




# A Customizable Security Risk Assessment Framework Using Multi-Attribute Decision Making for IoT Systems

Mofareh Waqdan<sup>1</sup> <sup>a</sup>, Habib Louafi<sup>2</sup> <sup>b</sup> and Malek Mouhoub<sup>1</sup> <sup>c</sup>

<sup>1</sup>Department of Computer Science, University of Regina, Regina, SK, Canada

<sup>2</sup>Department of Science and Technology, TELUQ University, Montreal, Canada

fi

**Keywords:** Internet of Things (IoT), Risk Assessment, Risk Parameters, Multi-Attribute Decision Making (MADM), Simple Additive Weighting (SAW), Weighting Product (WP).

**Abstract:** The advent of the Internet of Things (IoT) has transformed how we conduct our daily lives and engage with technology. The seamless integration of connected devices, from household to industrial equipment, has ushered in a new era of interconnectivity. Nevertheless, this swift expansion of the IoT also presents novel security concerns that must be addressed. We present a customizable framework for assessing the risk of deploying and utilizing IoT devices in various environments. We dynamically calculate risk scores for different devices, considering their importance to the system and their vulnerabilities, among other parameters. The framework we propose improves on existing research by considering the important parameters of the devices, their vulnerabilities and how they impact the overall risk assessment. The importance of these devices and the severity of vulnerabilities are incorporated in the framework using well-known Multi-Attribute Decision Making (MADM) methods, namely, Simple Additive Weighting (SAW) and Weighting Product (WP). The risk is assessed on a setup comprised of a set of IoT devices widely deployed in healthcare systems, such as emergency rooms.

## 1 INTRODUCTION


The “Internet of Things” is a concept that refers to the connection of daily physical objects or devices to the Internet or each other. This allows them to share information and perform specific functions through the network (Kumar et al., 2019). IoT enables sophisticated services to be offered by connecting all objects so that the Internet is used to mediate seamless connectivity and data transfer between them (Ray, 2018).


The IoT ecosystem contains various smart objects located in different constrained environments that communicate with each other or with the Internet and share data using different methods and protocols. In other words, the IoT device can be defined as any device (cyber or physical) having an IP address and connected to a network (Radanliev et al., 2018).


The availability, integrity, and confidentiality of data are significant concerns for manufacturers and consumers of IoT systems. There are four layers in

any IoT architecture: Sensor, network, middleware, and application (Shameli-Sendi et al., 2016a). In the Sensor layer, the sensed information, stored in local or cloud storage, is not encrypted, making it vulnerable to security attacks. In the network layer, the communication between IoT devices is known to be vulnerable to attacks (Opoku et al., 2024; Falola et al., 2023). In the middleware layer, attackers can degrade the firmware version of IoT devices using malicious applications. Then, an attack could be carried out on the degraded and outdated firmware version. In the Application layer, operating systems could have backdoors that lead to security issues.

Cyber risk refers to the probability that an undesirable event occurs and the level of impact it would have. According to the National Institute of Standards and Technology (NIST), we need to consider the probability that a possible threat exploits a vulnerability to assess the risk and the resulting impact of this event on the system or organization. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (ISO/IEC) have defined IT risk as the possibility of a threat exploiting an organization’s asset vulnerabil-

<sup>a</sup>  <https://orcid.org/0000-0003-4916-3911>

<sup>b</sup>  <https://orcid.org/0000-0002-3247-3115>

<sup>c</sup>  <https://orcid.org/0000-0001-7381-1064>

ities and causing damage. Risk assessment considers the likelihood of an event and its impact on the organization.

Cybersecurity risk is the likelihood of compromised sensitive information, critical assets, or reputation due to a cyber attack or breach within an organization's network. Asset, threat, and vulnerability are critical components of information security risk. The Open Web Application Security Project (OWASP) test guide defines risk as a product of likelihood and impact, where likelihood and impact are assigned specific values. Various definitions of risk exist, taking into account threats and vulnerabilities.

Contemporary approaches focus on IoT risk assessment using only Risk and Likelihood impacts. They do not consider the critical parameters of vulnerabilities of IoT devices.

In this paper, we propose a customizable security risk assessment framework, which considers different and diverse risk assessment parameters, providing more insightful risk scoring. Different parameters are involved in the risk assessment, which normally contribute differently to the final score of the assessment. Therefore, different weights must be assigned to these parameters to provide a more precise and personalized risk assessment framework that can be applied in different environments. Our proposed risk assessment framework for IoT environments is developed based on these key factors, which is not only innovative, but also highly practical. Furthermore, our proposed framework can be applied in various IoT scenarios in different sectors, ensuring its wide applicability.

The paper is structured as follows. In section 2, we review the most important security risk assessment solutions and frameworks proposed in the literature. Section 3 presents our customizable security risk assessment framework, the parameters used, and the application of the MADM methods. Section 4 presents the simulation setup and results. Lastly, section 5 concludes the paper.

## 2 RELATED WORK

Kandasamy et al. (Kandasamy et al., 2020) proposed a risk prioritization approach, dividing risks into four distinct categories: Ethical, Privacy, Security, and Technical risks. They also classify Risk Assessment theories into several categories, including, Dempster-Shafer theory, Game-Theoretic computing, Failure Mode Effects Analysis, and Cybersecurity Game (CSG), which study how attackers, defenders, and users make decisions about cybersecu-

rity. Their analysis provides a thorough examination of the various risks associated with IoT across diverse domains, such as finance, healthcare, and others.

Radanliev et al. (Radanliev et al., 2020) discussed a self-adapting and dynamic supply chain system. This system utilizes real-time intelligence, AI, and ML to detect cyber-risks. The authors also conducted a literature review to examine the impact of state-of-the-art supply chain technologies and their connected cyber risks. Additionally, they developed a method to reduce cyber risks in assessing Industrial IoT and Industry 4.0 supply chain integration.

Kumar et al. (Kumar et al., 2020) introduced a model incorporating regression analysis, utilizing predefined and authorized specification limits to maintain cyber risks associated with critical information infrastructure within the organization's predetermined boundaries. Additionally, their algorithm forecasted the capability of the risk assessment process, enabling utilities to proactively implement security measures.

Malik and Tosh (Malik and Tosh, 2022) presented a model for quantitatively assessing an organization's security posture, evaluating security controls, and understanding associated risks. They further provided a detailed explanation of the formulations and evaluated the proposed model in an industrial scenario. Their risk evaluation approach implicates determining risks related to all assets belonging to a system, estimating the risks, and prioritizing them.

In Jasour et al. (Jasour et al., 2022), challenges related to cyber threats and risk assessment for connected and autonomous vehicles (CAV) were highlighted. A dynamic risk management framework has been proposed to address highly dynamic operational environments and associated dynamic threats and vulnerabilities. The framework functions through four sequential steps: validation of the risk profile, selection and training of the risk assessment model, performance of adaptive and real-time security monitoring, and evaluation, validation, and updating of the model. In contrast to existing rigid risk assessment approaches, this framework promotes an exploration of risks across various risk profiles. However, their work was only validated on a network of vehicles.

In Chen et al. (Chen et al., 2020), a model was proposed to study the behavior of cyber attacks on power grids. This model takes into account the attackers' subjective attitudes towards their targets and the characteristics of potential targets. In addition, the authors have incorporated two supplementary models based on historical events data analysis: the probability response model, which is used to describe the selection of attack targets, and the utility attenuation

model, which is used to describe the allocation of attack resources.

Matsuda et al. (Matsuda et al., 2021) Proved the presence of cyber risks in their research and introduced a secure implementation for Industry 4.0 elements like AI, IoT, and the Object Linking and Embedding for Process Control Unified Architecture (OPC UA). Their proposed method has benefits for clarifying the impact of cyber attacks on real-world industrial control systems. This is achieved through penetration tests on an actual machine-based testbed.

Matheu et al. (Matheu et al., 2020) analyzed current cybersecurity certification schemes and the potential challenges to making them applicable to the IoT ecosystem. They examined current efforts related to risk assessment and testing processes, which are widely recognized as the processes to build a cybersecurity certification framework. They presented a cybersecurity certification framework for IoT that integrates research and technical tools and processes with policies and governance structures, and analyzed it against identified challenges from a multidisciplinary perspective.

Radanliev et al. (Radanliev et al., 2019) presented a transformation roadmap for the standardization of IoT risk impact assessment and transformation design imperatives. They described how IoT companies can achieve their target state based on their current state with a Goal-Oriented approach. The new method they presented for applying the roadmap include IoT Risk Analysis through Functional Dependency, Network-based Linear Dependency Modeling, IoT risk impact assessment with a Goal-Oriented Approach, and a correlation between the Goal-Oriented Approach and the IoT maturity model (IoTMM).

Bahizad (Bahizad, 2020) highlighted the importance of security in IoT systems, where there are many IoT devices connected to each other using different communication methods. The paper investigates the increasing concerns related to the growing number of IoT devices and proposes recommendations for the development of these devices to minimize potential risks.

Wangyal et al. (Wangyal et al., 2020) extracted 28 risk factors using the risk breakdown structure method and expanded this traditional view to include others (physical, psychological) critical to business operations. They also proposed and quantitatively evaluated countermeasures for all the risks extracted. Their findings help clarify IoT security and its relation to non-cyber risks for properly implementing IoT systems.

Lee (Lee, 2020) reviewed IoT cybersecurity technologies and cyber risk management frameworks.

Moreover, it presents a four-layer IoT cyber risk management framework. He also applied a linear programming method to allocate financial resources to multiple IoT cybersecurity projects.

Affia et al. (Affia et al., 2023) proposed a security risk management framework for IoT architecture and a hackathon learning model to teach participants how to apply it in real-world scenarios. They conducted an action research study by integrating the hackathon model into a cybersecurity course for students to learn how to apply the framework effectively. The IoT Assurance-Security Reference Model (IoTASRM) and hackathon model interventions helped students learn IoT security risk management and apply the framework to real-world situations.

Tariq et al. (Tariq et al., 2023) reviewed security issues related to IoT architecture, including connectivity, communication, and management protocols. They examined current attacks, threats, and cutting-edge solutions and set security objectives as benchmarks for evaluating IoT solutions.

To summarize, most of the different approaches reviewed in this section can be used in specific industries, technological contexts, or IoT environments. However, it is important to note that the effectiveness of these methods may change depending on factors such as organizational structure and operational processes. It is also worth mentioning that these methods do not take into account the situations in which attackers can exploit vulnerabilities present in IoT devices. Hence, there is a need for a customizable solution that allows organizations to tailor the risk assessment process to their specific IoT environment, considering their infrastructure's unique device characteristics, requirements, and vulnerabilities.

### 3 PROPOSED RISK ASSESSMENT FRAMEWORK

The customizable risk assessment framework we propose for IoT systems is based on three parameters, namely "Risk Likelihood", "Impact Likelihood", and "Device Vulnerability Score". This framework, including these parameters and their relationships, is presented in Figure 1.

#### 3.1 Risk Evaluation

Every resource within the organization, whether it is physical equipment, digital tools, services, or personnel, is susceptible to risks that can jeopardize its confidentiality, integrity, and accessibility. Risk involves the potential danger posed to these resources,

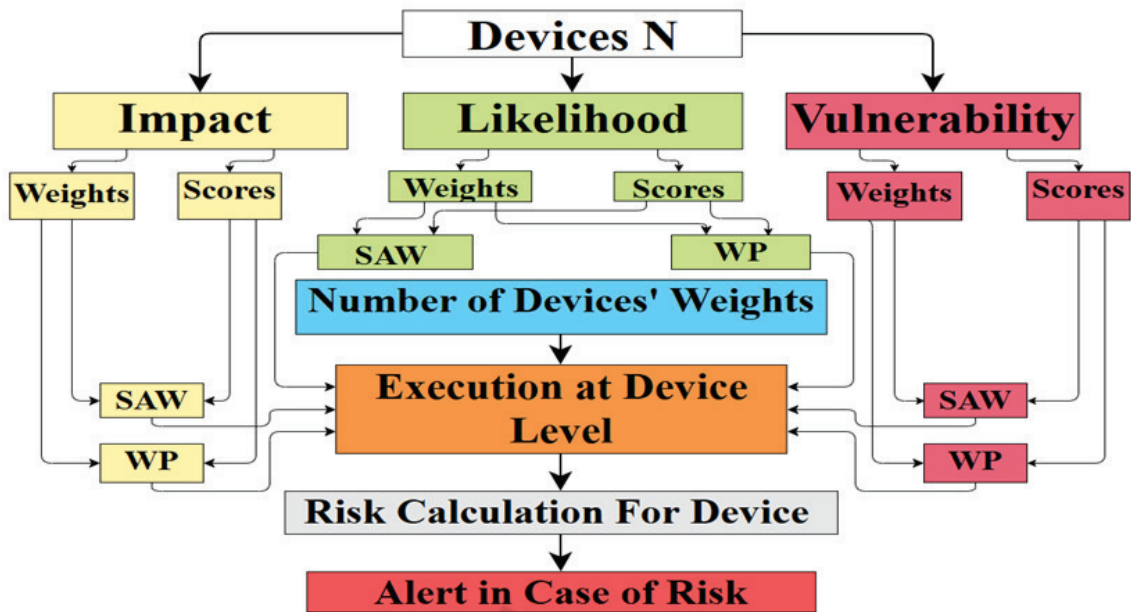


Figure 1: Proposed Framework.

the probability that such dangers occur and the resulting impact on the business. In our context, understanding both the impact and the likelihood of threats is crucial due to their direct implications on business operations. The formula for conducting a comprehensive risk evaluation is given by Equation 1.

$$\mathbb{R}(a) = \mathbb{I}(a) \times \mathbb{P}(a) \times \mathbb{V}(a) \quad (1)$$

where  $a$  represents any asset (e.g., “Remote heart monitor”),  $\mathbb{I}$  represents the risk impact due to vulnerabilities and cybersecurity issues, and  $\mathbb{P}$  is the probability (likelihood) of that risk taking place. The variable  $\mathbb{V}$  represents the attack surface coverage, which is affected by the number of vulnerabilities present in the device and their severity levels.

To evaluate risk, impact ( $\mathbb{I}$ ) and likelihood ( $\mathbb{P}$ ) will be represented separately through different sets of parameters. However, since each parameter in these sets affects the system differently, and with the complexity of IoT systems and multiple criteria and objectives, it is often necessary to use a structured approach. This is where Multi-Attribute Decision Making (MADM) methods can be helpful (Yoon and Hwang, 1995; Hwang and Yoon, 2012). There are many MADM methods, ranging from simple weighted scoring methods, such as the “Simple Additive Weighting (SAW)” and “Weighting Product (WP)”, to more advanced approaches, such as the Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS).

For simplicity reasons, in this paper, we use the

SAW and WP methods and their impact on the risk impact evaluation. Moreover, these two methods are context-dependent and suitable for our decision problem (Shameli-Sendi et al., 2016b) (Louafi et al., 2018). By utilizing these models, we aim to make informed and effective decisions through a comprehensive and rigorous evaluation of the relevant factors.

### 3.2 Risk Impact Evaluation ( $\mathbb{I}$ )

Since the risk impact category  $\mathbb{I}$  greatly influences the assessment of risk and its consequences for the organization and assets, it is crucial to examine its underlying causes in depth. The suggested framework for risk assessment considers several essential factors that contribute to the impact of the risk, including the network factor (N), the protocol factor (P), the network design (D) and the attack attributes (A). These factors are detailed in the following, as well as their assigned weights:

**Network Attacks/Issues (N):** IoT networks are potentially connected to the Internet and are part of a more extensive network that provides fast and reliable services. However, being part of a network also makes them vulnerable to various issues that can directly impact the device’s functionality and indirectly affect the entire IoT network. Many network-related problems and attacks can increase the risk impact, such as denial-of-service (DoS), distributed denial-of-service (DDoS), man-in-the-middle (MITM), packet sniffing, and traffic analysis.

We assign a weight of 0.30 to this parameter as it directly targets the infrastructure, which can cause disruptions, data breaches, or unauthorized access. Mitigating these risks is crucial to maintain operational integrity and protect sensitive information.

**Protocol Issues (P):** Another factor that directly impacts the likelihood of risk is the choice of protocol utilized by IoT devices. IoT devices employ numerous protocols for communication and network functions. Examples include MQTT, ZigBee, Bluetooth, and RFID, all commonly used but susceptible to certain vulnerabilities and attacks of the protocols.

Since protocols serve as the backbone of IoT network communication, and attackers can exploit their vulnerabilities to compromise security of the entire system, we assign a weight of 0.25 to this parameter.

**Network Design Issues (D):** The network’s arrangement and configuration also have a direct impact on determining overall security. For example, a network with more intermediate systems provides more opportunities for attackers, thus substantially increasing the risk. In such scenarios, the potential for compromised devices increases and the exposure factor of the IoT network also increases. Hence, this factor is fundamentally crucial in assessing the overall impact of risk. Furthermore, the design of the network infrastructure influences its resilience against attacks and ability to facilitate secure communication.

Since poor network design can introduce vulnerabilities, create single point of failure, or hinder effective security controls, we assign 0.30 to this parameter. Emphasizing network design issues helps to build a robust and secure architecture.

**Attack Attribute (A):** The importance of security attributes varies significantly under different circumstances. For example, DoS and DDoS attacks impact availability, while Replay attacks impact confidentiality or integrity. Understanding the attributes of potential attacks provides valuable information for risk impact assessment. This includes knowledge of attack vectors, techniques, motivations, and potential impact.

Although important for informed security decision making, attack attributes are relatively more reactive compared to other parameters, and thus receive a slightly lower weight of 0.15.

The different weights assigned to the risk impact parameters (e.g., N, P, D, and A) are summarized in Table 1. Note that different weights can be assigned to these parameters to reflect the importance and con-

tribution of each one to overall risk evaluation. The weights used in our case were determined based on the characteristics of IoT and the associated security challenges. Also, each parameter is provided with a justification for its weight. It is also important to highlight that security experts can adjust these parameters to fit the system, industry, or environment’s needs.

Table 1: The Risk Impact Parameters and their Assigned Weights.

Risk Impact Parameter	Assigned Weight
Network Attacks/Issues (N)	0.30
Protocol Issues (P)	0.25
Network Design Issues (D)	0.30
Attack Attribute (A)	0.15

Given all the aforelisted factors, we propose to evaluate the risk impact for a given asset  $a$  using the SAW and WP methods, as shown in the following equations:

$$\mathbb{I}_{SAW}(a) = \sum_{i=1}^n w_i I_i(a) \quad \mathbb{I}_{WP}(a) = \prod_{i=1}^n (I_i(a))^{w_i}$$

where,  $I_i(a)$  and  $w_i$  represent risk impact of the parameter  $i$  of the asset  $a$ , such as the “Protocol Issues (P)”, and its assigned weight, respectively.  $n$  is the number of the parameters involved in the evaluation of  $\mathbb{I}$ , which is equal to 4 (e.g., N, P, D, and A). Note that, this number can be increased if other parameters are considered, which makes our framework scalable.

### 3.3 Risk Likelihood Evaluation ( $\mathbb{P}$ )

In addition to the immediate danger posed to assets by cybersecurity issues, the probability of a vulnerability being exploited and the threat becoming real is crucial. Thus, in assessing the likelihood of a security risk occurring, we consider four factors: device attack history (H), device layer security (L), device criticality (C), and device application of use (M). These parameters are further elaborated, and different weights are assigned and justified in the following sections.

**Device Attack History (H):** This parameter reflects the number of times a device has been targeted and attacked in the past, making it an essential metric for predicting the device’s future vulnerability. For instance, if we consider an IoT device located in a highly secured facility, it might have been targeted multiple times in the past, given the sensitive nature of the data it holds. The parameter helps us identify such devices with a history of frequent attacks, making them more prone to security breaches in the future.

While understanding a device’s historical vulnerabilities can offer insights into potential weaknesses, it may not always accurately predict current security risks.

Therefore, this parameter is assigned a relatively lower weight of 0.20, reflecting its importance in context but acknowledging that other factors may carry more weight in determining overall security priorities.

**Device Layer (L):** IoT is a system that operates within multiple layers of architecture. Each layer consists of different devices with varying levels of functionality. Due to this diversity, the vulnerability of IoT to cyberattacks varies significantly across these layers. For instance, assets at the sensor layer are considerably less exposed to attacks and associated risks compared to those at the network or application layers. Likewise, the business layer presents a lower risk profile than the network layer.

Therefore, it is essential to consider the likelihood of an attack and the resulting risks in relation to the specific deployment layer. Thus, we assign a weight of 0.30 to acknowledge the need to establish a connection between the probability of an attack and the resulting risk within the IoT layer.

**Device Criticality (C):** As we increasingly rely on the Internet of Things to manage various aspects of our lives, it is essential to recognize that some devices of the Internet of Things are more critical than others. These devices play a vital role in ensuring our safety and security, and as a result, they are likely to be targeted by cybercriminals. When a critical IoT device is compromised, the consequences can be catastrophic and even life-threatening.

This particular parameter holds significant importance in likelihood evaluation as it provides insight into the device’s purpose. Hence, a weight of 0.35 is assigned to this parameter.

**Device Application/Environment of Use (M):** IoT applications can vary depending on individual needs, preferences and perspectives. They can have critical uses, such as in a healthcare environment where IoT devices are used for remote patient monitoring, medication adherence tracking, facility security cameras, and improving healthcare delivery, where they have a direct impact on human life. However, they can be used in less important applications, such as connected toothbrushes or smart umbrellas, where the impact of cyberattacks is generally less immediate and direct than in healthcare.

Therefore, it is crucial to assess the likelihood of an attack and eventual risk with the IoT application of

use. While important, the weight we assign for this parameter is 0.15, as it may not always be as critical as the device’s inherent security features or its overall criticality.

The different weights assigned to the risk likelihood parameters (e.g., H, L, C, and M) are summarized in Table 2. Similarly, different weights can be assigned to these parameters to reflect the importance and contribution of each one to overall risk evaluation.

Table 2: The Risk Likelihood Parameters and their Assigned Weights.

Risk Likelihood Parameters	Assigned Weight
Device Attack History (H)	0.20
Device Layer (L)	0.30
Device Criticality (C)	0.35
Device Application of Use (M)	0.15

After considering the given likelihood parameters and their weights, we propose to assess the risk likelihood of an asset  $a$  using the SAW and WP method, as shown in the following equations:

$$\mathbb{P}_{\text{SAW}}(a) = \sum_{i=1}^n w_i P_i(a) \quad \mathbb{P}_{\text{WP}}(a) = \prod_{i=1}^n (P_i(a))^{w_i}$$

where,  $P_i(a)$  and  $w_i$  represent probability of risk taking place for the parameter  $i$  of the asset  $a$ , such as the “Device Attack History (A)”, and its assigned weight, respectively.  $n$  is the number of the parameters involved in the evaluation of  $\mathbb{P}$ , which is equal to 4 (e.g., H, L, C, and M). Similarly, this number can be increased if other parameters are considered, which makes our framework scalable.

### 3.4 Attack Surface Coverage ( $\mathbb{V}$ )

In many real-world scenarios, assessing the overall risk to an asset and an organization based solely on risk impact and likelihood may be insufficient. This becomes particularly evident when considering systems facing numerous security challenges, such as IoT systems. IoT devices introduce a range of vulnerabilities that can compromise the security of the systems they are integrated into. Due to their unique characteristics, IoT devices lack many security mechanisms, such as encryption, authentication protocols, and access controls, leading to various security attacks, such as unauthorized access or data breaches. Security at the device level is essential, as different devices have different security issues.

A vulnerable device is more exposed to attacks when compared to a device with no or low vulnerability. The National Vulnerability Database (NVD) (National Institute of Standards and Technology (NIST),

2024b), which is managed and maintained by the National Institute of Standards and Technology (NIST), is an extensive collection of security vulnerabilities. It offers information on vulnerabilities found in various systems, such as software, hardware, and firmware.

In our framework, we utilize the NVD database to obtain vulnerability scores for different IoT devices and evaluate the attack surface coverage associated with each device. The NVD ranks vulnerabilities using a Common Vulnerability Scoring System (CVSS) (Mell et al., 2006), which assigns numerical scores to vulnerabilities based on their severity and potential impact. The CVSS scores range from 0.0 to 10.0, with higher scores indicating more severe vulnerabilities. These scores and their normalized versions and severity levels are presented in Table 3.

Table 3: CVSS Scores and their Normalized Versions and Severity Levels, Based on CVSS v3.x Ratings (National Institute of Standards and Technology (NIST), 2024a).

CVSS Score	Normalized Score	Severity Level
0.0	0	No Vulnerability
0.1 to 3.9	0.1 to 0.39	Low severity
4.0 to 6.9	0.4 to 0.69	Medium severity
7.0 to 8.9	0.7 to 0.89	High severity
9.0 to 10.0	0.9 to 1	Critical severity

As each IoT device may have 0 or more discovered vulnerabilities, each of which has a certain severity level (CVSS score), we propose to evaluate the attack surface coverage ( $\mathbb{V}$ ) using the SAW and WP methods, as shown in the following equations:

$$\mathbb{V}_{\text{SAW}}(a) = \sum_{i=1}^m w_i C(a) \quad \mathbb{V}_{\text{WP}}(a) = \prod_{i=1}^m (C(a))^{w_i}$$

where,  $C(a)$  is the cruciality of the asset  $a$  to the entire system and  $w_i$  the weight associated with it, which is evaluated as the normalized CVSS score.  $m$  represents the number of vulnerabilities present in the asset  $a$ .

The cruciality of an asset  $a$  to the entire system represents how that asset is important and critical to the system it is connected to. Hence, we propose to evaluate the cruciality with values ranging from 0 to 1, with higher values indicating higher cruciality.

### 3.5 Number of Devices

In a practical context, we may have several devices of the same type, meaning that they share the same characteristics that are involved in the evaluation of the risk. Therefore, we need a mechanism to incorporate such information in the evaluation of  $\mathbb{I}$ ,  $\mathbb{P}$ , and  $\mathbb{V}$ .

As proposed in (Waqdan et al., 2023; Waqdan. et al., 2023), we propose to multiply the ratio of each device type with each of the three functions  $\mathbb{I}$ ,  $\mathbb{P}$ , and  $\mathbb{V}$ . Table 4 shows the device type ratios and their corresponding weights. For instance, if for a given device type  $a$ , we have 8 devices and the total of devices is 10, the weight that needs to be used is 1, as the ratio of the device type  $a$  is greater than 60%.

Table 4: Device Type Weight Allocation through Their Ratios.

Device Type Ratio	Ratio Weight
Over 60%	1
40% to 60%	0.7
20% to 39%	0.5
Below 20%	0.2

### 3.6 Overall Risk Evaluation ( $\mathbb{R}$ )

After evaluating the three functions  $\mathbb{I}$ ,  $\mathbb{P}$ , and  $\mathbb{V}$ , the overall risk  $\mathbb{R}$ , which is stated in Equation 1, becomes as shown in Equation 2 and Equation 3, using the SAW and WP methods respectively.

$$\mathbb{R}_{\text{SAW}}(a) = \sum_{i=1}^m w_i I_i(a) \times \sum_{i=1}^m w_i P_i(a) \times \sum_{i=1}^m w_i V_i(a) \quad (2)$$

$$\mathbb{R}_{\text{WP}}(a) = \prod_{i=1}^m (I_i(a))^{w_i} \times \prod_{i=1}^m (P_i(a))^{w_i} \times \prod_{i=1}^m (V_i(a))^{w_i} \quad (3)$$

After calculating the overall risk  $\mathbb{R}$ , which returns a score between 0 and 1, we provide the end-user with a guide that helps him/her interpreting the returned score, as shown in Table 5.

Table 5: Risk Ranges and Criticality.

Risk Score ( $\mathbb{R}$ )	Risk Level
0.0 to 0.2	Very low
0.2 to 0.3	Low
0.3 to 0.6	Medium
0.6 to 0.8	High
0.8 to 1.0	Very high

## 4 SIMULATION AND VALIDATION

As our framework was designed with application-specific parameters, we tested and validated it in the healthcare industry. This validation was carried out through a practical simulation of a hospital emergency room involving twenty interconnected IoT devices. Table 6 shows the list of IoT devices,

their numbers, along with their vulnerabilities and the CVSS of each one. In this setup, we selected 10 Smart sensors (*Shekar Endoscope*), 6 insulin pumps (*Insulet Omnipod 19191*), and 4 Remote heart monitors (*BIOTRONIK CardioMessenger II*).

To demonstrate the real-world applicability of our framework, we evaluated it through two use cases of MADM methods with different parameter weights and device properties.

The assigned scores for the three types of IoT devices are extracted from our work (Waqdan et al., 2023), (Waqdan. et al., 2023) , to further emphasize the practicality of our approach.

In the following, we illustrate the risk evaluation using the two MADM methods considered in this paper, i.e., SAW and WP.

Table 6: The List of IoT Devices Used in the Simulation Setup.

IoT Device	Qty.	Vulnerability	Vulnerability No.	CVSS
Shekar Endoscope	10	Exploit memory corruption	CVE-2017-10724	8.8
Insulet Omnipod 19191	6	Weak Authentication	CVE-2020-10627	8.1
BIOTRONIK CardioMessenger II	4	Sensitive Info. Not Encrypted	CVE-2019-18254	4.6

### 4.1 Risk Evaluation

In this section, we will assess the risk using the SAW and WP methods. Hence, all devices are evaluated in SAW and WP with their parameter weights.

Among all the devices used in a hospital’s emergency room, three devices are highly important: i) Insulin Pumps, ii) Medical Sensors, and iii) Remote Heart Monitors. For instance, Medical sensors like Endoscopes and Borescopes are essential, as real-time health monitors use them to present patient statistics to doctors. Doctors then use this data to make informed decisions. Therefore, we need to calculate the risk associated with Medical Sensors, along with the other types of devices.

These three devices and their scores (extracted from (Waqdan et al., 2023)), and assigned weights (which are presented in Table 1 and Table 2), are summarized in Table 8 and Table 9. The Latter show also the evaluated risk impact (I) and likelihood (P) for the three devices considered using the SAW and WP methods.

Regarding the evaluation of the attack surface cov-

erage (V), we use normalized CVSS and the cruciality of the devices. The normalized CVSS are computed from the CVSS values listed in Table 6 and are reported in Table 7. The latter shows also the cruciality scores we propose. These cruciality scores are assigned to the three types of devices, as follows:

- *Medical Sensors (Shekar Endoscope)*: They are very important and numerous medical and clinical decisions rely on the outcomes they provide. However, they do not represent an immediate life threat to the patient’s life. Additionally, they mostly hold or transmit video feeds and pictures. Hence, we assign a cruciality score of 0.20 to this device.
- *Insulin Pumps (Insulet Omnipod Insulin Management System insulin pump product ID 19191)*: They are implanted in the patient’s body, preventing insulin delivery or adjusting pump settings. Thus, they could seriously threaten the patient’s life. Therefore, we assign a cruciality score of 0.35 to emphasize its importance.
- *Remote Heart Monitors (BIOTRONIK CardioMessenger II)*: They are vital to a patient’s medical care despite not being implanted in their body. They serve as crucial links between the patient and their healthcare provider, transmitting essential data about their heart health. The device’s importance cannot be overstated, as any malfunction or failure could result in severe harm or even death for the patient. Due to this significant danger, the device has been assigned a higher cruciality score of 0.45.

Similarly, Table 10 shows the evaluated attack surface coverage (R) for the three devices, using SAW and WP methods.

Table 7: IoT Devices, Their Normalized CVSS and Their Cruciality Values.

IoT Device	CVSS	Normalized CVSS	Cruciality
Shekar Endoscope	8.8	0.88	0.20
Insulet Omnipod 19191	8.1	0.81	0.45
BIOTRONIK CardioMessenger II	4.6	0.46	0.35

#### 4.1.1 Risk Evaluation for “Medical Sensor”

**Evaluation of I:** We evaluate the risk impact of the Medical Sensor using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 1 for this device (see Table 4). As



Table 8: Risk Impact Evaluation Using SAW and WP.

Impact Criteria	Medical Sensors		Insulin Pumps		Heart Monitors	
	Score	Weight	Score	Weight	Score	Weight
N	1	0.3	1	0.3	1	0.3
P	0.5	0.25	0.75	0.25	0.5	0.25
D	1	0.3	1	0.3	0.3	0.3
A	0.5	0.15	1	0.15	0.3	0.15
<b>Ratio W.</b>	0.7		0.5		0.5	
$\mathbb{I}_{SAW}$	0.56		0.468		0.28	
$\mathbb{I}_{WP}$	0.530		0.465		0.244	

Table 9: Risk Likelihood Evaluation Using SAW and WP.

Prob. Criteria	Medical Sensors		Insulin Pumps		Heart Monitors	
	Score	Weight	Score	Weight	Score	Weight
H	0.5	0.2	1	0.2	1	0.2
L	1	0.3	0.75	0.3	0.3	0.3
C	1	0.35	1	0.35	1	0.35
M	1	0.15	1	0.15	1	0.15
<b>Ratio W.</b>	0.7		0.5		0.5	
$\mathbb{P}_{SAW}$	0.63		0.462		0.395	
$\mathbb{P}_{WP}$	0.609		0.458		0.348	

Table 10: Attack Surface Coverage Evaluation Using SAW and WP.

Vuln. Criteria	Medical Sensors		Insulin Pumps		Heart Monitors	
	Score	Weight	Score	Weight	Score	Weight
V	0.20	0.88	0.35	0.81	0.45	0.46
<b>Ratio W.</b>	0.7		0.5		0.5	
$\mathbb{V}_{SAW}$	0.123		0.141		0.103	
$\mathbb{V}_{WP}$	0.169		0.213		0.346	

shown in Table 8, the risk impact for the Medical Sensor is calculated as follows:

$$\mathbb{I}_{SAW}(\text{Medical Sensor}) = 0.56 \quad (4)$$

$$\mathbb{I}_{WP}(\text{Medical Sensor}) = 0.530 \quad (5)$$

**Evaluation of  $\mathbb{P}$ :** Similarly, we evaluate the likelihood risk of the Medical Sensor, using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 1 for this device (see Table 4). As shown in Table 9, the risk likelihood for the Medical Sensor is calculated as follows:

$$\mathbb{P}_{SAW}(\text{Medical Sensor}) = 0.63 \quad (6)$$

$$\mathbb{P}_{WP}(\text{Medical Sensor}) = 0.609 \quad (7)$$

**Evaluation of  $\mathbb{V}$ :** Similarly, we evaluate the attack surface coverage of the Medical Sensor, using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 1 for this device (see Table 4). As shown in Table 10, the attack surface coverage for the Medical Sensor is calculated as follows:

$$\mathbb{V}_{SAW}(\text{Medical Sensor}) = 0.7 \times 0.20 \times 0.88 = 0.123 \quad (8)$$

$$\mathbb{V}_{WP}(\text{Medical Sensor}) = 0.7 \times (0.20^{0.88}) = 0.169 \quad (9)$$

**Evaluation of  $\mathbb{R}$ :** The overall security risk is calculated using the results obtained from the risk impact (Equation 4 and Equation 5), the likelihood impact (Equation 6) and Equation 7), and the attack surface coverage (Equation 8 and Equation 9). Thus, the overall risk is evaluated as follows:

$$\begin{aligned} \mathbb{R}_{SAW}(\text{Medical Sensor}) &= \mathbb{I}_{SAW}(\text{Medical Sensor}) \times \\ &\quad \mathbb{P}_{SAW}(\text{Medical Sensor}) \times \\ &\quad \mathbb{V}_{SAW}(\text{Medical Sensor}) \\ &= 0.04346 \end{aligned} \quad (10)$$

$$\begin{aligned} \mathbb{R}_{WP}(\text{Medical Sensor}) &= \mathbb{I}_{WP}(\text{Medical Sensor}) \times \\ &\quad \mathbb{P}_{WP}(\text{Medical Sensor}) \times \\ &\quad \mathbb{V}_{WP}(\text{Medical Sensor}) \\ &= 0.0549 \end{aligned} \quad (11)$$

#### 4.1.2 Risk Evaluation for ‘‘Insulin Pumps’’

**Evaluation of  $\mathbb{I}$ :** Similar to the Medical Sensor, the risk impact of the Insulin Pump is evaluated using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 0.7 for this device (see Table 4). As shown in Table 8, the risk impact for the Insulin Pump is calculated as follows:

$$\mathbb{I}_{SAW}(\text{Insulin Pump}) = 0.468 \quad (12)$$

$$\mathbb{I}_{WP}(\text{Insulin Pump}) = 0.465 \quad (13)$$

**Evaluation of  $\mathbb{P}$ :** Similarly, the risk likelihood of the Insulin Pump is evaluated using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 0.7 for this device (see Table 4). As shown in Table 9, the risk impact for the Insulin Pump is calculated as follows:

$$\mathbb{P}_{SAW}(\text{Insulin Pump}) = 0.462 \quad (14)$$

$$\mathbb{P}_{WP}(\text{Insulin Pump}) = 0.458 \quad (15)$$

**Evaluation of  $\mathbb{V}$ :** Similarly, we evaluate the attack surface coverage of the Insulin Pump, using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 0.7 for this device (see Table 4). As shown in Table 10, the attack surface coverage for the Insulin Pump is calculated as follows:

$$\mathbb{V}_{SAW}(\text{Insulin Pump}) = 0.5 \times 0.35 \times 0.81 = 0.141 \quad (16)$$

$$\mathbb{V}_{WP}(\text{Insulin Pump}) = 0.5 \times (0.35^{0.81}) = 0.213 \quad (17)$$

**Evaluation of  $\mathbb{R}$ :** The overall security risk is calculated using the results obtained from the risk impact (Equation 12 and Equation 13), the likelihood impact (Equation 14) and Equation 15), and the attack surface coverage (Equation 16 and Equation 17). Thus, the overall risk is evaluated as follows:

$$\begin{aligned}\mathbb{R}_{SAW}(\text{Insulin Pump}) &= \mathbb{I}_{SAW}(\text{Insulin Pump}) \times \\ &\quad \mathbb{P}_{SAW}(\text{Insulin Pump}) \times \\ &\quad \mathbb{V}_{SAW}(\text{Insulin Pump}) \\ &= 0.0307\end{aligned}\quad (18)$$

$$\begin{aligned}\mathbb{R}_{WP}(\text{Insulin Pump}) &= \mathbb{I}_{WP}(\text{Insulin Pump}) \times \\ &\quad \mathbb{P}_{WP}(\text{Insulin Pump}) \times \\ &\quad \mathbb{V}_{WP}(\text{Insulin Pump}) \\ &= 0.0455\end{aligned}\quad (19)$$

#### 4.1.3 Risk Evaluation for “Remote Heart Monitor”

**Evaluation of  $\mathbb{I}$ :** Similarly, the risk impact of the Remote Heart Monitor is evaluated using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 0.7 for this device (see Table 4). As shown in Table 8, the risk impact for the Remote Heart Monitor is calculated as follows:

$$\mathbb{I}_{SAW}(\text{Remote Heart Monitor}) = 0.28 \quad (20)$$

$$\mathbb{I}_{WP}(\text{Remote Heart Monitor}) = 0.244 \quad (21)$$

**Evaluation of  $\mathbb{P}$ :** Similarly, the risk likelihood of the Remote Heart Monitor is evaluated using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 0.7 for this device (see Table 4). As shown in Table 9, the risk impact for the Remote Heart Monitor is calculated as follows:

$$\mathbb{P}_{SAW}(\text{Remote Heart Monitor}) = 0.395 \quad (22)$$

$$\mathbb{P}_{WP}(\text{Remote Heart Monitor}) = 0.348 \quad (23)$$

**Evaluation of  $\mathbb{V}$ :** Similarly, we evaluate the attack surface coverage of the Remote Heart Monitor, using the SAW and WP methods. Then, it is multiplied by the device ratio weight, which is equal to 0.7 for this device (see Table 4). As shown in Table 10, the attack surface coverage for the Remote Heart Monitor is calculated as follows:

$$\begin{aligned}\mathbb{V}_{SAW}(\text{Remote Heart Monitor}) &= \\ &\quad 0.5 \times 0.45 \times 0.46 = 0.103\end{aligned}\quad (24)$$

$$\begin{aligned}\mathbb{V}_{WP}(\text{Remote Heart Monitor}) &= \\ &\quad 0.5 \times (0.45^{0.46}) = 0.346\end{aligned}\quad (25)$$

**Evaluation of  $\mathbb{R}$ :** Similarly, the overall security risk is calculated using the results obtained from the risk impact (Equation 20 and Equation 21), the likelihood impact (Equation 22) and Equation 23), and the attack surface coverage (Equation 24 and Equation 25). Thus, the overall risk for the Remote Heart Monitor is evaluated as follows:

$$\begin{aligned}\mathbb{R}_{SAW}(\text{Remote Heart Monitor}) &= \\ &\quad \mathbb{I}_{SAW}(\text{Remote Heart Monitor}) \times \\ &\quad \mathbb{P}_{SAW}(\text{Remote Heart Monitor}) \times \\ &\quad \mathbb{V}_{SAW}(\text{Remote Heart Monitor}) \\ &= 0.0114\end{aligned}\quad (26)$$

$$\begin{aligned}\mathbb{R}_{WP}(\text{Remote Heart Monitor}) &= \\ &\quad \mathbb{I}_{WP}(\text{Remote Heart Monitor}) \times \\ &\quad \mathbb{P}_{WP}(\text{Remote Heart Monitor}) \times \\ &\quad \mathbb{V}_{WP}(\text{Remote Heart Monitor}) \\ &= 0.0295\end{aligned}\quad (27)$$

## 4.2 Discussion and Analysis

The obtained results of the three risk functions,  $\mathbb{I}$ ,  $\mathbb{P}$ , and  $\mathbb{V}$ , as well as the overall risk  $\mathbb{R}$  are presented in Figure 2, Figure 3, Figure 4, and Figure 5, respectively. Besides, the overall security risk scores are summarized in Table 11. Using the SAW method, the overall security risk for the Medical Sensors is evaluated using the Impact set of parameters with their assigned weights, the Likelihood parameters with their assigned weights, the Curuciality of IoT devices with their CVSS scores. Then, we used the number of devices, expressed with the device ratio’s weights.

For the Medical Sensors, the overall security risk score obtained using SAW is 0.0434, while the score escalated to 0.0549 when WP is used with the same device parameters. On the other hand, for the Insulin Pumps, the overall security risk score evaluated using SAW is 0.03073. On the contrary, for the same device, using WP, the overall security risk is 0.04559. This risk is also affected by the number of devices (devices ratio) since the setup has fewer Insulin Pump devices than the Medical Sensors. Furthermore, for our last set of devices, the Remote Heart Monitors, using SAW, the overall risk is 0.01145, while the overall score using WP is 0.0295. Besides, adding weights to the parameters used gives more insight and objectivity to the results obtained. Moreover, these weighting system brings more flexibility and adaptability to business owners, stakeholders, or even security experts, who can tune these parameters in a way suitable for the system industry or environment. Additionally, the customizability of our framework makes it usable in various IoT applications.

Table 11: Overall Security Risk, as Evaluated Using the SAW and WP Methods.

Method	IoT Devices		
	Medical Sensors	Insulin Pumps	Heart Monitors
SAW	0.0434	0.0307	0.01145
WP	0.0549	0.04559	0.02951

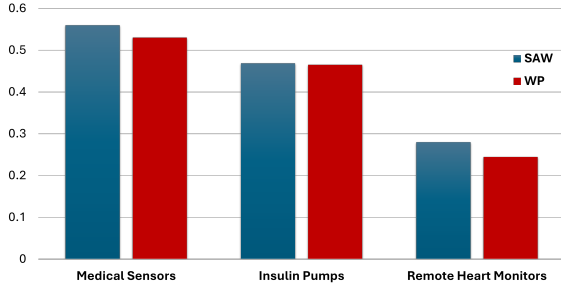


Figure 2: Impact Evaluation Using SAW and WP.

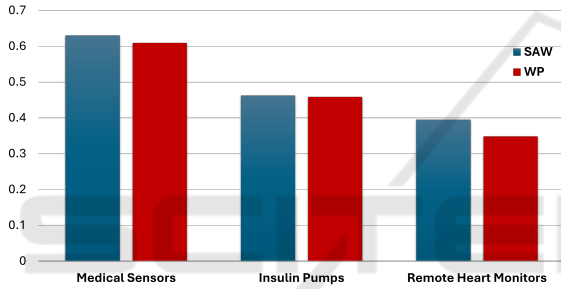


Figure 3: Likelihood Evaluation Using SAW and WP.

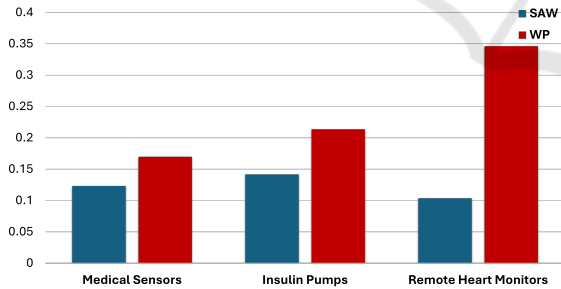


Figure 4: Attack Surface Coverage Evaluation Using SAW and WP.

## 5 CONCLUSION

IoT technology creates new security risks for organizations. To evaluate these risks, organizations need to develop a comprehensive Risk Assessment Framework for IoT. The framework should identify, assess, and respond to potential risks.

In this paper, we proposed a customizable security risk assessment framework that takes into account

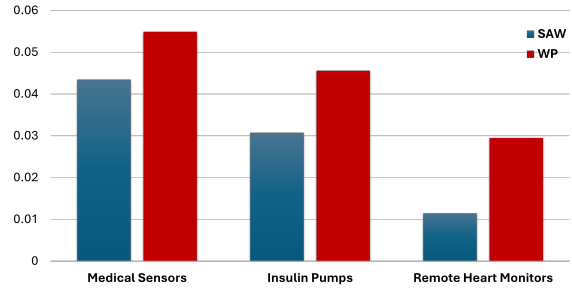


Figure 5: Overall Security Risk Evaluation Using SAW and WP.

critical factors such as risk impact, likelihood impact, and device vulnerability. Since the IoT devices involved in the risk do not affect the entire system, they are connected to, equally, their risk should be calculated differently. Therefore, in our framework, we evaluated the importance of each IoT device using a weighting system, which reflects how the device is important and critical to the entire system. We also considered the vulnerabilities that may be present in the IoT devices, which represent a risk to the entire system if they are not patched. Then, to take into account the assigned weights in the calculation of the overall risk, we used two widely used MADM methods, namely SAW and WP. These two methods are tested together to understand the impact of the approach utilized. Then, the security experts can analyze the results and decide which method is the most appropriate to his context and environment.

## REFERENCES

Affia, A.-a. O., Nolte, A., and Matulevičius, R. (2023). IoT Security Risk Management: A Framework and Teaching Approach. *Informatics in Education*.

Bahizad, S. (2020). Risks of increase in the IoT devices. In *2020 7th IEEE international conference on cyber security and cloud computing (CSCloud)/2020 6th IEEE international conference on edge computing and scalable cloud (EdgeCom)*, pages 178–181. IEEE.

Chen, B., Yang, Z., Zhang, Y., Chen, Y., and Zhao, J. (2020). Risk assessment of cyber attacks on power grids considering the characteristics of attack behaviors. *IEEE Access*, 8:148331–148344.

Falola, O., Louafi, H., and Mouhoub, M. (2023). Optimizing iot device fingerprinting using machine learning. In *Innovations in Digital Forensics*, pages 293–317. World Scientific.

Hwang, C.-L. and Yoon, K. (2012). *Multiple attribute decision making: methods and applications a state-of-the-art survey*, volume 186. Springer Science & Business Media.

Jasour, A., Huang, X., Wang, A., and Williams, B. C. (2022). Fast nonlinear risk assessment for au-

- onomous vehicles using learned conditional probabilistic models of agent futures. *Autonomous Robots*, 46(1):269–282.
- Kandasamy, K., Srinivas, S., Achuthan, K., and Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, 2020(1):1–18.
- Kumar, D., Khan, A. H., Nayyar, H., and Gupta, V. (2020). Cyber Risk Assessment Model for Critical Information Infrastructure. In *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, pages 292–297. IEEE.
- Kumar, S., Tiwari, P., and Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big data*, 6(1):1–21.
- Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future internet*, 12(9):157.
- Louafi, H., Coulombe, S., and Cheriet, M. (2018). A TOPSIS-based QoE model for adapted content selection of slide documents. *Multimedia Tools and Applications*, 77(20):26741–26768.
- Malik, A. A. and Tosh, D. K. (2022). Dynamic risk assessment and analysis framework for large-scale cyber-physical systems. *EAI Endorsed Transactions on Security and Safety*, 8(30).
- Matheu, S. N., Hernandez-Ramos, J. L., Skarmeta, A. F., and Baldini, G. (2020). A survey of cybersecurity certification for the internet of things. *ACM Computing Surveys (CSUR)*, 53(6):1–36.
- Matsuda, W., Fujimoto, M., Hashimoto, Y., and Mitsunaga, T. (2021). Cyber Security Risks of Technical Components in Industry 4.0. In *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*, pages 1–7. IEEE.
- Mell, P., Scarfone, K., and Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy*, 4(6):85–89.
- National Institute of Standards and Technology (NIST) (2024a). Common Vulnerability Scoring System (CVSS).
- National Institute of Standards and Technology (NIST) (2024b). National Vulnerability Database (NVD).
- Opoku, S. M., Louafi, H., and Mouhoub, M. (2024). Iot device identification based on network traffic analysis and machine learning. In *2024 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–8.
- Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R., and Huth, M. (2018). Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance.
- Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., Maddox, L., and Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, 3(1):1–21.
- Radanliev, P., De Roure, D. C., Maple, C., Nurse, J. R., Nicolescu, R., and Ani, U. (2019). Cyber Risk in IoT Systems.
- Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences*, 30(3):291–319.
- Shameli-Sendi, A., Aghababaei-Barzegar, R., and Cheriet, M. (2016a). Taxonomy of information security risk assessment (ISRA). *Computers & security*, 57:14–30.
- Shameli-Sendi, A., Louafi, H., He, W., and Cheriet, M. (2016b). Dynamic optimal countermeasure selection for intrusion response system. *IEEE Transactions on Dependable and Secure Computing*, 15(5):755–770.
- Tariq, U., Ahmed, I., Bashir, A. K., and Shaikat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, 23(8):4117.
- Wangyal, S., Dechen, T., Tanimoto, S., Sato, H., and Kanai, A. (2020). A Study of Multi-viewpoint Risk Assessment of Internet of Things (IoT). In *2020 9th International Congress on Advanced Applied Informatics (IIAI-AAI)*, pages 639–644. IEEE.
- Waqdan, M., Louafi, H., and Mouhoub, M. (2023). A Comprehensive Risk Assessment Framework for IoT-Enabled Healthcare Environment. In *Proceedings of the 20th International Conference on Security and Cryptography*, pages 667–672. SciTePress.
- Waqdan, M., Louafi, H., and Mouhoub, M. (2023). An IoT Security Risk Assessment Framework for Healthcare Environment. In *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 01–08. IEEE.
- Yoon, K. P. and Hwang, C.-L. (1995). *Multiple attribute decision making: an introduction*. Sage publications.