyzing the best alternative was the one because, from a security perspective, the impact probability is 73.12% for the economic level, 66.04% for the social level, and 57.66% for the environmental level. The best alternative is around the 30% of security level, which is lower than the 70% defined as the goal in this study, but they are the lower values of impact in Bayesian simulation. The level could be improved by adding some security mechanisms in the future. The worst alternative was number 4 because the probability of impact in economic level is 86.05%, social 77.15%, and environmental 67.28%, which reduces the level of security in economic impact to around 20%.

Table 4.9 Performance indices of IoT security Bayesian Model

IoT factors (Input variables)				Impact (Output variables)			Score
Severity	**Scalability**	**Attack Surface**	**Interdependency**	**Economic**	**Social**	**Environmental**	
100%	50%	50%	60%	73.12%	66.04%	57.66%	1
100%	100%	50%	60%	76.56%	69.08%	60.26%	3
100%	100%	100%	60%	77.91%	70.25%	61.26%	4
100%	100%	100%	100%	86.05%	77.15%	67.28%	6
70%	100%	50%	60%	73.40%	66.30%	57.88%	2
70%	50%	50%	100%	84.86%	76.22%	66.43%	5

With the alternatives and scoring defined we will proceed to use the BBMW principles. BBWM is based on BWM, an MCDM method that can be used in various phases of solving an MCDM problem. According to [61], BBMW can be used to evaluate alternatives against criteria, especially in cases where objective metrics are not available to evaluate alternatives, and the BBMW process is the following:

1. Identify the best and the worst criteria or the alternatives before conducting the pairwise comparisons among the criteria or the alternatives.
2. Using two pairwise comparisons formed based on two opposite references (consider-the-opposite-strategy) in a single optimization model to mitigate possible anchoring bias during the process of conducting pairwise comparisons.

Table 4.10 Best worst method to calculate the weights of the IoT factor for evaluating security risk level.

Criteria Number	**Criterion 1**	**Criterion 2**	**Criterion 3**	**Criterion 4**
Names of Criteria	Severity	Scalability	Attack-Surface	Interdependency
Select the Best	Scalability			
Select the Worst	Interdependency			
Best to Others	Severity	Interdependency	Attack-Surface	Scalability
Risk Behaviors	2	6	5	1
Others to the Worst	Interdependency			
Severity	8			
Susceptibility	1			
Attack-Surface	4			
Scalability	7			
Weights	Severity	Scalability	Attack-Surface	Interdependency
	0,31976744	0,05813953	0,12790698	0,49418605
Ksi*	0,14534884			

The application of BBMW was made using the Table 4.10 [61]. We used the alternatives from Table 1. We can observe in alternatives 4 and 6 of Table 1, that the factor “interdependency” is the one with the major contribution to the impact. Whereas the factor “risk behaviors" is the one that does not affect significantly when changing its value. We can also observe that the factor “vulnerability” is the second one with a

relevant contribution to affect the impact value. This analysis is brought to the BBMW matrix in Table 8.9. The weight of the factors. So, the factor Severity is 0.319 (32%), Scalability is 0.058 (5.8%), Attack surface is 0.1279 (12.8%), and interdependency 0.494 (49.4%). The sum of all these values is 100%.

Decision matrix

To define the components of the decision matrix, we establish the weight on a scale from 1 to 10 for the different elements that make up the criteria, sub-criteria, and options of the MCDA model. In this case, the organization criterion is formed by the sub-criteria domain, pillar, system, security configurations, and vulnerabilities. The domain sub-criteria have as options the economic, social, and environmental axes. The pillars sub-criterion has as options health, energy, waste management, traffic, agriculture, home, which are the verticals where IoT solutions are used. Finally, the systems sub-criteria have the options IT, OT, and IoT, which represent the systems connected to the IoT device (See Figure 4.22).

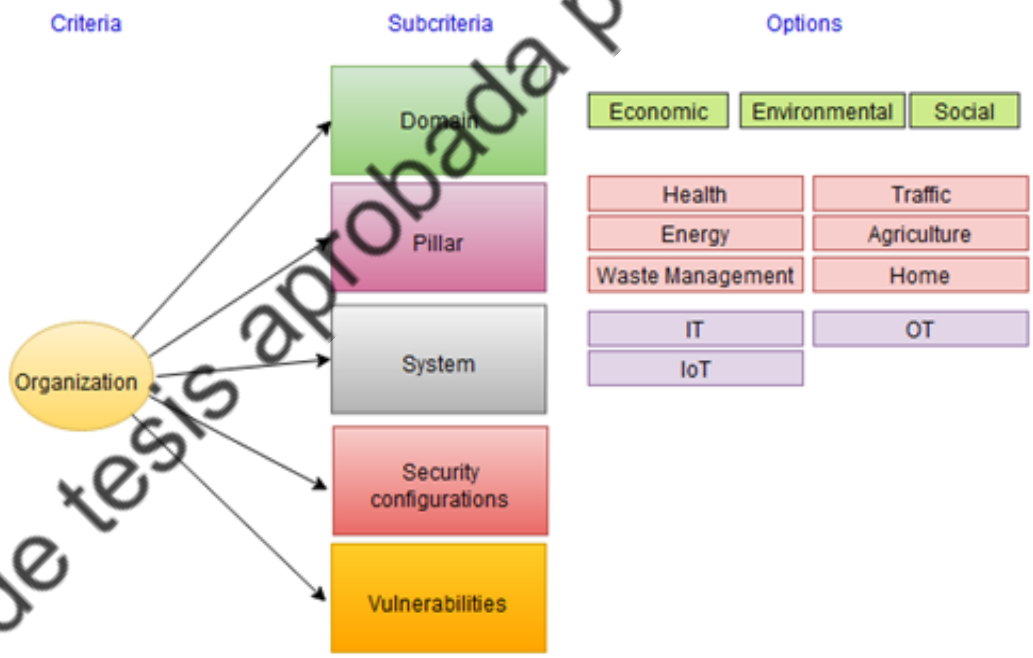


Figure 4.22 Criteria, subcriteria, and options for the factor organization.

Security configurations are related to the factor severity. The severity criterion has the criteria confidentiality, integrity, availability, traceability, authenticity as depicted in Figure 4.23.

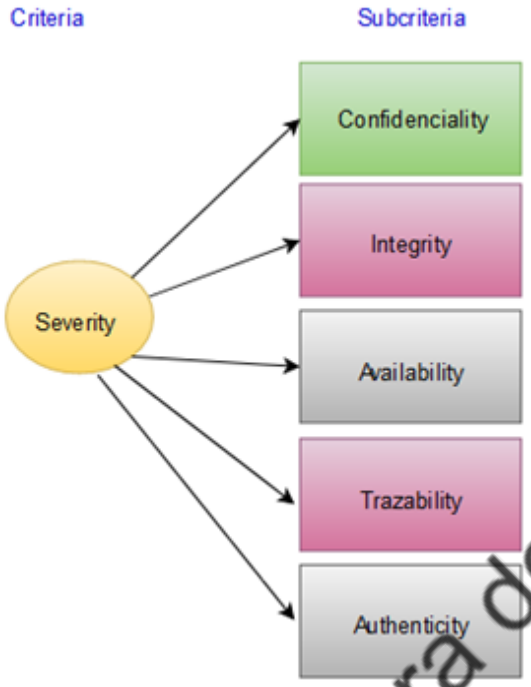


Figure 4.23 Criteria, subcriteria, and options for the factor severity.

The risk behaviors criterion has the sub-criteria impact/degradation, probability of occurrence, propagation time, the coverage area of propagation, previous attacks, as shown in Figure 4.24.

Figure 4.24 Criteria, subcriteria, and options for the factor risk behavior.

The attack surface criterion has the following sub-criteria: number of IoT devices, Threats, number of IoT layers, as illustrated in Figure 4.25.

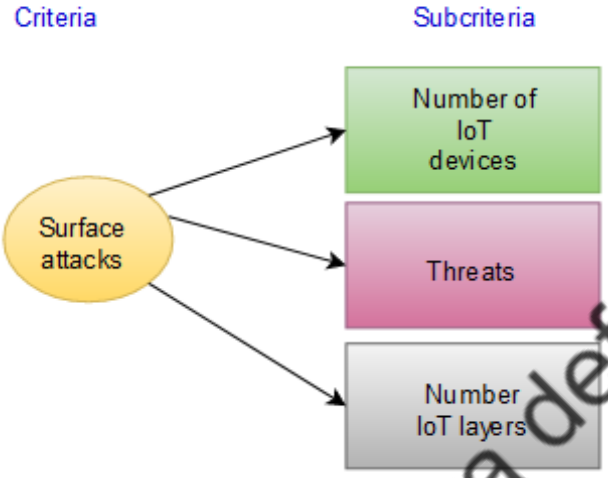


Figure 4.25 Criteria, subcriteria and options for the factor surface attack.

Finally, the interdependency criterion comprises upstream, downstream, functional, geographical, cybernetic as depicted in Figure 4.26

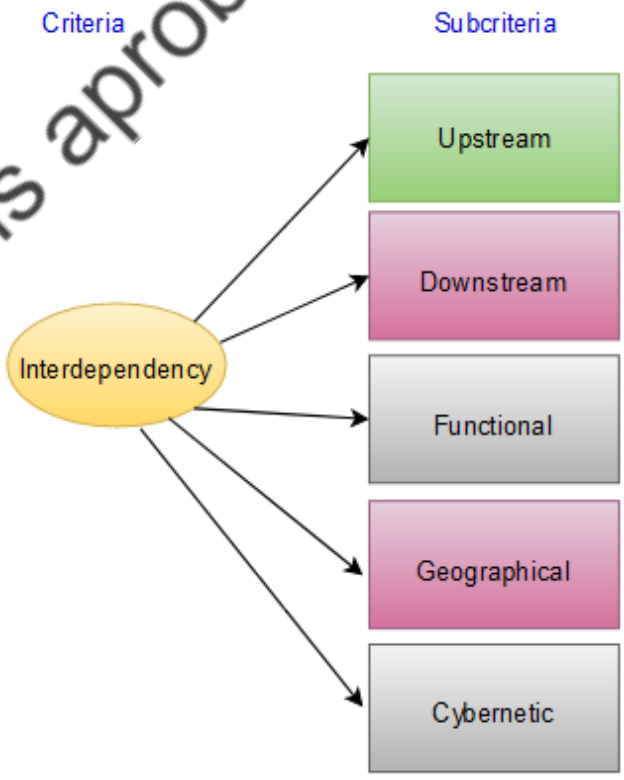


Figure 4.26 Criteria, sub-criteria, and options for the factor interdependency.

The weights of the criteria associated with IoT security risk can have different formats and sources. In the following, we describe the proposed sources for obtaining the values of the weights. The organization domain is at the top level and is more focused on the desired levels by the organization using the IoT solution at the strategic level. In this domain, we have the economic, social, and environmental levels supported by the IT, OT, and IoT pillars and systems. The levels of impact desirable are shown in Table 4.11. In our study, we selected for our proposal to have a security value higher than 70%, representing an acceptable security value.

Table 4.11 Security level based on the possible values of impact.

Security level	Impact level
80%-100%	Very Low
50%-80%	Low
30-50%	Medium
10%-30%	High
0-10%	Critic

Security configurations are those established by the organization based on the criticality of its information or application or compliance with regulations. For example, HIPPA for the case of health. In this proposal, we rely on the compliance class proposed by [67], based on the pillars of confidentiality, availability, integrity. However, since risk analysis proposals such as MAGERIT consider two additional security pillars, we include traceability and authenticity, proposing a modification of the class compliance as shown in Table 4.12.

Table 4.12 Compliance class for the level of security in IoT systems.

Compliance class	Description	Confidentiality	Integrity	Availability	Authenticy	Traceability	Score
Class 0	An imperceptible impact could happen in the IoT system.	Low	Low	Low	Low	Low	1-2
Class 1	The impact that could occur on the IoT system is limited.	Low	Medium	Medium	Medium	Medium	3-4
Class 2	Besides class 1, the IoT system withstands significant impacts to availability.	Medium	Medium	High	Medium	High	5-6
Class 3	Besides class 2, the IoT system protects sensitive data.	High	Medium	High	High	High	6-7
Class 4	Besides class 3, data compromise and loss of control have a critical impact on the IoT system.	High	High	High	High	High	8-10

Finally, vulnerabilities refer to the level due to security breaches expected from the IoT system. We rely on the proposal to establish a hardening process focused on compliance with CIS Controls. Additionally, the vulnerability value is defined using the Common Vulnerability Scoring System Version 3 (CVSSv3) shown in Table 4.13. In the IoT system, vulnerabilities could be present in each layer, so an aggregation of the vulnerability value according to the equations is proposed.

Table 4.13 The scores for CVSSv3.

Score	Severity
0	Null
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

The surface attack is based on Relative Attack Surface Quotient (RASQ), which measures the attack ability of an operating system and is obtained by multiplying the number of surfaces or elements that the attack vector can attack. Extrapolating to the IoT system, we have that the element is attackable in all the layers of the IoT system based on the interfaces, technologies, and applications used in the IoT system. The attack surface increases as a function of the number of IoT devices in the system. On the other hand, we have the threats that can affect the devices and elements of each IoT layer. We identified the threats concerning the CIS controls defined to establish a security level for the organization. In this case, we would have a numerical value given by the attack surface based on the IoT layers multiplied by the number of devices according to the following equations:

$$Attack\ suface\ IoT\ system = \frac{Attack\ suface(Perception + Network + Application)}{3} \quad \text{Equation 4.14}$$

$$Attack\ surface(Layer) = \frac{(\sum_{i=1}^{n} threat)}{n} \quad \text{Equation 4.15}$$

In this case, we rely on common characteristics of IoT devices to get an approximation. But it is crucial to evaluate any element of an IoT device that could increase its security risk and, therefore, affect the entire system.

The following criterion is the interdependence of the IoT system with other IT/OT and IoT systems. This interdependence value would be numerical and would be given by the dependency value generated by the IoT system: in the following subcriteria:

1. Upstream
2. Downstream
3. Functional
4. Geographical
5. Cybernetic

Finally, we have the risk behaviors criterion with a numerical and more probabilistic characteristic. Since we cannot know with certainty the impact or degradation of a system beforehand, we can only estimate it. The only way to have a real value would be in a post-mortem process, i.e., when the attack has occurred, but in our case, the objective of risk assessment is to be projective, so we rely on possibilities. Other elements are the probability of occurrence, propagation time, impact propagation coverage area, which will be probabilistic numerical values because we cannot know with certainty until a post-mortem process, so we rely on estimates. The sub-criteria previous attacks would be the only one that could be a non-probabilistic value since it would be estimated based on the analysis of previous events, and that could happen again. At this point, we are interested in observing how to integrate these sub-criteria represented by probabilistic values to obtain a value that integrates the projections made and the previous evidence, so we chose to take advantage of the contributions of Bayesian networks to estimate this value. A screenshot of the decision matrix for our MCDA proposal is shown in Table 4.14.

The objective of the MCDA is to establish a risk value for IoT systems. A weight has been established for each of the three criteria based on a total value out of 100 percent. Each criterion has a set of subcriteria, the case for “organization” has the subcriteria domains, pillars and systems. The criteria “scalability” has the subcriteria impact, probability of occurrence, propagation time and propagation coverage. Once the sub-criteria have been established, their corresponding weights have been defined based on a total value of 100% of their criteria. Thus, the criteria “organization” in sub-criterion has a value of 60%, pillars 25% and systems 15%. Finally, for the scalability, the values of the subcriteria have been established over 100% of the total value of the criterion as impact or degradation 50%, probability of occurrence 30%, propagation time 10% and propagation coverage 10%.

Table 4.14 MCDA to evaluate the security risk value for IoT systems.

Components	**Organization (54,9%)**				
	Domains	Pillars	Systems	Security configurations	Vulnerabilities
Weight	30%	20%	20%	10%	20%
Components	Scalability (12,39%)				
	Impact / degradation	P. Ocurrence	P.time	P.coverage	Previous Attacks
Weight	40%	30%	10%	10%	10%
Components	Attack Surface (11,92%)			Susceptibility (6,19%)	
	Number IoT dev.	Threats	Number IoT layers	No extra components	
Weight	40%	40%	40%	100%	
Components	Severity (7,18%)				
	Confidencialit y	Integrity	Avalability	Trazability	Authenticity
Weight	40%	20%	20%	10%	10%
Components	Interdependency (4,52%)				
	Upstream	Downstrea m	Functional	Geographical	Cybernetic
Weight	20%	20%	20%	20%	20%
Components	Uncertainty (2,9%)				
	No extra components				
Weight	100%				
***Domain (30%)**	Economic	Social	Environment al		
Weight	60%	25%	15%		

The next step is defining a value for each IoT system to evaluate. The value is set in range of 1 to 10, this is due to maintain normalization with others scoring tools like CVSS. A close value to 10 represents a major dependency of the risk factor with the IoT system. To stablish the value of IoT system the equations development in the mathematical model could be used.

4.4 Case of study: Evaluation IoT risk for smart home system

EXPERIMENTATION: MAGERIT applied to IoT systems

We focus on the application of MAGERIT to evaluate the IoT systems of the experiment 5 to observe how MAGERIT addresses the eight assumptions. To develop this experiment, we have had the support of undergraduate students from the School of Systems Engineering from EPN who have developed a degree project about the application of MAGERIT for security risk analysis in a Smart home. The phases of MAGERIT are show in the Figure 4.27.

Amenazas	robabilidad	Probabilidad	[D] Disponibil	[I] Integrid	[C] Confidenci
[E.2] Errores del administrador	0,01	MB	43%	26%	32%
[E.15] Alteración accidental de la información	1	M		33%	
[E.18] Destrucción de información	0,1	B	70%		
[E.19] Fugas de información	1	M			70%
[A.5] Suplantación de la identidad del usuario	1	M	50%	40%	30%
[A.6] Abuso de privilegios de acceso	0,1	B	38%	38%	28%
[A.11] Acceso no autorizado	0,01	MB	42%	42%	
[A.15] Modificación deliberada de la información	0,01	MB		32%	
[A.18] Destrucción de información	0,01	MB	40%		
[A.19] Divulgación de información	0,01	MB			24%

Figure 4.27 Screenshoot process to evaluate risk based on MAGERIT.

MAGERIT focuses on the evaluation of the critical assets of the organizations, for which it establishes a value based on the availability, integrity and confidentiality for each asset. Then evaluate the impact on each asset based on the degradation that can be generated by potential threats. Finally, we evaluate the risk based on the impact and probability of the occurrence of the threat. To apply MAGERIT in the IoT context the first aspect was identify the critical assets of the IoT system, but we identified two relevant aspects:

i) Several IoT devices could have similar criticality value.

ii) Include all IoT devices for analysis would be very time consuming given the large number of IoT devices.

A possible solution could be grouped IoT devices based on the requirements of confidentiality, integrity and availability; the IoT device could be classification into one of the five classes and based on that score define the level of risk based on the matrix of impact and risk. Additionality, MAGERIT doesn't has a typification for IoT devices. A IoT devices has capabilities for computer systems but also for network equipment. A possible solution is adding this typification in the list of assets.

MAGERIT considers the relationship of dependencies between assets, in the context of IoT this degree of dependency between devices can be considered high for the dependency of type: downstream, upstream, logical among others. But it would be important take in consideration other possible dependencies such as the relationship between attacks. MAGERIT evaluates the impact of the attacks independently, but an attack could be executed as a function of a first attack. For instance, if the probability of an attack 1 is 0.3 and there is evidence that the probability of an attack 2 happening if attack 1 previously existed is 0.7. Then the probability of the existence of the attack 1 is 0.5. It would be important to take in consideration the account of this relationship of the attacks in the methodology of risk analysis.

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$ Equation 4.16

MAGERIT focuses mainly on assets, in the context of IoT there are several IoT devices that can support different domains (energy, traffic, waste management) and their affectation can have impacts on the normal operation of cities or countries. So, it would be important consider the impact on the social, economic and environmental contexts due to the degradation of IoT device due to different attacks or threats.

IOT RISK

We define a system to evaluate. In the case of the smart home, we consider that the contribution is more to the social context with 65%, followed by the environmental at 25% and finally economic with 10% (See Table 4.15).

Table 4.15 Proposal of weights for economic, social and environmental domains

	Domain		
IoT system	0,6		
	Economic	Social	Enviromental
	0,6	0,25	0,15
IoTX	6	6	6
IoTY	5	6	6
IoTZ	2	6	6

Next, we define the pillars that would be associated. In the case of the smart home has a contribution to home conditions of 75%, the smart home can also contribute to health aspects of the people who live in the home of 10%, improvement in energy of 10% and administration of waste of 5%. In this case we would not have a contribution to the traffic or agriculture pillars (Table 4.16). Next, we established the security requirements for smart home solution. In this case we assume three systems: voice assistant, smart lights and a health check. We evaluate its relation to the security requirements in Table 4.17 and security class in Table 4.18. Also, we define the attack surface in Table 4.19

Table 4.16 Proposal of weights for pillars

Pillars					
0,25					
Health	**Energy**	**Waste M**	**Traffic**	**Agriculture**	**Home**
0,2	**0,55**	**0,05**	**0,1**	**0,05**	**0,05**
6	3	2	1	1	2
6	3	2	1	1	2
6	3	2	1	1	2

Table 4.17 Proposal of weights for pillars

	Confidenciality	**Integrity**	**Auntenticity**	**Trazability**	**Availability**
IoT X	High	High	High	Medium	Low
IoT Y	High	High	High	High	High
IoT Z	Medium	Medium	Medium	Medium	Medium

Table 4.18 Proposal weights for IoT security class

System	**Class**
IoT X	4
IoT Y	4
IoT Z	2

Table 4.19 Proposal weights for attack surface

Layer	**Process**	**Type**	**Weight**
Physical	Secure and centralize records	Data	1
	Encrypted communication protocols	Channel	10
	Strong and secure passwords	Method	10
	Last stable firmware or operating system version	Method	10
Communication	Monitoring of communication protocols	Method	7
	Ports used in a range different for the known ports	Channel	8
	Protocols used have encryption	Channel	9
	Separate wireless network	Channel	8
Application	Safe coding practices	Method	8
	Explicit error checking for all internal development software	Method	8
	Adquired software support	Method	7
	Up-to-date and trusted third-party component	Channel	8
	Encryption of tested and standarized algortihms	Method	8
	Personnel trained in secure software development	Method	7
	Static and dynamic code analysis	Channel	7
	Separate production and non-production systems	Method	5
	Web application firewall	Channel	5

Next, we define the importance of the weight of each of the layers for the smart home solution to attack surface in the Table 4.20. Then, in Table 4.21, we identify the possible threats to the smart home solution for each IoT layer. Then, we define the values of IoT systems related with each risk factors in Table 4.22, Table 4.23, and Table 4.24.

Table 4.20 Proposal weights for importance of IoT layers.

IoT Layers and unknown factors	Weight percentage (0-1)
Physical layer	0,5
Communication layer	0,2
Application layer	0,2
Uncertainty	0,1

Table 4.21 Proposal weights for threats to IoT layers

	Total possible threats	Threat 1	Threat 2	Threat 3	Attack Surf
Physical layer	3,5	0	0	0	0,00
		Threat 1	Threat 2	Threat 3	
Communication layer	7,6	0,5	0,5	0	0,03
		Threat 1	Threat 2	Threat 3	
Application layer	13,2	0,1	0,1	0	0,00
Total attack surface		8,71			

Table 4.22 Proposal weights for Scalability factors

IoT system	Scalability (12,39%)				
	Impact / degradation	P. Ocurrence	P.time	P.coverage	Previous Attacks
	0,4	0,3	0,1	0,1	0,1
IoTX	3	1	2	3,00	2,00
IoTY	5	4	3	2,00	1,00
IoTZ	6	5	4	5,00	2,00

Table 4.23 Proposal weights for attack surface factors

IoT system	Attack Surface (11,92%)		
	Number IoT dev.	Threats	Number IoT layers
	0,4	0,4	0,2
IoTX	3	1	2
IoTY	5	4	3
IoTZ	6	5	4

Table 4.24 Proposal weights for Severity factors

IoT system	Severity (7,18%)				
	Confidenciality	Integrity	Avalability	Trazability	Authenticity
	0,4	0,2	0,2	0,1	0,1
IoTX	1	2	3	4	5
IoTY	2	5	3	4	5
IoTZ	3	4	3	4	5

Finally, Table 4.25 shows the risk values for the IoT systems evaluated. In this case, the system IoTY shows a major risk value (4.10/10) than other IoT systems evaluated. However, from the data on Table 8.5, the value of 4.10 represents of 41% of possible economic impact, which is below the umbral to consider it in the development of systemic risk.

Exemplifying, from the three IoT devices: voice assistant (IoT-X), health check (IoT-Y) and smart lights (IoT-Z). The risk analysis gives an overview of that the device IoT-Y may generate a higher risk, and this may be consistent with the type of information (sensitive). From the data on Table 8.5, the value of 4.10 represents 41% of possible economic impact, which is below the threshold to consider it in the development of systemic risk. Additionally, with the quantitative risk value, could be complement with an economic valuation as CVAR. If we establish a valuation of a ransomware attack could reach $2,000, the security risk of the IoT-Y system would represent $800.

Table 4.25 Risk values for IoT systems

IoT system	Organization	Scalability	Attack Surface	Severity	Susceptibility	Interdependency	Uncertainity	Risk Total (/10)
	54,9	**12,39**	**11,92**	**7,18**	6,19	**4,52**	2,9	
IoTX	4,82	2,20	2,00	2,30	3,00	2,30	2,00	3,67
IoTY	4,46	3,80	3,30	4,20	4,00	3,30	3,00	4,10
IoTZ	3,38	5,00	3,50	5,20	5,00	3,50	1,00	3,76

4.5 Summary and Implications

MAGERIT allows a security risk classification focused on each asset but does not provide a comprehensive view of the entire IoT solution. Additionally, regarding the assets, it does not have a specific classification for IoT devices in its catalogue. MAGERIT does not analyse the possible impact on strategic objectives related to economic, social or environmental aspects. Also, MAGERIT focus more on the valuation of assets in a qualitative manner with low, medium and high values or a map of risk colours (green, yellow, red). On the other side, a quantitative risk value allows establish a monetary value for the security risk to evaluate the cost-benefit in the implementation of security controls.

An important aspect of MAGERIT versus other risk methodologies is that it assesses the interoperability between assets. But in the context of IoT is important to assess of interdependence, not only of the assets of the organization, also to the IT and OT solutions of organizations or verticals that interrelation with IoT systems.

Finally, MAGERIT does not carry an evaluation of the attack surface based on the number of devices. This is important in the context of IoT because one of the particularities is the large number of IoT devices that are projected to be used in different verticals, and even more with the deployment of sixth and seventh generation of mobile networks, the number of IoT devices will drive further growth. Table 4.26 shows a comparative in the application of MAGERIT and the IoT risk proposal to evaluate IoT systems.

Table 4.26 Comparative between MAGERIT vs IoT-Risk

Methodology	Computer Security risk analysis (MAGERIT)	IoT Risk
Focus on	Assets	Context (social, environmental, economic)
Priority	Top of critical assets	Top of group of critical assets
Dependency of	Assets	Assets /Threats
Type Assets	Individual critical assets	Grouped critical assets (based on classes or security levels)
Security factors on the assets	Confidentiality, Integrity, Availability, Trazability and Authenticity	Confidentiality, Integrity, Availability, Trazability and Authenticity
Vulnerabilities	Overall approach	Based on IoT layers (application, communication, device)
Attack surface	Doesn´t include in the methodology.	Based on relation among systems and IoT layers.

CHAPTER 5

5. CONCLUSIONS

In this thesis, the importance of IoT in digital transformation processes and the security aspects that are generated by the intrinsic characteristics of IoT devices have been studied. In this context, the risk factors associated with IoT devices that can be considered more relevant when a security risk analysis process is carried out have been investigated.

In chapter 3, the risk factors associated with IoT devices and that are considered relevant for security risk assessment processes, as well as their relationships, have been defined. The results presented allow answer to objective 1 and 2 raised in this investigation. In general, the established macro factors are described below:

Organization domain. Considers the evaluation of the strategic objectives of IoT systems based on their application domain, such as energy, traffic, health, home, and based on the pillars that support the application domain, such as technology, economy, environment, and society.

Dependency/interdependency domain: Considers the evaluation of the interdependencies created based on the interconnections between IoT devices or IT and OT systems.

Attack surface domain: Considers the evaluation of the attack surface based on the number of IoT devices, communication methods and channels, and vulnerabilities in each layer of the IoT model.

Susceptibility domain: Considers the evaluation of the susceptibility of IoT devices based on characteristics such as their physical location, application domain and vulnerabilities.

Severity domain: Considers the evaluation of the impact of the solution based on the application domain, type of device and type of information.

Scalability domain: Considers the evaluation of the scalability of an attack based on the interdependence, number of devices, which allows evaluating the possible cascade or domino effects of security attacks.

Uncertainty domain: Considers factors that cannot be easily determined, such as the action of an attacker deciding to attack at a given time, which is why projections are considered.

Chapter 4 has presented how these factors can be used in a risk assessment methodology. The analysis methodology presented is based on MCDA (multicriteria analysis) and the important contribution is that a quantitative assessment is presented that can be complemented with financial analysis to evaluate the possibility that the risk exceeds the absorption capacity of the organizations. The methodology encompasses a top-down vision based on risk analysis based on the impact on strategic objectives.

The methodologies discussed in this study such as FAIR, TARA, MAGERIT or ISO 27005, can be considered to assess the security risk in IoT systems, but is recommended to consider their adaptation to include elements such as the number of IoT devices that affect the surface of attack, and that can modify the behaviour of the risk due to the scalability that a security attack could have.

BIBLIOGRAPHY

1. Tanseer, N. Kanwal, M. N. Asghar, A. Iqbal, F. Tanseer and M. Fleury, "Real-time content-based communication load reduction in the Internet of multimedia things", *Appl. Sci.*, vol. 10, no. 3, pp. 1152, Feb. 2020, [online] Available: https://www.mdpi.com/2076-3417/10/3/1152.

2. M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh and G. Wang, "Security and attack vector analysis of IoT devices" in Security Privacy and Anonymity in Computation Communication and Storage, Cham, Switzerland:Springer, pp. 593-606, 2017.

3. V. Kumar, G. Oikonomou and T. Tryfonas, "Traffic forensics for IPv6-based wireless sensor networks and the Internet of Things", *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, pp. 633-638, Dec. 2016.

4. X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao and W. Yu, "Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey case study and research opportunities", *IEEE Access*, vol. 7, pp. 79523-79544, 2019.

5. Radanliev, P.; De Roure, D.; Page, K.; Nurse, J.R.C.; Montalvo, R.M.; Santos, O.; Maddox, L.T.; Burnap, P. Cyber Risk at the Edge: Current and Future Trends on Cyber Risk Analytics and Artificial Intelligence in the Industrial Internet of Things and Industry 4.0 Supply Chains. December 2020. Available online: https://www.preprints.org/manuscript/201903.0123/v2 (accessed on 19 January 2021).

6. Kieras, T.; Farooq, J.; Zhu, Q. RIoTS: Risk analysis of IoT supply chain threats. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020.

7. J. R. C. Nurse, S. Creese and D. De Roure, "Security Risk Assessment in Internet of Things Systems," in *IT Professional*, vol. 19, no. 5, pp. 20-26, 2017, doi: 10.1109/MITP.2017.3680959.

8. Kannengiesser, U.; Müller, H. Towards viewpoint-oriented engineering for Industry 4.0: A standards-based approach. In Proceedings of the 2018 IEEE

Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 15–18 May 2018; pp. 51–56.

9. Banafa, A. 2 The Industrial Internet of Things (IIoT): Challenges, requirements and benefits. In Secure and Smart Internet of Things (IoT): Using Blockchain and AI; River Publishers: Gistrup, Denmark, 2018; pp. 7–12.
10. M. D. Lytras, A. Visvizi, M. Torres-Ruiz, E. Damiani and P. Jin, "IEEE access special section editorial: Urban computing and well-being in smart cities: Services applications policymaking considerations", IEEE Access, vol. 8, pp. 72340-72346, 2020.
11. R. O. Andrade, S. G. Yoo, L. Tello-Oquendo and I. Ortiz-Garcés, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities," in IEEE Access, vol. 8, pp. 228922-228941, 2020, doi: 10.1109/ACCESS.2020.3046442.
12. Z. Xiaojian, C. Liandong, F. Jie, W. Xiangqun and W. Qi, "Power IoT security protection architecture based on zero trust framework," 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), 2021, pp. 166-170, doi: 10.1109/CSP51677.2021.9357607.
13. Draft NISTIR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks Out for Public Comment. NIST. (2022). Retrieved 20 June 2022, from https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy.
14. Arampatzis, T., et al. (2005) A Survey of Security Issues in Wireless Sensors Networks, in Intelligent Control. Proceeding of the IEEE International Symposium on, Mediterrean Conference on Control and Automation, 719-724.
15. Al-Sarawi, Shadi, Mohammed Anbar, Rosni Abdullah, and Ahmad B. Al Hawari. 2020. Internet of Things Market Analysis Forecasts, 2020–2030. Paper presented at 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, July 27–28; pp. 449–53.
16. Andrade, R.O.; Yoo, S.G. A Comprehensive Study of the Use of LoRa in the Development of Smart Cities. *Appl. Sci.* 2019, *9*, 4753. https://doi.org/10.3390/app9224753

17. Roberto O. Andrade, Sang Guun Yoo, Luis Tello-Oquendo, Iván Ortiz-Garcés, Chapter 12 - Cybersecurity, sustainability, and resilience capabilities of a smart city, Editor(s): Anna Visvizi, Raquel Pérez del Hoyo,Smart Cities and the un SDGs,Elsevier,2021,Pages 181-193,ISBN 9780323851510, https://doi.org/10.1016/B978-0-323-85151-0.00012-9.

18. Andrade, Roberto & Yoo, Sang Guun & Cazares, Maria. (2019). A COMPREHENSIVE STUDY OF IOT FOR ALZHEIMER'S DISEASE.

19. R. O. Andrade, S. G. Yoo, L. Tello-Oquendo and I. Ortiz-Garcés, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities," in *IEEE Access*, vol. 8, pp. 228922-228941, 2020, doi: 10.1109/ACCESS.2020.3046442.

20. Telecommunication Standardization Sector of ITU. Series Y: Global information infrastructure, internet protocol aspects and next-generation networks. In Recommendation ITU-T Y, 2060–Overview of the Internet of Things; IUT: Geneva, Switzerland, 2012; pp. 1–6.

21. Andrade, Roberto & Tello Oquendo, Luis & Ortiz, Iván. (2021). Cybersecurity Risks of IoT on Smart Cities. 10.1007/978-3-030-88524-3_1.

22. Echeverría, A.; Cevallos, C.; Ortiz-Garces, I.; Andrade, R.O. Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation. *Appl. Sci.* 2021, *11*, 3260. https://doi.org/10.3390/app11073260

23. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP J. Inf. Secur. 2020, 2020, 8

24. Andrade, R.; Ortiz-Garcés, I.; Tintin, X.; Llumiquinga, G. Factors of Risk Analysis for IoT Systems. *Risks* 2022, *10*, 162. https://doi.org/10.3390/risks10080162

25. Barriga, J.J.; Sulca, J.; León, J.L.; Ulloa, A.; Portero, D.; Andrade, R.; Yoo, S.G. Smart Parking: A Literature Review from the Technological Perspective. *Appl. Sci.* 2019, *9*, 4569. https://doi.org/10.3390/app9214569

26. Roberto O Andrade, Sang Guun Yoo, Cognitive security: A comprehensive study of cognitive science in cybersecurity, Journal of Information Security and Applications, Volume 48, 2019, 102352, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2019.06.008.

27. R. O. Andrade, I. Ortiz-Garcés and M. Cazares, "Cybersecurity Attacks on Smart Home During Covid-19 Pandemic," *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2020, pp. 398-404, doi: 10.1109/WorldS450073.2020.9210363.

28. S. Singh and N. Singh, "Internet of Things (IoT): Security challenges business opportunities & reference architecture for E-commerce", Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT), pp. 1577-1581, Oct. 2015.

29. Lopez-Vargas, M. Fuentes and M. Vivar, "Challenges and opportunities of the Internet of Things for global development to achieve the united nations sustainable development goals", IEEE Access, vol. 8, pp. 37202-37213, 2020.

30. F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-Turjman, et al., "Cyber security threats detection in Internet of Things using deep learning approach", IEEE Access, vol. 7, pp. 124379-124389, 2019.

31. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A survey on IoT security: Application areas security threats and solution architectures", IEEE Access, vol. 7, pp. 82721-82743, 2019.

32. Laszka, B. Potteiger, Y. Vorobeychik, S. Amin and X. Koutsoukos, "Vulnerability of transportation networks to traffic-signal tampering", Proc. ACM/IEEE 7th Int. Conf. Cyber-Phys. Syst. (ICCPS), pp. 1-10, Apr. 2016.

33. P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues and Y. Park, "Authentication protocols in Internet of vehicles: Taxonomy analysis and challenges", IEEE Access, vol. 8, pp. 54314-54344, 2020.

34. S. Soltan, M. Yannakakis and G. Zussman, "REACT to cyber attacks on power grids", IEEE Trans. Netw. Sci. Eng., vol. 6, no. 3, pp. 459-473, Jul. 2019.

35. R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems", J. Water Resour. Planning Manage., vol. 143, no. 5, May 2017.

36. Butun, P. Osterberg and H. Song, "Security of the Internet of Things: Vulnerabilities attacks and countermeasures", IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 616-644, 1st Quart. 2020.

37. Fahmideh, M.; Yan, J.; Shen, J.; Mougouei, D.; Zhai, Y.; Ahmad, A. A Comprehensive Framework for Analyzing IoT Platforms: A Smart City Industrial Experience. Smart Cities 2021, 4, 588-622. https://doi.org/10.3390/smartcities4020031

38. Pal, S.; Jadidi, Z. Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. Appl. Sci. 2021, 11, 9393. https://doi.org/10.3390/app11209393

39. Ferrara, P., Mandal, A.K., Cortesi, A. et al. Static analysis for discovering IoT vulnerabilities. Int J Softw Tools Technol Transfer 23, 71–88 (2021). https://doi.org/10.1007

40. R. Wang, H. Song, Y. Jing, K. Yang, Y. Guan and J. Sun, "A Sensor Attack Detection Method in Intelligent Vehicle with Multiple Sensors," 2019 IEEE International Conference on Industrial Internet (ICII), 2019, pp. 219-226, doi: 10.1109/ICII.2019.00047.

41. N. Bhushana Samyuel, Benjamin A. Shimray, Securing IoT device communication against network flow attacks with Recursive Internetworking Architecture (RINA), ICT Express, Volume 7, Issue 1, 2021, Pages 110-114, ISSN 2405-9595, https://doi.org/10.1016/j.icte.2020.08.001.

42. Fan Wu, Min Gao, Junliang Yu, Zongwei Wang, Kecheng Liu, Xu Wang, Ready for emerging threats to recommender systems? A graph convolution-based generative shilling attack, Information Sciences, Volume 578,2021, Pages 683-701,ISSN 0020-0255

43. S. K. Lala, A. Kumar and S. T., "Secure Web development using OWASP Guidelines," *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2021, pp. 323-332, doi: 10.1109/ICICCS51141.2021.9432179.

44. Toapanta, S.M.T.; Pesantes, R.P.R.; Gallegos, L.E.M. Impact of Cybersecurity Applied to IoT in Public Organizations in Latin America. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 154–161

45. Aydos, M.; Vural, Y.; Tekerek, A. Assessing risks and threats with layered approach to Internet of Things security. Meas. Control 2019, 52, 338–353

46. Popescu, T.; Popescu, A.; Prostean, G. IoT Security Risk Management Strategy Reference Model (IoTSRM2). Future Internet 2021, 13, 148

47. Levitsky, D. Assessing Risk in IoT Systems. Ph.D. Thesis, California Polytechnic State University, San Luis Obispo, CA, USA, 2018.

48. Siksnelyte-Butkiene, I.; Zavadskas, E.K.; Streimikiene, D. Multi-Criteria Decision-Making (MCDM) for the Assessment of Renewable Energy Technologies in a Household: A Review. Energies 2020, 13, 1164. https://doi.org/10.3390/en13051164

49. Blessing, Lucienne & Chakrabarti, Amaresh. (2009). DRM, a Design Research Methodology. 10.1007/978-1-84882-587-1.

50. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. PLoS Med. **2009**, 6, e1000097

51. Ibrahim, M.; Al-Hindawi, Q.; Elhafiz, R.; Alsheikh, A.; Alquq, O. Attack Graph Implementation and Visualization for Cyber Physical Systems. Processes 2020, 8, 12. https://doi.org/10.3390/pr8010012

52. Hallouin, Thibault & Bruen, Michael & Kelly-Quinn, Mary & Christie, Michael & Bullock, Craig & Kelly, Fiona & Feeley, Hugh. (2016). Multi-Criteria Decision Analysis and Ecosystems Services: knowledge gaps and challenges for policy and decision-making.

53. Bank of England. Could a cyber attack cause a systemic impact in the financial sector? (2018) Bank of England. Available at: https://www.bankofengland.co.uk/quarterly-bulletin/2018/2018-q4/could-a-cyber-attack-cause-a-systemic-impact-in-the-financial-sector (Accessed: November 30, 2022).

54. Vermersch P, Martinelli V, Pfleger C, Rieckmann P, Alonso-Magdalena L, Galazka A, Dangond F, Phillips L. Benefit-risk Assessment of Cladribine Using Multi-criteria Decision Analysis (MCDA) for Patients With Relapsing-remitting

Multiple Sclerosis. Clin Ther. 2019 Feb;41(2):249-260.e18. doi: 10.1016/j.clinthera.2018.12.015. PMID: 30846120.

55. Ruggeri, M.; Cadeddu, C.; Roazzi, P.; Mandolini, D.; Grigioni, M.; Marchetti, M. Multi–Criteria–Decision–Analysis (MCDA) for the Horizon Scanning of Health Innovations an Application to COVID 19 Emergency. Int. J. Environ. Res. Public Health 2020, 17, 7823. https://doi.org/10.3390/ijerph17217823

56. Renato Carauta Ribeiro and Edna Dias Canedo. 2020. Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security. In The 21st Annual International Conference on Digital Government Research (dg.o '20). Association for Computing Machinery, New York, NY, USA, 175–184. DOI:https://doi.org/10.1145/3396956.3398252

57. Zenonas Turskis, Nikolaj Goranin, Assel Nurusheva, Seilkhan Boranbayev, Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach, Informatica 30(2019), no. 1, 187-211, DOI 10.15388/Informatica.2019.203

58. Ganin AA, Quach P, Panwar M, Collier ZA, Keisler JM, Marchese D, Linkov I. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Anal. 2020 Jan;40(1):183-199. doi: 10.1111/risa.12891. Epub 2017 Sep 5. PMID: 28873246.

59. Umm-e-Habiba, & Asghar, S. (2009). A survey on multi-criteria decision making approaches. 2009 International Conference on Emerging Technologies. doi:10.1109/icet.2009.5353151

60. Jafar Rezaei, Best-worst multi-criteria decision-making method,Omega,Volume 53,2015,Pages 49-57,ISSN 0305-0483,https://doi.org/10.1016/j.omega.2014.11.009.

61. Rezaei, J. (2020). A Concentration Ratio for Non-Linear Best Worst Method. International Journal of Information Technology & Decision Making, 19(3), pp. 891-907.

62. J. Wu, L. Yin and Y. Guo, "Cyber Attacks Prediction Model Based on Bayesian Network," 2012 IEEE 18th International Conference on Parallel and Distributed Systems, 2012, pp. 730-731, doi: 10.1109/ICPADS.2012.117.

63. Zhang, Qi, Zhou, Chunjie, Tian, Glen, Xiong, Naixue, Qin, Yuanqing, & Hu, Bowen. (2018). A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. IEEE Transactions on Industrial Informatics, 14(6), pp. 2497-2506.

64. Gürkan Sin, Krist V. Gernaey, Improving the Morris method for sensitivity analysis by scaling the elementary effects, Editor(s): Jacek Jeżowski, Jan Thullie, Computer Aided Chemical Engineering, Elsevier,Volume 26,2009,Pages 925-930,ISSN 1570-7946,ISBN 9780444534330, https://doi.org/10.1016/S1570-7946(09)70154-3.

65. Zhang, X. Y., Trame, M. N., Lesko, L. J., & Schmidt, S. (2015). Sobol Sensitivity Analysis: A Tool to Guide the Development and Evaluation of Systems Pharmacology Models. CPT: pharmacometrics & systems pharmacology, 4(2), 69–79. https://doi.org/10.1002/psp4.6

66. Depaoli Sarah, Winter Sonja D., Visser Marieke. (2020). The Importance of Prior Sensitivity Analysis in Bayesian Statistics: Demonstrations Using an Interactive Shiny App, Frontiers in Psychology, 11, https://www.frontiersin.org/article/10.3389/fpsyg.2020.608045 . doi:10.3389/fpsyg.2020.608045

67. C. Bormann, M. Ersue, and A. Keranen, “Terminology for Constrained-Node Networks,” RFC 7228 (Informational), Internet Engineering Task Force, May 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7228.txt

APPENDICES

Appendix A

Survey to identify risk factors.

The following are the questions asked in the focus group based on the assumptions raised in relation to security risks in IoT systems. Each question has been coded as a variable to subsequently carry out the factorial analysis.

- **Var1:** Cyberattacks on IoT systems could affect to economic, social or environmental domains?
- **Var2:** Cyberattacks to IoT systems could be affected to other IoT, IT and OT systems.
- **Var3:** The growth of number of IoT devices could increase the probability of cyberattacks?
- **Var4:** Cyberattacks on IoT systems could generate shock on markets or risk systemic events?
- **Var5:** Security configurations on IoT devices depends of domains or pillars where IoT devices will be used?
- **Var6:** Interdependency of IoT device with other IoT, IT, and OT systems could increase the probability to attack IoT systems and cause bigger damage?
- **Var7:** The growth on the number of IoT devices could increase the susceptibility to suffer cyberattacks on organizations due to the large surface attack?
- **Var8:** Vulnerabilities on IoT devices could increase the probability of cyber-attacks to IoT systems?
- **Var9:** IoT devices are susceptible to specific type of cyberattacks?
- **Var10:** Previous attack allows the execution of new attacks?
- **Var11:** Attacks could be executed on different layers?
- **Var12:** Security configurations on IoT device could increase the susceptibility to be attacked?

- **Var13:** Cyberattacks could generate degradation in the operation of IoT devices?
- **Var14:** Cyberattacks could affect to CIA on IoT systems?
- **Var15:** Cyberattacks could be scaled from one layer of IoT system to other one.
- **Var16:** The frequency of cyberattacks could increase the successful of them?
- **Var17:** Short times on the propagation of cyberattacks could increase the damage of cyberattacks?
- **Var18:** Cyberattack could affect different layers of IoT systems increase the surface of damage?
- **Var19:** The risk value will depend on the probability that threats can capitalize on IoT systems, but also on related systems, such as IT and OT.
- **Var20:** The risk, severity and probability values will depend on the level of dependency and interdependency between IT, OT and IoT systems?
- **Var21:** Risk and severity values will depend on the relationship of IT, IoT and OT systems to the social, economic and environmental pillars supported by IoT solutions?
- **Var22:** The value of the risk will depend on the type of information in the IoT device, its physical location and the application supporting the IoT solution?
- **Var23:** The value of the risk will depend on the security controls in place to protect the IoT device information.
- **Var24:** The value of the risk will depend on the type of attacks on the social, economic and environmental pillars supported by the IoT solution?
- **Var25:** The value of the risk will depend on the number of attacks on IoT systems and the relationship these attacks may have to improving their effectiveness?
- **Var26:** The value of the risk will depend on the value of the surface attack and the vulnerability score of the IoT system?

- **Var27:** Cyberattacks on IoT systems could affect to economic, social or environmental domains?

The Figure A.1 and Figure A.2 show screenshots of the questions developed in google forms. A total of 70 responses by security experts were collected for the factor analysis.

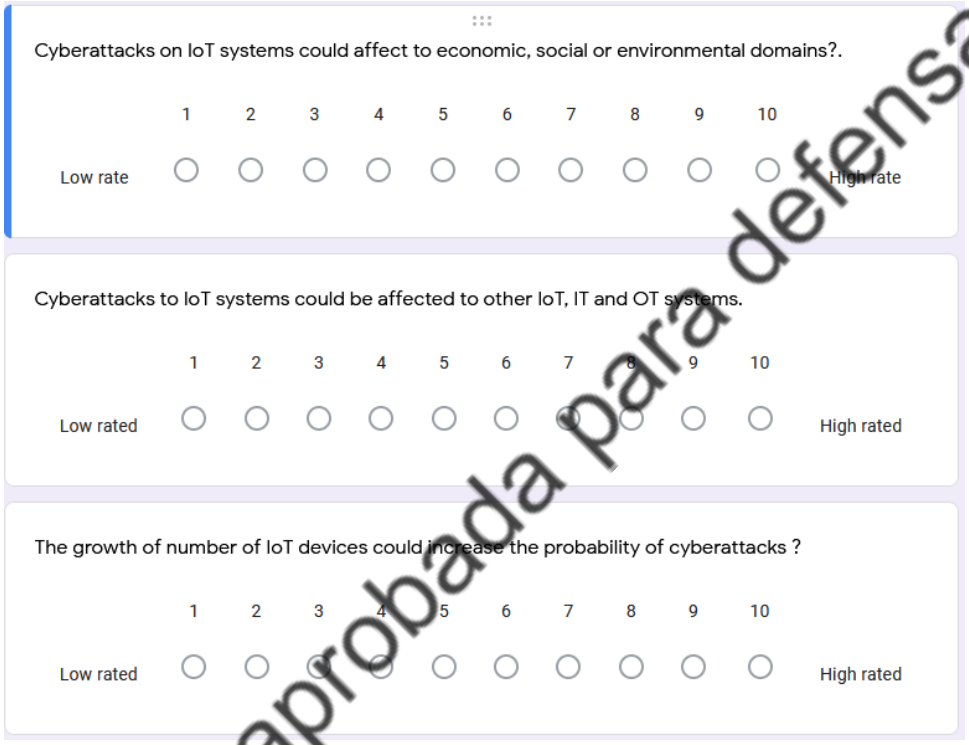


Figure A.1 Screenshot of questions developed in Google Forms

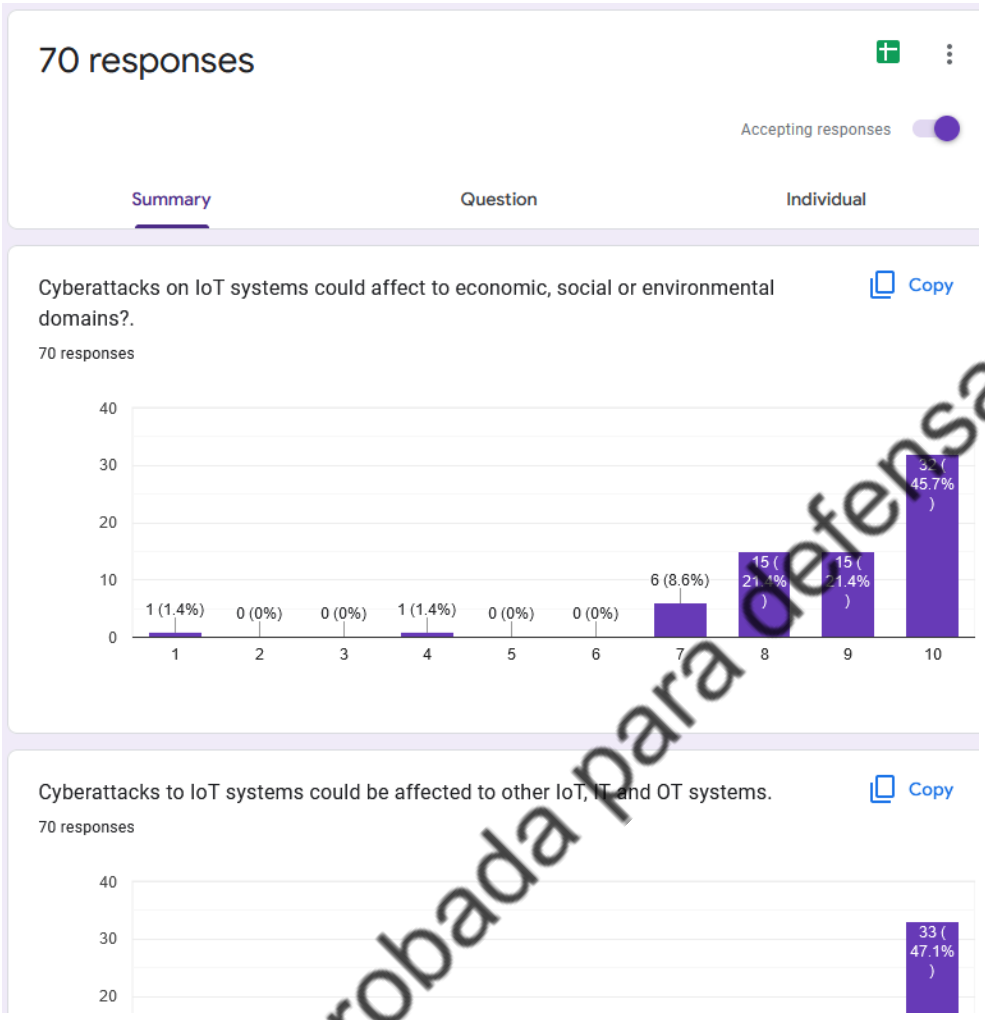


Figure A.2 Screenshot of the number of responses and the responses by security experts based in categorical data.

Appendix B

Results of factors analysis categorical CATPCA

Factor analysis allows analyse the main components that have the greatest contribution to the variance (information). In the case of this study the components are associated with IoT device´s factors affecting on the security risks in IoT systems. The objective of factor analysis is grouped and reduced the information of the 27 variables (questions) to a smaller number of variables.

The results obtained from the survey of security experts were analysed through factor analysis. The Table B.1 shows total explained variance. From component 7 to component 27 the variance contribution is not significant. Since the component 8 the values are less than zero. Form factor analysis the number of components can be reduced to seven.

Subsequently, using the correlation matrix, was possible identify the relation of each one of the 27 questions with the seven main components. It has been considered that values that are strongly related were those that exceed 0.3. While correlation values less than 0.3 are considered with weak relation.

The analysis has been carried out using the SPSS tool. To corroborate the results, form factor analysis also has been carried considering the data as non-categorical variables, obtaining similar results of 7 main components. Figure B.1 and Figure B.2 show screenshots of results obtained from SPSS using CATPCA. Figure B.4 show the correlational matrix, the results are similar those obtained previously.

Table B.1 Performance indices of IoT security Bayesian Model

	Autovalores iniciales			Sumas de cargas al cuadrado de la extracción	
Component	Total	% de variance	% acumulado	Total	% de variance
1	14,822	54,895	54,895	14,822	54,895
2	3,344	12,385	67,280	3,344	12,385
3	3,218	11,918	79,197	3,218	11,918
4	1,938	7,178	86,375	1,938	7,178
5	1,671	6,190	92,565	1,671	6,190
6	1,219	4,516	97,081	1,219	4,516
7	,788	2,919	100,000	,788	2,919
8	1,321E-15	4,892E-15	100,000	1,321E-15	4,892E-15
9	1,228E-15	4,547E-15	100,000	1,228E-15	4,547E-15
10	6,611E-16	2,449E-15	100,000	6,611E-16	2,449E-15
11	5,464E-16	2,024E-15	100,000	5,464E-16	2,024E-15
12	3,544E-16	1,313E-15	100,000	3,544E-16	1,313E-15
13	2,572E-16	9,525E-16	100,000	2,572E-16	9,525E-16
14	1,807E-16	6,691E-16	100,000	1,807E-16	6,691E-16
15	1,168E-16	4,326E-16	100,000	1,168E-16	4,326E-16
16	9,277E-17	3,436E-16	100,000	9,277E-17	3,436E-16
17	-2,212E-17	-8,194E-17	100,000	2,212E-17	8,194E-17
18	-7,544E-17	-2,794E-16	100,000	7,544E-17	2,794E-16
19	-8,739E-17	-3,237E-16	100,000	8,739E-17	3,237E-16
20	-1,868E-16	-6,919E-16	100,000	1,868E-16	6,919E-16
21	-2,690E-16	-9,963E-16	100,000	2,690E-16	9,963E-16
22	-3,215E-16	-1,191E-15	100,000	3,215E-16	1,191E-15
23	-4,025E-16	-1,491E-15	100,000	4,025E-16	1,491E-15
24	-5,847E-16	-2,166E-15	100,000	5,847E-16	2,166E-15
25	-8,110E-16	-3,004E-15	100,000	8,110E-16	3,004E-15
26	-1,247E-15	-4,620E-15	100,000	1,247E-15	4,620E-15
27	-1,657E-15	-6,137E-15	100,000	1,657E-15	6,137E-15

Table B.2 Matriz de componentea

	Componente													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
VAR 1	,732	-,007	,498	-,012	,361	-,293	-,009	,000	,000	,000	,000	,000	,000	,000
VAR 2	-,077	,789	,190	-,519	-,037	-,115	,228	,000	,000	,000	,000	,000	,000	,000
VAR 3	,735	-,165	,545	,140	,086	-,325	,052	,000	,000	,000	,000	,000	,000	,000
VAR 4	,713	,377	,379	-,236	-,182	,190	-,285	,000	,000	,000	,000	,000	,000	,000
VAR 5	,714	-,199	,149	-,111	-,126	,301	,557	,000	,000	,000	,000	,000	,000	,000
VAR 6	,661	,105	-,454	-,130	,204	,522	,126	,000	,000	,000	,000	,000	,000	,000
VAR 7	,400	,736	,297	,215	,010	,019	,405	,000	,000	,000	,000	,000	,000	,000
VAR 8	,709	-,356	,409	,255	-,354	,112	,028	,000	,000	,000	,000	,000	,000	,000
VAR 9	,850	,056	,161	-,215	,426	,091	-,114	,000	,000	,000	,000	,000	,000	,000
VAR 10	,296	,942	,025	,062	-,123	-,068	-,008	,000	,000	,000	,000	,000	,000	,000
VAR 11	,621	,061	,636	-,014	,376	,209	-,148	,000	,000	,000	,000	,000	,000	,000
VAR 12	,835	-,254	-,353	-,095	-,134	-,274	,106	,000	,000	,000	,000	,000	,000	,000
VAR 13	,648	-,065	-,671	,173	-,042	-,281	,118	,000	,000	,000	,000	,000	,000	,000
VAR 14	,314	-,010	,474	,794	-,104	,186	-,013	,000	,000	,000	,000	,000	,000	,000
VAR 15	,790	,430	-,029	-,082	-,361	-,126	-,192	,000	,000	,000	,000	,000	,000	,000
VAR 16	,732	,158	-,519	,039	,311	,249	-,093	,000	,000	,000	,000	,000	,000	,000
VAR 17	,373	,591	-,500	,418	,217	-,180	-,084	,000	,000	,000	,000	,000	,000	,000
VAR 18	,892	-,137	-,261	-,199	,024	,267	-,070	,000	,000	,000	,000	,000	,000	,000
VAR 19	,977	-,185	-,023	-,095	,030	,025	-,014	,000	,000	,000	,000	,000	,000	,000
VAR 20	,958	-,127	,186	-,073	,156	-,016	-,034	,000	,000	,000	,000	,000	,000	,000
VAR 21	,923	-,069	,053	-,151	,267	-,214	,000	,000	,000	,000	,000	,000	,000	,000
VAR 22	,917	-,289	-,014	,020	-,141	-,218	,084	,000	,000	,000	,000	,000	,000	,000
VAR 23	,935	-,291	-,060	-,005	-,186	,046	,024	,000	,000	,000	,000	,000	,000	,000
VAR 24	,670	,154	-,289	,641	,181	,032	,003	,000	,000	,000	,000	,000	,000	,000
VAR 25	,840	,087	-,006	-,153	-,498	-,065	-,109	,000	,000	,000	,000	,000	,000	,000
VAR 26	,827	,153	-,132	,052	-,470	,172	-,147	,000	,000	,000	,000	,000	,000	,000
VAR 27	,915	-,119	-,216	-,190	,145	-,210	,030	,000	,000	,000	,000	,000	,000	,000

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	14,822	54,895	54,895	14,822	54,895	54,895
2	3,344	12,385	67,280	3,344	12,385	67,280
3	3,218	11,918	79,197	3,218	11,918	79,197
4	1,938	7,178	86,375	1,938	7,178	86,375
5	1,671	6,190	92,565	1,671	6,190	92,565
6	1,219	4,516	97,081	1,219	4,516	97,081
7	,788	2,919	100,000			
8	1,321E-15	4,892E-15	100,000			
9	1,228E-15	4,547E-15	100,000			
10	6,611E-16	2,449E-15	100,000			
11	5,464E-16	2,024E-15	100,000			
12	3,544E-16	1,313E-15	100,000			
13	2,572E-16	9,525E-16	100,000			
14	1,807E-16	6,691E-16	100,000			
15	1,168E-16	4,326E-16	100,000			

Figure B.1 Performance indices of IoT security Bayesian Model

Component	1	2	3	4	5	6
1	,677	,548	,162	,265	,347	,153
2	-,219	-,126	,938	,226	,044	-,063
3	-,156	,515	,225	-,621	-,322	,413
4	-,162	-,123	-,118	,523	-,187	,798
5	-,652	,574	-,173	,292	,308	-,189
6	-,131	-,272	,008	-,367	,802	,361

Figure B.2 Performance indices of IoT security Bayesian Model

	Component					
	1	2	3	4	5	6
CyberattacksonIoTsystemscouldaffecttoeconomicsocialor_A	,732	-,007	,498	-,012	,361	-,293
CyberattackstoIoTsystemscouldbeaffectedtootherIoTITa	-,077	,789	,190	-,519	-,037	-,115
ThegrowthofnumberofIoTdevicescouldincreasetheprobabili	,735	-,165	,545	,140	,086	-,325
CyberattacksonIoTsystemscouldgenerateshockonmarketsorr	,713	,377	,379	-,236	-,182	,190
SecurityconfigurationsonIoTdevicesdependsofdomainsorpil	,714	-,199	,149	-,111	-,126	,301
InterdependencyofIoTdevicewithotherIoTITandOTsystems	,661	,105	-,454	-,130	,204	,522
ThegrowthonthenumberofIoTdevicescouldincreasethesusce	,400	,736	,297	,215	,010	,019
VulnerabilitiesonIoTdevicescouldincreasetheprobabilityof	,709	-,356	,409	,255	-,354	,112
IoTdevicesaresusceptibletospecifictypeofcyberattacks	,850	,056	,161	-,215	,426	,091
Previousattackallowstheexecutionofnewattacks	,296	,942	,025	,062	-,123	-,068
Attackscouldbeexecutedondifferentlayers	,621	,061	,636	-,014	,376	,209
SecurityconfigurationsonIoTdevicecouldincreasethesuscept	,835	-,254	-,353	-,095	,134	-,274
CyberattackscouldgeneratedegradationintheoperationofIoT	,648	-,065	-,671	,173	-,042	-,281
CyberattackscouldaffecttoCIAonIoTsystems	,314	-,010	,474	,794	-,104	,186
CyberattackscouldbescaledfromonelayerofIoTsystemtooth	,790	,430	-,029	-,082	-,361	-,126
Thefrequencyofcyberattackscouldincreasethesuccessfuloft	,732	,158	-,519	,039	,311	,249
Shorttimesonthepropagationofcyberattackscouldincreaseth	,373	,591	-,500	,418	,217	-,180
CyberattackcouldaffectdifferentlayersofIoTsystemsincreas	,892	-,137	-,261	-,199	,024	,267
Theriskvaluewilldependontheprobabilitythatthreatscanc	,977	-,185	-,023	-,095	,030	,025
Theriskseverityandprobabilityvalueswilldependonthelev	,958	-,127	,186	-,073	,156	-,016
RiskandseverityvalueswilldependontherelationshipofIT	,923	-,069	,053	-,151	,267	-,214
Thevalueoftheriskwilldependonthetypeofinformationin	,917	-,289	-,014	,020	-,141	-,218

Figure B.3 Performance indices of IoT security Bayesian Model

Appendix C

Results of correlational analysis

An additional strategy to evaluate the relationships that exist between the 27 variables is the use of correlational analysis. The 27 variables are numerical variables and tries to explain certain doubts or frequently related with cyberattacks, IoT, security and causes.

We can show in the Figure C.1 that there is a dependency between these questions. A high positive correlation value is from the following variables:

- Var (3, 18, 19, 20.21.27) with Var (1,8, 11, 19,21,27).
- Var4 with Var (5,7,12, 16, 25)
- Var12 with Var5
- Var16 with Var6
- Var7 related to (4, 17)
- Var8 related to (1, 3, 11,14, 20, 23, 26)

We can note that the growth of IoT devices creates a high probability of attacks and in an economic, social and environmental environment. Additionality, the severity depends on the risk and the vulnerability values of the IoT system. This could be intuited by knowing a little about these issues, but it is always good to show how related one is to the other.

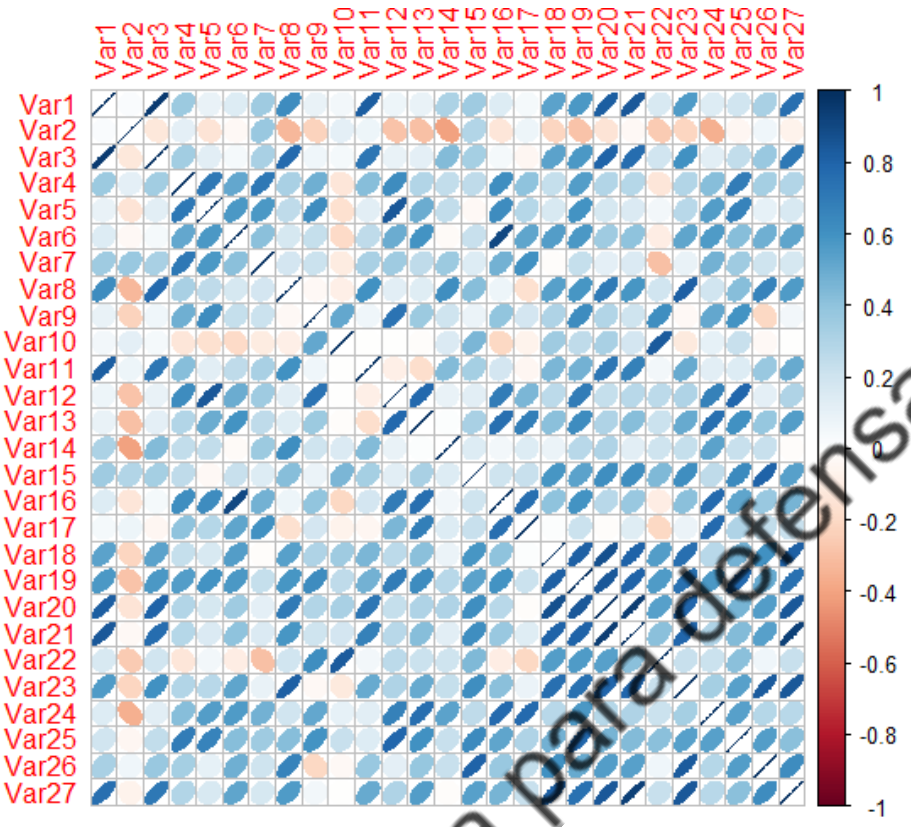


Figure C.1 Result of correlational analysis based on the 27 variables.

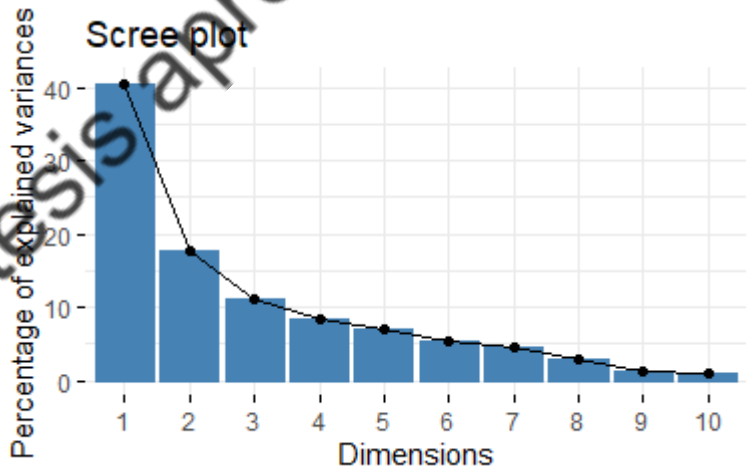


Figure C.1 Graph of dimensions based on the concentration of variance.