applied sciences

MDPI

Article

Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation

Aarón Echeverría [1], Cristhian Cevallos [1], Ivan Ortiz-Garces [1,*] and Roberto O. Andrade [2]

[1] Escuela de Ingeniería en Tecnologías de la Información, FICA, Universidad de Las Américas, Quito 170125, Ecuador; aaron.echeverria@udla.edu.ec (A.E.); cristhian.cevallos.moreno@udla.edu.ec (C.C.)
[2] Facultad de Ingeniería en Sistemas, Escuela Politécnica Nacional, Quito 170525, Ecuador; roberto.andrade@epn.edu.ec
* Correspondence: ivan.ortiz@udla.edu.ec

Abstract: The inclusion of Internet of Things (IoT) for building smart cities, smart health, smart grids, and other smart concepts has driven data-driven decision making by managers and automation in each domain. However, the hyper-connectivity generated by IoT networks coupled with limited default security in IoT devices increases security risks that can jeopardize the operations of cities, hospitals, and organizations. Strengthening the security aspects of IoT devices prior to their use in different systems can contribute to minimize the attack surface. This study aimed to model a sequence of seven steps to minimize the attack surface by executing hardening processes. Conducted a systematic literature review using Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) techniques. In this way, we were able to define a proposed methodology to evaluate the security level of an IoT solution by means of a checklist that considers the security aspects in the three layers of the IoT architecture. A risk matrix adapted to IoT is established to evaluate the attack surface. Finally, a process of hardening and vulnerability analysis is proposed to reduce the attack surface and improve the security level of the IoT solution.

Keywords: Internet of Things (IoT); hardening process; cybersecurity risk; penetration test

Citation: 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

Academic Editor: Young-Gab Kim

Received: 15 February 2021
Accepted: 5 March 2021
Published: 6 April 2021

1. Introduction

The Internet of Things (IoT) is a set of interrelated electronic devices, mechanical and digital machines, objects, animals, or people that have unique identifiers. IoT can transfer data over a network without requiring human-to-human interaction or the interposition of a human being with a computer [1]. With the emergence of IoT, there are multiple devices connected to a telecommunication network, from household appliances to industrial machines. All these devices can be controlled remotely without requiring human presence or interaction. With the advancement and development of IoT, the study of autonomous device networks has been given more priority.

However, IoT devices are expose to a series of threats. The most common threats are viruses and denial of service (DOS) attacks. Table 1 indicates the category of IoT attacks based on infrastructure components [2].

The exponential growth of IoT devices is surround by security and privacy risks. IoT implementations must be build ensuring easy and secure control [3]. The process of developing IoT systems requires in-depth knowledge in various areas, such as risks, threats, and vulnerabilities, to guarantee secure systems. By having massive IoT devices connected, cybersecurity measures must be defined to carry out an in-depth defense of the devices and information that are transmitted. To minimize threats in IoT, fluid policies must apply in the implementation processes.

The International Telecommunication Union (ITU) defines cybersecurity as the set of tools, policies, security concepts, security safeguards, guidelines, risk management methods, actions, training, best practices, insurance, and technologies that can be used to

protect the assets of the organization and users in the cyber environment [4]. Cybersecurity in IoT is a factor that must be considered in the implementation and development of IoT devices, because an IoT device with its default configuration is a notorious victim for cybercriminals.

Table 1. Internet of Things (IoT) attacks.

IoT Devices and Peripherals	Gateways and Internal Network	Cloud Servers and Control Devices
Brute force	Injection attack	SQL injection
Buffer overflow	Man in the middle (MITM)	Distributed denial of service (DDOS)
Rolling code attacks	DNS poisoning	Weak authentication
Sybil attack	Wormhole	Back door and exploits

In this same approach, Center for Internet Security (CIS) defines methodologies based on hardening that increase the security levels of different types of devices, which serve to mitigate the most attacks common against various information systems and networks. There are 20 CIS Controls that are classified as basic, foundational, and organizational that are applied to reduce the attack vectors of network, adjacent, local, and physical [5]. The hardening process needs a risk assessment to identify the points or elements where hardening should be implemented. So, in addition to the CIS Controls, there are standards that allow processes, such as risk assessment, information security management, and standardization of IoT architectures. One of the main organizations that is responsible for generating and standardizing these standards is the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

In the same way, ISO is a worldwide federation of national standards bodies that is responsible for developing international standards. The development of various standards is normally carried out through ISO technical committees. There are multiple ISO standards, such as the ISO/IEC 30,141, ISO/IEC 27,001, ISO/IEC 31,000, and ISO/IEC 25,010 standards, will be used as a basis. The ISO/IEC 30,141 standard is a reference architecture for IoT designers and developers. The ISO/IEC 27,001 standard is a guideline oriented to Information Security Management Systems (ISMS), which allows compliance with the confidentiality and integrity of ISMS [6]. The ISO/IEC 31,000 standard is a guide that makes it possible to measure the impact of different risks according to the type of activity to be carried out and according to the nature of the risk [7]. The ISO/IEC 25,010 standard is a model that allows the evaluation of product quality. The characteristics and quality properties of a software product are determined [8].

In the same vein, Open Web Application Security Project (OWASP) IoT methodology is a project carried out by professionals specialized in the field of cybersecurity for reducing the risks and the impact of various vulnerabilities, both external and internal [9]. This project indicates the attack surface areas of IoT devices, such as: ecosystem, device memory, device physical interfaces, device web interfaces, device firmware, device network services, administrative interface, local data storage, cloud web interface, third-party backend Application Programming Interfaces (APIs), update mechanism, mobile application, vendor backend APIs, ecosystem communication, network traffic, authentication, authorization, privacy, and hardware. There are elements of the attack surface that are more vulnerable, and they do not depend on third parties. So, the hardening process will be applied to these elements to reduce vulnerabilities and allow the correct functioning of the IoT system. Based on the literature review, there are few proposals that provide a step-by-step guide to validate IoT security. Most of the research related to IoT assessment are based on risks analysis but they do not consider the aspects of attack surface of IoT devices. Therefore, based on this gap, we propose an evaluation of attack surface based on Relative Attack Surface Quotient (RASQ) proposal. A second gap is the adaptation of risk tools for IoT systems, our contribution in this study is defined a risk matrix based on the impact which

is define for compliance classes and the probability of occurrence of cyberattacks. A third contribution of this study is providing a 17-step security checklist steps for IoT system to determine the risk and attack surface in each layer of the IoT architecture. Finally, a case study was conducted to validate the security methodology proposal for IoT systems.

This paper discusses a review of literature related to cybersecurity, risk analysis, and implementation tests in IoT solutions to know the advantages and disadvantages of IoT. At the end of the literature review, a practicable cybersecurity model is proposed using the best existing norms, standards, guides, and methodologies. This model allows the implementation of secure IoT systems for professionals and researchers. The main objective of the proposed model is to reduce risks, threats, and vulnerabilities in IoT systems.

The rest of the paper is organized, as follows. In Section 2, a search of related papers to review is presented. In Section 3, an analysis of previous works is performed. Section 4 contains the proposed solution where all the development carried out is explained step by step. Section 5 presents the results found in the development of the proposal. Section 6 contains the discussion based on the results finally obtained, and Section 7 presents the conclusions and future work.

2. Related Work

IoT consists of two architectural models that operate through layers, each of which has its specific function, and has its own protocols [10]. Figure 1 indicates the architectures that exist in IoT.

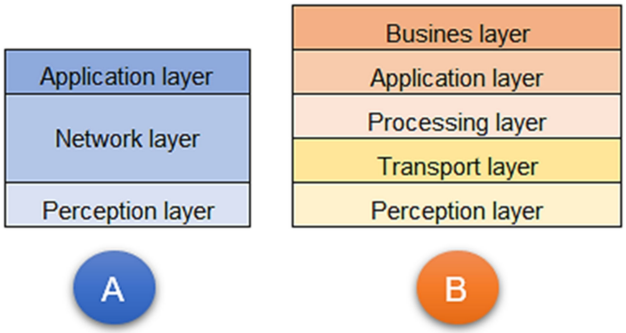

Figure 1. IoT architecture based on layering model.

The three-layer model A consists of the application layer, the network layer, and the perception layer. The B model has the same layers except the network layer, and additionally it consists the business layer, the processing layer, and transport layer; see Table 2.

Table 2. IoT architecture based on layering models.

Layer	Description
Three-layer Architecture	
Application	Services or applications that allow the analysis of the information obtained.
Network	Responsible for communication between the perception layer and the application layer.
Perception	Hardware or physical layer where sensors and actuators are used.
Five-layer Architecture	
Transport	Responsible for transmitting information from the perception layer to the processing layer.
Processing	It stores the transport layer data and processes it using services, such as a database.
Business	Business models are resolved, data privacy and applications are managed.

Cyberattacks violates the purpose of the IoT system take advantage of vulnerabilities on software or hardware level. Leite et al. [11] summarizes the main vulnerabilities reported for IoT devices based on the OWASP Internet of Things Project. They classify these vulnerabilities by test routine groups. In this context, Tien et al. [12] presents the Universal Firmware vulnerability Observer (UFO). UFO is a system that discovers vulnerabilities in the firmware of IoT devices. It scrutinizes the embedded file system of the firmware, identifies vulnerabilities, and scans for password leaks. The UFO tool was designed based on IoT firmware verification standards, such as OWASP, UL-2900, and ICSA Labs. Through analysis, the authors concluded that 73% of firmware files contain vulnerabilities in their embedded Linux kernel, 22% of firmware files leak passwords, and 6% of firmware files contain hidden backdoors.

Lee et al. [13] explore vulnerabilities of IoT services focusing on three aspects: device itself, wearable gateway, and server. They perform the following attack scenarios: namely an illegal device pairing attack, a fake wearable gateway attack, and an insecure code-based attack. The authors analyze these attacks using the OWASP IoT Top 10 attacks in IoT systems guide and propose solutions to prevent these attacks.

W. Zhang et al. [14] implement three types of honeypots to capture malicious behaviors. Based on the Common Vulnerabilities and Exposures (CVE) CVE-2017-17215 they implement a honeypot that simulates specific UPnP services of the router. Universal Plug and Play (UPnP) details are limited, they used the firmware of a real IoT device to match the vulnerability and allow high interaction in the honeypot. Simple Object Access Protocol (SOAP) service ports were added to the honeypot to provide honeynet capabilities and features. The authors provided a hybrid service of a real device and simulation honeypots.

K. Li et al. [15] propose an open-source intelligence framework (OSIF) that enables intelligent event-based cyber threats to be analyzed. OSIF performs machine learning through data mining to extract event-related information. It uses vulnerabilities and CVEs to store the profile of threat actors. The authors performed a structural and conceptual evaluation of critical threats on the dataset collected from dozens of websites.

On this point, developing a process to reduce these vulnerabilities using cybersecurity approaches is relevant. For instance, Sengan et al. [16] investigates security issues in smart city infrastructure development. The method used focuses on threats and security data. They provide a high-level Hybrid Smart City Cyber Security Architecture (HSCCA) for the creation of a smart city considering important factors, such as valuable data collection, caching, retrieval, and organization of network resources. The authors recommend a context-specific security configuration for cyber-physical systems.

Visoottiviseth et al. [17] designed and developed "A System for Preventing IoT Device Attacks on Home Wi-Fi Router" (SPIDAR) to protect home Wi-Fi networks. The elements used for this system were a home Wi-Fi router, a Raspberry Pi, and a web application to prevent attacks and display attack statistics to home users. In addition, they used the Snort Intrusion Prevention System (IPS) that analyzes the behavior of IoT devices in use. SPIDAR prevents five main types of attacks specified in the OWASP IoT Top 10 vulnerabilities 2018.

Additionally, Visoottiviseth, Akarasirwong, and Chaiyasart [18] develop a penetration testing system for IoT devices called PENTOS. This system automatically collects information from IoT devices through wireless communication. The system allows users to perform various types of penetration testing on their IoT devices, such as password attack, web attack, and wireless attack. This system aims to raise user awareness by providing basic information on OWASP's top 10 IoT vulnerabilities.

Shu et al. [19] related with a security and privacy analysis of IoT toys for children. Three IoT toys were examined to gain an understanding of the smart toy security and privacy landscape. Through a static and dynamic analysis, vulnerabilities related to the inappropriate use of encryption and authentication, reuse of the Positive Operating System Test (POST) token, confidential user information in crash reports and secret keys in the source code were discovered. Additionally, a small set of third-party analytics platforms receive data from all examined toys, possibly allowing for detailed user data collection.

These vulnerabilities violate individual toy privacy policies, as well as federal Children's Online Privacy Protection Act (COPPA) regulations for handling children's data.

M. Mohsin et al. [20] present the IoTChecker framework that allows IoT configurations to be semantically modeled. The purpose is to stop security configuration anomalies and analyze IoT-specific threat vectors. To perform the analysis of the configurations, the context of interactions and dependencies of the IoT systems is described. The evaluation carried out includes the security classifications and security analysis of the configurations of 954 IoT products. The automated approach used allows it to be scalable, easily manageable, formally verifiable, and free from errors induced by tedious manual configurations.

Similar approach was performed by Akatyev et al. [21]. The authors conduct a study focused on IoT systems that were used in smart homes. The proposed objective is to anticipate cyber threats to these IoT systems. The authors propose a user centric IoT network model for the near future. The characteristics, devices, services, and data flows of this network are described. This network model describes the most common attacks, such as intrusions, death, privacy failure, and extensible device involvement. To conclude, they carry out a threat analysis based on these use cases, which describes the cyber-physical risks that allow demonstrating the potential for device exploitation.

A. Di Giorgio et al. [22] propose a security framework and advanced tools to adequately manage vulnerabilities and react in a timely manner to threats. This proposed architecture fills the gap between computing and theoretical control approaches. S. Rizvi et al. [23] analyze critical devices and associated vulnerabilities and highlights the need for rigorous security controls. It evaluates the attack vectors for IoT devices focused on central, such as healthcare, retail, and home. This paper identifies the threats caused by device-level vulnerabilities, the application of appropriate security controls to close vulnerabilities and minimize the possibility of threats occurring.

However, it is important to improve cybersecurity in IoT systems through guidelines or standards. In that way, Matheu-García et al. [24] proposes an IoT security certification methodology that allows to evaluate security solutions for large-scale IoT deployments in an automated way. The certification approach is carried out using the security risk assessment and testing methodologies presented by the European Telecommunications Standards Institute (ETSI). The guides and standards presented by ETSI are based on the international standards ISO/IEC 31,000 and ISO/IEC 29,119. The authors carry out a security risk assessment composed of risk identification, risk estimation, and risk assessment activities. The security tests performed consist of design and implementation tests, and the development of test environment. This certification process includes monitoring the devices during their life cycle.

Khan et al. [25] proposes an ontology that allows establishing security guidelines for interoperability and understanding between smart home actors. The authors indicate the security guidelines to be performed to exchange knowledge. This research allows understanding the concepts that interact in the smart home ecosystem. The authors proposed two use cases for demonstrating how the ontology is applied to automate the execution of security guidelines. J. Li [26] synchronizes in a matrix the vulnerabilities of the OWASP IoT Top 10 project and the 25 most dangerous Common Weakness Enumeration (CWE)/ SysAdmin, Audit, Network, and Security (SANS) software bugs. He realizes a security framework that allows to review code vulnerabilities having a higher accuracy of the findings.

N. Teodoro, C. Serrão [27] identify the relationship between lack of security and Software Development Life Cycle (SDLC). Based on this analysis, the authors present a set of security automation tools and methodologies that are used in the course of the SDLC to improve the quality of Web applications. In the same vein, J.D.V Mohino et al. [28] defines a new software development model in which security aspects are evaluated in any phase taking advantage of agile models. This model identifies vulnerabilities from early stages to achieve adequate levels of quality and functionality. In the same line, K. Rindell et al. [29] perform a study where they identify incompatibilities between security approaches to agile

software development, map common activities, processes, practices and artifacts from different guides and standards, such as Microsoft Security Development Lifecycle (SDL), ISO, and OWASP Software Assurance Maturity Model (SAMM).

In the same context, Anderson et al. [30] demonstrates deficiencies of the ISO/IEC 80,001 standard. This standard due to its outdatedness provides low levels of cybersecurity. This problem occurs due to the evolution of cybersecurity and the long time that exists to review and publish international standards. The authors identified that the following areas require priority in the review of the cybersecurity levels they possess emergency access areas, de-identification of health data, physical locks on devices, data backup, disaster recovery, third-party components in the product life cycle roadmap, transmission confidentiality and transmission integrity. This research presents improvements to the ISO/IEC 80,001 standard to improve security levels and increase the protection provided by cybersecurity.

In the same vein, Azaliah et al. [31] extensively explore various IoT technologies used in healthcare services and their security challenges. The authors propose an IoT security risk model for healthcare. The goal is to provide a comprehensive risk management process based on ISO/IEC 27,005. This model performs an iterative IoT risk management process, because IoT risks are variable.

I. Skierka [32] examines the convergence of safety and security risks in healthcare for medical systems in Europe. The analysis conducted indicates that the management of safety and security risks in medical systems require the implementation of existing governance, including regulation, standards, and industry best practices. The authors present policy and industry recommendations for improving the cybersecurity of medical systems in Europe. This paper draws comparisons with cybersecurity guidelines, technical controls, standards, and best practices in the U.S. medical device security arena.

Additionality, Safa et al. [33] presents an information security management model aimed at mitigating the risk of information security breaches in an industrial environment. Using ISO/IEC 27005, Harmonized Threat and Risk Assessment (HTRA), Conducting Security Risk Analysis (CORAS), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Allegro, the risks to the organization's assets are identified. The model presented by the authors mitigates information security risk for both service providers and service consumers in this environment. Huang, S. Nazir [34] evaluates Internet of Medical Things (IoMT) security using the analytic network process (ANP). The performed approach uses the ISO/IEC 27,002 standard. The results of this research show that handling international standards allows obtaining secure IoMT devices.

V. Casola et al. [35] propose an approach oriented to the analysis of security of IoT systems through an almost completely automated process of threat modeling and risk assessment. This approach allows identifying the security controls to implement to mitigate existing security risks. This research is based on the ISO/IEC 30,141 standard directives.

In the same line, M. Ngamboé et al. [36] assess the risks in implantable cardiac electronic devices (CIED) using the ISO/IEC 27,005 standard and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 guide. Using a methodical approach, they perform the analysis in three parts that are actor-based, scenario-based and combined. These analyzes make it possible to determine the impact of attacks and measure the probability of the occurrence of threats. The results obtained by the authors indicate that vulnerabilities in CIED's Radio Frequency (RF) interface represent an acceptable risk. Network and Internet connections in the rest of the system represent a potential risk.

Under this context, the use of risk assessment is a key element for enhanced process. In this way, Kieras et al. [37] performs a modification of the attack tree model to analyze supply chain risks. This model allows to obtain precise data that describes complex systems of critical Information and Communication Technologies (ICT) and IoT infrastructure. Through case studies, it was found that structural uncertainties constitute a major challenge for the usefulness of this model, and therefore require special attention. The use cases allow to determine that the safety of the components and the reliability of the suppliers can be

estimated with an accuracy of 50%, these results show a maximum possible error in the risk assessment of 14%. This percentage of the risk assessment reflects a wide variety of discrete structural errors.

K. Kandasamy et al. [38] conduct a review of the main existing cyber risk assessment methodologies and their suitability for IoT systems. The cybersecurity frameworks analyzed were National Institute of Standards and Technology, Operationally Critical Threat, Asset, and Vulnerability Evaluation, Threat Assessment & Remediation Analysis, and International Standards Organization. Risk vectors for IoT and Internet of Medical Things (IoMT) were analyzed. Through study, analysis and review, the authors present a method for assessing the risks of IoT systems through the quantification of risk vectors. This method leads to effective risk mitigation strategies and techniques.

I. Lee [39] reviews IoT cybersecurity technologies and cyber risk management frameworks. The author presents a four-layer IoT cyber risk management framework for allocating financial resources to multiple IoT cybersecurity projects. In addition, a proof-of-concept of the management framework is performed.

Ruan [40] presents various types of risks that span strategic, regulatory, and systemic sectors. The author conducts a cyber risk analysis, the need to measure cyber risk, its current challenges, and a review of the cost of cybercrime. To measure cyber risk, it uses current methods, such as Common Vulnerability Scoring System (CVSS), CORAS, stochastic modeling, Monte Carlo simulation, and Cyber Value at Risk and Factor Analysis of Information Risk (FAIR). Additional classifies risk factors into technological, non-technological, inherent and control factors.

The last step, after development a risk assessment is enhanced cybersecurity IoT systems. In this way, Yigit et al. [41] mention that IoT devices can have various vulnerabilities that can lead to serious breaches and security compromises. Therefore, the author emphasizes that hardening IoT systems is of vital importance. The author proposes an algorithm that uses compact attack charts to find a cost-effective solution to protect IoT systems. Extract all the attack vectors that affect critical resources and select the exploit that can be used. The results of the experiment indicate that the proposed algorithm is scalable with the size of the network and IoT nodes.

Maillet-Contoz et al. [42] present an approach to facilitate the integration, verification, and then functional validation of device security based on modeling and simulation. This approach enables you to increase the quality of your design, ensure better overall system performance, and make it easier to expand the number of end devices. The objective of this proposal is to allow the implementation, verification, and validation of an end-to-end security solution.

In this same line, Stine et al. [43] propose a computer risk scoring system for evaluating medical devices. This system, using the spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (STRIDE) model, uses a security questionnaire to weight the risks. To test the efficiency of the system, the authors used three test scenarios with medical devices.

Sancho et al. [44] run a system to classify security threats, computing their criticality according to the Bug Bar technique, in order to address the threats in order of priority. The authors correlated the severity risk values and the results calculated by the new approach. This proposal could complement the information from Security Information and Event Management (SIEM) systems and help in the prediction of criticalities of future threats. B. Javed et al. [45] focus on recommended design considerations for IoT devices with the goal of achieving security by default. Default security is achieved by design, focusing on features, such as processing power, power availability, memory, and bandwidth requirements.

3. Analysis of Previous Works

As we have analyzed the hardening process needs to follow a proper methodology. Research shows that there are different approaches that can be adopted to develop the

hardening process. Under this context, our research question arises which are the most used leverages to perform a hardening of IoT solutions under a proper methodology and following the best practices established by the specialized organizations in the field of cybersecurity.

To answer the research question, we have conducted a Systematic Literature Review (SLR) based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology; see Figure 2. We select the following scientific databases: MDPI, IEEE Xplorer, Elsevier, and Springer, and define the following search queries:

- "IoT" AND "hardening"
- "IoT" AND "risk Analysis"
- "IoT" AND "cybersecurity testing"
- "IoT" AND "cybersecurity assessment"
- "IoT" AND "risk" AND "best practice"

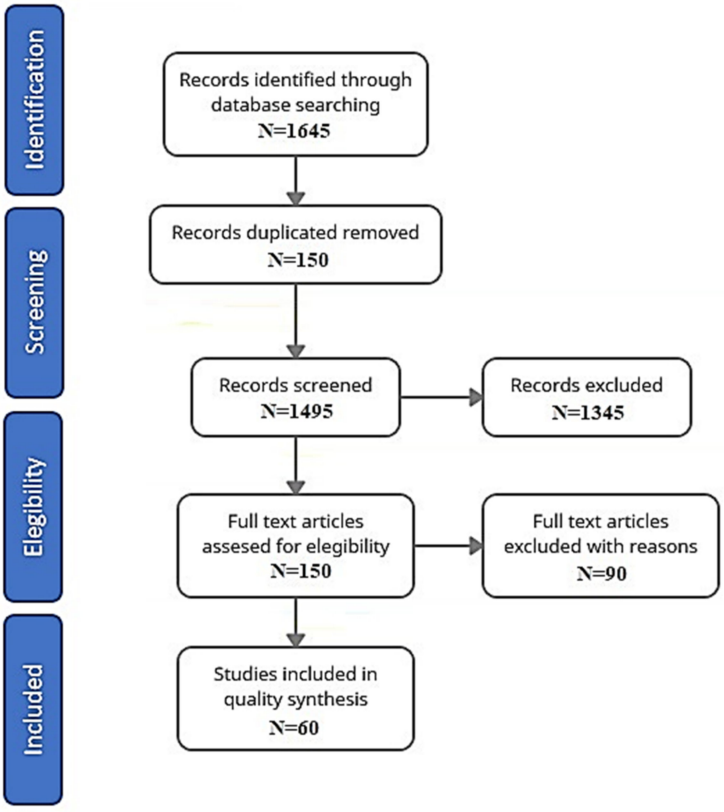

Figure 2. Literature review based on PRISMA methodology.

In the identification stage, we found 1645 articles, and then we removed 150 duplicates records. In the screening stage, we excluded 1495 records. Then, in the eligibility stage, we excluded 90 records. Finally, in the included stage, we included 60 studies for quality synthesis; see Figure 2.

Once the 1645 records have been loaded, we can see, in Figure 3, the most relevant keywords, according to the Rayyan tool used for the screening process.

Based on the qualitative analysis carried out using the systematic review tool Rayyan, we identified nine proposals based on OWASP, ISO, risk analysis, among others, used in research conducted from 2016 to 2021; see Table 3.

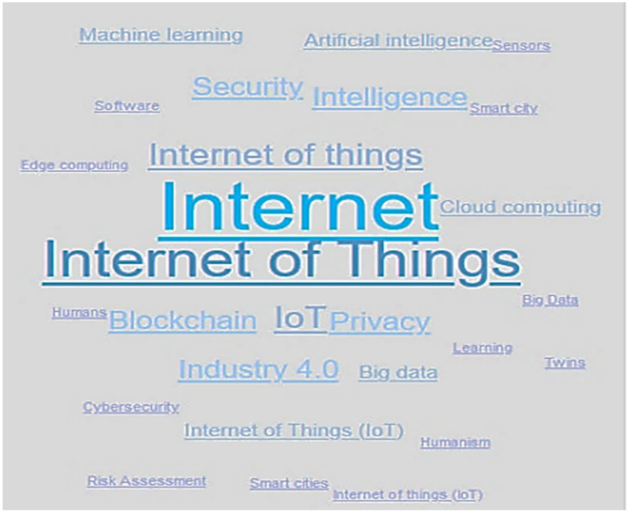

Figure 3. Word cloud generated by Rayyan based on the records identified in the Systematic Literature Review (SLR).

Table 3. Results of the selected papers to review.

Top	Proposals	Description	Reference
1	Based on OWASP	Leveraging based on OWASP is focus on using the IoT Top 10 2018 to do an analysis of IoT vulnerabilities.	[9,12,13,17,18,26–29]
2	Based on CVE	It is a list of records. With an identification number, description, for known cybersecurity vulnerabilities.	[14,15]
3	Based on ISO	The use of ISO standards allows determining risks to specific elements of IoT.	[20,30,31,33,34]
4	Based on risk analysis	It focuses on the analysis of the use of ISO standards.	[16,19,21,24,25,32,35,37–39,43]
5	Based on vulnerability management	The approach allows to identify which are the most known vulnerabilities.	[22,23]
6	Based on NIST	The NISTIR 8228 standard helps organizations better understand and manage cybersecurity and privacy risks with IoT devices.	[36]
7	Based on CVSS	Free and open industry standard for evaluating security vulnerabilities.	[40,41]
8	Based on hardening	The implementation of hardening allows to reduce the attack surface.	[42]
9	Based on security validation	Ensures the security of the entire IoT system implementation process.	[44,45]

Based on the analysis of the literature review, we can see in Figure 4 that there are more contributions based on risk analysis, followed by research using OWASP guidelines and ISO standards. There are not a favorable number of contributions related to hardening in IoT systems. This has motivated the present research to focus on the topic of hardening.

One aspect that caught our attention from the literature review is that we did not find in the identified records any leverages for the enhancement of IoT solutions based on CIS (Critical Security Controls). CIS proposals by SysAdmin, Audit, Network, and Security (SANs) institute presents hardening guides developed by cybersecurity professionals. Leveraging CIS is very practical to bring security hardening to a very practical and technical

level. CIS helps to strengthen security against the most common attack vectors and its focus on establishing specific controls helps to control hardware and software assets; see Table 4.

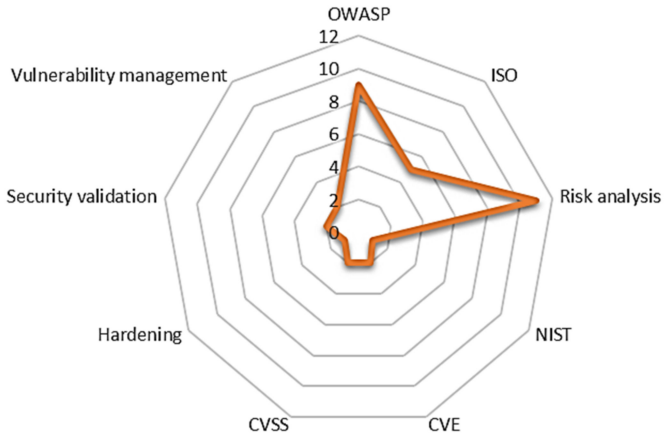

Figure 4. Projected research based on proposals.

Table 4. Center for Internet Security (CIS) Controls.

Top	Controls and Resources
1	Inventory and control of hardware assets
2	Inventory and control of software assets
3	Continuous vulnerability management
4	Controlled use of administrative privileges
5	Secure configuration of hardware and software
6	Maintenance, monitoring and analysis of audit logs

The application of CIS allows to quickly cover security issues versus times that can be long in risk analysis processes, especially in IoT systems that are dynamic and grow in number of devices daily, so waiting for the processes that lead identification of vulnerabilities, qualitative or quantitative analysis can generate a considerable time gap where you can receive an attack. Unlike traditional systems, those based on IoT even have a capacity to amplify the attack due to their level of complexity, which leads to more practical solutions, without obviously neglecting the risk analysis processes, which undoubtedly need to adapt to this new reality.

4. Proposed Solution

In this study the qualitative and experimental method is applied. Using the qualitative method, a systematic literature review conduct focused on the analysis of IoT cybersecurity norms, standards, models, and methodologies raised from 2016 to 2021 by international organizations, such as ISO, OWASP, NIST, and CIS. The aim of the analysis is to propose a methodology to determine the security level on IoT system based on seven steps that include: establish the purpose and requirements; perform a risk analysis to enable the correct operation of the IoT system; disable unnecessary protocols, services, and configurations; determine the attack surface; execute the vulnerability analysis; process hardening in the IoT system to strengthen the system against any risk or attack vector; and the last step is the validation of the security IoT system; see Figure 5.

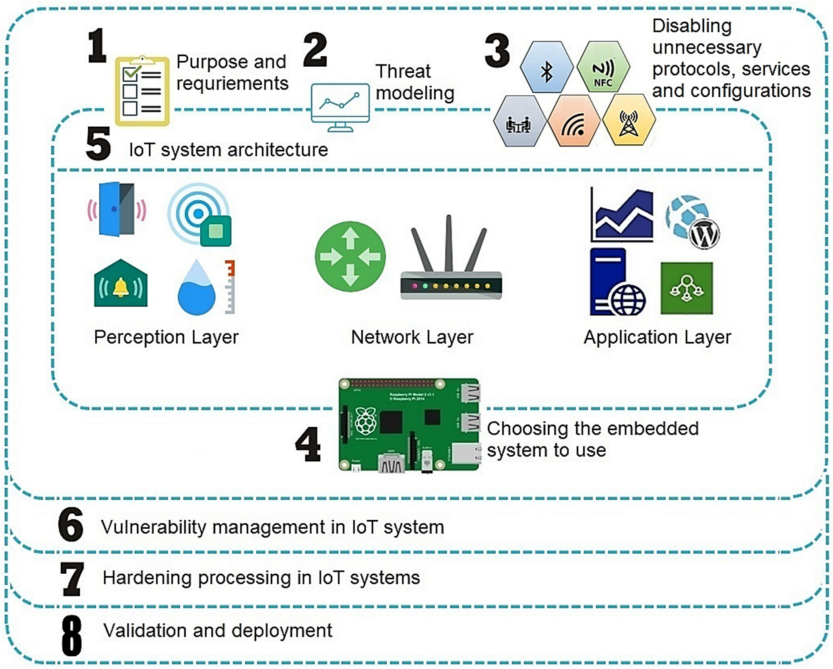

Figure 5. Proposed model for security hardening on IoT systems.

Figure 6 indicates the process for execute the propose model for security hardening on IoT systems. The method consists, in the first place, in selecting the best tools to be used. With the selection of the elements for the evaluation of the method, a port scan is performed to determine the exposed ports of the IoT system. The weaknesses that affect the correct function of the system are established with the vulnerability management. To determine the attack surface, many attacks are carried out on the IoT system to know which attacks it is prone to. The purpose of the hardening process is to reduce the risks and the impact on the IoT system. If these decreases, the experiment ends. Otherwise, it is repeated from the port scan until the risks and the impact of the IoT system are at low levels.

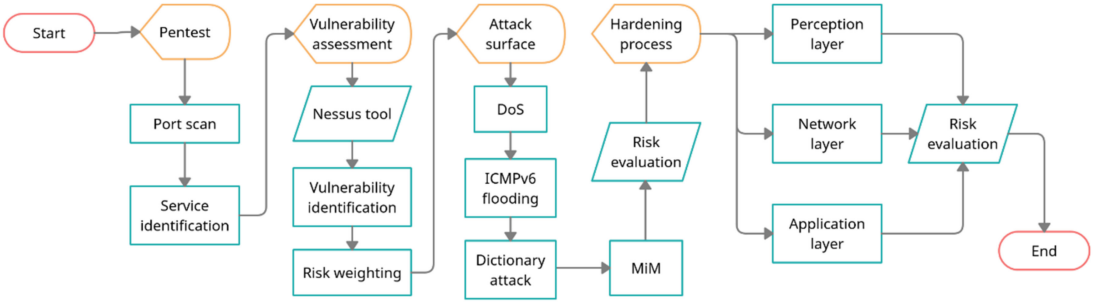

Figure 6. Risk evaluation process.

In the following, we describe the details of each step in the methodology proposal.

4.1. Step 1. Purpose and Requirements

The IoT purpose and requirements established for the proposed mode are as follows:

- Purpose of the system: Define the objective and scope of the IoT system.
- System behavior: Synthesize all the activities and configurations that the system is going to perform.
- System management requirements: Specify how the system will be monitored and controlled.

- Security requirements: Capabilities provided by the system in confidentiality, integrity, and availability.

4.2. Step 2. Risk Assessment

There are multiple operations and objectives served by IoT systems. A risk assessment is needed to determine the impacts involving the system. OWASP IoT Top 10 [9] proposes the most common vulnerabilities in IoT systems; see Table 5.

Table 5. Top ten attacks in IoT systems.

Top	Vulnerability
1	Weak, guessable, or hardcoded passwords
2	Insecure network services
3	Insecure ecosystem interfaces
4	Lack of secure update mechanism
5	Use of insecure or outdated components
6	Insufficient privacy protection
7	Insecure data transfer and storage
8	Lack of device management
9	Insecure default settings
10	Lack of physical hardening

Depending on the application of the IoT system, a risk assessment may require a higher compliance class to mitigate the determined level of risk. The compliance classes are based on the confidentiality, integrity, and availability (CIA triad) levels of the IoT system [46]. Confidentiality protects information of the IoT system. Integrity maintains the original properties of IoT system against unauthorized access. Availability ensures that IoT system are accessible at any time to authorized elements [47]. The risk impact is calculated with the levels of the CIA triad generating compliance classes. Class 0 has the lowest impact, and class 4 has the highest impact. The compliance classes were weighted from 1 to 5, representing the risks of the CIA triad; see Table 6.

Table 6. Compliance class associated with confidentiality, integrity, and availability (CIA).

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

For calculating the risk of all vulnerabilities in the OWASP IoT Top 10 project by summing the compliance class score and the probability of incidence, we propose the matrix of risk in Figure 7.

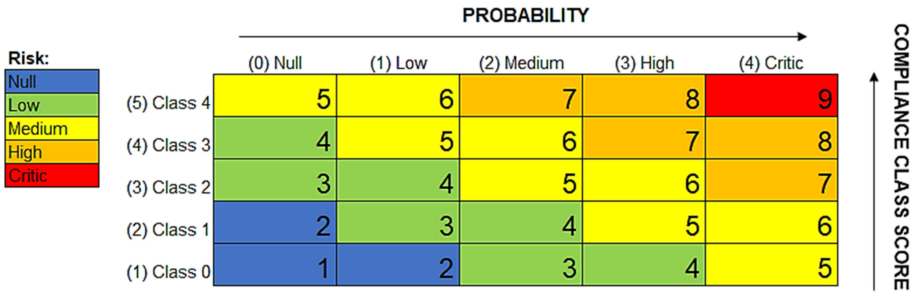

Figure 7. Risk and impact matrix.

The result of the risk value should have a scale from 1 to 10 according to the Euclidean standard [48]. The elements of the scale to classify the risk are critic, high, medium, low, and null; see Table 7.

Table 7. Risk score.

Weight	Scale
9	Critic
7–8	High
5–6	Medium
3–4	Low
1–2	Null

4.3. Step 3. Disabling Unnecessary Protocols, Services, and Configurations

To maintenance an adequate level of cybersecurity Table 8 shows a proposal checklist of security aspects for IoT systems development since our systematic literature review.

Table 8. IoT system elements checklist.

Layer	Step	Process	Type
Perception	1	Secure and centralize records.	Data
	2	Encrypted communication protocols.	Channel
	3	Strong and secure password.	Method
	4	Latest stable firmware or operating system version.	Method
Network	5	Monitoring of communication protocols.	Method
	6	Ports used are in a range different from the known ports.	Channel
	7	Protocols used have encryption.	Channel
	8	Separate wireless network.	Channel
Application	9	Safe coding practices.	Method
	10	Explicit error checking for all internally developed software.	Mehtod
	11	Acquired software support.	Method
	12	Up-to-date and trusted third-party components.	Channel
	13	Encryption of tested and standardized algorithms.	Method
	14	Personnel trained in secure software development.	Method
	15	Static and dynamic code analysis.	Channel
	16	Separate production and non-production systems.	Method
	17	Web Application Firewall (WAFs).	Channel

4.4. Step 4. Attack Surface

The attack surface is defined as the sum of all possible exposures to security risks. It is the set of known, unknown and potential vulnerabilities [49]. Studies of attacks, such as buffer overflow and symlink attacks, require the attacker to analyze the system to know what type of attack can breach the target, use a channel to reach the system, and invoke various methods to send and receive data from the system [44]. The following, Figure 8, indicates the components associated with attack surface of IoT systems based on RASQ proposal [50].

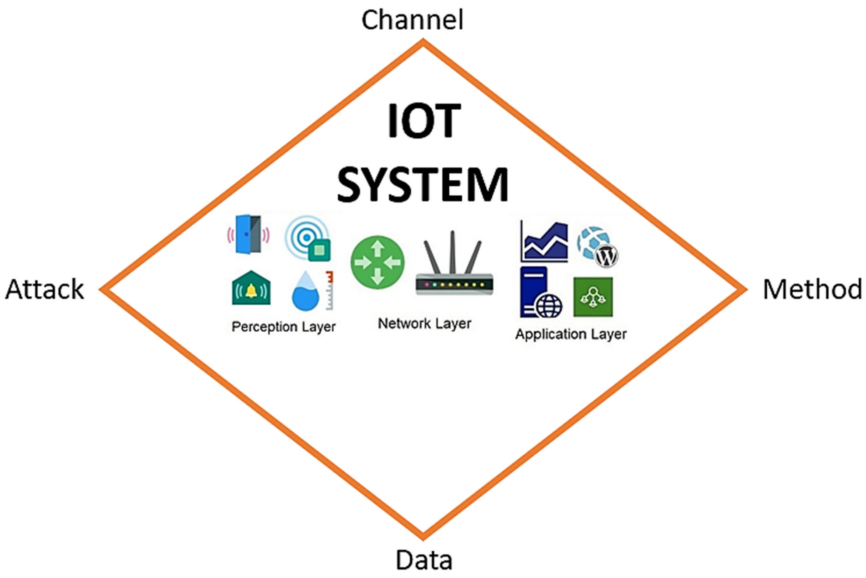

Figure 8. IoT attack surface variables.

An adaptation of the RASQ proposal was made to focus on IoT systems. The following equation was used to determine the attack surface:

$$Attack\ surface\ IoT\ system = \frac{Attack\ surface\ (Perception + Network + Application)}{3}, \quad (1)$$

$$Attack\ surface\ (Layer) = \frac{\left(\sum_{i=1}^{n} risk_{Step\ n}\right)}{n}, \quad (2)$$

where "n" is the step number specified in the Table 9. The total attack surface of the IoT system is calculated according to the Equation (1), by adding the attack surface in each layer and dividing by the number of layers of the IoT architecture used. The attack surface in each layer is calculated based on Equation (2), multiplied the risk value associated with each step, and then divided by the number of steps to get an approximate average of the risks that exist in that layer.

Table 9. Common Vulnerability Scoring System Version 3 (CVSSv3) rating.

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

4.5. Step 5. Vulnerability Management

Vulnerability management is an assessment of the ability of a system or application, including current security controls and procedures, to resist various weaknesses, such as: misconfigurations, default installations, buffer overflows, missing patches, design flaws, operating system defects, application defects, open services, and default passwords [51]. The vulnerability management life cycle is a primary process that helps to locate and remedy system weaknesses before they are exploited, and this cycle should be performed monthly. In this phase vulnerabilities of the IoT system are identified. You can use automated tools that detect vulnerabilities when scanning the system such as Nessus, OpenVas, Acunetix, Qualys, and InsightVM, among others.

All serious insecurities associated with the system are permanently assessed, corrected, and eliminated to ensure a fault-free system. The risk assessment summarizes the vulnerability and level of risk identified for each of the selected assets. To determine the risk level of an asset, it is done through Common Vulnerability Scoring System Version 3 (CVSSv3), where there are five levels according to the severity of the risk; see Table 9.

It is the process of reducing vulnerabilities based on the results obtained. According to the analysis carried out, risks can be avoided, transferred, mitigated, or accepted. The best IoT-oriented hardening controls were established using the CIS Controls guide [52]. To calculate the average number of vulnerabilities based on the CVSSv3 system, the CVSSv3 value for all vulnerabilities will be summed up and divided by the number of vulnerabilities found, as in Formula (3).

$$CVSSv3\ vulnerability\ average = \frac{\left(\sum_{i=1}^{n} CVSSv3_{Step\ n}\right)}{n}. \quad (3)$$

4.6. Step 6. Hardening Process

The CIS Controls are a set of cyber defense-oriented exams that provides methods to stop today's most widespread and dangerous attacks. These controls anticipate and focus a smaller number of actions with high results [4]. The 20 CIS controls were analyzed. The controls related to IoT are distributed in the three-layer architecture (Figure 6) for the protection of the IoT system; see Figure 9.

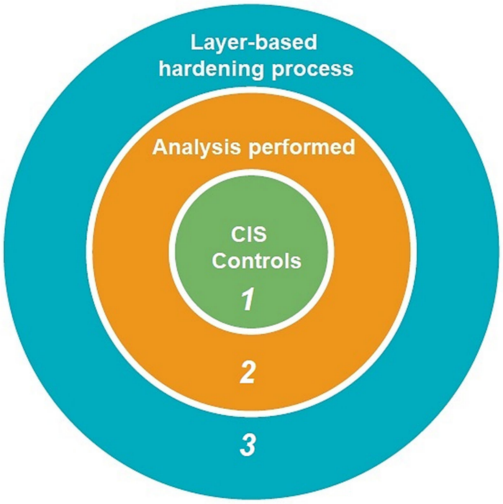

Figure 9. CIS Controls distribution in layer-based hardening process.

The hardening controls were applied to each of the layers of the implemented IoT architecture; see Table 10. To harden a specific device, CIS offers specific hardening guides for cloud providers, desktop software, server software, mobile devices, network devices, and operating systems.

Table 10. Hardening controls in IoT system.

Layer	Controls	Description
Perception	Secure and centralize records. Encrypted communication protocols. Strong and secure password. Latest stable version of firmware or operating system.	In the perception layer, devices, sensors, actuators, embedded systems must have adequate security levels to reach their maximum potential.
Network	Traffic configuration rules. Install the latest stable version of any security update on all network devices. Multi factor authentication and encrypted sessions. Exclusive management network. Inventory of network gateways. Deny unauthorized connections in the network gateways. Block malicious IP addresses. Inventory of wireless access points. Wireless data encryption. Separate wireless network.	At the network layer, you will actively establish, implement, and manage the security configuration of the network infrastructure using rigorous configuration and change management controls to prevent attackers from exploiting vulnerable services and configurations. To harden a specific network device, you can use the CIS Benchmark hardening guides, such as the following CIS Cisco Firewall, CIS Cisco Wireless LAN Controller, CIS Cisco IOS, CIS Juniper OS, CIS Palo Alto Firewall [53].
Application	Safe coding practices. Explicit error checking for all internally developed software. Acquired software support. Up-to-date and trusted third-party components. Encryption of tested and standardized algorithms. Personnel trained in secure software development. Static and dynamic code analysis tools. Separate production and non-production systems. Web Application Firewall (WAFs).	In the application layer, the security life cycle of all internal software developed and acquired must be managed to prevent, detect, and correct security weaknesses. To harden a specific application, you can use the CIS Benchmark hardening guides, such as the following CIS Apache HTTP Server [54], CIS Apache Tomcat, CIS Microsoft IIS [55], CIS Microsoft SharePoint, CIS Microsoft SQL Server, CIS MIT Kerberos, CIS MongoDB, CIS NGINX Benchmark, CIS Oracle Database [56], CIS Oracle MySQL [57], CIS VMware ESXi [58].

4.7. Step 7. Validation

The entire previous process is validated with the proposed risk formula to determine the risks involved in the IoT system. The attack surface is validated with Equations (1) and (2). To determine the risks in the vulnerabilities, it is done with the Nessus tool where the risk of the vulnerabilities is weighted in the CVSSv3 scale. To validate the IoT system, maturity levels have been proposed based on risk, attack surface, and vulnerabilities on the CVSSv3 scale. The appropriate IoT system maturity levels are 0 and 1 because the risk is zero or low, the attack surface is between 1 and 4, and the vulnerabilities on the CVSSv3 scale range from 0 to 3.9. Maturity level 2 is recommended for researchers working in a development environment. Maturity levels 3 and 4 indicate that there is not an adequate hardening process to reduce risks, so the hardening process should be performed again; see Table 11.

Table 11. IoT system mature levels.

Mature Level	Risk	Attack Surface (AS)	Vulnerability CVSSv3 (V)
4	Null	$1 \leq AS \leq 2.9$	$V = 0$
3	Low	$3 \leq AS \leq 4.9$	$0.1 \leq V \leq 3.9$
2	Medium	$5 \leq AS \leq 6.9$	$4.1 \leq V \leq 6.9$
1	High	$7 \leq AS \leq 8.9$	$7.0 \leq V \leq 8.9$
0	Critical	$9 \leq AS \leq 10$	$9.0 \leq V \leq 10.0$

5. Case Study

To demonstrate the efficiency of the proposed model, a case study was proposed in which the maturity level should be less than 1. The case study consists of two cases in which the first one will not apply the hardening process to demonstrate the high level of risk that IoT systems have, so in the verification phase it will show a level of maturity with risks. The test will be done again but with the hardening process to demonstrate the efficiency of the proposed solution in the verification step.

5.1. Expirimental Setup

Embedded systems are a fundamental part of IoT, because, with their fast processing both at the hardware and software level, they can carry out specific activities in real time [59]. In the case study, the Arduino Mega 2560 and Raspberry Pi 3B+ embedded systems were used. Figure 10 indicates the diagram and the elements used in the three-tier architecture. In the perception layer, the following sensors were used: temperature, humidity, gas, and ultrasound. In the network 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 from the sensors.

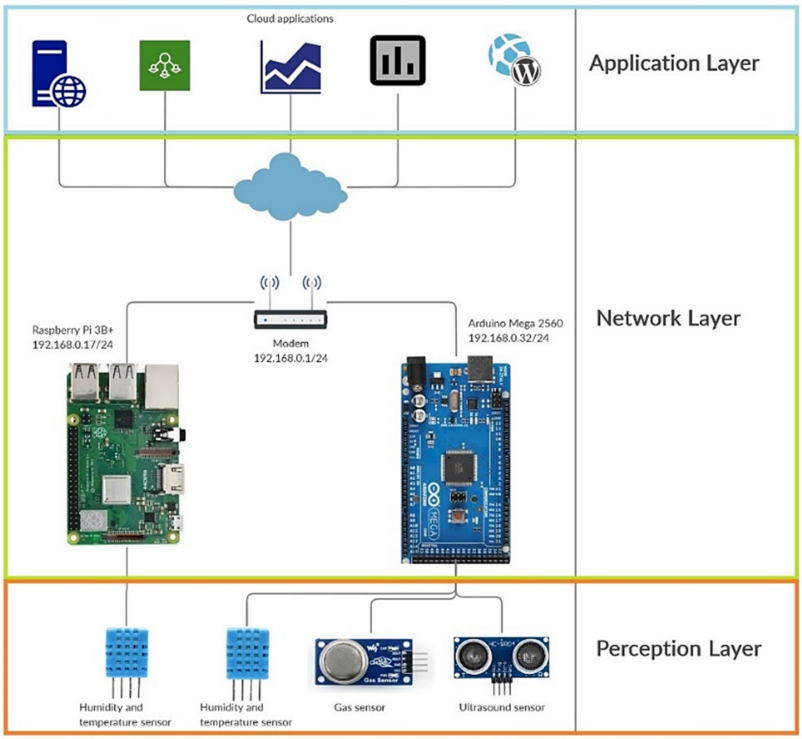

Figure 10. IoT architecture employed.

5.2. Step 1. Purpose and Requirements

The following, Table 12, defines the purpose and system requirements that were defined for the case study.

Table 12. Case study purposes and requirements.

Item	Description
Purpose of the system	Collect data from sensors to visualize it in an application.
System behavior	The sensors will collect data that will be sent to the Arduino and Raspberry Pi embedded systems. The embedded systems will send the data to cloud applications for visualization.
System managements requirement	The elements will be monitored by remote access where the continuity of the IoT system will be verified.
Security requirements	The system is required to be constantly available to be able to visualize the data in real time. It must not be prone to dictionary and DOS attacks.

5.3. Step 2. Risk Assessment

The realized IoT system will not be in an operating environment but the data will transit through the Internet for visualization. Based on the requirements of step 1, we analyzed the potential risks involved in the IoT system according to the vulnerabilities of the OWASP IoT Top 10 project; see Table 13.

Table 13. Case study risk.

OWASP IoT Top 10 Vulnerabilities	Compliance Class Score	Probability	Risk Result
Weak, guessable, or hardcoded passwords	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
Insecure 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

5.4. Step 3. Disabling Unnecessary Protocols, Services, and Configurations

The communication protocols used in the embedded systems were Secure Shell (SSH), Hypertext Transfer Protocol (HTTP), and Virtual Network Computing (VNC). The communication protocols used in the embedded systems were SSH, HTTP, and VNC. To qualify the ports, a default scan was performed, where the Hypertext Markup Language (HTML) code used in one of the ports was obtained; see Figure 11. The following, Table 14, indicates the ports and services that were found in the port scan.

Table 14. Vulnerability on test scenario using Raspberry 3B+.

Device	Model	Host	Port Protocol	State	Service
Raspberry Pi	3B+	192.168.0.17	22 TCP	Open	SSH
	3B+	192.168.0.17	80 TCP	Open	HTTP
	3B+	192.168.0.17	5900 TCP	Open	VNC
Arduino	Mega 2560	192.168.0.32	80 TCP	Open	HTTP

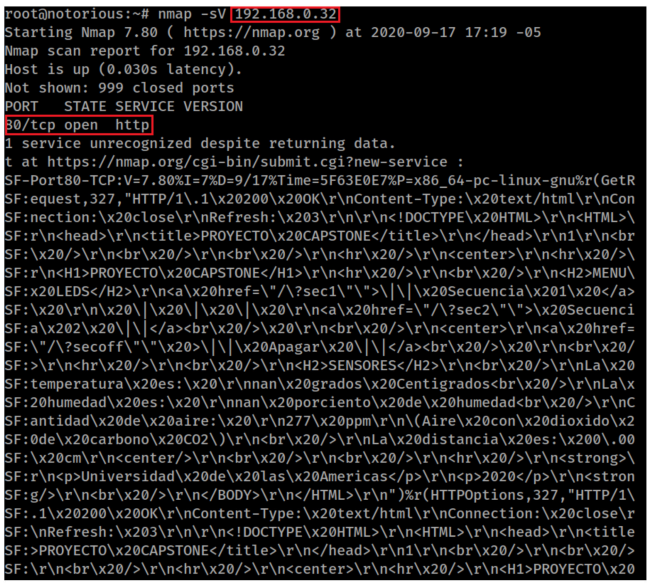

Figure 11. Ports scan.

5.5. Step 4. Attack Surface

Table 15 below indicates the risk in each step of the IoT System elements checklist.

Table 15. Checklist score.

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
	14	4	5	9
	15	4	5	9
	16	4	5	9
	17	4	5	9

Table 16 shows the attack surface area for each layer.

Table 16. Attack surface.

Layer	Equation	Value Replacement	Result
Perception layer	$\frac{\left(\sum_{i=1}^{n} risk_{Step\ n}\right)}{n}$	$\frac{(9+9+9+1)}{4}$	7
Network layer	$\frac{\left(\sum_{i=5}^{n} risk_{Step\ n}\right)}{n}$	$\frac{(7+9+7+8)}{4}$	7.8
Application layer	$\frac{\left(\sum_{i=16}^{n} risk_{Step\ n}\right)}{n}$	$\frac{(9+9+1+1+9+9+9+9+9)}{9}$	7.2

To calculate the attack surface in the IoT system, the attack surface of each layer was summed.

$$Attack\ surface\ IoT\ system = \frac{(7 + 7.8 + 7.2)}{3}, \quad (4)$$

$$Attack\ surface\ IoT\ system = 7.33 \quad (5)$$

5.6. Step 5. Vulnerability Management

A vulnerability scan was performed with the Nessus tool. The vulnerabilities found in the embedded systems are vulnerabilities due to lack of patches and unstable versions; see Table 17.

Table 17. Vulnerabilities founded on test scenario using Raspberry 3B+.

IP	CVE	CVSSv3	Risk	Port Protocol	Vulnerability
192.168.0.17	CVE-2019-6798	9.8	Critical	80 TCP	phpMyAdmin 4.× < 4.8.5
	CVE-2019-6798	9.8	Critical	80 TCP	phpMyAdmin 4.× < 4.8.5
	CVE-2019-11768	9.8	Critical	80 TCP	phpMyAdmin prior to 4.8.6
	CVE-2019-11768	9.8	Critical	80 TCP	phpMyAdmin prior to 4.8.6
	CVE-2019-9517	9.1	Critical	80 TCP	Apache 2.4.× < 2.4.41
	CVE-2020-5504	8.8	High	80 TCP	phpMyAdmin 4.× < 4.9.4/5.× < 5.0.1
	CVE-2019-0220	7.8	High	80 TCP	Apache 2.4.× < 2.4.39
	CVE-2019-12616	6.5	Medium	80 TCP	phpMyAdmin 4.× < 4.9.0
	CVE-2020-1927	6.1	Medium	80 TCP	Apache 2.4.× < 2.4.42
	CVE-2020-1934	6.1	Medium	80 TCP	Apache 2.4.× < 2.4.42

To discover different weaknesses of the embedded systems, various attacks were carried out such as denial of services (DoS), Internet Control Message Protocol version 6 (ICMPv6) flooding, dictionary attack, and man in the middle (MITM); see Table 18.

Table 18. Attacks in the IoT test scenario.

IP	CVSSv3	Risk	Port Protocol	Attack Application	Result
192.168.0.17	7.5	High	80 TCP	DoS Slow HTTP Test	Effective
	0	Null	80 TCP	DoS Hping 3	Ineffective
	7.5	High	80 TCP	DoS Evil Foca	Effective
	0	Null	ICMPv6	Flood THCP-IPV6	Ineffective
	9.8	Critical	22 TCP	Dictionary Hydra	Effective
	9.8	Critical	5900 TCP	Dictionary Hydra	Effective
	9.8	Critical	ARP	MITM Evil Foca	Effective
192.168.0.32	7.5	High	80 TCP	DoS Slow HTTP Test	Effective
	7.5	High	80 TCP	DoS Hping3	Effective
	7.5	High	80 TCP	DoS Evil Foca	Effective

Formula (3) is used to calculate the average number of vulnerabilities based on the CVSSv3 system, resulting in 7.5. This indicates that most of the vulnerabilities are in the high category.

5.7. Step 6. Hardening Process

The obtained values of risk, attack surface and CVSSv3 indicate that the IoT system has a maturity level equal to 1; see Table 19. The hardening process should be applied, changing the ports to a different range of known ports, and patching the vulnerabilities.

Table 19. IoT system mature levels.

Risk	Attack Surface (AS)	Vulnerability CVSSv3 (V)	Maturity Level
7	7.3	7.5	1

The risks found in the attack surface were mitigated through the hardening process. The hardening process performed in this environment was to change the number of ports of the services found with the port scan. Ports were changed to a different port range from the known ports. Arduino Mega 2560 firmware was updated. The hardening guide CIS Debian Linux 9 Benchmark [60] was applied to the Raspberry Pi 3B + operating system. This hardening guide focuses on disable unused filesystems, configure software updates, filesystem integrity checking, secure boot settings, access control, warning banners, network configuration, disable danger network protocols, configure firewall, logging and auditing, system file permissions, users, and group settings.

Virtual Local Area Networks (VLANs) and Access Control Lists (ACL) were applied on the network device used. With the ACL created only the management VLAN can have remote access to the Arduino Mega 2560 and the Raspberry Pi 3B+. A pool was created with the Media Access Control Address (MAC) of the embedded systems. A policy was created to block the network interface when connecting a device that does not have its MAC registered in the pool. Virtual management network was created that is the only one that has access to the IoT devices; see Figure 12. Additionally, the process of hardening the system and the updates of the services was carried out, thus mitigating the vulnerabilities found; see Table 18.

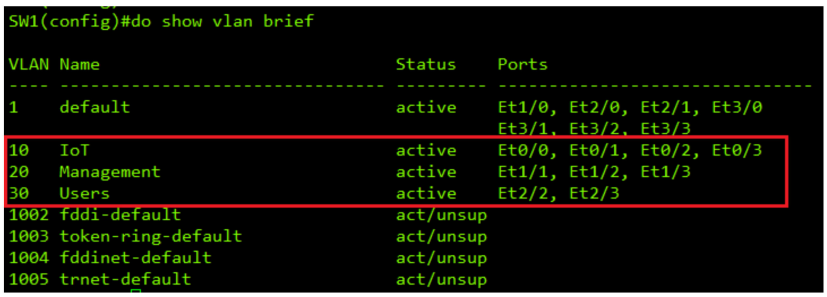

Figure 12. VLANs created for hardening process.

The IoT system is no longer susceptible to OWASP IoT Top 10 vulnerabilities. The calculated risk is in the null category; see Table 20.

The aim of this step is to use communication protocols that have an adequate level of encryption and do not involve risks in their implementation. There are communication protocols that do not have an adequate level of security. Changing the port number of the protocols that will be used reduces the probability of a threat occurring on the attack surface. When using a range of ports different from the range of known ports, it is more difficult to determine which port is open and which service it hosts; see Table 21.

Table 20. Case study risk post-hardening.

OWASP IoT Top 10 Vulnerabilities	Compliance Class Score	Probability	Risk Result
Weak, guessable, or hardcoded passwords	1	0	1
Insecure network services	2	0	2
Insecure ecosystem interfaces	2	0	2
Lack of secure update mechanism	1	1	2
Use of insecure or outdated components	1	0	1
Insufficient privacy protection	1	0	1
Insecure data transfer and storage	1	1	2
Lack of device management	1	0	1
Insecure default settings	1	0	1
Lack of physical hardening	1	0	1

Table 21. Port range of communication ports.

Range	Category
0–1023	Known ports
1024–49,151	Registered ports
49,152–65,535	Dynamic and private ports

The ports were changed to a different range of known ports. When performing the recognition with the Nmap tool, it was validated that the proposed solution is effective because it was not possible to identify any exposed port in the IoT devices, as indicated in Table 22; see Figure 13.

Table 22. Services found of IoT test scenario.

Device	Model	Host	Port Protocol	State	Service
Raspberry Pi	3B+	192.168.0.17	22 TCP	Closed	SSH
	3B+	192.168.0.17	80 TCP	Closed	HTTP
	3B+	192.168.0.17	5900 TCP	Closed	VNC
Arduino	Mega 2560	192.168.0.32	80 TCP	Closed	HTTP

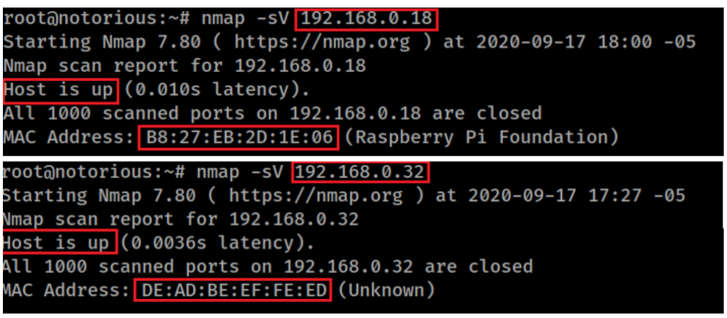

Figure 13. Ports scan Raspberry Pi.

Using the new values of the risk in each step, we proceeded to calculate the attack surface in each layer of the IoT system; see Table 23.

Table 23. Attack surface.

Layer	Equation	Value Replacement	Result
Perception layer	$\frac{\left(\sum_{i=1}^{n} risk_{Step\ n}\right)}{n}$	$\frac{(2+1+1+1)}{4}$	1.25
Network layer	$\frac{\left(\sum_{i=5}^{n} risk_{Step\ n}\right)}{n}$	$\frac{(2+1+1+2)}{4}$	1.5
Application layer	$\frac{\left(\sum_{i=16}^{n} risk_{Step\ n}\right)}{n}$	$\frac{(2+2+1+1+1+2+1+2+2)}{9}$	1.5

The attack surface of the IoT system was recalculated but with the new values of each layer.

$$Attack\ surface\ IoT\ system = \frac{(1.25 + 1.5 + 1.5)}{3}, \quad (6)$$

$$Attack\ surface\ IoT\ system = 1.42. \quad (7)$$

Vulnerability analysis was performed again with the Nessus tool. The CVSSv3 weighting obtained null values, which indicates that the system was correctly patched, and the vulnerabilities previously found were corrected; see Table 24.

Table 24. Vulnerabilities founded post-hardening.

IP	CVE	CVSSv3	Risk	Port Protocol	Vulnerability
192.168.0.17	CVE-2019-6798	0	Null	80 TCP	phpMyAdmin 4.× < 4.8.5
	CVE-2019-6798	0	Null	80 TCP	phpMyAdmin 4.× < 4.8.5
	CVE-2019-11768	0	Null	80 TCP	phpMyAdmin prior to 4.8.6
	CVE-2019-11768	0	Null	80 TCP	phpMyAdmin prior to 4.8.6
	CVE-2019-9517	0	Null	80 TCP	Apache 2.4.× < 2.4.41
	CVE-2020-5504	0	Null	80 TCP	phpMyAdmin 4.× < 4.9.4/5.× < 5.0.1
	CVE-2019-0220	0	Null	80 TCP	Apache 2.4.× < 2.4.39
	CVE-2019-12616	0	Null	80 TCP	phpMyAdmin 4.× < 4.9.0
	CVE-2020-1927	0	Null	80 TCP	Apache 2.4.× < 2.4.42
	CVE-2020-1934	0	Null	80 TCP	Apache 2.4.× < 2.4.42

By changing the default configurations based on the proposed methodology, the risks caused by the attacks were mitigated; see Table 25.

Table 25. Attacks founded post-hardening.

IP	CVSSv3	Risk	Port Protocol	Attack Application	Result
192.168.0.17	0	Null	80 TCP	DoS Slow HTTP Test	Ineffective
	0	Null	80 TCP	DoS Hping 3	Ineffective
	0	Null	80 TCP	DoS Evil Foca	Ineffective
	0	Null	ICMPv6	Flood THCP-IPV6	Ineffective
	0	Null	22 TCP	Dictionary Hydra	Ineffective
	0	Null	5900 TCP	Dictionary Hydra	Ineffective
	0	Null	ARP	MITM Evil foca	Ineffective
192.168.0.32	0	Null	80 TCP	DoS Slow HTTP Test	Ineffective
	0	Null	80 TCP	DoS Hping3	Ineffective
	0	Null	80 TCP	DoS Evil Foca	Ineffective

All vulnerabilities found based on the CVSSv3 scale represent zero risk. Therefore, the average number of vulnerabilities based on the CVSSv3 system is 0.

5.8. Step 7. Validation

The values obtained for risk, attack surface and CVSSv3 indicate that the system has a maturity level equal to 4; see Table 26. Properly applying the hardening process ensures that the parameters to be evaluated will be at an adequate level.

Table 26. IoT system mature levels.

Risk	Attack Surface (AS)	Vulnerability CVSSv3 (V)	Maturity Level
1.4	1.42	0	4

6. Discussion

In this work, a model has been presented that allows to reduce the risk levels in the IoT system, attack surface, and vulnerabilities by means of the correct execution of the hardening process. IoT systems without a prior procedure contain multiple weaknesses, to know the weaknesses of the system is done through a risk analysis and vulnerability assessments. These procedures are crucial to understand the risks that surround the system. To mitigate these risks, the hardening process is carried out in the layers of the IoT system.

According to the study carried out, most of the improvement models are based on risk analysis based on specific ISO standards. These models pursue policy compliance within specific timeframes, while CIS is agile and fast implementation with effective results. Risk analysis applied to IoT systems are slow and do not adapt to the constant changes that arise. It evaluates more policy compliance with a larger number of controls [61]. CIS uses fewer controls, and its exploitation is more practical, so it is compatible with development cycles, such as DevOps. Table 27 shows the comparison between CIS and risks.

Table 27. CIS versus risk compliance.

CIS	Risk
Continuously assess	Assess in specific periods
Incorporate the feedback of others	Evaluates policy compliance
Tried-and-true scoring methods	Only one scoring method
Align with NIST 800-53 and PCI-DSS V3.	Align with ISO
Continuous cycle of vulnerability assessment and mitigation	Continuous cycle of vulnerability assessment and mitigation
Reports demonstrate compliance with CIS controls	Reports demonstrate compliance with appropriate policies

To calculate the attack surface of the IoT system, a model based on the RASQ proposal was presented. The risk is calculated in each step of the IoT system elements checklist (Table 8). To obtain the attack surface of the entire IoT system, the attack surface of each layer is added up and divided by 3. A scale is used to determine whether the attack surface value is adequate. This scale has the values of critic, high, medium, low, and null.

To model all the threats that surround IoT systems, the analysis carried out by the OWASP IoT Top 10 project was considered. This project allows us to identify the threats that generate the most risks in IoT devices. As IoT systems are vulnerable to various attack vectors, compliance classes were used, which can more accurately determine system risks based on levels of confidentiality, integrity, and availability.

When using an embedded system for IoT purposes, the communication protocols to be used must be considered. Today, most embedded systems use protocols that do not contain adequate encryption. In the proposed methodology, to reduce notable risks, the use of protocols with high encryption levels and making the port change of the protocols used stand out.

In a usual port scan with the Nmap tool, the range of known ports (Table 21) exposed is obtained. In the present methodology to reduce the probability of determining the exposed ports in the IoT system, it is proposed to use a range of ports different from the known ports. Without applying the proposed methodology, four exposed ports were found using the SSH, HTTP, and VNC protocols. When applying the proposed methodology,

the port changes were made, so, when performing the scan again with Nmap, it was not determined which ports are exposed.

To determine the weaknesses of the IoT system, the Nessus tool was used. This tool allows to know the vulnerabilities caused by bad configurations, default installations, buffer overflows, lack of patches, design defects, operating system defects, application defects, open services, and default passwords found in the IoT system. When performing the vulnerability analysis without applying the proposed methodology, ten vulnerabilities were found with critical, high, and medium risk levels. Through a due process of hardening, the vulnerabilities found were mitigated, and, to verify that there are no risks and weaknesses, the vulnerability analysis was carried out again where no risk was found in the system.

When using default configurations, IoT systems have always been vulnerable to various types of attacks that seek to compromise the system and prevent its continuity. Some of these attacks aim to achieve full control of the IoT device. To find out how vulnerable IoT devices are, denial of service attacks, IpV6 flooding, dictionary, and man in the middle (MITM) were carried out. Without applying the proposed methodology, ten attacks were carried out, where eight were effective and two were ineffective. When applying the proposed methodology, no attack was effective.

In response to the research question that initiated this paper, this work identified the relationship between IoT and inadequate levels of system maturity. To evaluate the effectiveness of the proposed methodology, a case study was conducted. Without applying the hardening process, the maturity level is equal to 3 because the risk is equal to 7, the attack surface is equal to 7.3, and the vulnerabilities in CVSSv3 scale is equal to 7.5. Applying the hardening process, the maturity level is equal to 0 because the risk is equal to 4, the attack surface is equal to 1.42, and the vulnerabilities in CVSSv3 scale is equal to 0.

7. Conclusions

The qualitative analysis conducted on the scientific submissions of “IoT” AND “risk” AND “best practice” from 2016 to 2021 indicates that these papers were aligned to cover specific needs related to risk and threat analysis. However, the analysis reflects that there is a lack of research papers related to hardening and security validations. The contributions of the research analyzed allow the risks to be determined by means of standards proposed by international organizations, such as ISO, OWASP, and NIST.

IoT devices are growing exponentially, they register more risks and multiple threats, such as DOS, distributed denial of service (DDOS), MITM, buffer overflow, flooding attacks, malware, etc. Given this problem and the lack of IoT security validations, a solution was generated. The proposed solution is a cybersecurity model based on hardening for secure IoT implementations. This model consists of three phases. In the first phase, a threat modeling is performed to identify the risks and the communication protocols to be used. In the second phase, a vulnerability analysis is performed, and, in the third phase, the hardening process based on CIS controls is applied to reduce existing risks.

The fundamental axis of the proposed solution is hardening. The best hardening guides are proposed by CIS. The CIS controls guide was analyzed, where the most relevant controls are distributed to the three layers of the IoT architecture. If a deeper hardening is needed, CIS offers specific hardening guides oriented to cloud providers, desktop software, server software, mobile devices, network devices, and operating systems.

In future research, a mathematical analysis of the checklist of the attack surface will be performed, performing random tests to know the minimum parameters that the IoT system needs to have an adequate level of maturity.

Author Contributions: Conceptualization, C.C. and I.O.-G.; analysis of previous works, A.E. and R.O.A.: proposed solution, A.E. and C.C.; formal analysis, I.O.-G. and R.O.A.; investigation, A.E. and I.O.-G.; writing–review and editing, A.E. and R.O.A.; project administration, A.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to restrictions on privacy policy on sensitive data categories.

Acknowledgments: The authors acknowledge to Universidad de Las Américas of Ecuador and his Engineer degree in Information Technology.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kaur, C. The Cloud Computing and Internet of Things (IoT). *Int. J. Sci. Res. Sci. Eng. Technol.* **2020**, 19–22. [CrossRef]
2. Rajendran, G. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–6. [CrossRef]
3. Abomhara, M.; Køien, G.M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]
4. International Telecommunication Union (ITU). Definitions and Terminology Relating to Building Confidence and Security in the Use of Information and Communication. 2010, pp. 20–22. Available online: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20.pdf (accessed on 13 January 2021).
5. The 20 CIS Controls & Resources Page. Available online: https://www.cisecurity.org/controls/cis-controls-list/ (accessed on 13 January 2021).
6. Beckers, K.; Heisel, M.; Solhaug, B.; Stølen, K. *ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant*; Springer: Berlin, Germany, 2014; pp. 315–344. [CrossRef]
7. De Oliveira, U.R.; Augusto, F.; Marins, S.; Rocha, H.M.; Antonio, V.; Salomon, P. The ISO 31000 Standard in Supply Chain Risk Management. *J. Clean. Prod.* **2017**. [CrossRef]
8. Haoues, M.; Sellami, A.; Ben-Abdallah, H.; Cheikhi, L. A guideline for software architecture selection based on ISO 25010 quality related characteristics. *J. Syst. Assur. Eng. Manag.* **2016**, *8*, 1–24. [CrossRef]
9. OWASP Internet of Things Project Page. Available online: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project (accessed on 14 January 2021).
10. Santos, L.; Silva, E.; Batista, T.; Cavalcante, E.; Leite, J.; Oquendo, F. An architectural style for internet of things systems. In Proceedings of the SAC '20: The 35th ACM/SIGAPP Symposium on Applied Computing, Brno, Czech Republic, 30 March–3 April 2020; pp. 1488–1497. [CrossRef]
11. Leite, C.; Gondim, J.; Caetano, M.F.; Alchieri, E.A. Pentest on Internet of Things Devices. In Proceedings of the 2019 XLV Latin American Computing Conference (CLEI), Panama, Panama, 30 September–4 October 2019; pp. 1–10. [CrossRef]
12. Tien, C.; Tsai, T.; Chen, I.; Kuo, S. UFO-Hidden Backdoor Discovery and Security Verification in IoT Device Firmware. In Proceedings of the 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Memphis, TN, USA, 15–18 October 2018; pp. 18–23. [CrossRef]
13. Lee, M.; Lee, K.; Shim, J.; Cho, S.; Choi, J. Security Threat on Wearable Services: Empirical Study using a Commercial Smartband. *IEEE Int. Conf. Consum. Electron.* **2016**. [CrossRef]
14. Zhang, W.; Zhang, B.; Zhou, Y.; He, H.; Ding, Z. An IoT Honeynet based on Multi-port Honeypots for Capturing IoT attacks. *IEEE Internet Things J.* **2019**, 1–9. [CrossRef]
15. Li, K.; Wen, H.; Li, H.; Zhu, H.; Sun, L. Security OSIF: Toward Automatic Discovery and Analysis of Event Based Cyber Threat Intelligence. *IEEE SmartWorld Ubiquitous Intell. Comput.* **2018**, 741–747. [CrossRef]
16. Sengan, S.; Subramaniyaswamy, V.; Nair, S.K.; Indragandhi, V.; Manikandan, J.; Ravi, L. Enhancing cyber-physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future Gener. Comput. Syst.* **2020**. [CrossRef]
17. Visoottiviseth, V.; Sakarin, P.; Thongwilai, J.; Choobanjong, T. Signature-based and Behavior-based Attack Detection with Machine Learning for Home IoT Devices. In Proceedings of the 2020 IEEE REGION 10 CONFERENCE (TENCON), Osaka, Japan, 16–19 November 2020; pp. 829–834. [CrossRef]
18. Visoottiviseth, V.; Akarasiriwong, P.; Chaiyasart, S.; Chotivatunyu, S. PENTOS: Penetration Testing Tool for Internet of Thing Devices. In Proceedings of the TENCON 2017-2017 IEEE Region 10 Conference, Penang, Malaysia, 5–8 November 2017; pp. 2279–2284. [CrossRef]
19. Chu, G.; Apthorpe, N.; Feamster, N. Security and Privacy Analyses of Internet of Things Children 's Toys. *IEEE Internet Things J.* **2018**. [CrossRef]
20. Mohsin, M.; Anwar, Z.; Zaman, F.; Al-shaer, E. IoTChecker: A Data-driven Framework for Security Analytics of Internet of Things Configurations. *Comput. Secur.* **2017**. [CrossRef]
21. Akatyev, N.; James, J.I. Evidence Identification in IoT Networks Based on Threat Assessment. *Future Gener. Comput. Syst.* **2017**. [CrossRef]

22. Di Giorgio, A.; Foglietta, C.; Galli, A.; Giuseppi, A.; Liberati, F.; Neri, A.; Panzieri, S.; Pascucci, F.; Proenca, J.; Pucci, P.; et al. Integrated Protection of Industrial Control Systems from Cyber-attacks: The ATENA Approach. *Int. J. Crit. Infrastruct. Prot.* **2018**. [CrossRef]
23. Rizvi, S.; Pipetti, R.; Mcintyre, N.; Todd, J. Threat Model for Securing Internet of Things (IoT) Network at Device-Level. *Internet Things* **2020**, 100240. [CrossRef]
24. Matheu-García, S.N.; Hernández-Ramos, J.L.; Skarmeta, A.F.; Baldino, G. Risk-based Automated Assessment and Testing for the Cybersecurity Certification and Labelling of IoT Devices. *Comput. Stand. Interfaces* **2018**. [CrossRef]
25. Khan, Y.; Ndubuaku, M. Ontology-Based Automation of Security Guidelines for Smart Homes. In Proceedings of the 2018 IEEE 4th World Forum Internet Things, Penang, Malaysia, 5–8 November 2017; pp. 35–40. [CrossRef]
26. Li, J. Vulnerabilities Mapping based on OWASP-SANS: A Survey for Static Application Security Testing (SAST). *Ann. Emerg. Technol. Comput.* **2020**, *4*, 1–8. [CrossRef]
27. Teodoro, N.; Serrão, C. Web application security: Improving Critical Web-based Applications Quality through in-depth Security Analysis. In Proceedings of the International Conference on Information Society (i-Society 2011), London, UK, 27–29 June 2011. [CrossRef]
28. Mohino, J.D.V.; Higuera, J.B.; Ram, J.; Higuera, B.; Antonio, J.; Montalvo, S. The Application of a New Secure Software Development Life Cycle (S-SDLC) with Agile Methodologies. *Electronics* **2019**, *8*, 1218. [CrossRef]
29. Rindell, K.; Hyrynsalmi, S.; Leppänen, V. Fitting Security into Agile Software Development. *Res. Anthol. Recent Trends Tools Implic. Comput. Program.* **2021**, 1026–1045. [CrossRef]
30. Anderson, S.; Williams, T. Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge? *Comput. Stand. Interfaces* **2017**, 1–10. [CrossRef]
31. Azaliah, N.; Bakar, A.; Makhtariah, W.; Ramli, W.; Hassan, N.H. The internet of things in healthcare: Anoverview, challenges and model plan for security risks management process. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *15*, 414–420. [CrossRef]
32. Skierka, I.M. The governance of safety and security risks in connected healthcare. *Living Internet Things Cybersecur. IoT* **2018**, 1–12. [CrossRef]
33. Safa, N.S.; Maple, C.; Watson, T. An Information Security Risk Management Model for Smart Industries. *Adv. Transdiscipl. Eng.* **2017**, *6*, 257–262. [CrossRef]
34. Huang, X.; Nazir, S. Evaluating Security of Internet of Medical Things Using the Analytic Network Process Method. *Secur. Commun. Netw.* **2020**, 1–14. [CrossRef]
35. Casola, V.; De Benedictis, A.; Rak, M.; Villano, U. Toward the automation of threat modeling and risk assessment in IoT systems. *Internet Things* **2019**, 100056. [CrossRef]
36. Ngamboé, M.; Berthier, P.; Ammari, N.; Dyrda, K.; Fernandez, J.M. Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED). *Int. J. Inf. Secur.* **2020**. [CrossRef]
37. Kieras, T.; Farooq, M.J.; Zhu, Q. Modeling and Assessment of IoT Supply Chain Security Risks: The Role of Structural and Parametric Uncertainties. *IEEE Symp. Secur. Priv.* **2020**. [CrossRef]
38. 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. *J. Inf. Secur.* **2020**. [CrossRef]
39. Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet* **2020**, *12*, 157. [CrossRef]
40. Ruan, K. Cyber Risk Measurement in the Hyperconnected World. In *Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics*; Academic Press: London, UK, 2019; pp. 75–86. ISBN 9780128121580. [CrossRef]
41. Yigit, B.; Gur, G.; Alagoz, F.; Tellenbach, B. Cost-Aware Securing of IoT Systems Using Attack Graphs. *Ad Hoc Netw.* **2019**, 23–25. [CrossRef]
42. Maillet-Contoz, L.; Michel, E.; Brun, P.; Leprêtre, K. End-to-end security validation of IoT systems based on digital twins of end-devices. IEEE 2020 Glob. *Internet Things Summit* **2020**. [CrossRef]
43. Stine, I.; Rice, M.; Dunlap, S.; Pecarina, J. A cyber risk scoring system for medical devices. *Int. J. Crit. Infrastruct. Prot.* **2017**. [CrossRef]
44. Sancho, J.C.; Caro, A.; Ávila, M.; Bravo, A. New approach for threat classification and security risk estimations based on security event management. *Future Gener. Comput. Syst.* **2020**, *113*, 488–505. [CrossRef]
45. Javed, B.; Iqbal, M.W.; Abbas, H. Internet of Things (IoT) Design Considerations for Developers and Manufacturers. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017; pp. 2–7. [CrossRef]
46. IoT Security Foundation. *IoT Security Compliance Framework*; IoTSF: George Square, Glasgow, Scotland, 2020.
47. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **2014**, *80*, 973–993. [CrossRef]
48. Manadhata, P.K.; Kaynar, D.K.; Wing, J.M. A Formal Model for a System's Attack Surface. *Mov. Target Defense. Adv. Inf. Secur.* **2011**, *54*, 1–28. [CrossRef]
49. Rizvi, S.; Orr, R.J.; Cox, A.; Ashokkumar, P.; Rizvi, M.R. Identifying the Attack Surface for IoT Network. *Internet Things* **2020**, *9*, 1–29. [CrossRef]
50. Howard, M.; Pincus, J.; Wing, J.M. Measuring Relative Attack Surfaces. In *Computer Security in the 21st Century*; Springer: Boston, MA, USA, 2005; pp. 110–138. [CrossRef]

51. Gregg, M.; Santos, O. *Certified Ethical Hacker (CEH) Version 10 Cert Guide*, 3rd ed.; Pearson IT Certification: River Street, Hoboken, NJ, USA, 2019; ISBN 9780789760524.
52. *Center for Internet Security CIS Controls 7.1*; Center for Internet Security, Inc.: East Greenbush, NY, USA, 2019.
53. Perminov, P.; Kosachenko, T.; Konev, A.; Shelupanov, A. Automation of information security audit in the Information System on the example of a standard "CIS Palo Alto 8 Firewall Benchmark". *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 2085–2088. [CrossRef]
54. Olencin, M.; Perha, J. Automated configuration of a Linux web server security. In Proceedings of the 2019 IEEE 15th International Scientific Conference on Informatics, Poprad, Slovakia, 20–22 November 2019; pp. 491–496. [CrossRef]
55. Mendes, N.; Neto, A.A.; Durães, J.; Vieira, M.; Madeira, H. Assessing and Comparing Security of Web Servers. In Proceedings of the 2008 14th IEEE Pacific Rim International Symposium on Dependable Computing, Taipei, Taiwan, 15–17 December 2008; pp. 313–322. [CrossRef]
56. Neto, A.A.; Vieira, M.; Madeira, H. An Appraisal to Assess the Security of Database Configurations. In Proceedings of the 2009 Second International Conference on Dependability, Athens, Greece, 18–23 June 2009. [CrossRef]
57. Newman, G.; DeFuria, R. Security Control Verification and Monitoring Subsystem for Use in a Computer Information Database System. U.S. Patent 8225409, 23 March 2006.
58. Spichkova, M.; Li, B.; Porter, L.; Mason, L.; Lyu, Y.; Weng, Y.; Spichkova, M.; Lyu, Y.; Weng, Y. ScienceDirect VM2: Automated security configuration and testing of virtual VM2: Automated security configuration machine images and testing of virtual machine images. *Procedia Comput. Sci.* **2020**, *176*, 3610–3617. [CrossRef]
59. Samie, F.; Bauer, L.; Henkel, J. IoT Technologies for Embedded Computing: A Survey. In Proceedings of the International Conference on Hardware/Software Codesign and System Synthesis, Pittsburgh, PA, USA, 2–7 October 2016; pp. 1–10. [CrossRef]
60. Prastika, D.P.; Triyono, J.; Lestari, U. Audit dam implementasi CIS Benchmark pada sistem operasi Linux Debian Server. *J. Jarkom* **2019**, *6*, 1–12.
61. Radanliev, P.; De Roure, D.; Nurse, J.R.C.; Nicolescu, R.; Huth, M.; Cannady, S.; Montalvo, R.M. Cyber risk impact assessment assessing the risk from the IoT to the digital Economy. *SN Appl. Sci.* **2020**, 1–12. [CrossRef]