games

Article

Defining Cyber Risk Scenarios to Evaluate IoT Systems

Roberto Andrade [1], Iván Ortiz [2], María Cazares [3,*], Gustavo Navas [3] and María Isabel Sánchez-Pazmiño [4]

[1] Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito 170525, Ecuador; roberto.andrade@epn.edu.ec
[2] Facultad de Ingeniería y Ciencias Aplicadas, Universidad de las Américas, Quito 170122, Ecuador; ivan.ortiz@udla.edu.ec
[3] IDEIAGEOCA Research Group, Universidad Politécnica Salesiana, Quito 170517, Ecuador; gnavas@ups.edu.ec
[4] Facultad de Posgrados, Universidad de las Américas, Quito 170122, Ecuador; mariaisabel.sanchez@udla.edu.ec
* Correspondence: mcazares@ups.edu.ec

Abstract: The growth of the Internet of Things (IoT) has accelerated digital transformation processes in organizations and cities. However, it has also opened new security challenges due to the complexity and dynamism of these systems. The application of security risk analysis methodologies used to evaluate information technology (IT) systems have their limitations to qualitatively assess the security risks in IoT systems, due to the lack of historical data and the dynamic behavior of the solutions based on the IoT. The objective of this study is to propose a methodology for developing a security risk analysis using scenarios based on the risk factors of IoT devices. In order to manage the uncertainty due to the dynamics of IoT behaviors, we propose the use of Bayesian networks in conjunction with the Best Worst Method (BWM) for multi-criteria decision-making to obtain a quantitative security risk value.

Keywords: cybersecurity; IoT; Bayesian network; multi-criteria analysis; risk analysis

check for updates

Citation: Andrade, R.; Ortiz, I.; Cazares, M.; Navas, G.; Sánchez-Pazmiño, M.I. Defining Cyber Risk Scenarios to Evaluate IoT Systems. *Games* **2022**, *14*, 1. https://doi.org/10.3390/g14010001

Academic Editors: Mohammad Mahdi Khalili, Xueru Zhang and Ulrich Berger

Received: 17 September 2022
Revised: 8 November 2022
Accepted: 17 November 2022
Published: 20 December 2022

1. Introduction

According to the World Economic Forum (WEF), "Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse events) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security" [1]. Regarding the World Economic Forum, in a systemic scenario, cyber-attack events reach the highest level, which disrupts consumer confidence in the financial sector. In this context, the WEF establishes three levels of systemic risk [1]:

- Level 1: the pervasiveness of technology could disrupt several organizations simultaneously;
- Level 2: interdependencies between organizations, as an organization's cybersecurity failure presents a potential risk of affecting its networking organizations;
- Level 3: cybersecurity failure, which could be systematically catastrophic to economies and societies. Multiple financial and social sectors could fail.

As stated by the World Economic Forum, there are 11 systemic cyber-attack patterns that could develop into systemic cyber-incidents [1]:

1. Repeated attacks;
2. Scattershot attacks;
3. Pervasive attacks;
4. Rolling attacks;

5. Transitive attacks;
6. Cascading attacks;
7. Shared resource consumption attacks;
8. Critical function attacks;
9. Regional attacks;
10. Service dependency attacks;
11. Coordinated supply chain attacks.

Moreover, depending on the number, timing, and scale, the cyber-attack patterns could significantly impact the economy and they could turn into a systemic event. In this context, the security implications of IoT systems could result in a potential systemic risk. Disruption can be increased by the addition of new devices and the inherent characteristics of IoT systems, such as heterogeneity of technologies, interconnection with IT/OT systems, and ease of scalability and growth. However, could IoT develop into a systemic risk? There are several reasons to consider this argument.

First, the large capability of interconnectivity. The IoT is an emerging technology with significant growth. In addition, future projections in this field reveal a continuous increase. For instance, McKinsey [2] estimates that the IoT could globally enable from USD 5.5 trillion to USD 12.6 trillion by 2030. Cisco [3] mentions that 500 billion IoT devices will be connected by 2030. Second, the expanding use of IoT in strategic sectors. Hence, McKinsey affirms that the financial rate (CAGR), between 2020 and 2030, will be of 37% in autonomous vehicles, 27% in productivity, 25% in inventory management, 24% in sales performance, 19% in health, 19% in environmental management, and 18% in energy administration.

Furthermore, the WEF [1] indicates that systemic cyber catastrophic events could be related to conditions such as higher loss severity due to long-term data corruption and power grid disruptions in companies. As shown in Figure 1, these two affecting variables could be applied to IoT systems research.

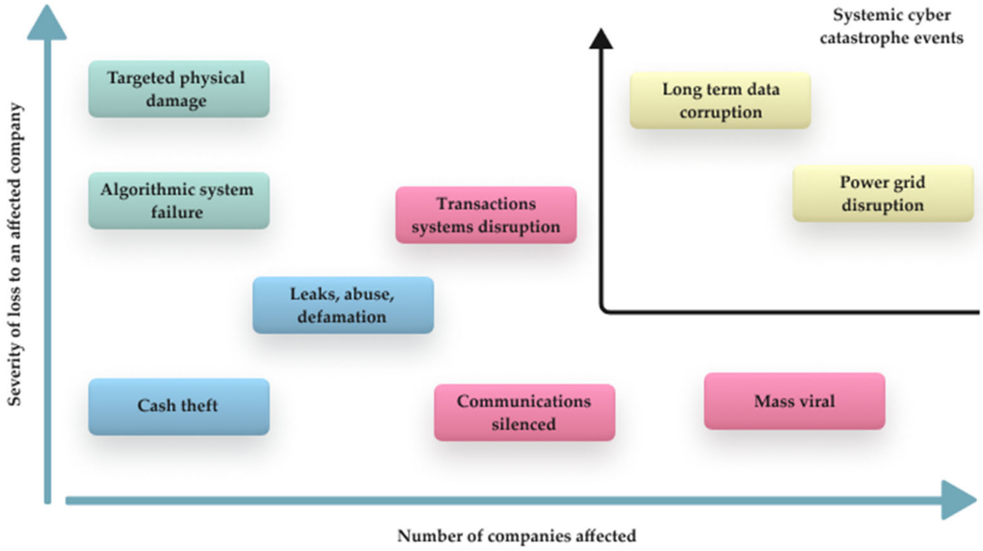

Systemic cyber catastrophe events
Targeted physical damage
Long term data corruption
Algorithmic system failure
Transactions systems disruption
Power grid disruption
Leaks, abuse, defamation
Cash theft
Communications silenced
Mass viral
Severity of loss to an affected company
Number of companies affected

Figure 1. Scale and intensity of cyber-attacks. The higher number of companies affected and the higher loss severity increase the probability of systemic cyber-risk.

Consequently, a security risk analysis is relevant for developing security strategies in IoT systems. According to Radanliev et al. [4], the analysis of the economic impact of IoT risk vector data allows for the generation of clear and rigorous mechanisms. This methodology is accepted by the industry, to measure, control, distribute and manage the critical data necessary to develop, implement and operate a cybersecurity system. This system must be cost-effective for enterprise infrastructure.

The risk assessment of IoT systems poses challenges not found in traditional information systems. There is a lack of rigorous dynamic risk evaluation versus periodic assessment techniques, due to the continuous disruptions of the IoT. Another consideration is the scale variability in IoT devices and systems; new appliances and "things" are rapidly added. This variability raises the dynamism and the temporality of device connections. Finally, Nurse et al. [5] mention the increasing stakeholder's heterogeneity capability of interacting within IoT ecosystems. Similarly, Kandasamy [6] establishes that existing risk frameworks will not address the new risks in the IoT ecosystem.

Therefore, there is a need to manage a dynamic risk assessment methodology that includes the variables of IoT systems. This procedure must identify limited or lack of data due to the continuous changes in new cyber-attacks or newly added IoT devices as well as the uncertainty factors due to the IoT system's complexity and dynamism. This constitutes the main research gap approach. In this study, we will use Bayesian networks to develop a dynamic risk assessment. The reason for this selection is based on the following considerations:

- Bayesian networks allow for real-time tracking of how event probabilities change as new evidence is introduced into the model;
- Bayesian networks define how the different network nodes are linked. Additionally, they study how the probabilities change after introducing some evidence into specific nodes;
- Bayesian networks could make predictions under scenarios of limited and uncertain data.

Bayesian networks have been used in several fields to determine risk assessment. For example, Deleuze et al. [7] propose a Bayesian belief network (BBN) for risk management in the power industry; the research mentions the capability of BBN to be applied in an uncertain environment. Szpyrka et al. [5] use a Bayesian network to evaluate the attacks in the telecommunication network. Hunte et al. [6] submit a risk assessment that resolves the identified limitations with RAPEX, for which there is no testing data, and the number of product conditions is unknown. Li et al. [7] suggest an improved risk assessment model based on a weighted BN, to develop a valuation of sea ice disaster risk.

Although Bayesian networks have been widely applied in the cybersecurity field [8–10] their use in the IoT domain is recent. It is a developing area because the IoT is a relatively new technology. In addition, the IoT has specific characteristics, such as components heterogeneity and limited capacity of hardware resources to establish security mechanisms and dynamic scenarios due to the introduction of new devices and functions.

Consequently, the Bayesian network can be an alternative for the evaluation of IoT security conditions. This study aims to propose a Bayesian network model to measure the risk in IoT scenarios. The following sections have been defined in this manuscript. Section 2 presents a systematic literature review (SLR) of related articles using Bayesian networks in cybersecurity. Section 3 discusses the methodology for designing a Bayesian network. Section 4 presents an application of the Bayesian network in IoT security risk assessment. Finally, Section 5 discusses the results obtained and concludes our research.

2. Literature Review

Nowadays, decision-making processes are supported by several models involving data processing and analysis [11,12]. Some of the most relevant are classified and mentioned in Table 1. These models can be used to design decision support systems (DSSs) to provide future scenarios for the decision-making process. Most of these models need data to predict future behaviors [13]. However, the IoT has certain particularities due to limited data. It requires methodology research that addresses complex and dynamic systems. Additionally, there is a continuous change in components and relationships [14]. This context of uncertainty on behaviors or patterns can be even more challenging in IoT systems security analysis. Therefore, under limited data and uncertainty conditions, probabilistic graphical models can be a good alternative.

Table 1. Classification of models for data analysis used in decision-making processes.

Regression	Classification	Neuronal Networks	Probabilistic Graphical Models
Decision tree regression (CART)	Logistic regression	Autoencoders	Bayesian belief net work
Random forest regression	Adaptive boosting (AdaBoost)	Conventional neural networks	Hidden Markov model
K-nearest neighbors regression (KNN)	Naïve Bayes	Recurrent neural net works	
Multivariate adaptive regression splines (MARS)	Support vector machine (SVM)		
Support vector regression (SVR)			

A probabilistic graphical model (PGM) or a graphical model results from the combination of the graph theory and the probability theory. Graphical models (GMs) are relevant because they allow the representation of complex systems such as social networks, proteins interaction and computer systems. Thus, the GM is a method to represent, interpret and learn from complex problems [15]. The GM comprises nodes and edges; the graph nodes represent random variables, and the edges represent the connection between nodes. The absence of edges between nodes indicates conditional independence.

Two Probabilistic Graphical Models are the hidden Markov model (HMM) and the Bayesian network. The hidden Markov model (HMM) is a graphical model where the edges of the graph are undirected, which implies that the graph could contain cycles or loops [16]. Alternatively, the Bayesian network is more restrictive; the edges of the graph are directed, so they permit one direction between edges [17].

2.1. Systematic Literature Review—Bayesian Networks Applied to Cybersecurity

In this research, we focus on Bayesian networks to understand and explain security attacks in IoT systems. Bayesian networks are applied in different fields, and cybersecurity is one of them. Kumar et al. [18] present a novel approach to predicting the reliability of safety-critical systems using the Bayesian belief network (BNN) model. Their study takes into consideration the quality attributes of the development life cycle software (SDLC) model. In Asvija et al. [19], the authors propose a Bayesian attack graph (BAG) to support administrators in identifying secure high-risk components in an IaaS stack by defining sensitive regions.

The work developed by Guan et al. [20] determines a decision model for network defenders of honeypot systems. It models the interaction between malicious users and defenders, by depicting the uncertain behaviors of the malicious users by the Bayesian model. In terms of IoT security, the research of Kalnoor et al. [21] advises a novel approach using a dynamic Bayesian algorithm that helps to obtain an HMM with a great number of parameters. The model is optimized by predicting a DDoS attack. Similarly, Toğaçar et al. [22] suggest a meta-heuristic optimization to reduce the time in Bayesian neural networks in detecting DDoS attacks.

This research develops a systematic literature review of Bayesian networks in cybersecurity by using PRISMA methodology. PRISMA methodology is based on four stages:

(i) Identification, which is related to evaluating previous studies from scientific databases and searching the use of Bayesian networks for IoT security. The previous studies were explored according to the following keywords: (a) “Security and (Bayes Network or Bayesian Network)”, (b) “Security attacks and (Bayes Network or Bayesian Network)” and (c) “Cybersecurity attacks and (Bayes Network or Bayesian Network)”. The used scientific databases were IEEE Xplorer, Scopus, ACM and Springer. The method search was performed to find previous studies accomplished in the last six years (2016–2022).

(ii) Blind screening review process, which implies that the authors of this research developed this procedure to evaluate previous studies. The procedure was achieved by using the Rayyan method.
(iii) Eligibility, as a full review of the documents was developed to identify relevant contributions to this study.
(iv) Inclusion, as a quality analysis of selected documents from the eligibility stage was established. In Figure 2, an overview of the PRISMA methodology used for this systematic literature review is shown. Table 2 shows the distribution of previous studies, related to the Bayesian network methods in cybersecurity, found in journals, books, conferences and documents.

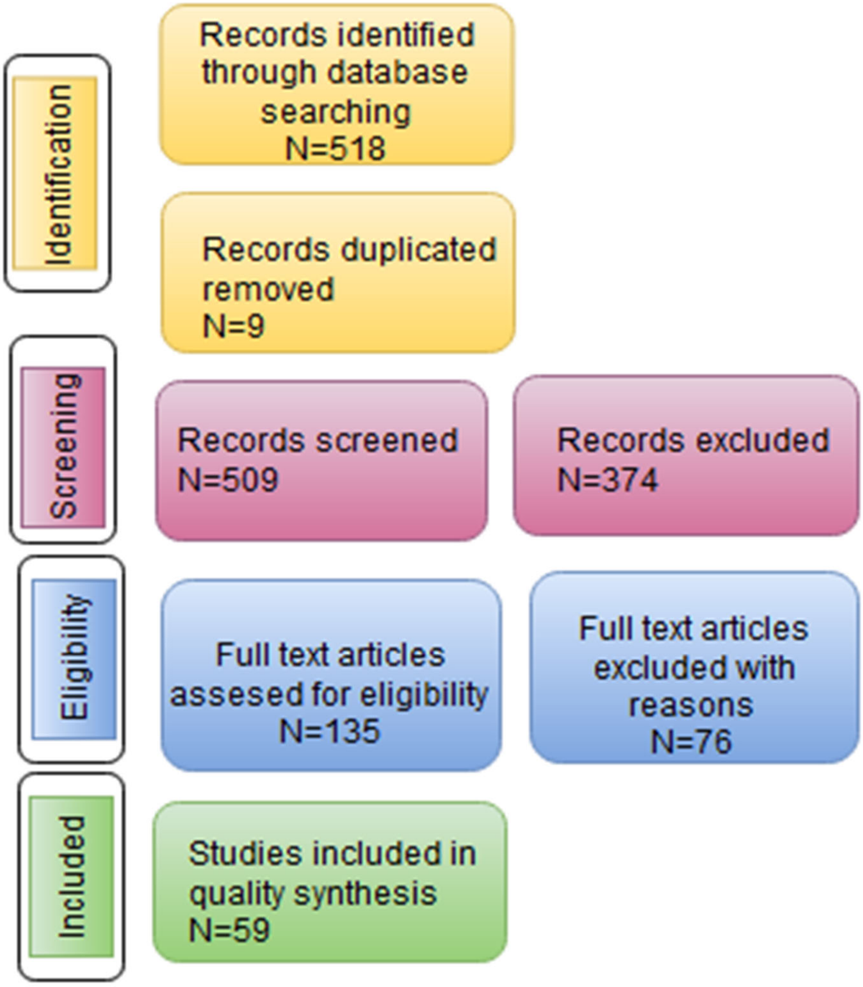

Identification
Records identified through database searching N=518
Records duplicated removed N=9
Screening
Records screened N=509
Records excluded N=374
Eligibility
Full text articles assesed for eligibility N=135
Full text articles excluded with reasons N=76
Included
Studies included in quality synthesis N=59

Figure 2. Systematic literature review of the use of Bayesian networks in cybersecurity.

Table 3 shows a summary of the main Bayesian network methods for areas related to cybersecurity. There are five application areas: Attack detection, risk management, IoT, awareness and defense mechanisms. According to this systematic literature review, attack detection reveals more contributions, followed by IoT and risk management. Regarding risk management, the found research covers different subjects of cybersecurity, such as industrial processes, information security, network security and cyber–physical systems. Connected to the scope of this study, IoT research is focused on: detecting attacks, situational awareness and classification of attacks and vulnerabilities. Nevertheless, few proposals were linked to Bayesian network methods for risk management in IoT systems.

Table 2. Topics related to Bayesian networks in cybersecurity.

Type of Manuscripts	Number of Works	Topics Related to Bayesian Networks
Journal	348	1. Markov–Bayes model [23]. 2. Combined naive Bayes [24]. 3. Bayesian learning [25,26]. 4. Bayes-net classifiers [27]. 5. Naïve Bayes filter [28]. 6. Bayesian inference [29,30]. 7. Dynamic Bayesian networks [31,32]. 8. Bayesian Stackelberg game [33]. 9. Bayesian Dempster–Shafer [34]. 10. Nonparametric Bayesian approach [35]. 11. Bayesian-graph theory [36].
Conference	210	
Book	3	
Chapters	92	

Table 3. Application areas of Bayesian networks in cybersecurity.

Application Areas	Number of Papers	Focus On
IoT	47	Detecting attacks [37]. Situational awareness [38]. Classification of attacks [39]. Classification of vulnerabilities [40].
Risk management/assessment	34	Industrial process [41]. Information security [42]. Network systems [43]. Cyber–physical systems [22]. Autonomous vehicles [24]. Attack graphs [44]. Cybersecurity protection [45].
Awareness	5	IoT security situational awareness [38]. Information attack in vehicular ad hoc network [24].
Defense mechanism	4	Advanced persistent threats [46]. Game theoretical approach [47].
Detection of attacks	158	Insider threat detection [48]. Resource-aware detection [49]. Detection in a cloud environment [50]. Abnormal event correlation [51]. Multiple attacks detection [52].

2.2. Risk Assessment Using Bayesian Networks

In recent years, the digital transformation has boosted different industries, such as health, energy, transportation and agriculture, to improve their processes' efficiency. Several technologies such as cloud, Big Data, IoT and machine learning have fostered this change. However, these technologies have also brought new cybersecurity challenges. The World Economic Forum (WEF) has ranked security attacks among the 10 top threats that could collapse the global economy. Subsequently, security solutions must be developed, for example, intrusion–detection systems, and new-generation firewalls, among others.

Accordingly, before establishing security controls, a good practice is to develop a risk assessment to identify weaknesses in the organization's systems. Thereafter, the procedure should be to define the best security control for improving the effectiveness of security protection. However, the development of an IoT risk analysis has some particularities that must be considered. For instance, Peng et al. [53] and Radanliev et al. [54] mention that the traditional risk analysis methodologies used in information systems do not adjust well to IoT characteristics, due to the components' heterogeneity, limited data to evaluate historical attacks, limited capability to embed security mechanisms and continuous change in the system's dynamics. This is due to the introduction of new devices and interconnections between IoT systems, OTs (operational technologies) and ITs (information technologies) systems.

Several proposals to evaluate the risk in IoT scenarios have been developed in this context. To be specific, Bahizad [55] proposes a risk ranking method to quantify IoT risk. This ranking method initiates a risk assessment approach exclusively for IoT systems by quantifying IoT risk vectors. Similarly, Kandasamy [6] proposes quantitatively evaluating countermeasures for risk factors. Meanwhile, Wangyal et al. [56] offer an approach for risk management based on evaluating IoT devices' strengths. These proposals are built on establishing variable relationships to calculate security risk. These factors are weighted based on data or judgment experts. Nevertheless, these proposals consider deterministic scenarios. This means that it is possible to have data for the risk assessment process, but this scenario is not always possible in IoT studies.

As Yang et al. and Peng et al. [53,54] mentioned, IoT systems are scenarios with limited data and uncertainty. For this reason, the use of a Bayesian network could be an alternative. The Bayesian network method for risk assessment processes is not new, and some research proposals have been addressed. For example, George et al. [41] determine a Bayesian model to evaluate information security and foster the attack route prediction method.

The evaluation method defines the overall system security and vulnerability severity degree. In Wang et al. [43], a simple security model based on defense graphs is proposed to quantitatively assess the likelihood of threats on autonomous vehicle components at available countermeasures. Moreover, Behfarnia and Eslami [44] consider a sensitivity analysis of Bayesian attack graphs to identify critical nodes for network protection. In this way, it solved the uncertainty problem in node assignment.

A Bayesian network assesses the future factors' (nodes) values in the absence of data or uncertainty. By establishing a set of premises, it is possible to define different scenarios where the best or worst conditions can be evaluated in relation to the studied risk. By determining the relevance of the considered factors in the risk assessment process, it is possible to improve their effectiveness. Therefore, using Bayesian networks in IoT systems could overcome data limitations and uncertainty.

3. Risk Methodologies in Complex and Dynamic Environments

IoT systems have intrinsic characteristics that must be considered in the applied model. They should be improved during the operation process to gain effectiveness. The IoT has been developed using different technologies such as Wi-Fi, ZigBee, Lora, NB-IoT and several other protocols such as TCP, UDP, MQTT and REST. These components result in a heterogeneity of IoT systems. Furthermore, these also add a higher interdependency mixed with other systems such as ITs (information technologies) and OTs (operational technologies).

Another particularity is the system dynamics due to its rapid capability to introduce new devices to the market. This condition results in IoT attack data that is not up to date or has limited information. In addition, these characteristics bring new challenges to cybersecurity operations, especially in attack detection and risk assessment. For this research scope, the focus will be on covering the gap related to the assessment of IoT systems. The use of Bayesian networks could be the considered approach to mitigate limited data and uncertainty.

A Bayesian network (BN), also called Bayesian belief network or Bayes nets, is a probabilistic graphical model for representing data about an uncertain scenario. Within this approach, each node corresponds to random variables, and each edge represents the conditional probability for the corresponding random variables [57]. A BN is linked to a directed dynamic acyclic graph (DAG); this means that no loop or self-connection is allowed in the model. According to Asvija et al. [19], the DAG model uses a priori causal assumptions and informs variable selection strategies for causal questions. The Bayesian network models can be inferred from experts' judgments or by data learning. Then, the

BN could use evidence to estimate probabilities for causal or subsequent events; the model is built from questions to conditional probabilities [17]. However, there are possible uses of assumptions, such as the conditional independence of all random variables. A feasible alternative approach could provide an intermediate approach between a fully conditional model and a fully conditionally independent model, to develop a probabilistic model with selected conditional independence assumptions. According to Kononenko et al. [58], the Bayesian classifier could be employed even though the conditional independence assumption is not entirely met. In this way, the probability estimation error does not change its classification order.

Therefore, the Bayesian network can achieve accurate predictions despite incomplete or lacking evidence. The BN provides a method to define a probabilistic model for complex problems by stating conditional independence assumptions for known variables while allowing the presence of unknown (latent) variables. Once a Bayesian network has been prepared, it can be used for reasoning. This reasoning is attained via inference by introducing evidence that sets variables in known states. Thereafter, it calculates the probability of event causes or possible outcomes. The following are some gains of the BN method:

- Model complex systems;
- Manage unknown (latent) variables;
- Manage data lack;
- Use probability distributions;
- Use judgment experts;
- Direct conception of model structure.

The methodology to build a Bayesian network is proposed by Scanagatta et al. [59] following four steps:

1. Identification and selection of nodes (factors). In scenarios where there is a lack of data for node modeling, the suggestion is to employ previous study cases or expert judgments.
2. Define the model structure; this includes the relations (links) between nodes [60]. Define the causal relationship between nodes by a set of directed edges. The direction is from the origin nodes to the destination nodes.
3. Determine the conditional probabilities of all nodes. Define prior elicitation from experts and/or from selected data.
4. Validation of the model structure. Assess the feasibility and accuracy of the model by expert judgment.

Based on Devore et al.'s and Mikkola et al.'s [61,62] proposal, the Bayesian network is performed to evaluate the risk security level of an IoT solution focusing on IoT device factors. The information about the contributing nodes (factors) of IoT devices is obtained from the literature review and expert judgment. A flowchart of the Bayesian network methodology for this research is shown in Figure 3. The Bayesian model uses Python (Google collaboration tool). PyBNN sets up the environment, as this software allows Python on the Bayesian network. PyBNN is used for Bayesian network beliefs, Pandas for data manipulation and NetworkX and Matplotlib for graph plotting.

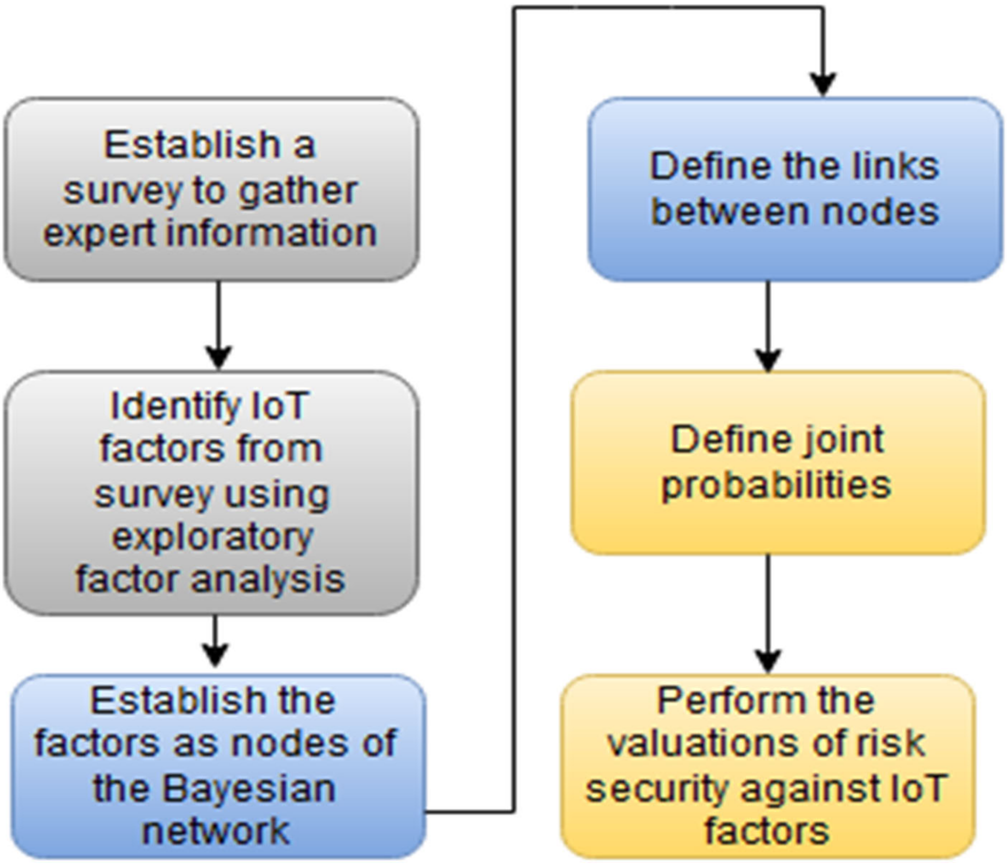

Establish a survey to gather expert information
Identify IoT factors from survey using exploratory factor analysis
Establish the factors as nodes of the Bayesian network
Define the links between nodes
Define joint probabilities
Perform the valuations of risk security against IoT factors

Figure 3. Methodology to build Bayesian networks for IoT risk security assessment.

4. Bayesian Network Structure

4.1. Key Factors of IoT Devices to Evaluate Risk Security

This section aims to build a Bayesian network to predict the impact of an IoT attack that affects the economic, social and environmental organization context. This BN is based on selected observations of security factors affected by IoT devices. In order to accomplish this research goal, an expert judgment process took place. This expert panel included 13 security experts (three from the academic sector, three from the industrial sector, five related to security standardization and legal institutions, and two from security solution vendors). The expert panel considered IoT device factors, which are directly related to risk security. To obtain information, the expert panel performed a survey using an exploratory factor analysis (EFA). The results are exhibited in Table 4.

4.2. Bayesian Network Model

The proposed Bayesian network is shown in Figure 4. It is based on the IoT device factor that could be affected by security attacks. The Bayesian network represents the following factors as nodes: severity, scalability, uncertainty and attack type. Severity is associated with the operation's consequence level of the application domain. The goal of developing the Bayesian network is to calculate its value. Scalability is related to the capability of security attacks that increase the infection area. Uncertainty is related to the unknown behaviors of IoT systems. These attacks could expand the level of damage. Finally, the type of attack is an external factor to IoT devices. Its behavior can be controlled by IoT systems. The attackers could decide to use one or several types of attack simultaneously. In another scenario, they could decide to stop the attack.

Accordingly, the proposed Bayesian network considers two variables: (i) To only study the IoT device factors that could be affected by security attacks. In this way, the research has control and can reduce the consequence level. (ii) To review how the IoT device factors could impact the domain factors which include economic, social and environmental components. For future research, the proposed Bayesian network will evaluate the severity level against the scalability, uncertainty and types of attacks.

The application domain considers the relationship between IoT solutions and environmental, social and economic characteristics. The pillars are related to finance, social and governance infrastructures that support the organization's operation. Furthermore, the IoT solutions domain includes health, agriculture, transportation and traffic, among others.

Table 4. Key factors related to IoT security and their main components from EFA.

Factors	Description
Vulnerabilities	The IoT device may have vulnerabilities in its layers (three on the ITU model). Therefore, the vulnerability value of an IoT model represents the overall value of all contributions in each layer.
Type of attack	Different types of attacks can compromise the confidentiality, availability and integrity of IoT devices.
Attack surface	The attack surface will be conditioned by the inherent organization characteristics in which the IoT solution has been implemented. The attack surface includes entry/exit points, transmission channels, protocols and data used in the IoT model layers (three layers in the ITU case). The number of used IoT devices can also increase the attack surface due to the growing number of entry/exit points, channels, protocols and data.
Interdependency	The IoT device interacts with different layers' protocols and technologies employed on the IoT system. The IoT device serves to build solutions that have a social, economic and environmental impact on the organization's domain or pillar. Interdependency is driven with other IT/OT systems or IoT systems to implement the required functionalities. This interdependency between domains and systems increases the attack's surface.
Severity	The severity will depend on the confidentiality, availability and integrity impact of the operations and information handled by the IoT device. The severity and security components impact (CIA) will depend on the target and type of attack. For example, an MITM attack will be focused on confidentiality, while a DoS attack will be focused on availability. The IoT device security protection–CIA will depend on the security requirements arising from the inherent characteristics of the domain or pillar. The vulnerability's presence can increase the likelihood of a significant impact on security components during an attack.
Application domain	The attack on IoT devices could affect economic, social and environmental operations. The domain or pillar requires certain security configurations, and it may have inherent vulnerabilities. The characteristics of the domain or location may increase the attacked IoT device's susceptibility.
Scalability	The behavior of the security attack may be conditioned by the IoT device's dependency on other IT/OT systems. The attack could come from IT/OT to the IoT, or vice versa. This could increase the attack's scalability. A higher number of devices could also increase attack scalability. Previous episodes could generate higher-impact attacks.
Susceptibility	The attack susceptibility is linked to the IoT device's susceptibility. The IoT device may have components in different layers (according to the ITU model: three layers), which could increase the attack susceptibility due to extra entry and exit points. The systems' interdependence could also affect the susceptibility. Exposure to a higher number of attacks and a shorter time between them can negatively affect equipment susceptibility.
Uncertainty	The security attack's effect on IoT systems can have a random behavior depending on different variables, such as attack transmission through IoT devices. There is a non-deterministic behavior to the attack because it is not possible to precisely establish the security condition of the IoT device or IT/OT system at the time of the attack.

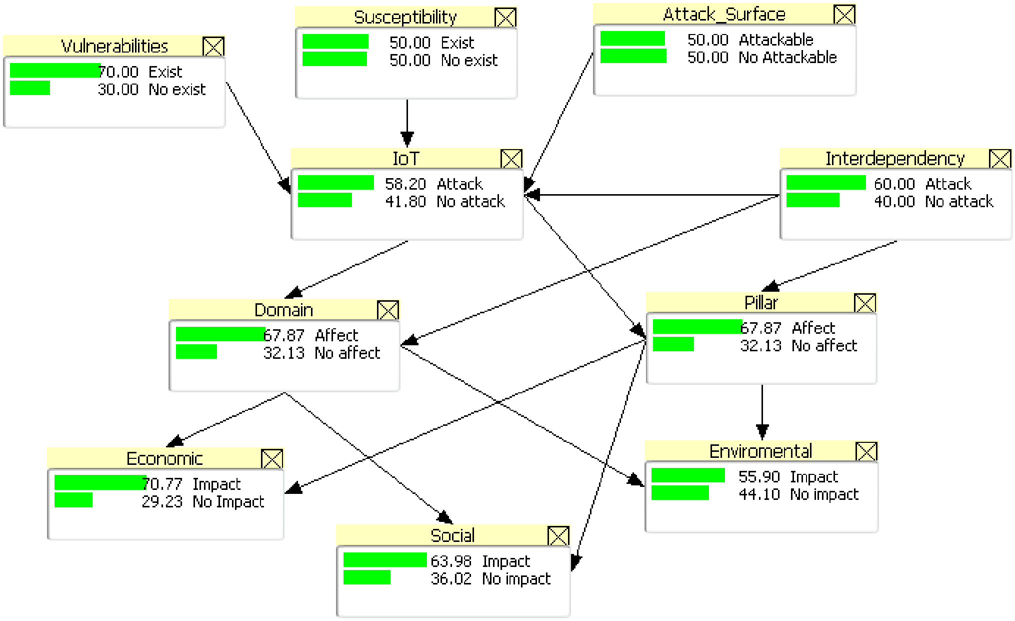


Figure 4. Economic, social and environmental nodes in Bayesian network model.

4.3. Probability Distribution of Bayesian Network Nodes

Designing a probabilistic graphical model could have a limited data problem. Consequently, approaching a fully conditional model requires an enormous amount of data to cover all cases, and the probability calculation may be unreasonably difficult [61]. Bayesian networks provide a model that works as an intermediate scenario between a fully conditionally independent model and a wholly conditional model. Bayesian networks could be designed using selected probability distributions or experts' panel knowledge. According to Mikkola et al. [62], the goal is reached using experts' experience on prior probability distributions.

Probability distributions can be estimated from data, although they can be challenging. It is common to use learning algorithms for this purpose. For example, assuming a Gaussian distribution for continuous random variables gradient ascent to estimate the distribution parameters [63]. The probability distributions given by security experts are shown in Tables 5 and 6.

Table 5. Node status of IoT devices based on cybersecurity.

Nodes	Nodes Status
Vulnerabilities	(1) exist; (2) no exist
Attack surface	(1) attackable; (2) no attackable
Interdependency	(1) exist; (2) no exist
Application domain	(1) impact; (2) no impact
Susceptibility	(1) exist; (2) no exist

Table 6. Node status of the application domain of IoT systems based on cybersecurity.

Nodes of Application Domain	Nodes Status
Domain	(1) impact; (2) no impact
Pillar	(1) impact; (2) no impact
Economic	(1) impact; (2) no impact
Environmental	(1) impact; (2) no impact
Social	(1) impact; (2) no impact

Regarding susceptibility, the attack surface and interdependence nodes may have two statuses, namely attack or not attack. While for the IoT nodes, they are related to four parent nodes, namely vulnerability, susceptibility, attack surface and interdependence. For example, P(I = T | V = T, N = T, S = T, Sy = T) represents the probability of the IoT device being attacked (TRUE = T). Depending on the probability of the attack, it could affect the vulnerability, the attack surface and the interdependence of the IoT device.

P(I = F | V = T, N = T, S = T, Sy = T) represents the probability that the IoT node is not attacked despite the existence of vulnerabilities, attack surface and interdependency. There could also be scenarios such as P(I = T | V = T, N = F, S = F, Sy = T), in which an IoT node can be attacked if there is a vulnerability and an interdependency of the IoT system. However, the attack surface has a low probability of being affected by the attack.

On the other hand, at pillar nodes or domains, IoT solutions could be impacted by an attack. For example, if the IoT solution is used in the medical field, it could affect the device in charge of the patient's vital signs, degrading the e-health solution's operability. Another example is a severe attack directed at the IoT devices that support smart traffic lights design. It could generate overcrowding problems that could affect the regular transportation domain operation.

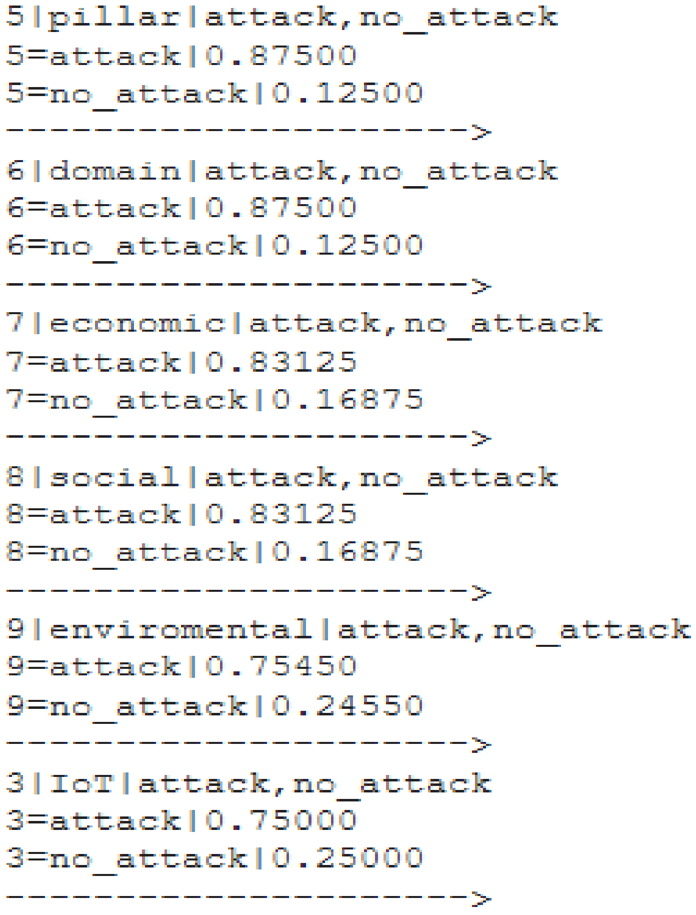
The operational processes in both the technological perspective domain and pillar are built on IT, OT and IoT systems. For pillar nodes, the eight probabilities could show four values corresponding to the likelihood of being attacked on the IoT node and the interdependence node related to IT/OT systems. For example, P(D = T | I = T, Sy = T) represents the probability that the domain is affected by the attack. This means that there is an attack from the IoT device and/or the interconnected IT/OT systems.

Finally, the economic, social and environmental nodes were defined. These nodes have two parent nodes corresponding to the domain nodes and pillar nodes. Therefore, there are eight joint probability values. For example, P(Ec = T | P = T, D = F) and P(Ec = F | P = T, D = F) represent the probability of having an influence in the economic domain due to the existence of a system attack effect. This impact is part of the pillar node, although there is no domain consequence.

5. Results: Risk Security Using Scenario Cases and Bayesian Networks

Bayesian networks allow us to observe node behavior based on evidence. This could affect prior values. For susceptibility, attack surface and interdependence, there are no significant probability modifications if attack evidence is added to the interdependence variable. This effect is shown in Figure 5.

The simulation of the Bayesian network, which evaluates the risk analysis, has been carried out on the free Google collaborate platform. It provides a 1 × 2.2 GHz processor with 1 core. The Bayesian network was tested with a set of nine nodes. In order to represent the risk factors of the IoT devices, four nodes were defined (vulnerability, susceptibility, attack surface and interdependency). Additionally, five nodes were determined to describe the organizational characteristics of the smart solution (domain, pillar, economic, social and environmental). The simulations are based on the number of nodes variation of the risk factors, which correspond to the devices that can be presented simultaneously. The computational time on the Google collaborative platform does not vary significantly between the different numbers of nodes. As a result, the values are presented in Table 7.



```
5|pillar|attack,no_attack
5=attack|0.87500
5=no_attack|0.12500
---------------------->
6|domain|attack,no_attack
6=attack|0.87500
6=no_attack|0.12500
---------------------->
7|economic|attack,no_attack
7=attack|0.83125
7=no_attack|0.16875
---------------------->
8|social|attack,no_attack
8=attack|0.83125
8=no_attack|0.16875
---------------------->
9|enviromental|attack,no_attack
9=attack|0.75450
9=no_attack|0.24550
---------------------->
3|IoT|attack,no_attack
3=attack|0.75000
3=no_attack|0.25000
---------------------->
```

Figure 5. Attack probabilities near 80% on economic and social variables due to interdependence influence.

Table 7. Computational time analysis of the Bayesian network.

Number Nodes	Computational Time (Seconds)
1	12 s
2	12 s
3	12.5 s
4	15 s

The attack probability on the social and economic levels rises to 83% and 75.4% on the environmental level. The probability of an IoT attack increases from 61.2% to 75%. It is relevant that an attack on OT/IT systems has a direct impact on pillars and domain systems.

The severity of security attacks depends on certain node conditions (IoT device factors). The methodology to evaluate the risk security of the IoT system is shown in Figure 6. The scenario is defined according to possible values associated with IoT security factors. The best/worst-case scenario is evaluated, and a risk value is estimated. To examine the conditions when the risk level could be relevant, specific scenarios/cases were developed. These cases are described in Table 8. For example, the vs. case represents a condition in which one or more vulnerabilities are present in a physical IoT device layer. Additionally, this IoT device is in an outdoor location which makes it more susceptible to physical attacks.

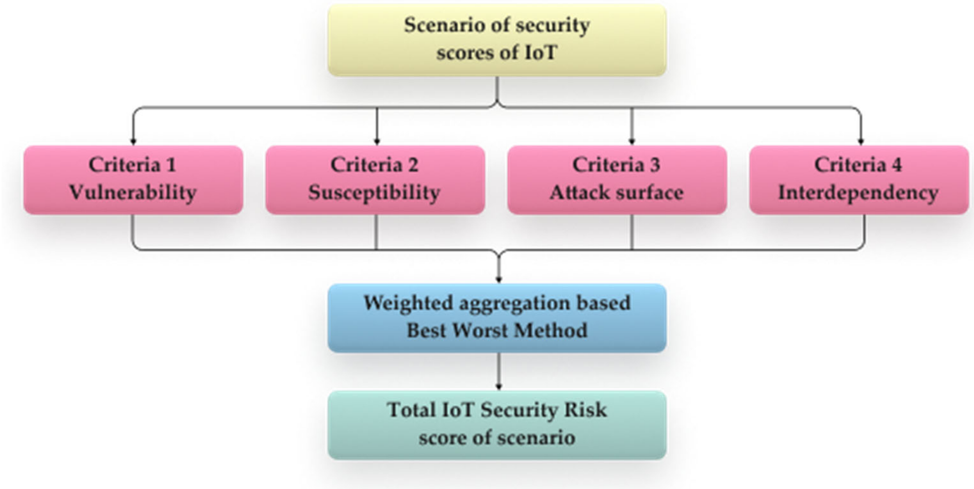

Scenario of security scores of IoT
Criteria 1 Vulnerability
Criteria 2 Susceptibility
Criteria 3 Attack surface
Criteria 4 Interdependency
Weighted aggregation based Best Worst Method
Total IoT Security Risk score of scenario

Figure 6. Methodology to evaluate IoT risk security score based on scenarios.

Table 8. Risk security according to the node status of an IoT device.

Case	Nodes	Description
VS	vulnerability; susceptibility	vulnerability = exist; susceptibility = exist
VI	vulnerability; interdependency	vulnerability = exist; interdependency = exist
VIAs	vulnerability; interdependency; attack surface	vulnerability = exist; interdependency = exist; attack surface = hackable
VSAsI	vulnerability; susceptibility; attack surface; interdependency	vulnerability = exist; susceptibility = exist; attack surface = hackable; interdependency = exist
VSI	vulnerability; susceptibility; interdependency	vulnerability = exist; susceptibility = exist; interdependency = exist

Table 9 shows that the impact probability increases when vulnerability or susceptibility is present. Additionally, the risk increases if the attack surface is attackable or if interdependency is present. The simultaneous combination of two IoT device factors generates a higher effect on the impact probability on economic, social, and environmental domains. In the case of security attacks, it can be observed that the interdependency node has a major impact on environmental, economic, and social domains.

Three factors directly influence the risk security impact in an IoT device: vulnerability, susceptibility and attack surface. Moreover, there could be a higher probability that an attacker could affect the vulnerability of IoT devices. In this simulation case, a value of 65% was set to indicate an attack impact. Additionally, the susceptibility can be represented as the exposure level of an IoT device. Hence, this research considers the probability that an IoT device could be susceptible to one or several attacks.

Therefore, this studied probability may vary depending on the experts' analysis. In addition, the attack surface variable is related to the layer entry/exit points, data, communication protocols and media used by IoT devices. The attack surface also directly correlates to the number of existing IoT devices. An increase in the number of IoT devices expands the attack surface because they could generate more entry and exit points. This condition offers an alternative attack path to the IoT device.

Table 9. Attack and impact probability using IoT security Bayesian model.

IoT Factors (Input Variables)				Impact (Output Variables)		
Vulnerability	**Susceptibility**	**Attack Surface**	**Interdependency**	**Economic**	**Social**	**Environmental**
70%	50%	60%	60%	70.77%	63.98%	55.90%
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%

The next variable that influences the IoT device is the interdependence generated by its interconnection with other IT and OT systems. The interdependency is not an intrinsic or direct factor of IoT devices. These interconnections are developed to generate digital transformation processes in organizations. For example, energy structure includes SCADA systems that, combined with IoT devices, allow for a physical element monitoring of the system. The parameters that can be measured include temperature, energy consumption and energy supply, among others.

Furthermore, there could be a probability that an attack occurs due to interdependency. By having an interconnection with IT/OT systems, the vulnerabilities of these systems can increase the risk security of the attack surface. This argument is based on the exposure to entry and exit points of the IoT system. A feasible scenario is an attack on an IT/OT system that could escalate to the IoT system. For this research, a 75% value was set to show an impact attack.

Once the values of the different scenarios have been determined, the factor weights were also established to calculate the risk value. Since there were several criteria to determine the risk value, the use of a multicriteria decision analysis (MCDA) was selected. The obtained values offer several alternatives, so the best and worst options related to risk scenarios were analyzed. To take advantage of the information from these alternatives, the Best Worst Method (BWM) proposal was considered [63]. The BWM is a multi-criteria decision-making method that uses two vectors of pairwise comparisons to determine the criteria weights. The process of calculating the weight using the BWM is shown in Figure 7. Ksi represents the threshold of reliability of BWM.

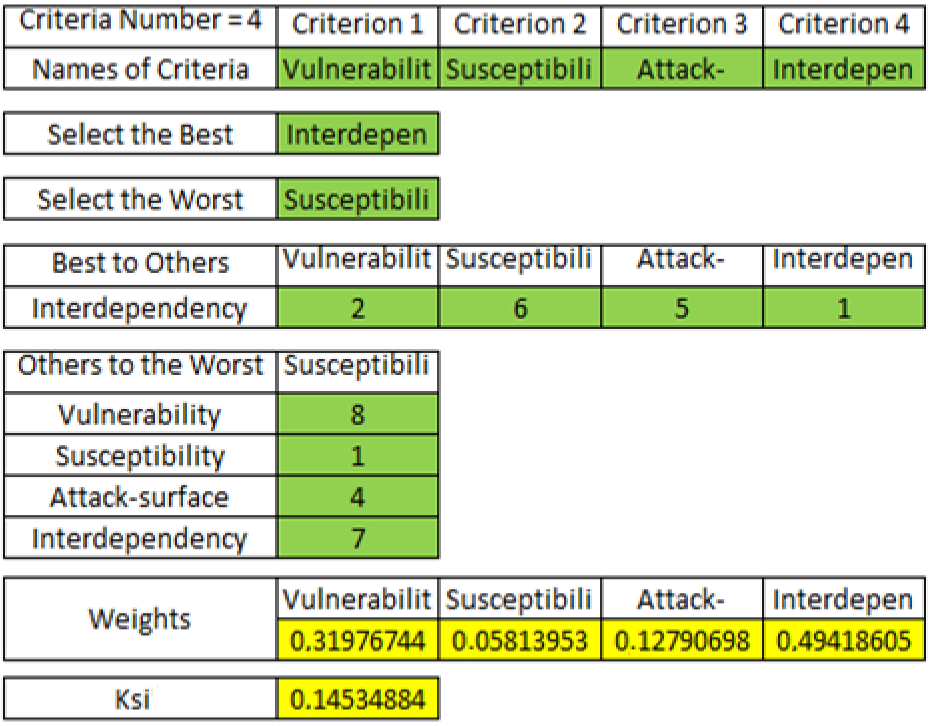
In this study, to obtain risk security values for IoT systems, the following function factors equation is proposed. It considers vulnerability, susceptibility, attack surface and interdependency.

$$Risk = w1 * vulnerability\ value + w2 * susceptibility\ value + w3 * attack\ surface + w4 * interdepedency\ value \qquad (1)$$

where w(i) represents the weight associated with the IoT security factor.

The values of vulnerability, susceptibility, attack surface or interdependency could be estimated using methods such as CVSS, DREAD, STRIDE or employing experts' judgment. For this study, an experts' judgment was used to show the risk security analysis methodology. The considered values were ranked in a scale from 1 to 10, aligned with specialized organizations such as NIST for CVSS values.

Table 10 shows the IoT risk-based analysis using Equation (1). For this evaluation, the following values were determined based on the expert panel: vulnerability 8/10, attack surface 5/10, susceptibility 3/10 and interdependency 6/10. Finally, the result value reaches 6,19/10 for the risk security of the studied IoT system.



Criteria Number = 4	Criterion 1	Criterion 2	Criterion 3	Criterion 4
Names of Criteria	Vulnerabilit	Susceptibili	Attack-	Interdepen

Select the Best	Interdepen

Select the Worst	Susceptibili

Best to Others	Vulnerabilit	Susceptibili	Attack-	Interdepen
Interdependency	2	6	5	1

Others to the Worst	Susceptibili
Vulnerability	8
Susceptibility	1
Attack-surface	4
Interdependency	7

Weights	Vulnerabilit	Susceptibili	Attack-	Interdepen
	0.31976744	0.05813953	0.12790698	0.49418605

Ksi	0.14534884

Figure 7. BWM to determine IoT factor weights for risk security level.

Table 10. Attack and impact probability for IoT security Bayesian model.

Factors	Vulnerability	Attack Surface	Susceptibility	Interdependency	IoT Risk Security
Weights	0.32	0.06	0.13	0.49	6.19
Values	8	5	3	6	

6. Discussion and Conclusions

IoT scenarios offer new organization opportunities for digital transformation processes. Complementarily, they also foster the entrance of new risk security factors due to the complexity and dynamism of these systems. Consequently, this drives the need to seek innovative alternatives for this risk analysis. Additionally, another IoT system consideration due to its dynamism is having incomplete or a lack of history patterns, which could lead to uncertain environmental decisions. In this study, we research the risk security of environmental, economic and social domains due to the security characteristics of IoT devices.

The research determines three main factors that directly influence or impact the risk security in an IoT device: vulnerability, susceptibility and attack surface.

The vulnerability variable is related to the IoT device's layer factors. The IoT device may have vulnerabilities in different layers (three on the ITU model). Moreover, the vulnerability value represents the overall value of all contributions in each layer of the IoT model. In addition, there could be a probability that an attacker could impact this vulnerability. This probability may vary according to the experts' analysis. In our simulation case, we defined a value of 65% for this impact attack.

The susceptibility variable is related to this kind of effect in an IoT device attack. The susceptibility can be represented as the exposure level of an IoT device. Thereafter, we define the probability that the IoT device could be susceptible to one or several attacks. In our simulation case, we determined a 65% value for this risk attack. This probability may also fluctuate according to the experts' analysis.

Subsequently, the attack surface variable is related to the entry/exit points, data, communication protocols and media IoT devices used in the device layers (three on the ITU model). The attack surface is directly correlated to the number of existing IoT devices. An increase in the number of IoT devices expands the attack surface because it generates more entry and exit points. Moreover, it could offer an alternative attack path for the IoT device.

Regarding the characteristics of IoT systems, the Bayesian network (BN) model was selected as the proper solution for this context. It can effectively evaluate the risk security in IoT systems. Explicitly, Bayesian models analyze under uncertainty and data-limited environments. They also provide a link between qualitative values and quantitative results for decision-making.

The BN results show that if we increase the confidence of an IoT attack factor, the probability of impacting the economic, social and environmental values could certainly change. The results demonstrate that the main factor in the proposed model is interdependence with IT and OT systems. This leads to a proposal of an attacker/IoT systems model. Its schema is exhibited in Figure 8.

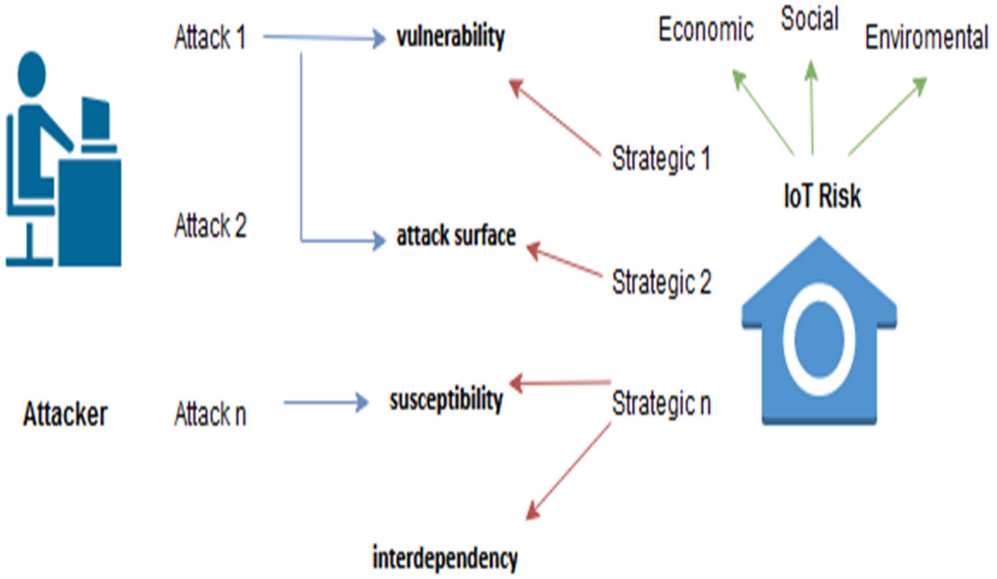


Figure 8. The Best Worst Method (BWM) determines the IoT factor weights to evaluate risk security levels.

The attacker can choose to attack any or all components: vulnerability, attack surface, susceptibility and interdependence. As a result, the economic, social and environmental elements supported by the IoT system will affect the organization's payoff. Considering the proposed IoT system security, alternative strategies could be established to reduce this impact possibility.

Author Contributions: Conceptualization, R.A. and M.C.; methodology, R.A.; validation, I.O.; formal analysis, R.A.; investigation, R.A.; resources, G.N. and M.C.; writing—review and editing, R.A.; visualization and editing, M.I.S.-P.; supervision, I.O.; project administration, I.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. World Economic Forum, Technology, Innovation and Systemic Risk. 2022. Available online: https://www.weforum.org/projects/technology-innovation-and-systemic-risk (accessed on 28 February 2022).
2. Mckinsey. 2022. Available online: https://www.mckinsey.com/alumni/news-and-insights/global-news/firm-news/the-accelerating-value-of-the-internet-of-things (accessed on 28 February 2022).

3. Zikria, Y.B.; Ali, R.; Afzal, M.K.; Kim, S.W. Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions. *Sensors* **2021**, *21*, 1174. [CrossRef] [PubMed]
4. Radanliev, P.; De Roure, D.C.; Nurse, J.R.C.; Montalvo, R.M.; Cannady, S.; Santos, O.; Maddox, L.; Burnap, P.; Maple, C. Future developments in standardization of cyber risk in the Internet of Things (IoT). *SN Appl. Sci.* **2020**, *2*, 169. [CrossRef]
5. Nurse, J.; Creese, S.; Roure, D. Security Risk Assessment in Internet of Things Systems. *IT Prof.* **2017**, *19*, 20–26. [CrossRef]
6. 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. Info. Secur.* **2020**, *2020*, 8. [CrossRef]
7. Deleuze, G.; Bertin, H.; Dutfoy, A.; Pierlot, S.; Pourret, O. Use of Bayesian Belief Networks for risk management in energy distribution. In *Probabilistic Safety Assessment and Management*; Spitzer, C., Schmocker, U., Dang, V.N., Eds.; Springer: London, UK, 2004. [CrossRef]
8. Szpyrka, M.; Jasiul, B.; Wrona, K.; Dziedzic, F. Telecommunications Networks Risk Assessment with Bayesian Networks. In *Computer Information Systems and Industrial Management. CISIM 2013. Lecture Notes in Computer Science*; Saeed, K., Chaki, R., Cortesi, A., Wierzchoń, S., Eds.; Springer: Berlin/Heidelberg, German, 2013; Volume 8104. [CrossRef]
9. Hunte, J.; Neil, M.; Fenton, N. Product risk assessment: A Bayesian network approach. *arXiv* **2020**, arXiv:2010.06698.
10. Li, M.; Hong, M.; Zhang, R. Improved Bayesian Network-Based Risk Model and Its Application in Disaster Risk Assessment. *Int. J. Disaster Risk Sci.* **2018**, *9*, 237–248. [CrossRef]
11. Pius, A.M.; Ogada, K.; Mwalili, T. Supervised Machine Learning Modelling of Demand for Outpatient Health-Care Services in Kenya using Artificial Neural Networks and Regression Decision Trees. In Proceedings of the 2021 22nd International Arab Conference on Information Technology (ACIT), Muscat, Oman, 21–23 December 2021; pp. 1–7. [CrossRef]
12. Dahal, S.; Schaeffer, R.; Abdelfattah, E. Performance of Different Classification Models on National Coral Reef Monitoring Dataset. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021; pp. 0662–0666. [CrossRef]
13. Chela, G.M.; Flores, M.; Gualli, T.G.; Andrade, R. Methodological Proposal for the Construction of a Decision Support System (DSS) Applied to IoT. In *Information and Knowledge in Internet of Things. EAI/Springer Innovations in Communication and Computing*; Guarda, T., Anwar, S., Leon, M., Mota Pinto, F.J., Eds.; Springer: Cham, Switzerland, 2022. [CrossRef]
14. Jantsch, A.; Anzanpour, A.; Kholerdi, H.; Azimi, I.; Siafara, L.C.; Rahmani, A.M.; TaheriNejad, N.; Liljeberg, P.; Dutt, N. Hierarchical dynamic goal management for IoT systems. In Proceedings of the 2018 19th International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 13–14 March 2018; pp. 370–375. [CrossRef]
15. Hongmei, L.; Wenning, H.; Wenyan, G.; Gang, C. Survey of Probabilistic Graphical Models. In Proceedings of the 2013 10th Web Information System and Application Conference, Washington, DC, USA, 10–15 November 2013; pp. 275–280. [CrossRef]
16. Rabiner, L.; Juang, B. An introduction to hidden Markov models. *IEEE ASSP Mag.* **1986**, *3*, 4–16. [CrossRef]
17. Cao, Y. Study of the Bayesian networks. In Proceedings of the 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT), Shenzhen, China, 17–18 April 2010; pp. 172–174. [CrossRef]
18. Kumar, P.; Singh, L.K.; Kumar, C.; Verma, S.; Kumar, S. A Bayesian Belief Network Model for Early Prediction of Reliability for Computer-Based Safety-Critical Systems. In Proceedings of the 2021 2nd International Conference on Range Technology (ICORT), Balasore, India, 5–6 August 2021; pp. 1–6. [CrossRef]
19. Asvija, B.; Eswari, R.; Bijoy, M.B. Security Threat Modelling With Bayesian Networks and Sensitivity Analysis for IAAS Virtualization Stack. *J. Organ. End User Comput. (JOEUC)* **2021**, *33*, 44–69. [CrossRef]
20. Guan, R.; Li, L.; Wang, T.; Qin, Y.; Xiong, W.; Liu, Q. A Bayesian Improved Defense Model for Deceptive Attack in Honeypot-Enabled Networks. In Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 10–12 August 2019; pp. 208–214. [CrossRef]
21. Kalnoor, G.; Gowrishankar, S. A model for intrusion detection system using hidden Markov and variational Bayesian model for IoT based wireless sensor network. *Int. J. Inf. Tecnol.* **2021**, *14*, 2021–2033. [CrossRef]
22. Toğaçar, M. Detecting attacks on IoT devices with probabilistic Bayesian neural networks and hunger games search optimization approaches. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*. [CrossRef]
23. Kalnoor, G.; Gowrishankar, S. A Framework Using Markov-Bayes' Model for Intrusion Detection in Wireless Sensor Network. In *ICDSMLA 2020*; Lecture Notes in Electrical, Engineering; Kumar, A., Senatore, S., Gunjan, V.K., Eds.; Springer: Singapore, 2022; Volume 783. [CrossRef]
24. Wisanwanichthan, T.; Thammawichai, M. A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM. *IEEE Access* **2021**, *9*, 138432–138450. [CrossRef]
25. Liu, Q.; Keller, H.B.; Hagenmeyer, V. A Bayesian Rule Learning Based Intrusion Detection System for the MQTT Communication Protocol. In Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021), Vienna, Austria, 17–20 August 2021; Association for Computing Machinery: New York, NY, USA, 2021; Volume 81, pp. 1–10. [CrossRef]
26. Sahu, A.; Davis, K. Structural Learning Techniques for Bayesian Attack Graphs in Cyber Physical Power Systems. In Proceedings of the 2021 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2–5 February 2021; pp. 1–6. [CrossRef]
27. Klassen, M.; Yang, N. Anomaly based intrusion detection in wireless networks using Bayesian classifier. In Proceedings of the 2012 IEEE Fifth International Conference on Advanced Computational Intelligence (ICACI), Nanjing, China, 18–20 October 2012; pp. 257–264. [CrossRef]

28. Berguig, Y.; Laassiri, I.; Hanaoui, S. DoS Detection Based on Mobile Agent and Naïve Bayes Filter. In Proceedings of the 2018 International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Kenitra, Morocco, 21–23 November 2018; pp. 1–6. [CrossRef]
29. Fu, Y.; He, Z. Bayesian-Inference-Based Sliding Window Trust Model Against Probabilistic SSDF Attack in Cognitive Radio Networks. *IEEE Syst. J.* **2020**, *14*, 1764–1775. [CrossRef]
30. Muñoz-González, L.; Sgandurra, D.; Barrère, M.; Lupu, E.C. Exact Inference Techniques for the Analysis of Bayesian Attack Graphs. *IEEE Trans. Dependable Secur. Comput.* **2019**, *16*, 231–244. [CrossRef]
31. Vaddi, P.K.; Pietrykowski, M.C.; Kar, D.; Diao, X.; Zhao, Y.; Mabry, T.; Ray, I.; Smidts, C. Dynamic bayesian networks based abnormal event classifier for nuclear power plants in case of cyber security threats. *Prog. Nucl. Energy* **2020**, *128*, 103479. [CrossRef]
32. Lin, P.; Chen, Y. Dynamic Network Security Situation Prediction based on Bayesian Attack Graph and Big Data. In Proceedings of the 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 14–16 December 2018; pp. 992–998. [CrossRef]
33. Zhang, Y.; Malacaria, P. Bayesian Stackelberg games for cyber-security decision support. *Decis. Support Syst.* **2021**, *148*, 113599. [CrossRef]
34. Durgadevi, V.; Ganeshkumar, P. Fuzzy integrated Bayesian Dempster-Shafer Theory to defend cross-layer heterogeneity attacks in Communication Network of Smart Grid. *Inf. Sci.* **2018**, *479*, 542–566. [CrossRef]
35. Alhakami, W.; Lharbi, A.A.; Bourouis, S.; Alroobaea, R.; Bouguila, N. Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection. *IEEE Access* **2019**, *7*, 52181–52190. [CrossRef]
36. Pirbhulal, S.; Gkioulos, V.; Katsikas, S. Towards Integration of Security and Safety Measures for Critical Infrastructures Based on Bayesian Networks and Graph Theory: A Systematic Literature Review. *Signals* **2021**, *2*, 771–802. [CrossRef]
37. Forti, N.; Battistelli, G.; Chisci, L.; Sinopoli, B. A Bayesian approach to joint attack detection and resilient state estimation. In Proceedings of the 2016 IEEE 55th Conference on Decision and Control (CDC), Las Vegas, NV, USA, 12–14 December 2016; pp. 1192–1198. [CrossRef]
38. Li, Y.; Liu, T.; Zhu, J.; Wang, X. *IoT Security Situational Awareness Based on Q-Learning and Bayesian Game*; Springer: Singapore, 2021; pp. 190–203. ISBN 978-981-16-5943-0.
39. Yesi, K.; Siti, N.; Deris, S.; Bhakti, Y. Improving Classification Attacks in IOT Intrusion Detection System using Bayesian Hyperparameter Optimization. In Proceedings of the 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 10 December 2020; pp. 146–151. [CrossRef]
40. Wang, J.; Guo, M. Vulnerability categorization using Bayesian networks. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW ′10), Oak Ridge, TN, USA, 21–23 April 2010; Association for Computing Machinery: New York, NY, USA, 2010; Volume 29, pp. 1–4. [CrossRef]
41. Priscilla, G.; Vadakkapaikkadu, R. Evolution of Safety and Security Risk Assessment methodologies to use of Bayesian Networks in Process Industries. *Process Saf. Environ. Prot.* **2021**, *149*, 758–775. [CrossRef]
42. Hui, B.-F.; Ma, Y.-L. Information Security Defense Evaluation Based on Bayesian Network. In Proceedings of the International Conference on Artificial Intelligence for Communications and Networks, Xining, China, 23–24 October 2021; Springer: Cham, Switzerland, 2021; pp. 3–7, ISBN 978-3-030-90199-8.
43. Wang, J.; Fan, K.; Mo, W.; Xu, D. A Method for Information Security Risk Assessment Based on the Dynamic Bayesian Network. In Proceedings of the 2016 International Conference on Networking and Network Applications (NaNA), Hakodate City, Japan, 23–25 July 2016; pp. 279–283. [CrossRef]
44. Behfarnia, A.; Eslami, A. Risk Assessment of Autonomous Vehicles Using Bayesian Defense Graphs. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; pp. 1–5. [CrossRef]
45. Isaac, M.; Sadegh, S.; Aad, M. Stochastic Simulation Techniques for Inference and Sensitivity Analysis of Bayesian Attack Graphs. In Proceedings of the International Conference on Science of Cyber Security, Shanghai, China, 13–15 August 2021; Springer: Cham, Switzerland, 2021.
46. Zhang, Q.; Zhou, C.; Tian, Y.-C.; Xiong, N.; Qin, Y.; Hu, B. A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2497–2506. [CrossRef]
47. Halabi, T.; Wahab, O.A.; Al Mallah, R.; Zulkernine, M. Protecting the Internet of Vehicles Against Advanced Persistent Threats: A Bayesian Stackelberg Game. *IEEE Trans. Reliab.* **2021**, *70*, 970–985. [CrossRef]
48. Thakkar, A.; Badsha, S.; Sengupta, S. Game theoretic approach applied in cybersecurity information exchange framework. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–7. [CrossRef]
49. Wall, A.; Agrafiotis, I. A Bayesian approach to insider threat detection. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2021**, *12*, 48–84.
50. Wahab, O.A.; Bentahar, J.; Otrok, H.; Mourad, A. Resource-Aware Detection and Defense System against Multi-Type Attacks in the Cloud: Repeated Bayesian Stackelberg Game. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 605–622. [CrossRef]
51. Hu, Z.; Yu, X.; Shi, J.; Ye, L. Abnormal Event Correlation and Detection Based on Network Big Data Analysis. *Comput. Mater. Contin.* **2021**, *69*, 695–711. [CrossRef]

52. Yang, C.; Shi, Z.; Zhang, H.; Wu, J.; Shi, X. Multiple Attacks Detection in Cyber-Physical Systems Using Random Finite Set Theory. *IEEE Trans. Cybern.* **2020**, *50*, 4066–4075. [CrossRef] [PubMed]
53. Peng, Q. Bayesian Networks for Data Prediction. In Proceedings of the 2009 International Forum on Computer Science-Technology and Applications, ChongQing, China, 25–27 December 2009; pp. 101–102. [CrossRef]
54. Radanliev, P.; de Roure, D.; Cannady, S.; Montalvo, R.M.; Nicolescu, R.; Huth, M. Economic impact of IoT cyber risk—Analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. In *Living in the Internet of Things: Cybersecurity of the IoT-2018*; Institution of Engineering and Technology: London, UK, 2018; pp. 1–9. [CrossRef]
55. Bahizad, S. Risks of Increase in the IoT Devices. In Proceedings of the 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 1–3 August 2020; pp. 178–181. [CrossRef]
56. Wangyal, S.; Dechen, T.; Tanimoto, S.; Sato, H.; Kanai, A. A Study of Multi-viewpoint Risk Assessment of Internet of Things (IoT). In Proceedings of the 2020 9th International Congress on Advanced Applied Informatics (IIAI-AAI), Kitakyushu, Japan, 1–15 September 2020; pp. 639–644. [CrossRef]
57. Al Mousa, A.; al Qomri, M.; al Hajri, S.; Zagrouba, R.; Chaabani, S. Environment Based IoT Security Risks and Vulnerabilities Management. In Proceedings of the 2020 International Conference on Computing and Information Technology (ICCIT-1441), Tabuk, Saudi Arabia, 9–10 September 2020; pp. 1–6. [CrossRef]
58. Kononenko, I.; Kukar, M. Chapter 3—Machine Learning Basics. In *Machine Learning and Data Mining*; Igor, K., Matjaž, K., Eds.; Woodhead Publishing: Sawston, Cambridge, 2007; pp. 59–105. ISBN 9781904275213. [CrossRef]
59. Scanagatta, M.; Salmerón, A.; Stella, F. A survey on Bayesian network structure learning from data. *Prog. Artif. Intell.* **2019**, *8*, 425–439. [CrossRef]
60. Piccininni, M.; Konigorski, S.; Rohmann, J.L.; Kurth, T. Directed acyclic graphs and causal thinking in clinical risk prediction modeling. *BMC Med. Res. Methodol.* **2020**, *20*, 179. [CrossRef]
61. Devore, J.L.; Berk, K.N.; Carlton, M.A. Joint Probability Distributions and Their Applications. In *Modern Mathematical Statistics with Applications. Springer Texts in Statistics*; Springer: Cham, Switzerland, 2021. [CrossRef]
62. Mikkola, P.; Martin, O.; Chandramouli, S.; Hartmann, M.; Pla, O.; Thomas, O.; Pesonen, H.; Corander, J.; Vehtari, A.; Kaski, S.; et al. Prior knowledge elicitation: The past, present, and future. *arXiv* **2021**, arXiv:2112.01380.
63. Xu, S.; Jia, B.; Liang, F. Learning Moral Graphs in Construction of High-Dimensional Bayesian Networks for Mixed Data. *Neural Comput.* **2019**, *31*, 1183–1214. [CrossRef]