A Multi-criteria Weighting Approach with Application to Internet of Things

Constanta Zoie RADULESCU*, Radu BONCEA, Adrian Victor VEVERA

National Institute for Research and Development in Informatics – ICI Bucharest,
8-10 Mareşal Averescu Avenue, 011455, Bucharest, Romania
zoie.radulescu@ici.ro (**Corresponding author*), radu.boncea@ici.ro, victor.vevera@ici.ro

Abstract: The diversity of Internet of Things (IoT) systems can be viewed from two points of view, one that consists of providing the necessary applications and another that can lead to a large number of security threats and attacks. The analysis of the influence between different IoT security requirements (IoT-SR) as well as the determination of the importance of each security requirement play a vital role in the issue of the effective evaluation of an IoT system. The diverse nature, importance, evaluation and influence of multiple IoT-SR are the main issues that make this problem a multi-criteria problem. Considering the qualitative nature of IoT-SR and the advantages of fuzzy sets in efficiently dealing with uncertainty, fuzzy subjective weighting methods can be used to address the problem. The paper proposes a Multi-Criteria Weighting Approach (MCWA) based on the Fuzzy DEMATEL method in combination with two weighting methods, aiming to analyze cause-and-effect relationships for a set of criteria and to calculate the criteria weights. An application of MCWA for IoT-SR is realized. The obtained results can open new ways for system security specialists to focus on security requirements determined to be of increased importance.

Keywords: Fuzzy DEMATEL, Fuzzy triangular numbers, Weightings methods, Internet of Things.

1. Introduction

The Internet of Things (IoT) is a very important inter-device environment in digital development today. The IoT can be defined as a network of intelligent devices that are involved in the collection, exchange and analysis of data. IoT incorporates different types of hardware, communication protocols and services. The number of interconnected devices in IoT platforms has increased considerably in the last decade. This has determined important changes in the daily activity and an increase in the quality of life. IoT applications are continuously developing in various fields such as smart home systems, smart agriculture, smart health, smart cities, etc. This diversity of IoT fields of applications can be viewed from two points of view, one that consists of providing the necessary applications and another that can lead to a large number of security threats and attacks. The analysis of the influence between different IoT security requirements (IoT-SR) as well as the determination of the importance of each security requirement play a vital role in the issue of the effective evaluation of the security of an IoT system. The diverse nature, importance, evaluation and influence of multiple IoT-SR are the main issues that make this problem a multi-criteria analysis problem. This problem can be solved by using multi-criteria weighting methods (Filip, Zamfirescu & Ciurea, 2017; Radulescu & Radulescu, 2018). Considering the qualitative nature of IoT-SR and the advantages of fuzzy sets in providing a wide range of options to decision-makers and efficiently dealing with uncertainty, a fuzzy weighting method can be considered to solve the problem. The paper proposes a Multi-Criteria Weighting Approach (MCWA), based on the Fuzzy DEMATEL method in combination with two weighting methods, aiming to analyse cause-and-effect relationships among a set of criteria and to compute the criteria weights. The MCWA is used to identify the most important criteria affecting a decision and to determine the direction and strength of relationships between them. MCWA calculates the weights and ranks the criteria, based on the associated weights. In the first stage, the main criteria are selected. These criteria are initially evaluated in linguistic terms and then are associated with triangular fuzzy numbers. In the second stage, the Fuzzy DEMATEL method is applied and the causality diagram, that can visualize the causal relationships of criteria, is constructed. Then, the weights associated with the criteria are calculated, based on two weighting methods. An application of the MCWA for IoT-SR is realized.

The remainder of the paper is structured as follows. A discussion about fuzzy theory in decision making and a few basic concepts of membership function and triangular fuzzy numbers are presented in section 2. In section 3 the Multi-Criteria Weighting Approach (MCWA) is described in steps. Section 4 contains some recent research in IoT security and section 5 presents the set of security requirements considered in this paper. An application of the proposed approach for IoT-SR is presented in section 6. Conclusions are given in Section 7.

https://doi.org/10.24846/v32i4y202301 ICI Bucharest © Copyright 2012-2023. All rights reserved

2. Fuzzy Set Theory in Decision Making

Fuzzy set theory was introduced by Zadeh (1965) as an extension of the classical notion of set and can be used for dealing with uncertainty and imprecision in decision making. Hence, fuzzy set theory can express and handle vague or imprecise judgments mathematically.

In decision making problems related to complex systems, the evaluation given by experts on qualitative criteria is expressed, in fuzzy formulation, by using linguistic terms instead of crisp values, based on experience and expertise of experts. Fuzzy set theory can be implemented to measure experts' subjective judgments. Ambiguous judgments can be transformed into fuzzy numbers.

Generally, a decision-maker makes evaluations often expressed in linguistic terms. Based on the definition of fuzzy sets, the concept of linguistic variables is introduced to represent a language typically adopted by a human expert (Wu, 2012). The values of linguistic variables are not numbers, but linguistic terms, this being the manner in which decision makers can express their evaluations. In practice, the linguistic values can be represented by fuzzy numbers, and the triangular fuzzy numbers are commonly used (Radulescu, 2017).

In the following, a few basic concepts of membership function and triangular fuzzy number are recalled.

A fuzzy subset A of a set X is defined by a membership function $F_A : X \to [0;1]$. The function value of $F_A(x)$ for the fuzzy set A is called the membership value of x in A and represents the degree of truth that x is an element of A. When the membership value of x is 1, it means that x is absolutely in A. When the membership value of x is 0, it means that x is absolutely not in A. For ambiguous cases, real numbers between 0 and 1 are assigned.

Let X be a linear space over $\mathbb{R}$. A fuzzy set A of X is convex if:

$F_A(\lambda x_1 + (1-\lambda)x_2) \geq \min(F_A(x_1), F_A(x_2))$ for every $x_1, x_2 \in X$ and $\lambda \in [0;1]$.

A fuzzy set A in X is normal if $\max_{x \in X} F_A(x) = 1$.

In the literature, there are several definitions for fuzzy numbers. In the present paper, the definition of a fuzzy number from (Lewis, 1997) will be used and that is "A fuzzy number is a fuzzy subset N in $\mathbb{R}$ which is convex and normal".

A triangular fuzzy number (TFN) is a mathematical representation of a fuzzy set, which is a subset of the set of real numbers, in which the degree of membership of a value to the set is described by a triangular membership function. It is defined by three values: the minimum value (l), the maximum value (h), and the modal value (m), where m is the most likely value in the set and lies between l and h. The TFN (l,m,h) where l, m, h are real numbers and $l \leq m \leq h$ can be visualized as a triangle on a number line, with the three values serving as its vertices.

The TFN is a type of fuzzy number that is widely used in fuzzy mathematics and decision making due to its simple and intuitive structure. It provides a means of modeling uncertainty and imprecision in a flexible and scalable manner, making it a useful tool for addressing real-world problems.

TFNs are used as membership functions, corresponding to the elements in a set. The membership function for a set T is the following (Kaufmann & Gupta, 1988):

$$f_T(x) = \begin{cases} \dfrac{x-l}{m-l} & l \leq x \leq m \\ \dfrac{h-x}{r-m} & m \leq x \leq h \\ 0 & otherwise \end{cases}$$

In decision making, TFNs are used to represent uncertainty and imprecision in the data. The triangular membership function of a TFN allows decision makers to incorporate the subjective information about the degree of membership of a value to a fuzzy set into the analysis.

TFNs can be used in multicriteria decision making (MCDM) for subjective evaluating of alternatives based on multiple criteria. In MCDM multiple conflicting criteria are involved. The evaluations are often vague and uncertain, and the use of TFNs can help to better capture these uncertainties. In such problems, the decision maker (expert) can assign TFNs to the alternative's evaluation for the qualitative criteria and then use a suitable aggregation method to obtain alternatives ranking.

The use of TFNs in multicriteria decision making provides a means of modelling the uncertainty and imprecision in the decision-making process leading to more robust and informed decision-making outcomes.

TFN can also be used to represent the subjective evaluation of the qualitative criteria in order to obtain the criteria weights (coefficients of importance). The triangular membership function of a TFN allows decision makers to incorporate subjective information about the criteria into their evaluation. Then a weighting method can be applied to obtain the criteria weights. This allows for a more informed and systematic approach to decision-making, taking into consideration the subjective nature of the criteria evaluation.

The linguistic terms that describe the alternatives/ criteria evaluations can be mapped to fuzzy numbers, and then used in decision-making models, such as multi-criteria decision analysis or fuzzy logic. A linguistic term can be defined as a variable whose values are words or sentences in natural language. A fuzzy scale defined by a series of fuzzy sets depicts the levels of linguistic terms, which links the verbal and numerical expressions. Fuzzy scales: 9-level or 5-level, for relative importance, are commonly adopted (Liu et al., 2020).

Defuzzification converts the fuzzy results produced by aggregation methods into crisp values. Compared with a fuzzy value, a crisp value is more intuitive and easier to compare, because fuzzy sets have partial ordering (Liu et al., 2020).

3. A Multi-Criteria Weighting Approach Based on Fuzzy DEMATEL Method

DEMATEL (Decision-Making Trial and Evaluation Laboratory) is a method used to analyze cause-and-effect relationships among a set of variables in complex systems. It is used to identify the most important factors affecting a decision and to determine the direction and strength of relationships between variables. DEMATEL uses a combination of expert knowledge and mathematical techniques to create a cause-and-effect matrix which can be used to develop strategies and prioritize actions.

The DEMATEL method was developed in the Geneva Research Center of the Battelle Memorial Institute, by Gabus and Fontela (1972). To solve the fuzziness caused by expert's subjective judgment and to improve the accuracy of the DEMATEL, a Fuzzy DEMATEL method, with TFNs, is proposed by Wu and Lee (2007). The DEMATEL is based on digraphs (directed graphs) which can separate involved factors into cause group and effect group (Wu, 2012).

The MCWA proposed in this paper, based on Fuzzy DEMATEL, is presented (in steps) in the following.

Step 1. Identification of the decision target and selection of an expert.

Step 2. Definition of the criteria (factors) considered for the evaluation of causal relationships: $C = \{C_1, C_2, ..., C_n\}$.

Step 3. Designing of the fuzzy linguistic scale. For dealing with the uncertainty of human evaluations, the linguistic variable "influence" is used with five linguistic terms: No influence, Very low influence, Low influence, High influence and Very high influence that are expressed in positive TFN (l_i, m_i, h_i), i=1, 2, ... 5. The correspondence is made between the linguistic terms and TFNs (Table 1).

Table 1. The corresponding relations between the linguistic terms and TFNs

Nr. Crt.	Linguistic terms	TFNs
1	No influence	(0,0,0.25)
2	Very low influence	(0,0.25,0.5)
3	Low influence	(0.25,0.5,0.75)
4	High influence	(0.5,0.75,1)
5	Very high influence	(0.75,1,1)

Step 4. Evaluation of each criterion in relation to the other criteria, using the linguistic terms from Table 1 and generation of the initial direct-relation matrix $T = (t_{ij}), i, j = 1, 2, ..., n$, $t_{ij} \in$ {No influence, Very low influence, Low influence, High influence, Very high influence}. The principal diagonal elements of matrix T are $t_{ij} = 0$. Based on expert's experience and expertise, the evaluation is made between each pair of criteria from set C. Element t_{ij} denotes the appreciation (in linguistic terms) of the degree to which criterion i influences criterion j.

Step 5. Matrix T is transferred into the corresponding matrix of TFN (from last column of Table 1) and matrix $F = \left(f_{ij}\right), i, j = 1, 2, ..., n$, with arrays $f_{ij} = \left(l_{ij}, m_{ij}, h_{ij}\right)$, is obtained. The principal diagonal elements are $f_{ii} = \left(0, 0, 0\right)$. The use of linguistic terms and TFNs allows to incorporate of subjective expert evaluation.

ICI Bucharest © Copyright 2012-2023. All rights reserved

Step 6. The fuzzy data from matrix F are converted in crisp values. The defuzzification method of Opricovic and Tzeng (2004) is used.

The fuzzified matrix F is normalized and the normalized matrix $\overline{F} = \left(\overline{f}_{ij}\right), i, j = 1,2,...,n$; $\overline{f}_{ij} = (\overline{l}_{ij}, \overline{m}_{ij}, \overline{h}_{ij})$ is obtained:

$$\overline{l}_{ij} = \left(l_{ij} - l^{\min}\right) / \Delta_{\min}^{\max} \quad (1)$$

$$\overline{m}_{ij} = \left(m_{ij} - l^{\min}\right) / \Delta_{\min}^{\max} \quad (2)$$

$$\overline{h}_{ij} = \left(h_{ij} - l^{\min}\right) / \Delta_{\min}^{\max} \quad (3)$$

where: $l^{\min} = \min_{1 \le r,k \le n} l_{rk}$; $h^{\max} = \max_{1 \le r,k \le n} h_{rk}$;

$$\Delta_{\min}^{\max} = h^{\max} - l^{\min} \quad (4)$$

The normalization is necessary when:

$h^{\max} < 1$ or $l^{\min} > 1$. Otherwise, when $h^{\max} = 1$ and $l^{\min} = 0$ one has $\Delta_{\min}^{\max} = 1$ and $F = \overline{F}$.

The left and right normalized values are calculated:

$$l_{ij}^{*} = \overline{m}_{ij} / \left(1 + \overline{m}_{ij} - \overline{l}_{ij}\right) \quad (5)$$

$$h_{ij}^{*} = \overline{h}_{ij} / \left(1 + \overline{h}_{ij} - \overline{m}_{ij}\right) \quad (6)$$

The total normalized crisp values are calculated:

$$\overline{\overline{f}}_{ij} = \left[l_{ij}^{*}\left(1 - l_{ij}^{*}\right) + h_{ij}^{*} \times h_{ij}^{*}\right] / \left(1 - l_{ij}^{*} + h_{ij}^{*}\right) \quad (7)$$

The matrix of crisp values $A = \left(a_{ij}\right)$, i,j=1,2, …, n, is obtained:

$$a_{ij} = l_{\min}^{*} + \overline{\overline{f}}_{ij} \times \Delta_{\min}^{\max} \quad (8)$$

where: $l_{\min}^{*} = \min_{1 \le r,s \le n} l_{rs}^{*}$.

The matrix A is the direct relation matrix input for the DEMATEL method. The following calculations follow the DEMATEL method.

Step 7. Building $n \times n$ normalized matrix $\overline{A} = \left(\overline{a}_{ij}\right)$ from matrix A. In matrix $\overline{A}$ all principal diagonal elements are equal to zero.

$$s = \max\left(\max_{1 \le i \le m} \sum_{j=1}^{m} a_j, \max_{1 \le j \le m} \sum_{i=1}^{m} a_j\right) \quad (9)$$

$$\overline{a}_{ij} = a_{ij} / s \quad (10)$$

Step 8. Calculating of $n \times n$ total influence matrix $X = \left(x_{ij}\right)$:

$$X = \overline{A}\left(I - \overline{A}\right)^{-1} \quad (11)$$

where I is the identity matrix. Note that:

$$\lim_{h \to \infty} \overline{A}^{h} = 0 \quad (12)$$

Matrix X *serves for producing the causal* diagram map.

Step 9. Matrix X allows to express a relation between the criteria, covering both direct and indirect influences. For this purpose, appropriate indicators are used, defined as importance indicator (R^{+}) and relation indicator (R^{-}). They are determined using sums and differences of the row and column sums of matrix X corresponding to the i-th criterion. The sum of rows and the sum of columns of matrix X are calculated separately and denoted as vectors $P = (p_i)$ and $E = (e_j)'$:

$$p_i = \sum_{j=1}^{n} x_{ij}, \quad i = 1,2,...,n \quad (13)$$

$$e_j = \sum_{i=1}^{n} x_{ij}, \quad j = 1,2,...,n \quad (14)$$

The importance vector of indicators denoted by $R^{+} = (r_i^{+})$ and the relation vector of indicators denoted by $R^{-} = (r_i^{-})$ are calculated as follows:

$$r_i^{+} = p_i + e_i \quad (15)$$

$$r_i^{-} = p_i - e_i \quad (16)$$

Indicator r_i^{+} represents the total degree of influence among criteria, and the higher its value, the higher the importance of criterion i. In addition, indicator r_i^{-} represents the degree of causality among criteria. If r_i^{-} is positive, then criterion i influences other criteria, rather than being affected themselves, and belongs to the cause group. If r_i^{-} is negative, criterion i is influenced by other criteria and the criterion belongs to the effect group.

By mapping the vectors of indicators R^{+} and R^{-} the data can be visualized. Vector R^{+} represents the horizontal axis of the diagram called *importance or prominence*. The vertical axis, which is called *cause/effect relation*, is represented by vector R^{-}. The horizontal axis, "Importance" shows how much importance the criterion has, whereas the vertical axis "Relation" may divide criteria into cause group and effect group.

The causality diagram can visualize the causal relationships of criteria. Based on a causal diagram, the decision maker can make better

decisions by recognizing the difference between cause-and-effect criteria.

Step 10. Determination of criteria weights, using the DEMATEL method, is based on method 1, proposed by Baykasoglu et al. (2013) and Dalalah et al. (2011). In method 1, the criteria weights $W=(w_i), i=1,2,...,n$ are calculated as follows:

$$\alpha_i=\sqrt{\left(r_i^+\right)^2+\left(r_i^-\right)^2} \tag{17}$$

$$w_i=\alpha_i/\sum_{k=1}^{n}\alpha_k \tag{18}$$

In (Kobryń, 2017) a different approach for determining the criteria weights using DEMATEL was proposed. In method 2, the criteria weights $\overline{W}=\left(\overline{w}_i\right)$ are calculated as follows:

$$\overline{\alpha}_i=\frac{1}{2}\left(r_i^+ + r_i^-\right) \tag{19}$$

$$\overline{w}_i=\overline{\alpha}_i/\sum_{k=1}^{n}\overline{\alpha}_k \tag{20}$$

The weights obtained by using method 1 are compared with the weights obtained by using method 2. The final criteria weights $\overline{\overline{W}}=\left(\overline{\overline{w}_i}\right)$ are calculated as follows:

$$\overline{\overline{w}_i}=\left(\overline{w}_i+w_i\right)/2 \tag{21}$$

In the specialized literature there are numerous multi-criteria weighting methods. For a comparison of the DEMATEL method, proposed in the present approach, with other methods in the literature, without considering the fuzzy aspect in expert's subjective evaluation, the most frequently used weighting methods were chosen, mainly methods with a pairwise evaluation. These methods are: Analytical Hierarchy Process (AHP) (Saaty, 1977; Saaty, 1980), Analytical Network Process (ANP) (Saaty, 1996), Best Worst Method (BWM) (Rezaei, 2015), Step-wise Weight Assessment Ratio Analysis (SWARA) method (Keršuliene, Zavadskas & Turskis, 2010), and Interpretive Structural Modelling (ISM) (Raj, Shankar & Suhaib, 2008).

The comparison is presented in Table 2. It is important to note that the strengths and limitations of each method may depend on the specific problem and context of the decision-making process.

In method ANP, an extension of the AHP, the assumption of equal weight for each cluster to obtain a weighted super-matrix is not reasonable in practical situations. In DEMATEL there is a lower number of pairwise comparisons in contrast with AHP and ANP. Both DEMATEL and ISM can analyze the interrelationship among criteria. However, according to Kumar and Dixit (2018), ISM is a macro-oriented approach whereas DEMATEL is a relatively micro-oriented approach. ISM is based on a set of rules and uses a matrix-based approach to identify the relationships among criteria.

BWM focuses on ranking criteria based on their best and worst criteria. DEMATEL uses matrices to quantify the relationships among criteria, while BWM involves vectors of pairwise comparisons of the best and worst criteria of each criterion. BWM is particularly useful in balancing both positive and negative aspects of criteria.

The present approach was chosen because it allows a complex multi-criteria decision analysis from several points of view. It is a useful approach for capturing inter-dependencies among criteria, identifying cause-effect relationships, handle uncertainty and vagueness in the decision-making

Table 2. The comparison of DEMATEL method with AHP, ANP, BWM, SWARA and ISM methods

Criteria	Weighting multi-criteria methods					
	DEMATEL	AHP	ANP	BWM	SWARA	ISM
Dependent criteria	X		X			X
Does not require a hierarchical structure	X			X	X	X
Pairwise comparison	X	X	X	X	X	X
Micro-oriented approach	X	X		X	X	
Identification of causal relationships	X					X
Easy to understand and apply	X			X	X	
Provides a visual representation of the results	X					

ICI Bucharest © Copyright 2012-2023. All rights reserved

process, providing a visual representation of the results and determining the weights of criteria that reflect the relative importance of the criteria. The combination of Fuzzy DEMATEL with criteria weighting methods can improve the accuracy of decision-making in multi-criteria decision analysis. Fuzzy DEMATEL is most suitable for problems where causal relations between criteria are important and where the decision maker wants to understand the underlying structure of the problem. The weighting methods are more suitable for problems where the decision maker wants to focus on the relative importance of criteria.

This approach was proposed also because it is very suitable for determining the influence between IoT security requirements and finding the importance of each security requirement.

4. Recent Research in IoT security

Building secure IoT systems can only be achieved through a detailed understanding of the specific security needs of such systems (Balakumar & Kavitha, 2021; Duraisamy, Subramaniam & Robin, 2021; Năstase et al., 2017). In the specialized literature, a lot of aspects and requirements regarding the security of IoT systems are studied.

A recent survey (Farooq et al., 2022) covers the major security issues and open challenges encountered by IoT infrastructures. It also presents a study of solutions based on Machine learning used in IoT security. The challenges associated with Machine learning-based security solutions have been identified concerning IoT. The IoT security requirements taken into consideration, in this paper, are: Confidentiality, Integrity, Authentication, Authorization, Availability, Non-repudiation.

The research presented in (Akkad, Wills & Rezazadeh, 2023) focuses on the information flow's cybersecurity. The study uses technical security controls to count internet-based threats in IoT-enabled Smart Grids. It develops a model with seven security requirements and 45 security controls. The security requirements considered are: Authentication, Authorization, Confidentiality, Integrity, Availability, Privacy and Non-repudiation. A connection between security requirements, threats and STRIDE is emphasized.

The aim of the paper (Ogonji, Okeyo & Wafula, 2020) is to provide a review on IoT, with particular focus on privacy and security threats, attack surface, vulnerabilities and countermeasures. The paper proposes a threat taxonomy to address the security requirements and addresses to an integrated privacy and security perspective centred on the user. IoT user requirements and challenges are identified and discussed to highlight the baseline security and privacy needs and concerns of the user. The considered security requirements are: Identification, Authentication, Data Integrity, Trust, Data Confidentiality, Access Control, Data Privacy and Data Availability.

A similar paper is (Deep et al., 2022). Its purpose is to focus on security and privacy issues in IoT systems. Security issues are addressed for each layer in the IoT protocol stack. The main challenges and the key security requirements are identified. Existing security solutions from the layered context are presented. The considered layers are: perception layer, network layer, middleware layer and application layer.

In the paper (Jabangwe & Nguyen-Duc, 2020) a conceptual framework is proposed to help the identification of security concerns at the beginning of the development of an IoT solution. The framework uses known approaches and best practices and builds on existing IoT architecture research. The tiers and security requirements are considered in the framework. For application tier, the security requirements are: Confidentiality, Availability and Integrity. For network tier, the security requirements are: Confidentiality/ Integrity, Availability and Integrity. For sensor tier, the security requirements are: Confidentiality and Availability. For data tier, the security requirements are: Confidentiality, Availability and Integrity.

The study (Elhoseny et al., 2021) examines the current state of IoT security and confidentiality in the medical field. The authors discuss a number of attack use cases, countermeasures and solutions.

Although there are several papers presented above in the area of IoT-SR, they are specific to certain limited aspects of IoT. In the above reviews, the considered set of security requirements (criteria, factors) for IoT systems is often used in

various contexts. None of these reviews achieve a prioritization of these IoT-SR or an influence between them.

5. The Set of Security Requirements

The security requirements considered in this paper, for the MCWA application, are: Confidentiality, Manageability, Reliability, Access control, Resilience, Tamper protection, Incident response, Decentralization and Compliance.

Confidentiality: Confidentiality ensures that sensitive data transmitted by IoT devices and systems is protected from unauthorized access or theft. Unauthorized people should not be able to disclose confidential data stored in IoT devices (Farooq et al., 2022).

Manageability: Manageability refers to the ease with which an IoT system can be administered, monitored, and maintained. A manageable IoT system is one that is easily configurable, monitored, and updated, and that provides clear and concise information about its state and performance. Management of security in IoT systems includes: Identity Management, Trust Management (Ogonji, Okeyo & Wafula, 2020), Key Management (Khan et al., 2022).

Reliability: Reliability refers to the ability of an IoT system to perform its intended functions consistently and without interruption. Reliability helps to ensure that the system is available and functioning as expected, even in the face of adverse events or security incidents. It also refers to the property that guarantees consistent intended behaviour of an IoT system (Samaila et al., 2021). Availability is alternatively used for reliability and is defined as the probability of performance of an element of the IoT network system to give the desired output at a specific time under specific environmental conditions (Khan et al., 2022).

Access control: Access control helps to ensure that only authorized individuals and devices have access to sensitive data and systems. Access control is used to restrict the access of available resources against undesired access. Different from traditional systems, IoT mainly focuses on more ubiquitous services being accessed on top of a heterogeneous network architecture for people, things, devices, services, etc. (Khan et al., 2022).

Resilience: Resilience refers to the ability of a system, such as an IoT system, to maintain its core functionality and recover from adverse events, such as security incidents or natural disasters. It also refers to the ability of a IoT network to absorb the performance degradation under some failure pattern (random or intentional) and to continue delivering messages with an increasing number of compromised nodes (Erdene-Ochir et al., 2012). Resilience helps to minimize the impact of security incidents, reduce downtime, and ensure the availability of critical functions and data.

Tamper protection: Tamper protection helps to protect devices and systems from unauthorized access and manipulation, and to ensure the confidentiality, integrity, and availability of sensitive data and functions. In this kind of attack, the attacker obtains direct access to the hardware component of the nodes such as the microcontroller (Aarika et al., 2020). Tamper protection is especially important in IoT systems as they often contain sensitive data and control physical devices, making them attractive targets for attackers.

Incident response: Incident response is the process of identifying, assessing, and managing security incidents that occur within an IoT system. The goal of incident response is to contain the security breach, prevent further damage, and restore normal operations as quickly as possible. Key phases of an incident response and recovery procedure for IoT systems include planning, detection, analysis and response formulation, containment, eradication, recovery, and post-incident activity.

Decentralization: Decentralized IoT security helps to increase the overall security of the network by distributing control and responsibilities among multiple entities, reducing the risk of a single point of failure and improving data security. By decentralization, imposed by the prevalence of internet-enabled devices which call for additional management and control closer to their operating architectural layer, central points of failure are eliminated. Decentralization is view as the key to achieving resilience in the face of the uncertainty and variability that IoT systems are exposed to (Tsigkanos, Nastic & Dustdar, 2019).

Compliance: Compliance refers to the adherence to regulations, standards, and guidelines that are

ICI Bucharest © Copyright 2012-2023. All rights reserved

designed to ensure the security and privacy of IoT devices and systems. These regulations and standards aim to minimize the risk of cyber-attacks and data breaches in IoT system. (examples: General Data Protection Regulation –GDPR, The Federal Risk and Authorization Management Program – FedRAMP, The International Organization for Standardization –ISO/International Electrotechnical Commission – IEC 62443 series, The NIST Cybersecurity Framework).

6. Application of Multi-Criteria Weighting Approach

The aim of this section is to calculate and analyze the influence that exists between the requirements from a set of IoT-SR, to create a causality diagram between these requirements and to calculate the weights (coefficients of importance) associated with them. For this purpose, the proposed approach MCWA will be used. An expert with solid knowledge and experience in the field selects a set of important IoT-SR, based on experience and literature review.

The selected criteria for IoT systems are: Confidentiality (C_1), Manageability (C_2), Reliability (C_3), Access control (C_4), Resilience (C_5), Tamper protection (C_6), Incident response (C_7), Decentralization (C_8) and Compliance (C_9). Information on these security requirements can be found in section 5.

Using the linguistic terms defined in Table 1, the evaluation (matrix T) is obtained. Then matrix T is transferred into the corresponding F matrix of TFNs.

Using the defuzzification method presented in step 6 (Equations (1)-(8)), the elements of F matrix are aggregated to crisp values which represent the degree to which criteria have direct impacts on each other. The initial direct-relation matrix, for the DEMATEL method (Table 3), is obtained.

The normalized matrix $\overline{A} = \left(\overline{a}_{ij}\right)$, i,j=1, 2, …, 9 is calculated based on Equations (9) and (10). Then, the total influence matrix X is calculated, based on Equation (11). The total influence matrix X is displayed in Table 4.

The elements of importance vector of indicators (R^+) and relation vector of indicators (R^-) are calculated using sums and differences of the row and column sums of matrix X corresponding to

Table 3. The initial direct-relation F matrix

IoT-SR	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_1	0.000	0.500	0.267	0.967	0.267	0.733	0.500	0.267	0.033
C_2	0.733	0.000	0.733	0.967	0.967	0.500	0.500	0.967	0.733
C_3	0.733	0.500	0.000	0.733	0.733	0.967	0.733	0.733	0.733
C_4	0.500	0.500	0.500	0.000	0.267	0.967	0.733	0.733	0.033
C_5	0.733	0.267	0.733	0.733	0.000	0.733	0.733	0.500	0.500
C_6	0.500	0.733	0.267	0.267	0.500	0.000	0.500	0.267	0.267
C_7	0.967	0.733	0.733	0.733	0.733	0.967	0.000	0.500	0.967
C_8	0.033	0.267	0.500	0.500	0.733	0.033	0.733	0.000	0.500
C_9	0.733	0.500	0.967	0.500	0.967	0.733	0.267	0.733	0.000

Table 4. The total influence X matrix

IoT-SR	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_1	0.19	0.24	0.22	0.34	0.23	0.33	0.26	0.221	0.150
C_2	0.42	0.27	0.41	0.48	0.46	0.44	0.39	0.441	0.348
C_3	0.41	0.33	0.29	0.44	0.42	0.49	0.41	0.393	0.339
C_4	0.30	0.27	0.28	0.24	0.27	0.39	0.33	0.315	0.184
C_5	0.37	0.27	0.35	0.39	0.27	0.41	0.36	0.320	0.274
C_6	0.26	0.26	0.22	0.25	0.27	0.22	0.26	0.220	0.187
C_7	0.47	0.39	0.42	0.47	0.45	0.52	0.32	0.388	0.388
C_8	0.210	0.203	0.264	0.286	0.309	0.238	0.298	0.188	0.230
C_9	0.389	0.310	0.403	0.384	0.427	0.432	0.324	0.373	0.218

each criterion (Equations (13) to (16)). Vectors P, E, R^+ and R^- are displayed in Table 5. By mapping the vectors of indicators R^+ and R^-, the data can be visualized in a causality diagram (Figure 1). The causality diagram was built by the horizontal axis (R^+), which is the importance of the criteria, and the vertical axis (R^-), which is the degree of relation between criteria.

From the importance point of view (according to Figure 1), the most important three criteria are Incident response (C_7), Reliability (C_3) and Manageability (C_2). Among all criteria, Incident response (C_7) has the highest R^+ value, showing that it is of the most importance for the security requirement in IoT systems.

The vertical axis divides criteria into cause group and effect group. Characterized by positive values (R^- Column of Table 5), the cause group includes Manageability (C_2), Reliability (C_3), Incident response (C_7) and Compliance (C_9). All of these criteria influence other criteria rather than being affected themselves. The cause group can be subdivided into criteria with low and high importance (prominence) values (R^+ column of the Table 5). The Manageability (C_2), Incident response (C_7) and Reliability (C_3) criteria have very high relation values (1.131, 0.859. 0.670, respectively), and very high importance values (6.196, 6.765 and 6.368). Compliance (C_9) has a high relation value (0.943), but a small hight importance value (5.579). Changes in Compliance (C_9) will not have a major impact on other criteria.

Characterized by negative values (R^- Column of Table 5), the effect group includes the Confidentiality (C_1), Access control (C_4), Resilience (C_5), Tamper protection (C_6) and Decentralization (C_8) criteria. These criteria are

Table 5. The values of vectors P, E, R^+ and R^-

IoT-SR Symbol	IoT-SR	*P*	*E*	R^+	R^+ ranks	R^-
C_1	Confidentiality	2.176	3.028	5.204	8	-0.853
C_2	Manageability	3.664	2.533	6.196	3	1.131
C_3	Reliability	3.519	2.849	6.368	2	0.670
C_4	Access control	2.578	3.287	5.865	5	-0.709
C_5	Resilience	3.014	3.099	6.113	4	-0.085
C_6	Tamper protection	2.144	3.470	5.613	6	-1.326
C_7	Incident response	3.812	2.953	6.765	1	0.859
C_8	Decentralization	2.227	2.859	5.086	9	-0.632
C_9	Compliance	3.261	2.318	5.579	7	0.943

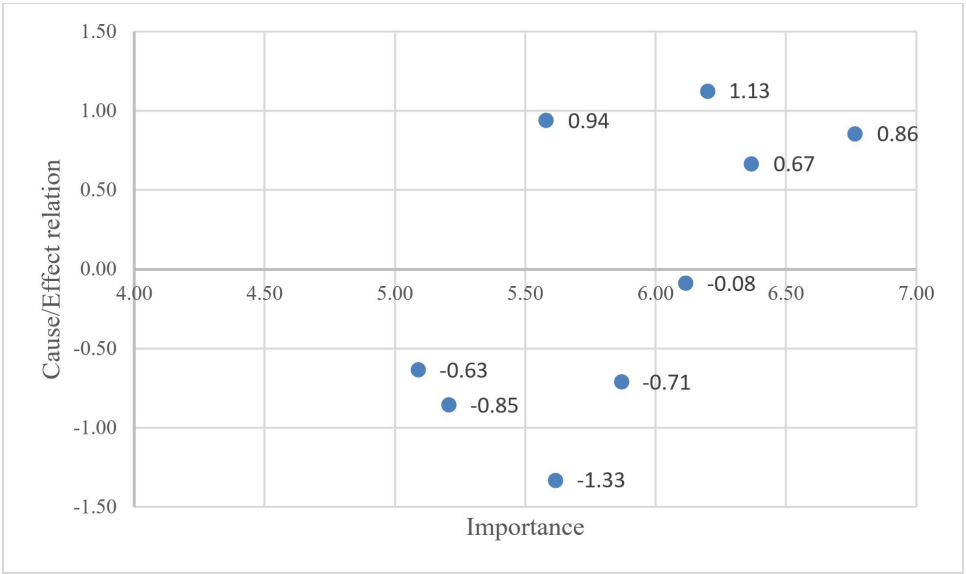

Figure 1. The causality diagram

ICI Bucharest © Copyright 2012-2023. All rights reserved

predominantly influenced by other factors rather than having high influencing power themselves. But Resilience (C_5) is strongly interconnected with other criteria (R^+ = 6.113) and has a relation value that is only slightly negative (R^- = -0.085). These values imply that this criterion is influenced by other criteria (Manageability (C_2), Reliability (C_3), Incident response (C_7) and Compliance (C_9)), but has considerable effects on other criteria (Confidentiality (C_1), Access control (C_4), Tamper protection (C_6) and Decentralization (C_8)). Although it is assigned to the effect group, Resilience criteria plays a decisive role.

The Tamper protection (C_6) criteria has neither strong importance (R^+ = 3.470) nor strong influences on other criteria (R^- = -1.326).

In the next step, the criteria weights are calculated based on Equations (17)-(21). The results are presented in Table 6.

Table 6. The criteria weights

IoT -SR	W	W Ranks	$\bar{W}$	$\bar{W}$ Ranks	$\bar{\bar{W}}$
C_1	0.099	8	0.082	8	0.091
C_2	0.118	3	0.139	2	0.129
C_3	0.120	2	0.133	3	0.127
C_4	0.111	5	0.098	6	0.105
C_5	0.115	4	0.114	5	0.115
C_6	0.108	6	0.081	9	0.095
C_7	0.128	1	0.144	1	0.136
C_8	0.096	9	0.084	7	0.090
C_9	0.106	7	0.124	4	0.115

Both the first and second weighting methods calculate the highest weight for the Incidence Response criterion. The biggest difference (of three positions) is observed for the Compliance (C_9) and Tamper protection (C_6) criteria. This difference is due to the fact that the second method takes into account the minus sign used in the computation of R^- entries. It is also observed that the order obtained with the first weighting method is identical to that obtained by vector R^+ ranks in Table 5.

7. Conclusion

The literature on IoT security is rapidly growing, and concerns a wide range of areas.

The present paper proposes a new Multi-Criteria Weighting Approach with application for IoT security requirements evaluation, influence, weighting and ranking. The approach has been described in steps. An application of the proposed approach was made by studying an illustrative example. The present approach has a simple mathematical form and has the ability to combine with other methods, especially in the part relating to the determination of weight criteria.

The approach finds a set of weights for the selected IoT security requirements, indicating that Incident response has the highest significance weight of 0.128 according to both methods, while Decentralization has the lowest weight (0.096), according to the method 1, and Tamper protection has the lowest weight (0.081), according to the method 2.

The Fuzzy DEMATEL method shows that Manageability, Incident response and Reliability influence other criteria rather than being affected themselves. The results obtained are based on the IoT security requirements assessment. This assessment can vary depending on the security requirements selected for an IoT system and is based on the specific needs and priorities of an organization that produces or uses an IoT system.

The main contributions of the proposed approach are that it enables to prioritize the criteria (weighting methods) and also helps to determine the relationships among them (fuzzy DEMATEL).

The results of the MCWA application can help security specialists to effectively evaluate an IoT system.

Acknowledgements

The research reported in this paper was supported by projects PN 23 38 01 01 “Contributions to the consolidation of emerging technologies specific to the Internet of Things and complex systems” and PN 23 38 04 01 “Resilient and interoperable communication systems based on distributed technologies and self-sovereign digital identity”, funded by the Romanian Core Program of the Ministry of Research, Innovation and Digitization, 2023-2026.

REFERENCES

Aarika, K., Bouhlal, M., Abdelouahid, R. A., Elfilali, S. & Benlahmar, E. (2020) Perception layer security in the internet of things. *Procedia Computer Science*. 175, 591-596. doi: 10.1016/j.procs.2020.07.085.

Akkad, A., Wills, G. & Rezazadeh, A. (2023) An information security model for an IoT-enabled Smart Grid in the Saudi energy sector. *Computers and Electrical Engineering*. 105, 108491. doi: 10.1016/j.compeleceng.2022.108491.

Balakumar, S. & Kavitha, A. R. (2021) Quorum-based blockchain network with IPFS to improve data security in IoT network. *Studies in Informatics and Control*. 30(3), 85-98. doi: 10.24846/v30i3y202108.

Baykasoglu, A., Kaplanoglu, V., Durmusoglu, Z. D. U. & Sahin C. (2013) Integrating Fuzzy DEMATEL and Fuzzy Hierarchical TOPSIS Methods for Truck Selection. *Expert Systems with Applications*. 40(3), 899-907. doi: 10.1016/j.eswa.2012.05.046.

Dalalah, D., Hajaneh, M. & Batieha, F. (2011) A Fuzzy Multi-criteria Decision Making Model for Supplier Selection. *Expert Systems with Applications*. 38(7), 8384-8391. doi: 10.1016/j.eswa.2011.01.031.

Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P. & Kashif Bashir, A. (2022) A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*. 33(6), e3935. doi: 10.1002/ett.3935.

Duraisamy, A., Subramaniam, M. & Robin, C. R. R. (2021) An optimized deep learning based security enhancement and attack detection on IoT using IDS and KH-AES for smart cities. *Studies in Informatics and Control*. 30(2), 121-131. doi: 10.24846/v30i2y202111.

Elhoseny, M., Thilakarathne, N. N., Alghamdi, M. I., Mahendran, R. K., Gardezi, A. A., Weerasinghe, H. & Welhenge, A. (2021) Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. *Sustainability*. 13(21), 11645. doi: 10.3390/su132111645.

Erdene-Ochir, O., Kountouris, A., Minier, M. & Valois, F. (2012) A new metric to quantify resiliency in networking. *IEEE Communications Letters*. 16(10), 1699-1702. doi: 10.1109/LCOMM.2012.081612.121191.

Farooq, U., Tariq, N., Asim, M., Baker, T. & Al-Shamma'a, A. (2022) Machine learning and the Internet of Things security: Solutions and open challenges. *Journal of Parallel and Distributed Computing*. 162, 89-104. doi: 10.1016/j.jpdc.2022.01.015.

Filip, F. G., Zamfirescu, C. B. & Ciurea, C. (2017) *Computer Supported Collaborative Decision- Making*. Cham, Switzerland, Springer International Publishing.

Gabus, A. & Fontela, E. (1972) *World Problems an Invitation to Further Thought within the Framework of DEMATEL*. Geneva, Switzerland, Battelle Geneva Research Center.

Jabangwe, R. & Nguyen-Duc, A. (2020) SIoT Framework: Towards an Approach for Early Identification of Security Requirements for Internet-of-things Applications. *e-Informatica Software Engineering Journal*. 14(1), 77-95. doi: 10.37190/e-Inf200103.

Kaufmann, A. & Gupta, M. M. (1988) *Fuzzy Mathematical Models in Engineering and Management Science*. Netherlands, Elsevier Science Publisher.

Keršuliene, V., Zavadskas, E. K. & Turskis, Z. (2010) Selection of rational dispute resolution method by applying new step-wise weight assessment ratio analysis (SWARA). *Journal of Business Economics and Management*. 11(2), 243-258. doi: 10.3846/jbem.2010.12.

Khan, Y., Su'ud, M. B. M., Alam, M. M., Ahmad, S. F., Salim, N. A. & Khan, N. (2022) Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. *Electronics*. 12(1), 88. doi: 10.3390/electronics12010088.

Kobryń, A. (2017) DEMATEL as a weighting method in multi-criteria decision analysis. *Multiple Criteria Decision Making*. 12, 153-167. doi: 10.22367/mcdm.2017.12.11.

Kumar, A. & Dixit, G. (2018) An analysis of barriers affecting the implementation of e-waste management practices in India: A novel ISM-DEMATEL approach. *Sustainable Production and Consumption*. 14, 36-52. doi: 10.1016/j.spc.2018.01.002.

Lewis, H. W. (1997) *The Foundations of Fuzzy Control*. Part of the International Federation for Systems Research International Series on Systems Science and Engineering book series (IFSR, volume 10). Boston, MA, USA, Springer Science & Business Media.

Liu, Y., Eckert, C. M. & Earl, C. (2020) A review of fuzzy AHP methods for decision-making with subjective judgements. *Expert Systems with Applications*. 161, 113738. doi: 10.1016/j.eswa.2020.113738.

Năstase, L., Sandu, I. E. & Popescu, N. (2017) An experimental evaluation of application layer protocols for the internet of things. *Studies in Informatics and Control*. 26(4), 403-412. doi: 10.24846/v26i4y201704.

ICI Bucharest © Copyright 2012-2023. All rights reserved

Ogonji, M. M., Okeyo, G. & Wafula, J. M. (2020) A survey on privacy and security of Internet of Things. *Computer Science Review*. 38, 100312. doi: 10.1155/2022/5724168.

Opricovic, S. & Tzeng, G.-H. (2004) Compromise solution by MCDM methods: a comparative analysis of VIKOR and TOPSIS. *European Journal of Operation Research*. 156(2), 445–455. doi: 10.1016/S0377-2217(03)00020-1.

Radulescu, C. Z. & Radulescu, M. (2018) Group decision support approach for cloud quality of service criteria weighting. *Studies in Informatics and Control*. 27(3), 275-284. doi: 10.24846/v27i3y201803.

Radulescu, C. Z. (2017) Cloud Provider's Services Evaluation Using Triangular Fuzzy Numbers. In: *2017 21st International Conference on Control Systems and Computer Science* (*CSCS*), *19-21 October 2017*, *Sinaia*, *Romania*. Institute of Electrical and Electronics Engineers Control Systems Society (IEEE). pp. 123-128.

Raj, T., Shankar, R. & Suhaib, M. (2008) An ISM approach for modelling the enablers of flexible manufacturing system: the case for India. *International Journal of Production Research*. 46(24), 6883-6912. doi: 10.1080/00207540701429926.

Rezaei, J. (2015) Best-worst multi-criteria decision-making method. *Omega*. 53, 49-57. doi: 10.1016/j.omega.2014.11.009.

Saaty, T. L. (1977) A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology*. 15(3), 234-281. doi: 10.1016/0022-2496(77)90033-5.

Saaty, T. L. (1980) *The Analytic Hierarchy Process: Planning, Priority Setting, Resources Allocation*. New York, NY, USA, McGraw-Hill Press.

Saaty, T. L. (1996) *Decision Making with Dependence and Feedback: The Analytic Network Process*. 4922(2). Pittsburgh, RWS Publications.

Samaila, M. G., Lopes, C., Aires, É., Sequeiros, J. B., Simoes, T., Freire, M. M. & Inácio, P. R. (2021) Performance evaluation of the SRE and SBPG components of the IoT hardware platform security advisor framework. *Computer Networks*. 199, 108496. doi: 10.1016/j.comnet.2021.108496.

Tsigkanos, C., Nastic, S. & Dustdar, S. (2019) Towards resilient Internet of Things: Vision, challenges and research roadmap. In: *Proceedings of the 2019 39th International Conference on Distributed Computing Systems* (*ICDCS*) *7-9 July 2019*, *Richardson*, *Texas*, *United States*. Institute of Electrical and Electronics Engineers Control Systems Society (IEEE). pp. 1754-1764.

Wu, W. W. & Lee, Y. T. (2007) Developing global managers' competencies using the fuzzy DEMATEL method. *Expert System with Application*. 32(2), 499–507. doi: 10.1016/j.eswa.2005.12.005.

Wu, W. W. (2012) Segmenting critical factors for successful knowledge management implementation using the fuzzy DEMATEL method. *Applied Soft Computing*. 12(1), 527-535. doi: 10.1016/j.asoc.2011.08.008.

Zadeh, L. A. (1965) Fuzzy sets. Information and Control. 8(3), 338–353. doi: 10.1016/S0019-9958(65)90241-X.