An integrated AHP MCDM based Type-2 Neutrosophic Model for Assessing the Effect of Security in Fog-based IoT Framework

Mohammad D. Alshehri

Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
Email: Alshehri@tu.edu.sa

Abstract

The term "Internet of Things" (IoT) refers to a network of connected, intelligent devices that are responsible for the collecting and dissemination of data. Because technology automates the tasks we do daily, our lives have become simpler as a result. However, with a typical architecture for the cloud and the Internet of Things, real-time data processing is not always practicable. This is particularly true for latency-sensitive apps. This eventually resulted in the development of fog computing. On the one hand, the fog layer may perform computations and data processing at the very edge of the network, which enables it to provide results more quickly. On the other hand, this pushes the attack surface closer to the machines themselves, which is a security risk. Because of this, the sensitive data that is stored on the layer is now susceptible to assaults. Therefore, considering the security of the fog-IoT is of the utmost significance. A system or platform's level of security is determined by a number of different elements. When it comes to conducting an accurate risk assessment, the sequence in which these considerations are considered is of the utmost importance. Because of this, determining the level of security offered by fog and IoT devices becomes a Multi-Criteria Decision-Making (MCDM) dilemma. This article presents a two-stage hybrid multi-criteria decision-making model that is based on type-2 neutrosophic numbers (T2NNs). The goal of this article is to give scientists and practitioners a decision-making tool that is both easy and versatile. The initial step of this process is determining the weights of criteria by the AHP method in the T2NN environment. Second, the T2NN-based Multi-Attributive Border Approximation area Comparison (MABAC) method is used to rank the various fog security based on IoT. Both of these methods are described in more detail below. With the help of the comparison study, the high reliability and robustness of the combined AHP and MABAC based type-2 neutrosophic model have been proven.

Keywords: Type-2 Neutrosophic; AHP; IoT and Security.

1. Introduction

It would seem that fog computing is an emerging technology that intensifies cloud computing by placing auxiliary processing, networking facility, and storage facilities close to the ground devices that create and absorb the generated data segments. As the Internet of Things (IoT) network continues to grow and new application areas are developed, an increasingly large amount of data is being generated by the ground IoT devices that are located at the network's edge [1] [2]. When this occurs, it is often not a practical option to send all of the created data to a faraway cloud data centre and expect excellent results in terms of Quality of Service (QoS). This is especially the case in the realm of applications that have demands for low latency. In addition, in a purely cloud-based situation, all of the private and sensitive data that is created by the sensors is uploaded to high-end cloud servers in order to be processed. As a result, the user has very little or no control over the data associated with their account. Therefore, the existence of the evident fog in the scene may be rationalised [3] [5].

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

In a three-layer Fog-IoT design, the middle tier is comprised of a fog layer. This layer makes it possible to handle data in a highly secure manner, and it also provides advantages for apps that are sensitive to latency. Depending on the nature of the application, the fog layer could be responsible for handling part of the processing and computing [6], [7]. The data is processed locally, similar to how fog computing works. As a result, less bandwidth from long-distance networks is used, and the total reaction time is sped up [8] [9]. Additionally, the computation of the data takes place located closer to the epicentre, which helps to restrict the spread of the data. Despite all of these positive aspects, using this technique does come with a few obstacles because everything in the world is flawless [10], [11].

The fog nodes are strategically placed at various locations between the terrestrial device and the cloud, which is the location of all of the business logic [12], [13]. As a result, the fog node is able to access all of the data, whether it is in the form of both the data that is received from the ground equipment and the control data that is delivered back to the devices. In addition to this, they have information on the real source of the data [14]. This introduces a new security flaw since any weakness in the security of the fog layer might put the absolute safety of the IoT system at risk due to the interconnected nature of the devices [15], [16]. The fact that the calculation of the vast majority of the data generated by IoT devices takes place directly at the edge of the network provides further evidence of the seriousness of this issue. It is well acknowledged that security is one of the most significant obstacles to implementing a fog-IoT scenario. As a result, obtaining a firm hold on it is of the biggest significance [17]–[19].

Security in a fog environment is made up of a number of different aspects, all of which need to be taken into consideration when thinking about the system's overall security.

When taken into consideration collectively, these aspects may help to maintain the integrity of the whole system. However, determining the sequence in which they need to be treated is still another significant obstacle that must be overcome. The Multi-Criteria Decision Making (MCDM) strategy is a technique that may be used to handle this problem. The MCDM approach is used to solve situations in which there are several possible paths to take and a variety of points of view from which to assess them. The MCDM method of decision-making takes into consideration both objective and subjective measurement data throughout the process of making decisions. At the beginning of the traditional technique, crisp values were the only ones that were employed for subjective assessment. Later on, in 1965, L. A. Zadeh came up with the fuzzy set theory in order to address the imprecision and uncertainty that arose throughout the decision-making process. In addition to this, it was said that the fuzzy system was only able to cope with the membership function. This was considered to be one of its most significant weaknesses [20], [21].

The fuzzy set theory is founded on the idea of membership function value, with linguistic factors being taken into consideration [22]. This theory attempts to assess confusing data using the views of experts and then matches those judgements with the values of membership functions. Nevertheless, it isn't always the case that expert judgements centre on membership ideals, particularly when there is a lack of knowledge or experience [23]. This is especially the case when In addition, the experts may be certain about the untruthfulness of their views, but not the truthfulness of their statements. Smarandache devised the neutrosophic set theory intending to resolve various decision-making scenarios that occurred in actual life. The fuzzy theory and the intuitionistic fuzzy set both contributed to the development of neutrosophic sets (IFS). Neutrosophic numbers have established themselves as a legitimate area of research, which enables one to recognise conflicting and indefinite data [24] [25]. The representation of type-1 neutrosophic numbers is a triplet that consists of the letters T, I, and F, with each letter originating from the interval [0, 1]. They are referred to as a membership value, also known as the truth value (T), a neutral value, also known as the indeterminacy real worth (I), and a non-membership value, also known as the falsity value (F). $(T_T, T_I, T_F), (I_T, I_I, I_F), and\ (F_T, F_I, F_F)$ are the forms that are used to describe T2NN. This means that each neutrosophic component is broken down into its truth, indeterminacy, and falsity subparts. The T2NN methodology is a more sophisticated form of the neutrosophic approach. It is an effective strategy for dealing with the imprecision or incompleteness of the experts' statements. Unfortunately, none of the prior research has offered a T2NN-based framework to predict the different pricing regimes for transportation.

Calculating the relevance of assessment criteria and ranking the many alternatives by the expansion of the AHP [24]–[28] and MABAC methodologies in the context of the T2NN system, correspondingly [29], [30].

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

Pamuar and iroviç presented the exceptional MCDM approach known as the MABAC method. The MABAC approach is a dependable instrument that may be used to make reasonable decisions [22], [31], [32]. It takes into account every conceivable aspect of the possible values of both profits and losses. The distance that separates each option from the region that serves as an estimate of the border is one of the most important tenets of the MABAC approach [33]–[35]. This method's mathematical procedure is straightforward, rational, and very systematic. The MABAC method has been extended to work in a variety of environments where there is a high degree of uncertainty [20], [21], [23].

By developing an easy and adaptable decision-making instrument, the purpose of this research is to assist in the impact of fog security in IoT. In light of this, the research indicates that a hybrid two-stage type-2 neutrosophic model should be constructed in order to answer the multi-criteria decision-making (MCDM) issue that was presented. The first step of the process involves computing the weights of criteria by a type-2 neutrosophic number (T2NN). During the second stage, the T2NN-based AHP method is used to evaluate the importance of the criteria, and the T2NN-based Multi-Attributive Border Approximation area Comparison (MABAC) technique is used to rank the different Fog security.

2. Problem Definition

The issue of security is often regarded as the most significant barrier to overcome before the widespread adoption of Internet of Things services and technology. When opposed to traditional IT systems, the Internet of Things' combination of physical and technological elements makes the prevalence of security vulnerabilities much greater than it already was. Because of the development of Fog computing, data is now handled at locations that are geographically closer to its points of origin. The fact that it is, as described above, makes it much more vulnerable to breaches of security. Data breaches have the potential to reveal the sensitive data of customers straightforwardly. The security assaults may even be able to interfere with the real operation of the IoT-enabled equipment, which may lead to a scenario that poses a risk to users' lives.
It has been hypothesised that fog computing will emerge as the primary support system for the Internet of Things (IoT) in the not-too-distant future. Inevitably, the consequence that stems from this merging is that the security component has to be designated high on the priority list to assure the successful delivery of this merger. This may be done by marking it as one of the highest priorities. Penetration testing, identification, trust management, privacy, and other related topics are among the most common concerns about this body's security.

The fact that fog nodes are tiny data handlers that are dispersed over a broad geographical region and are difficult to safeguard physically is the major challenge for fog computing. When taking into consideration the data that is created as a result of the nodes, it is necessary to first check the legitimacy of the nodes. The primary purpose of this contribution is to cut down on the amount of work that has to be done in order to prioritise the many aspects of security.
It's possible that using a security rating in a fog-IoT environment can help you improve security at the appropriate time.
The authors of this research have discovered many security variables and subfactors that are associated with the Fog-IoT environment. Several aspects of Fog-IoT security are taken into consideration, such as Authentication, Access Control, Penetration Testing, Trust, and Integrity, which are to be employed to strengthen the overall security of the Fog-IoT ecosystem. Table 1 shows the definition of the selected criteria. Figure 1 shows the hierarchy of the selected criteria.

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

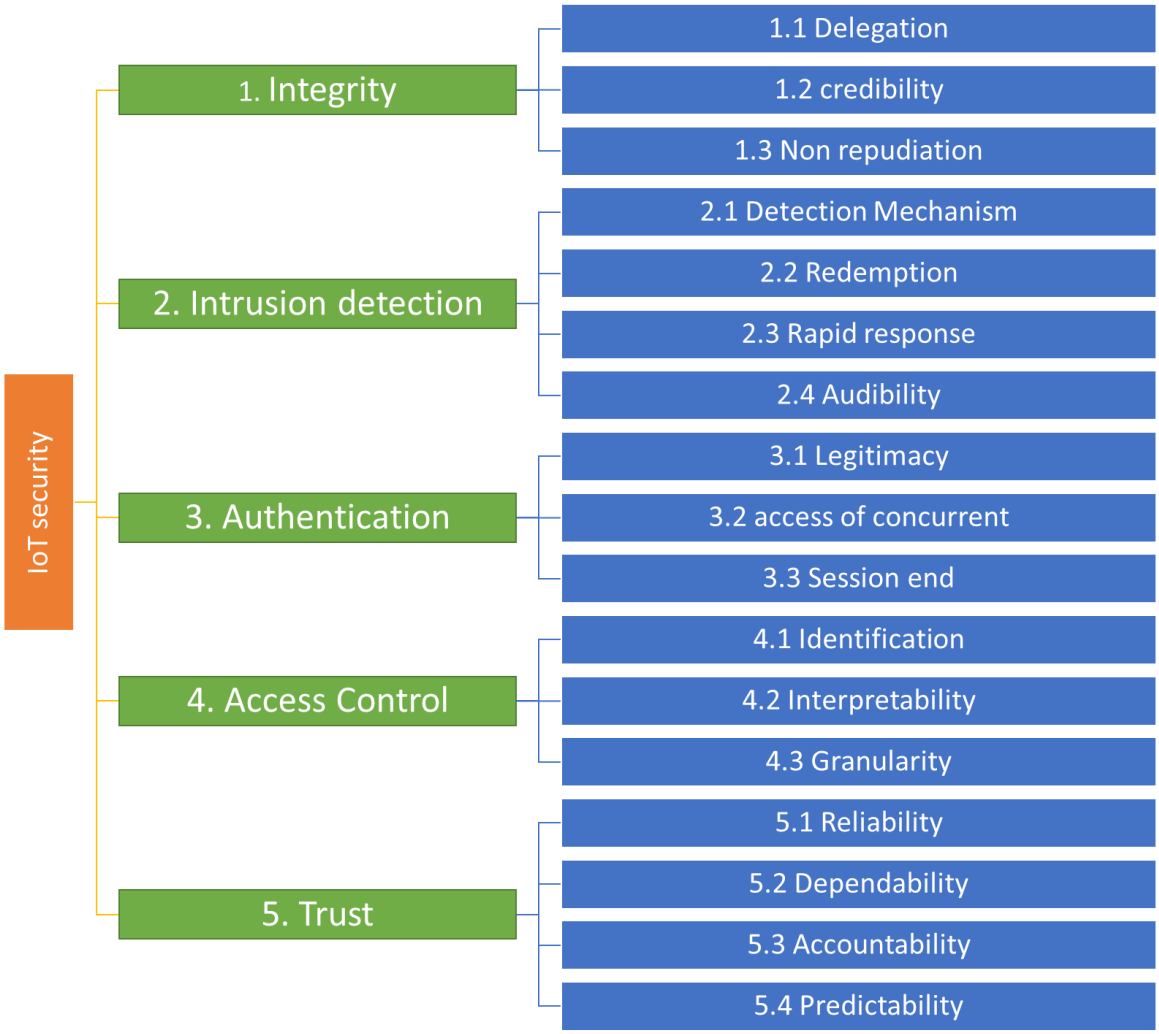

Figure 1: The hierarchy tree of the main and sub-criteria.

Table 1: The definition of main and sub-criteria [36].

Criteria	Sub criteria	Definition
1. Integrity	1.1 Delegation 1.2 Credibility 1.3 Non-repudiation	Integrity in the context of the Fog-IoT environment refers to verifying that the data produced out of IoT systems has not been modified from its original state. In order to maintain data integrity, information must be received at the receiving end exactly as it was sent by the sending end. In the case of the Fog-IoT paradigm, in which the data is created at a tremendous pace, one might reasonably anticipate that the data will be accurate. In healthcare IoT situations the minutest tampering can put someone's life in jeopardy. Thus, there is a critical necessity to address integrity to assuring security in the Fog-IoT situation. **1.1 Delegation** The act of giving another node more responsibility for something by delegating that responsibility to that node is known as delegation. This particular sub-factor has a very major influence on the system's overall integrity. **1.2 Credibility** Credibility in integrity is the degree to which nodes that are transporting data can be relied upon and trusted regarding the data that they are transporting and transmitting. **1.3 Non-repudiation**

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

		When discussing data integrity, the phrase "non-repudiation" refers to the capacity of a node to ensure that the data it has transmitted cannot be denied.
2. Intrusion detection	2.1 Detection Mechanism 2.2 Redemption 2.3 Rapid Response 2.4 Audibility	Intrusion Detection Systems, often known as IDS, are typically installed in a computer network in order to protect it from a variety of threats, such as insider assaults, port scanning attacks, an attack on virtualization machines, and many more. In a fog computing environment, an intrusion detection system (IDS) may be implemented to analyse log files, login patterns, and rules relevant to access control. In order to identify these types of covert assaults, the system has to be continuously monitored and subjected to behavioural analysis. Therefore, a safety monitoring system that is both precise and quick may avert security dangers that develop as a result of infiltration. **2.1 Detection Mechanism** Because early detection may lead to the development of a defence that is both quicker and more effective, the detection technique used in the case of intrusion detection has to be very quick. **2.2 Redemption** When we talk about systems having "redemption," we imply that if they are compromised in any way, they should be able to bounce back to their original condition as soon as possible. **2.3 Rapid Response** Response speed and detection accuracy are of the highest importance if intrusion detection is performed. **2.4 Audibility** Auditability is a concept that refers to the examination of the evidence of harmful behaviour at the time of presentation. It is used in the context of intrusion detection.
3. Authentication	3.1 Legitimacy 3.2 Access to concurrent 3.3 Session end	Since IoT services are provided to a large number of end customers by front fog nodes, identification is the most important issue that needs to be taken into consideration to guarantee data safety in a Fog-IoT context. Authentication is seen as a significant security risk by a number of scientists working at a variety of fog node levels. Identification was not given a lot of thought in the early stages of the Internet of Things design, which consisted mostly of feeding data straight into cloud servers. On the other hand, the introduction of a fog layer in the centre has led to a rise in the number of fog nodes that are scattered throughout a large geographical region, which has led to an increase in the difficulty of authenticating users. The standard Public Key Network cannot be used since it offers lower levels of efficiency and worse levels of scalability. Identification may be controlled by identifying its component parts and then focusing on those parts individually. **3.1 Legitimacy** When it comes to authentication, legitimacy is a quality that determines whether or not access is granted following what is reasonable and acceptable. **3.2 access to concurrent** It is the capability of allowing several users or processes to log in at the same time to a computer system. When it comes to the authentication of the system, a failure in the management of this sub-factor might have a direct impact. **3.3 Session ending** Because it is required to dissolve the connection at a specific point in time, the session ending serves a crucial function in

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

		managing the system's validity. This is because the session must be terminated at a certain point in time.
4. Access Control	4.1 Identification 4.2 Interpretability 4.3 Granularity	Users are often required to pay for the services they make use of when fog computing is involved. Because of this, there is an extremely low level of trust among them. Three different sorts of entries are feasible in the situation, based on the fundamental structure of the Fog-IoT, and those include user-fog/cloud access, fog-cloud connects directly, and access among the distributed virtualization. Therefore, in light of the data presented above, it is possible to draw the conclusion that the authentication process in fog computing plays an essential part in guaranteeing the safety of the whole system. **4.1 Identification** Identification, in the context of access control, refers to the process through which a user's access may be recognised as and when it is required. **4.2 Interpretability** It is described as the capacity to integrate into a system without causing any kind of disruption to the natural environment that is already there. Interoperability brings about changes to the access condition, which in turn affects the security component. **4.3 Granularity** Granularity refers to the ability to access the smallest piece of data that is included inside a database. Only the user with proper authorization may access this site.
5. Trust	5.1 Reliability 5.2 Dependability 5.3 Accountability 5.4 Predictability	The decentralised system's most fundamental component is trust in its users. Because of the lack of overall system security, it is impossible to place complete faith in the individual computing units that make up a distributed system. Therefore, a trust assessment is of the highest necessity in order to guarantee safe and effective communication. Given the diversity of the nodes, the trust mechanism that was used in the cloud environment is unable to be immediately adapted to the Fog-IoT environment. As a result, in order to address concerns about dependability and security, an effective trust model is essential. **5.1 Reliability** The term "reliability" refers to the degree to which the fog node can be relied on to provide accurate results as a result of the way it behaves. **5.2 Dependability** Dependability may be defined as the quality of being able to be relied upon to be accountable for carrying out its designated functions in the context of trust. **5.3 Accountability** When we talk about accountability, we imply that each individual node in the fog network needs to have genuine obligations for security confirmation. **5.4 Predictability** When discussing reliability, the word "predictability" refers to the ability of a node to be anticipated in order to estimate its behaviour throughout the normal communication procedure in a fog environment.

3. Methodology

In this part, some preliminary information is presented, as well as the hybrid type-2 neutrosophic model for evaluation impact of fog security based on IoT.

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

3.1 Preliminaries

Definition 1 [37]

Let K stand for the confined space where the conversation is allowed, and let F[0,1] the set of all triangular neutrosophic numbers represent it F[0,1]. In Z, the symbol that stands for a type 2 neutrosophic number set (T2NNS) is R. $\check{R} = \{\langle k, \check{T}_{\check{R}}(k), \check{I}_{\check{R}}(k), \check{F}_{\check{R}}(k), k \in K\rangle\}$ where $\check{T}_{\check{R}}(k): K \to F[0,1], \check{I}_{\check{R}}(k): K \to F[0,1], \check{F}_{\check{R}}(k): K \to F[0,1]$. T2NNS $\check{T}_{\check{Q}}(k) = \left(\check{T}_{\check{T}_{\check{R}}}(k), \check{T}_{\check{I}_{\check{R}}}(k), \check{T}_{\check{F}_{\check{R}}}(k)\right)$, $\check{I}_{\check{Q}}(k) = \left(\check{I}_{\check{T}_{\check{R}}}(k), I_{\check{I}_{\check{R}}}(k), \check{I}_{\check{F}_{\check{R}}}(k)\right)$, $\check{F}_{\check{Q}}(k) = \left(\check{F}_{\check{T}_{\check{R}}}(k), \check{F}_{\check{I}_{\check{R}}}(k), \check{F}_{\check{F}_{\check{R}}}(k)\right)$ named truth, indeterminacy, and falsity memberships of k in R for each $k \in K: 0 \le \check{T}_{\check{R}}(k)^3 + \check{I}_{\check{R}}(k)^3 + \check{F}_{\check{R}}(k)^3 \le 3$, Let $\check{R} = \langle\left(\left(\check{T}_{\check{T}_{\check{R}}}(k), \check{T}_{\check{I}_{\check{R}}}(k), \check{T}_{\check{F}_{\check{R}}}(k)\right), \left(\check{I}_{\check{T}_{\check{R}}}(k), I_{\check{I}_{\check{R}}}(k), \check{I}_{\check{F}_{\check{R}}}(k)\right), \left(\check{F}_{\check{T}_{\check{R}}}(k), \check{F}_{\check{I}_{\check{R}}}(k), \check{F}_{\check{F}_{\check{R}}}(k)\right)\right)\rangle$ refers to a type-2 neutrosophic number.

Definition 2[37]

Consider $\check{R}_1 = \langle\left(\left(\check{T}_{\check{T}_{\check{R}_1}}(k), \check{T}_{\check{I}_{\check{R}_1}}(k), \check{T}_{\check{F}_{\check{R}_1}}(k)\right), \left(\check{I}_{\check{T}_{\check{R}_1}}(k), I_{\check{I}_{\check{R}_1}}(k), \check{I}_{\check{F}_{\check{R}_1}}(k)\right), \left(\check{F}_{\check{T}_{\check{R}_1}}(k), \check{F}_{\check{I}_{\check{R}_1}}(k), \check{F}_{\check{F}_{\check{R}_1}}(k)\right)\right)\rangle$ and

$\check{R}_2 = \langle\left(\left(\check{T}_{\check{T}_{\check{R}_2}}(k), \check{T}_{\check{I}_{\check{R}_2}}(k), \check{T}_{\check{F}_{\check{R}_2}}(k)\right), \left(\check{I}_{\check{T}_{\check{R}_2}}(k), I_{\check{I}_{\check{R}_2}}(k), \check{I}_{\check{F}_{\check{R}_2}}(k)\right), \left(\check{F}_{\check{T}_{\check{R}_2}}(k), \check{F}_{\check{I}_{\check{R}_2}}(k), \check{F}_{\check{F}_{\check{R}_2}}(k)\right)\right)\rangle$ are two T2NNS then there are some operations in this numbers

$$\check{R}_1 \oplus \check{R}_2 = \begin{pmatrix} \begin{pmatrix} \check{T}_{\check{T}_{\check{R}_1}}(k) + \check{T}_{\check{T}_{\check{R}_2}}(k) - \check{T}_{\check{T}_{\check{R}_1}}(k) \cdot \check{T}_{\check{T}_{\check{R}_2}}(k), \\ \check{T}_{I_{\check{R}_1}}(k) + \check{T}_{I_2}(k) - \check{T}_{I_{\check{R}_1}}(k) \cdot \check{T}_{I_{\check{R}_2}}(k), \\ \check{T}_{\check{F}_{\check{R}_1}}(k) + \check{T}_{\check{F}_{\check{R}_2}}(k) - \check{T}_{\check{F}_{\check{R}_1}}(k) \cdot \check{T}_{\check{F}_{\check{R}_2}}(k) \end{pmatrix}, \\ \left(\check{I}_{\check{T}_{\check{R}_1}}(k) \cdot \check{I}_{\check{T}_{\check{R}_2}}(k), I_{\check{I}_{\check{R}_1}}(k) \cdot I_{\check{I}_{\check{R}_2}}(k), \check{I}_{\check{F}_{\check{R}_1}}(k) \cdot \check{I}_{\check{F}_{\check{R}_2}}(k)\right), \\ \left(\check{F}_{\check{T}_{\check{R}_1}}(k) \cdot \check{F}_{\check{T}_2}(k), \check{F}_{\check{I}_{\check{R}_1}}(k) \cdot \check{F}_{\check{I}_{\check{R}_2}}(k), \check{F}_{\check{F}_{\check{R}_1}}(k) \cdot \check{F}_{\check{F}_{\check{R}_2}}(k)\right) \end{pmatrix} \quad (1)$$

$$\check{R}_1 \otimes \check{R}_2 = \begin{pmatrix} \left(\check{T}_{\check{T}_{\check{R}_1}}(k) \cdot \check{T}_{\check{T}_{\check{R}_1}}(k), \check{T}_{\check{I}_{\check{R}_1}}(k) \cdot \check{T}_{\check{I}_{\check{R}_1}}(k), \check{T}_{\check{F}_{\check{R}_1}}(k) \cdot \check{T}_{\check{F}_{\check{R}_1}}(k)\right), \\ \begin{pmatrix} \check{I}_{\check{T}_{\check{R}_1}}(k) + \check{I}_{\check{T}_{\check{R}_2}}(k) - \check{I}_{\check{T}_{\check{R}_1}}(k) \cdot \check{I}_{\check{T}_{\check{R}_2}}(k), \\ I_{\check{I}_{\check{R}_1}}(k) + I_{\check{I}_{\check{R}_2}}(k) - I_{\check{I}_{\check{R}_1}}(k) \cdot I_{\check{I}_{\check{R}_2}}(k), \\ \check{I}_{\check{F}_{\check{R}_1}}(k) + \check{I}_{\check{F}_{\check{R}_2}}(k) - \check{I}_{\check{F}_{\check{R}_1}}(k) \cdot \check{I}_{\check{F}_{\check{R}_2}}(k) \end{pmatrix}, \\ \begin{pmatrix} \check{F}_{\check{T}_{\check{R}_1}}(k) + \check{F}_{\check{T}_{\check{R}_2}}(k) - \check{F}_{\check{T}_{\check{R}_1}}(k) \cdot \check{F}_{\check{T}_2}(k), \\ \check{F}_{\check{I}_{\check{R}_1}}(k) + \check{F}_{\check{I}_{\check{R}_2}}(k) - \check{F}_{\check{I}_{\check{R}_1}}(k) \cdot \check{F}_{\check{I}_{\check{R}_2}}(k) \\ \check{F}_{\check{F}_{\check{R}_1}}(k) + \check{F}_{\check{F}_{\check{R}_2}}(k) - \check{F}_{\check{F}_{\check{R}_1}}(k) \cdot \check{F}_{\check{F}_{\check{R}_2}}(k) \end{pmatrix} \end{pmatrix} \quad (2)$$

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

$$\vartheta\breve{R}_1 = \begin{pmatrix} \left(1-\left(1-\breve{T}_{\breve{T}_{\breve{R}_1}}(k)\right)^{\vartheta}, 1-\left(1-\breve{T}_{\breve{I}_{\breve{R}_1}}(k)\right)^{\vartheta}, 1-\left(1-\breve{T}_{\breve{F}_{\breve{R}_1}}(k)\right)^{\vartheta}\right), \\ \left(\left(\breve{I}_{\breve{T}_{\breve{R}_1}}(k)\right)^{\vartheta}, \left(I_{\breve{I}_{\breve{R}_1}}(k)\right)^{\vartheta}, \left(\breve{I}_{\breve{F}_{\breve{R}_1}}(k)\right)^{\vartheta}\right), \\ \left(\left(\breve{F}_{\breve{T}_{\breve{R}_1}}(k)\right)^{\vartheta}, \left(\breve{F}_{\breve{I}_{\breve{R}_1}}(k)\right)^{\vartheta}, \left(\breve{F}_{\breve{F}_{\breve{R}_1}}(k)\right)^{\vartheta}\right) \end{pmatrix} \quad (3)$$

$$\breve{R}_1^{\vartheta} = \begin{pmatrix} \left(\left(\breve{T}_{\breve{T}_{\breve{R}_1}}(k)\right)^{\vartheta}, \left(\breve{T}_{\breve{I}_{\breve{R}_1}}(k)\right)^{\vartheta}, \left(\breve{T}_{\breve{F}_{\breve{R}_1}}(k)\right)^{\vartheta}\right), \\ \left(1-\left(1-\breve{I}_{\breve{T}_{\breve{R}_1}}(k)\right)^{\vartheta}, 1-\left(1-I_{\breve{I}_{\breve{R}_1}}(k)\right)^{\vartheta}, 1-\left(1-\breve{I}_{\breve{F}_{\breve{R}_1}}(k)\right)^{\vartheta}\right), \\ \left(1-\left(1-\breve{F}_{\breve{T}_{\breve{R}_1}}\right)^{\vartheta}, 1-\left(1-\breve{F}_{\breve{I}_{\breve{R}_1}}(k)\right)^{\vartheta}, 1-\left(1-\breve{F}_{\breve{F}_{\breve{R}_1}}(k)\right)^{\vartheta}\right) \end{pmatrix} for\ \vartheta > 0 \quad (4)$$

Definition 3[37]

$$\breve{R}_1 \oplus \breve{R}_2 = \breve{R}_2 \oplus \breve{R}_1, \breve{R}_1 \otimes \breve{R}_2 = \breve{R}_2 \otimes \breve{R}_1 \quad (5)$$

$$\vartheta\left(\breve{R}_1 \oplus \breve{R}_2\right) = \widetilde{\vartheta R}_1 \oplus \widetilde{\vartheta R}_2, \left(\breve{R}_1 \otimes \breve{R}_2\right)^{\vartheta} = \breve{R}_1^{\vartheta} \otimes \breve{R}_2^{\vartheta} \quad (6)$$

$$\vartheta_1\breve{R}_1 \oplus \vartheta_2\breve{R}_2 = (\vartheta_1+\vartheta_2)\breve{R}_1, \breve{R}_1^{\vartheta_1} \oplus \breve{R}_1^{\vartheta_2} = \breve{R}_1^{(\vartheta_1+\vartheta_2)} \quad (7)$$

Definition 4 [37]

The score function can be computed as:

$$S(\breve{R}_1) = \frac{1}{12}\begin{pmatrix} 8+\left(\breve{T}_{\breve{T}_{\breve{R}_1}}(k)+2\left(\breve{T}_{\breve{I}_{\breve{R}_1}}(k)\right)+\breve{T}_{\breve{F}_{\breve{R}_1}}(k)\right)- \\ \left(\breve{I}_{\breve{T}_{\breve{R}_1}}(k)+2\left(\breve{I}_{\breve{I}_{\breve{R}_1}}(k)\right)+\breve{I}_{\breve{F}_{\breve{R}_1}}(k)\right)- \\ \left(F_{\breve{T}_{\breve{R}_1}}(k)+2\left(\breve{F}_{\breve{I}_{\breve{R}_1}}(k)\right)+\breve{F}_{\breve{F}_{\breve{R}_1}}(k)\right) \end{pmatrix} \quad (8)$$

$$A(\breve{R}_1) = \frac{1}{4}\begin{pmatrix} \left(\breve{T}_{\breve{T}_{\breve{R}_1}}(k)+2\left(\breve{T}_{\breve{I}_{\breve{R}_1}}(k)\right)+\breve{T}_{\breve{F}_{\breve{R}_1}}(k)\right)- \\ \left(F_{\breve{T}_{\breve{R}_1}}(k)+2\left(\breve{F}_{\breve{I}_{\breve{R}_1}}(k)\right)+\breve{F}_{\breve{F}_{\breve{R}_1}}(k)\right) \end{pmatrix} \quad (9)$$

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

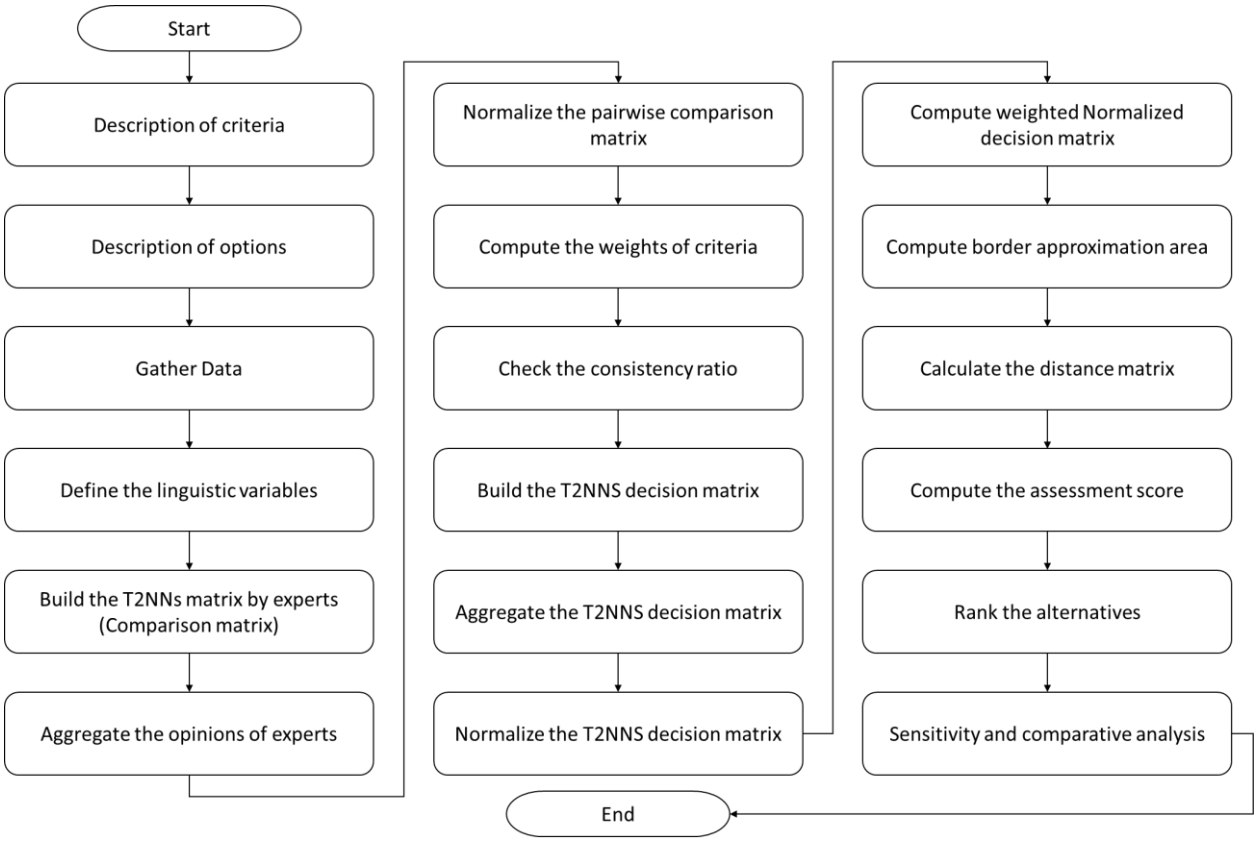

Figure 2: The steps of the methodology.

3.2 An Integrated Type-2 Neutrosophic Model

The flowchart of the mixed type-2 neutrosophic approach for the evaluation of fog security based on IoT is shown in Figure 2. The model consists of two distinct phases. In the first step, the reputation of the requested experts is evaluated within the context of the T2NNs network by making a trade-off between their level of experience and level of knowledge. To tackle the MCDM issue that has been explored, the second step entails the formulation of a strategy known as the T2NNs-AHP-MABAC technique. To provide more clarification, the brand-new T2NNs-AHP approach is utilised to determine the relevance of the criterion, while the brand-new T2NNs-MABAC method is put to use in order to rank the available options.

1. Build the pairwise comparison matrix by the opinions of experts

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

$$D=\begin{pmatrix}\begin{bmatrix}\left(\left(\check{T}_{\check{R}_1^{(1)}}(k),\check{T}_{\check{I}_{\check{R}_1^{(1)}}}(k),\check{T}_{\check{F}_{\check{R}_1^{(1)}}}(k)\right),\\ \left(\check{I}_{\check{T}_{\check{R}_1^{(1)}}}(k),I_{\check{I}_{\check{R}_1^{(1)}}}(k),\check{I}_{\check{F}_{\check{R}_1^{(1)}}}(k)\right),\\ \left(\check{F}_{\check{T}_{\check{R}_1^{(1)}}}(k),\check{F}_{\check{I}_{\check{R}_1^{(1)}}}(k),\check{F}_{\check{F}_{\check{R}_1^{(1)}}}(k)\right)\end{bmatrix} & \cdots & \begin{bmatrix}\left(\left(\check{T}_{\check{T}_{\check{R}_1^{(1)}}}(k),\check{T}_{\check{I}_{\check{R}_1^{(1)}}}(k),\check{T}_{\check{F}_{\check{R}_1^{(1)}}}(k)\right),\\ \left(\check{I}_{\check{T}_{\check{R}_1^{(1)}}}(k),I_{\check{I}_{\check{R}_1^{(1)}}}(k),\check{I}_{\check{F}_{\check{R}_1^{(1)}}}(k)\right),\\ \left(\check{F}_{\check{T}_{\check{R}_1^{(1)}}}(k),\check{F}_{\check{I}_{\check{R}_1^{(1)}}}(k),\check{F}_{\check{F}_{\check{R}_1^{(1)}}}(k)\right)\end{bmatrix}\\ \vdots & \ddots & \vdots\\ \begin{bmatrix}\left(\left(\check{T}_{\check{T}_{\check{R}_1^{(2)}}}(k),\check{T}_{\check{I}_{\check{R}_1^{(2)}}}(k),\check{T}_{\check{F}_{\check{R}_1^{(2)}}}(k)\right),\\ \left(\check{I}_{\check{T}_{\check{R}_1^{(2)}}}(k),I_{\check{I}_{\check{R}_1^{(2)}}}(k),\check{I}_{\check{F}_{\check{R}_1^{(2)}}}(k)\right),\\ \left(\check{F}_{\check{T}_{\check{R}_1^{(2)}}}(k),\check{F}_{\check{I}_{\check{R}_1^{(2)}}}(k),\check{F}_{\check{F}_{\check{R}_1^{(2)}}}(k)\right)\end{bmatrix} & \cdots & \begin{bmatrix}\left(\left(\check{T}_{\check{T}_{\check{R}_1^{(2)}}}(k),\check{T}_{\check{I}_{\check{R}_1^{(2)}}}(k),\check{T}_{\check{F}_{\check{R}_1^{(2)}}}(k)\right),\\ \left(\check{I}_{\check{T}_{\check{R}_1^{(2)}}}(k),I_{\check{I}_{\check{R}_1^{(2)}}}(k),\check{I}_{\check{F}_{\check{R}_1^{(2)}}}(k)\right),\\ \left(\check{F}_{\check{T}_{\check{R}_1^{(2)}}}(k),\check{F}_{\check{I}_{\check{R}_1^{(2)}}}(k),\check{F}_{\check{F}_{\check{R}_1^{(2)}}}(k)\right)\end{bmatrix}\end{pmatrix}$$

Where $\check{T}_{\check{T}_{\check{R}_1^{(1)}}}(k)$ refers to the first expert and $\check{T}_{\check{T}_{\check{R}_1^{(2)}}}(k)$ refers to the second expert

2. Replace the opinions of experts by the linguistic type 2 scale [37]

3. Aggregate the pairwise comparison matrix into one matrix as

$$X=\begin{pmatrix}\begin{bmatrix}\left(\left(\check{T}_{\check{T}_{\check{R}_1}}(k),\check{T}_{\check{I}_{\check{R}_1}}(k),\check{T}_{\check{F}_{\check{R}_1}}(k)\right),\\ \left(\check{I}_{\check{T}_{\check{R}_1}}(k),I_{\check{I}_{\check{R}_1}}(k),\check{I}_{\check{F}_{\check{R}_1}}(k)\right),\\ \left(\check{F}_{\check{T}_{\check{R}_1}}(k),\check{F}_{\check{I}_{\check{R}_1}}(k),\check{F}_{\check{F}_{\check{R}_1}}(k)\right)\end{bmatrix} & \cdots & \begin{bmatrix}\left(\left(\check{T}_{\check{T}_{\check{R}_1}}(k),\check{T}_{\check{I}_{\check{R}_1}}(k),\check{T}_{\check{F}_{\check{R}_1}}(k)\right),\\ \left(\check{I}_{\check{T}_{\check{R}_1}}(k),I_{\check{I}_{\check{R}_1}}(k),\check{I}_{\check{F}_{\check{R}_1}}(k)\right),\\ \left(\check{F}_{\check{T}_{\check{R}_1}}(k),\check{F}_{\check{I}_{\check{R}_1}}(k),\check{F}_{\check{F}_{\check{R}_1}}(k)\right)\end{bmatrix}\\ \vdots & \ddots & \vdots\\ \begin{bmatrix}\left(\left(\check{T}_{\check{T}_{\check{R}_1}}(k),\check{T}_{\check{I}_{\check{R}_1}}(k),\check{T}_{\check{F}_{\check{R}_1}}(k)\right),\\ \left(\check{I}_{\check{T}_{\check{R}_1}}(k),I_{\check{I}_{\check{R}_1}}(k),\check{I}_{\check{F}_{\check{R}_1}}(k)\right),\\ \left(\check{F}_{\check{T}_{\check{R}_1}}(k),\check{F}_{\check{I}_{\check{R}_1}}(k),\check{F}_{\check{F}_{\check{R}_1}}(k)\right)\end{bmatrix} & \cdots & \begin{bmatrix}\left(\left(\check{T}_{\check{T}_{\check{R}_1}}(k),\check{T}_{\check{I}_{\check{R}_1}}(k),\check{T}_{\check{F}_{\check{R}_1}}(k)\right),\\ \left(\check{I}_{\check{T}_{\check{R}_1}}(k),I_{\check{I}_{\check{R}_1}}(k),\check{I}_{\check{F}_{\check{R}_1}}(k)\right),\\ \left(\check{F}_{\check{T}_{\check{R}_1}}(k),\check{F}_{\check{I}_{\check{R}_1}}(k),\check{F}_{\check{F}_{\check{R}_1}}(k)\right)\end{bmatrix}\end{pmatrix}$$

4. Normalize the pairwise comparison matrix

5. Convert the T2NNs into a crisp value by Eq. (8)

6. Compute the weights of criteria

7. Check the consistency ratio

$$CR=\frac{CI}{RI}$$

$$CI=\frac{lambda-n}{n-1}$$

Where CI refers to the consistency index and RI refers to random index

8. Build the decision matrix by the criteria and alternatives

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

$$M = \begin{pmatrix} \left[\left(\left(\check{T}_{\check{T}_{\check{R}_{11}^{(1)}}}(k), \check{T}_{\check{I}_{\check{R}_{11}^{(1)}}}(k), \check{T}_{\check{F}_{\check{R}_{11}^{(1)}}}(k)\right), \left(\check{I}_{\check{T}_{\check{R}_{11}^{(1)}}}(k), I_{\check{I}_{R1_1^{(1)}}}(k), \check{I}_{\check{F}_{\check{R}_{11}^{(1)}}}(k)\right), \left(\check{F}_{\check{T}_{\check{R}_{11}^{(1)}}}(k), \check{F}_{\check{I}_{\check{R}_{11}^{(1)}}}(k), \check{F}_{\check{F}_{\check{R}_{11}^{(1)}}}(k)\right)\right) \cdots \left(\left(\check{T}_{\check{T}_{\check{R}_{1n}^{(1)}}}(k), \check{T}_{\check{I}_{\check{R}_{1n}^{(1)}}}(k), \check{T}_{\check{F}_{\check{R}_{1n}^{(1)}}}(k)\right), \left(\check{I}_{\check{T}_{\check{R}_{1n}^{(1)}}}(k), I_{\check{I}_{\check{R}_{1n}^{(1)}}}(k), \check{I}_{\check{F}_{\check{R}_{1n}^{(1)}}}(k)\right), \left(\check{F}_{\check{T}_{\check{R}_{1n}^{(1)}}}(k), \check{F}_{\check{I}_{\check{R}_{1n}^{(1)}}}(k), \check{F}_{\check{F}_{\check{R}_{1n}^{(1)}}}(k)\right)\right) \\ \vdots \quad \ddots \quad \vdots \\ \left(\left(\check{T}_{\check{T}_{\check{R}_{m1}^{(2)}}}(k), \check{T}_{\check{I}_{\check{R}_{m1}^{(2)}}}(k), \check{T}_{\check{F}_{\check{R}_{m1}^{(2)}}}(k)\right), \left(\check{I}_{\check{T}_{\check{R}_{m1}^{(2)}}}(k), I_{\check{I}_{\check{R}_{m1}^{(2)}}}(k), \check{I}_{\check{F}_{\check{R}_{m1}^{(2)}}}(k)\right), \left(\check{F}_{\check{T}_{\check{R}_{m1}^{(2)}}}(k), \check{F}_{\check{I}_{\check{R}_{m1}^{(2)}}}(k), \check{F}_{\check{F}_{\check{R}_{m1}^{(2)}}}(k)\right)\right) \cdots \left(\left(\check{T}_{\check{T}_{\check{R}_{mn}^{(2)}}}(k), \check{T}_{\check{I}_{\check{R}_{mn}^{(2)}}}(k), \check{T}_{\check{F}_{\check{R}_{mn}^{(2)}}}(k)\right), \left(\check{I}_{\check{T}_{\check{R}_{mn}^{(2)}}}(k), I_{\check{I}_{\check{R}_{mn}^{(2)}}}(k), \check{I}_{\check{F}_{\check{R}_{mn}^{(2)}}}(k)\right), \left(\check{F}_{\check{T}_{\check{R}_{mn}^{(2)}}}(k), \check{F}_{\check{I}_{\check{R}_{mn}^{(2)}}}(k), \check{F}_{\check{F}_{mn_1^{(2)}}}(k)\right)\right)\right] \end{pmatrix}$$

Where m refers to the alternatives and n refers to the criteria. The experts used the linguistic terms [37] to evaluate the criteria and alternatives and build the decision matrix.

9. Aggregate the T2NNS decision matrix

$$G = \left(\begin{array}{c} \left(\left(1 - \prod_{d=1}^{D}\left(1 - \check{T}_{\check{T}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta}\right), \left(1 - \prod_{d=1}^{D}\left(1 - \check{T}_{\check{I}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta}, \left(1 - \prod_{d=1}^{D}\left(1 - \check{T}_{\check{F}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta}\right)\right)\right) \\ \prod_{d=1}^{D}\left(1 - \check{I}_{\check{T}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta}, \prod_{d=1}^{D}\left(1 - \check{I}_{\check{I}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta}, \prod_{d=1}^{D}\left(1 - \check{I}_{\check{F}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta}, \\ \prod_{d=1}^{D}\left(1 - \check{F}_{\check{T}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta}, \prod_{d=1}^{D}\left(1 - \check{F}_{\check{I}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta}, \prod_{d=1}^{D}\left(1 - F_{\check{F}_{\check{R}_{ij}^{(d)}}}(k)\right)^{\vartheta} \\ T\ truth \\ I\ Indterminacy \\ F\ falisty \\ d = 1 \\ D\ number\ of\ experts \\ i = 1,2,3 \ldots, m; j = 1,2,3, \ldots n \end{array}\right)$$

(10)

10. Normalize the decision matrix, then compute the score function

$$Nr = \frac{S(\check{R}_{ij}) - \min_{1 \le i \le m} S(\check{R}_{ij})}{\max_{1 \le i \le m} S(\check{R}_{ij}) - \min_{1 \le i \le m} S(\check{R}_{ij})} \quad (11)$$

11. Compute the weighted normalized decision matrix

Multiply the weights of criteria by the normalized decision matrix to compute the weighted normalized decision matrix WNr

12. Compute the border approximation area

$$B_j = \prod_{i=1}^{m} (WNr)^{\frac{1}{m}} \quad (12)$$

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

13. Calculate the distance matrix

$$T_{ij} = WNr_{ij} - B_j \quad (13)$$

14. Rank the alternatives

The alternatives are ranked based on the sum of the score in the previous step.

4. Experimental Results

Acquiring combined qualitative and quantitative metrics is a good way to maintain security in a fog-based Internet of Things environment. In comparison to quantitative evaluation, qualitative evaluation is often simpler to carry out. Professionals from the development sector and academic institutions are now attempting to establish security policies to safeguard the environment indicated above. In addition, modern high-end security techniques are meant to provide precise results within a certain amount of time. In light of the information presented above, the researchers participating in this study are attempting to objectively assess the level of security offered by Fog-IoT. In order to do this, the authors have suggested using the T2NNs-AHP and MABAC hybrid approach, which is the most appropriate technique for prioritising the security criteria and selecting the best fog in IoT. After conducting a study of the relevant literature, a hierarchy of security factors and sub-factors has been compiled and is shown in Figure 1.
The use of a questionnaire allowed for the solicitation of advice from industry professionals, which was then put toward the purpose of data collection. The questionnaire was distributed to three professionals who have a background in the development sector and academic institutions.

1. The information that was obtained from the specialist was in the form of language in table 2. Tables 1, and 2 in the appendix show the pairwise of the rest of the experts.
2: The language comparison matrix pairwise was then turned into a numerical one by applying the scale that was supplied, and the results of this conversion are displayed in Table 3.
3. The information that was gathered from the specialists is compiled using equation (8), and the combined pairwise comparison matrix can be seen in table 4.

Table 2: Pairwise comparison matrix by the first expert.

	F₁	**F₂**	**F₃**	**F₄**	**F₅**
F₁	1	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>
F₂	1/<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	1	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>
F₃	1/<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	1/<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	1	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>
F₄	1/<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	1/<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	1/<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	1	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>
F₅	1/<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	1/<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	1/<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	1/<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	1

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

Table 3: The score value of the pairwise comparison matrix by the first expert.

	F_1	F_2	F_3	F_4	F_5
F_1	1	0.695833	0.75	0.833333	0.75
F_2	1.437126	1	0.9	0.695833	0.9625
F_3	1.333333	1.111111	1	0.833333	0.9625
F_4	1.2	1.437126	1.2	1	0.766667
F_5	1.333333	1.038961	1.304348	1.304348	1

Table 4: Aggregated pairwise comparison matrix.

	F_1	F_2	F_3	F_4	F_5
F_1	1	0.830556	0.820833	0.805556	0.85
F_2	1.225362	1	0.855556	0.759722	0.873611
F_3	1.235209	1.175523	1	0.811111	0.941667
F_4	1.244444	1.323486	1.234783	1	0.805556
F_5	1.185185	1.171683	1.151473	1.249597	1

Table 3 in the appendix shows the normalization pairwise comparison matrix. Then compute the weights of the criteria. The weights of the criteria are shown in figure 3.

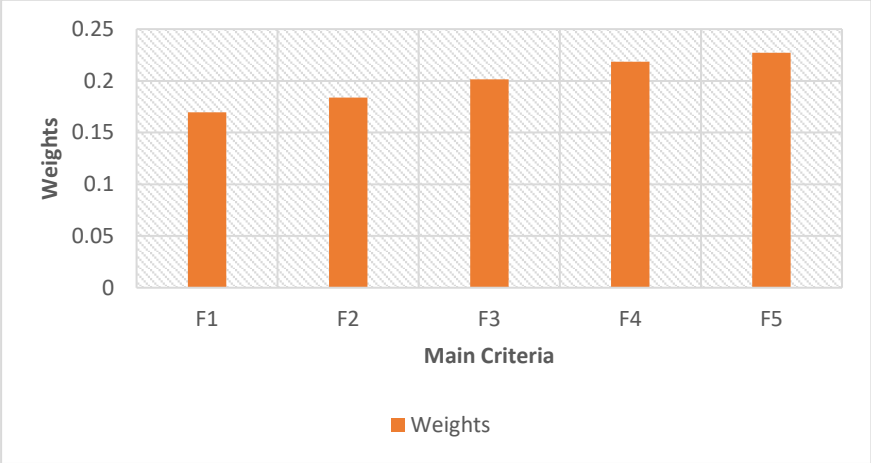

Figure 3: The weights of level 1 (main factors)

We applied the previous steps to get the weights of the sub-criteria. First, start with building the pairwise comparison matrix for sub-criteria based on the first sub-criteria. Tables 4, 5 and 6 in Appendix show the pairwise comparison, aggregated and normalization of main criteria F1. Then apply the steps in all main criteria to compute the local weights of sub-criteria. Then compute the global weights of the criteria by multiplying the weights of the main criteria by the weights of each sub-criteria to obtain the global weights of all criteria. Table 5 shows the weights of global and local criteria. Table 5 shows the local and global weights of the criteria. Figure 4 shows the local and global weights.

Table 5: Local and global weights

Main criteria	weights main criteria	Sub criteria	Weights sub-criteria	Global weights
F1	0.169429	F1.1	0.290652	0.049245
		F1.2	0.335473	0.056839
		F1.3	0.373875	0.063345
F2	0.183687	F2.1	0.213207	0.039163
		F2.2	0.233791	0.042944
		F2.3	0.257487	0.047297
		F2.4	0.295515	0.054282

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

F3	0.201375	F3.1	0.288135	0.058023
		F3.2	0.338148	0.068095
		F3.3	0.373717	0.075257
F4	0.218421	F4.1	0.29798	0.065085
		F4.2	0.327628	0.071561
		F4.3	0.374392	0.081775
F5	0.227088	F5.1	0.218047	0.049516
		F5.2	0.230504	0.052345
		F5.3	0.253901	0.057658
		F5.4	0.297548	0.06757

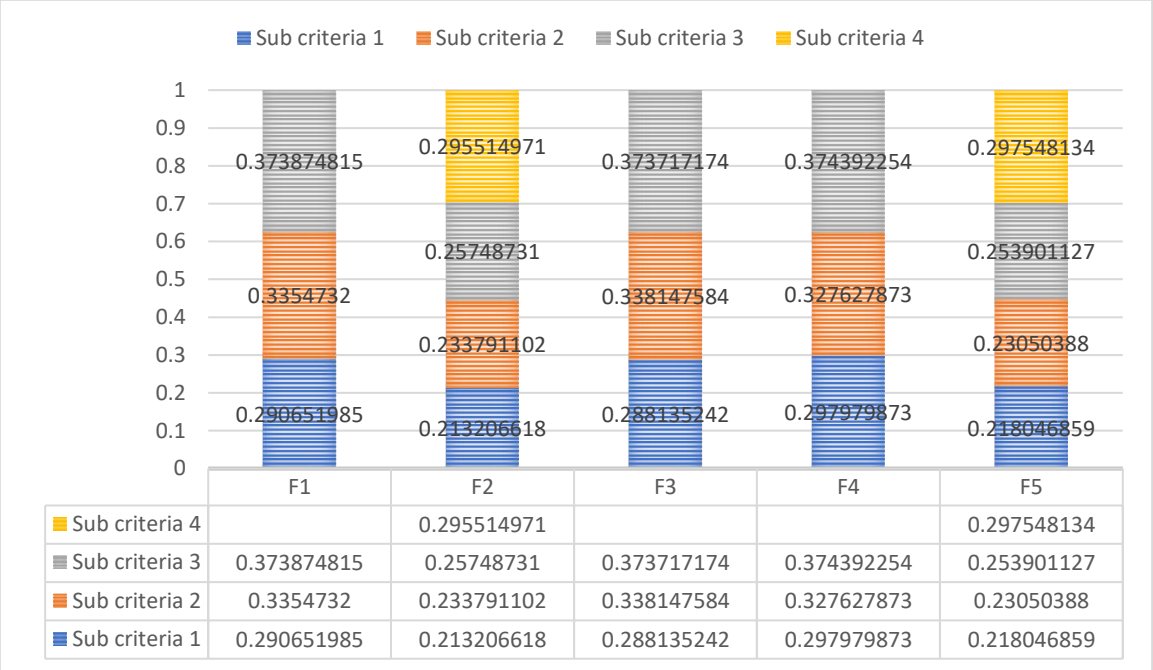

Figure 4: The local weights of sub-criteria.

Build the decision matrix via three experts between criteria and alternatives. This study used 5 patches of fog as an alternative to select the best one. Table 7 in the appendix shows the decision matrix of the first expert. Then convert the opinions of experts by the T2NNS. Then convert the T2NNS into a crisp value as shown in table 8 in the appendix. Then aggregate this decision matrix into one matrix as shown in table 9 in the appendix. Normalize the decision matrix as shown in table 6. Then compute the weighted normalized decision matrix as shown in table 10 in the appendix. Then compute the border value. Then compute the distance from weighted normalization and border approximation area as shown in table 11 in the appendix. Then rank the alternatives as shown in figure 5. From figure 5 fog 3 is the best alternative and fog 5 is the worst alternative.

Table 6: The normalized aggregated decision matrix.

	A_1	A_2	A_3	A_4	A_5
$F_{1.1}$	0.900992	0.773403	1.072845061	1.156168	0.968691
$F_{1.2}$	0.916621	1.138817	0.798579055	1.027719	-0.36101
$F_{1.3}$	1.178483	1.321321	1.17848292	1.226096	1.16658
$F_{2.1}$	-0.19523	-0.03118	-0.11450652	-0.03118	-0.10149
$F_{2.2}$	1.106695	0.906199	1.07024122	1.234283	1.02858
$F_{2.3}$	1.220503	1.029349	1.22050347	0	1.257264
$F_{2.4}$	1.418685	0.960959	1.369990339	0.960959	0.960959
$F_{3.1}$	1.114507	1.234283	1.11450652	0.773403	0.906199
$F_{3.2}$	1.180628	0.885485	1.177615871	0.885485	0.987881
$F_{3.3}$	1.094236	1.02626	1.056958917	0.881539	0.881539
$F_{4.1}$	1.131512	1.061344	1.197295022	1.197295	0.916623

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

$F_{4.2}$	1.230186	1.230186	1.06134442	1.094236	1.024068
$F_{4.3}$	1.338145	1.264623	1.33814456	1.374905	1.186201
$F_{5.1}$	1.157328	1.157328	1.22907883	1.263797	1.006883
$F_{5.2}$	0.968361	0.968361	1.197285742	0.94731	0
$F_{5.3}$	0.949514	1.006526	1.230186296	0.973634	1.08985
$F_{5.4}$	0	0.905209	0.905209379	1.197286	0.905209

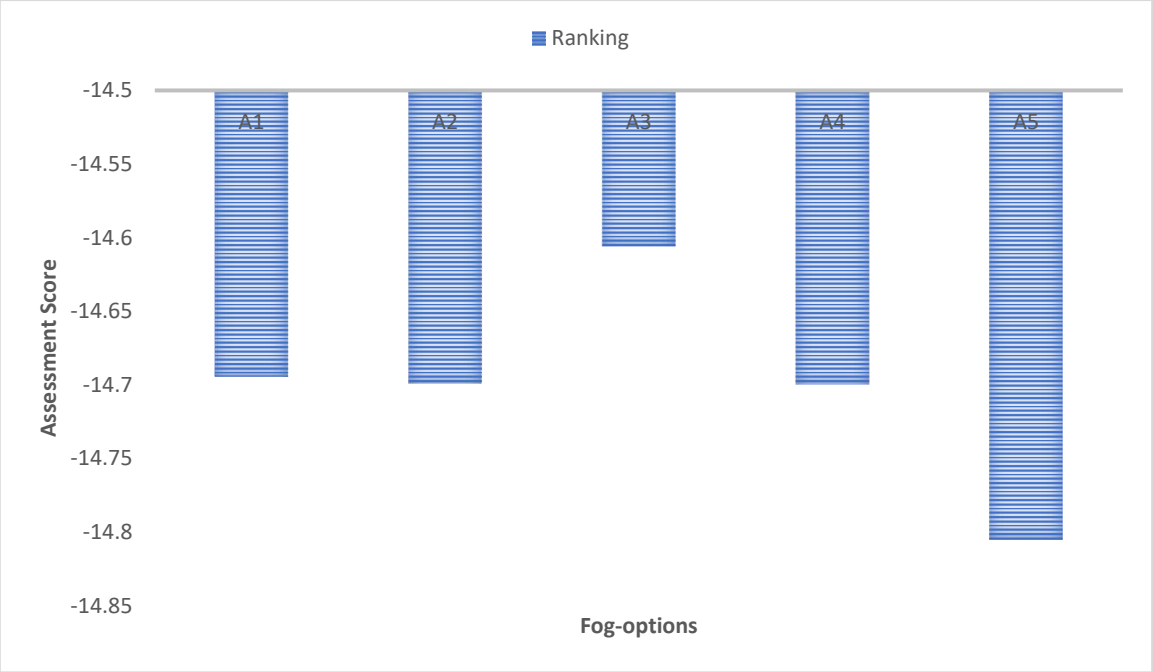

Figure 5: The Fog ranking.

The evaluation of the many components of fog-IoT security provides a number of potential strategies for ensuring the safety of the whole network. By identifying and defining the components that contribute to security, this assessment sheds light on many previously unknown aspects of the topic. The examination of security aspects related to Fog-IoT and the influence those elements have on security will make it easier to estimate how strong the security is. Finding out the relationship between the components that contribute to security in a fog environment is made easier by a framework that is organised hierarchically.

Quantitative analysis is a useful tool for finding the high-order issues that need to be addressed while maintaining the scenario's overall level of safety.

In this study effort, the writers have used an empirical method in order to compile a list of the elements relating to security. The data was gathered from several professionals, and quantitative analysis of the data was carried out using the T2NNS-AHP-MABAC approach. Additionally, T2NN-AHP was used to compute the weights of criteria and T2NNs-MABAC was used in order to rank the alternatives.

Comparative Study

In order to explore the hybrid type-2 neutrosophic model's dependability for use in the assessment of impact security in IoT, a comparison study with the T2NN-based TOPSIS and T2NN-CRITIC technique is carried out. The findings of the comparison are shown in Table 6. According to the data shown in this table, three T2NN-based methods conclude that A3 is the optimal method. In addition, both our model and the T2NN-based TOPSIS technique provide the same ranking of the five different fog. As a consequence of this, one may reach the reasonable inference that the hybrid type-2 neutrosophic model for the assessment of the impact Fog security in IoT is quite trustworthy.

Table 7: The comparison between the proposed model and previous works.

Alternatives	Proposed model	CRITIC-MABAC Model[38]	TOPSIS[37]
A1	A3	A3	A3
A2	A1	A1	A1
A3	A2	A2	A2

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

A4	A4	A4	A4
A5	A5	A5	A5

5. Conclusion

It is necessary to classify security variables and describe their driving sub-factors in order to ensure overall security for an environment in which the network devices are spread out across a large geographical region and communication happens at a consistent rate. It is clear from the research that was conducted and the literature that was examined that there is no such known, thorough, and full method that provides security throughout the whole Fog-IoT situation. It is necessary to prioritise the many security criteria in order to have access to security in a comprehensive Fog-IoT environment. The hybrid technique that has been suggested provides a quantitative analysis of the aspects that affect security by the hierarchy that has been described and their ranking appropriately. This study introduces the hybrid MCDM model under type 2 neutrosophic numbers. The T2NNS based on AHP-MABAC was used to evaluate the impact of fog security in IoT. The AHP method is used to compute the weights of the criteria. The T2NN MABAC was used to rank the alternatives. This study used 5 alternatives, 5 main criteria and 17 sub-criteria.

References

[1] N. Tariq *et al.*, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, p. 1788, 2019.

[2] C. Thota, R. Sundarasekar, G. Manogaran, R. Varatharajan, and M. K. Priyan, "Centralized fog computing security platform for IoT and cloud in healthcare system," in *Fog computing: Breakthroughs in research and practice*, IGI global, 2018, pp. 365–378.

[3] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment," in *2015 6th International Conference on the Network of the Future (NOF)*, 2015, pp. 1–3.

[4] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2017.

[5] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "IoT survey: An SDN and fog computing perspective," *Computer Networks*, vol. 143, pp. 221–246, 2018.

[6] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[7] M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)," *Computing*, vol. 101, no. 7, pp. 791–818, 2019.

[8] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020.

[9] P. Karthika, R. Ganesh Babu, and P. A. Karthik, "Fog computing using interoperability and IoT security issues in health care," in *Micro-Electronics and Telecommunication Engineering: Proceedings of 3rd ICMETE 2019*, 2020, pp. 97–105.

[10] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 92–96, 2019.

[11] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog computing and the internet of things: A review," *big data and cognitive computing*, vol. 2, no. 2, p. 10, 2018.

[12] S. Javanmardi, M. Shojafar, R. Mohammadi, A. Nazari, V. Persico, and A. Pescapè, "FUPE: A security driven task scheduling approach for SDN-based IoT–Fog networks," *Journal of information security and applications*, vol. 60, p. 102853, 2021.

[13] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of things journal*, vol. 3, no. 6, pp. 854–864, 2016.

[14] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the internet of things (CTM-IoT)," *in Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 12th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2017)*, 2018, pp. 533–543.

[15] A. A. Mutlag, M. K. Abd Ghani, N. al Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, 2019.
[16] A. Rauf, R. A. Shaikh, and A. Shah, "Security and privacy for IoT and fog computing paradigm," in *2018 15th Learning and Technology Conference (L&T)*, 2018, pp. 96–101.
[17] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing IoT-enabled applications at the fog layer," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 16, 2019.
[18] B. Mukherjee, R. L. Neupane, and P. Calyam, "End-to-end IoT security middleware for cloud-fog communication," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2017, pp. 151–156.
[19] K. Dubey, S. C. Sharma, and M. Kumar, "A secure iot applications allocation framework for integrated fog-cloud environment," *Journal of Grid Computing*, vol. 20, no. 1, p. 5, 2022.
[20] H. Alyami *et al.*, "Effectiveness evaluation of different IDSs using integrated fuzzy MCDM model," *Electronics*, vol. 11, no. 6, p. 859, 2022.
[21] M. D. Alshehri, F. K. Hussain, and O. K. Hussain, "Clustering-driven intelligent trust management methodology for the internet of things (CITM-IoT)," *Mobile networks and applications*, vol. 23, no. 3, pp. 419–431, 2018.,
[22] M. Pouyakian, A. Khatabakhsh, M. Yazdi, and E. Zarei, "Optimizing the Allocation of Risk Control Measures Using Fuzzy MCDM Approach: Review and Application," *Linguistic Methods Under Fuzzy Information in System Safety and Reliability Analysis*, pp. 53–89, 2022.
[23] M. D. Alshehri and F. K. Hussain, "A comparative analysis of scalable and context-aware trust management approaches for internet of things," *in Neural Information Processing: 22nd International Conference, ICONIP 2015, November 9-12, 2015, Proceedings, Part IV 22*, 2015, pp. 596–605.
[24] M. Abdel-Basset, M. Mohamed, and A. K. Sangaiah, "Neutrosophic AHP-Delphi Group decision making model based on trapezoidal neutrosophic numbers," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 5, pp. 1427–1443, 2018.
[25] E. Bolturk and C. Kahraman, "A novel interval-valued neutrosophic AHP with cosine similarity measure," *Soft Computing*, vol. 22, no. 15, pp. 4941–4958, 2018.
[26] M. Abdel-Basset, M. Mohamed, and F. Smarandache, "An extension of neutrosophic AHP–SWOT analysis for strategic planning and decision-making," *Symmetry*, vol. 10, no. 4, p. 116, 2018.
[27] M. Abdel-Basset, M. Mohamed, Y. Zhou, and I. Hezam, "Multi-criteria group decision making based on neutrosophic analytic hierarchy process," *Journal of Intelligent & Fuzzy Systems*, vol. 33, no. 6, pp. 4055–4066, 2017.
[28] M. A. Basset, M. Mohamed, A. K. Sangaiah, and V. Jain, "An integrated neutrosophic AHP and SWOT method for strategic planning methodology selection," *Benchmarking: An International Journal*, vol. 25, no. 7, pp. 2546–2564, 2018.
[29] P. Liu and S. Cheng, "An improved MABAC group decision-making method using regret theory and likelihood in probability multi-valued neutrosophic sets," *International Journal of Information Technology & Decision Making*, vol. 19, no. 05, pp. 1353–1387, 2020.
[30] D. Pamucar, M. Yazdani, R. Obradovic, A. Kumar, and M. Torres-Jiménez, "A novel fuzzy hybrid neutrosophic decision-making approach for the resilient supplier selection problem," *International Journal of Intelligent Systems*, vol. 35, no. 12, pp. 1934–1986, 2020.
[31] X. Peng and J. Dai, "Approaches to single-valued neutrosophic MADM based on MABAC, TOPSIS and new similarity measure with score function," *Neural Computing and Applications*, vol. 29, no. 10, pp. 939–954, 2018.
[32] P. Ji, H. Zhang, and J. Wang, "Selecting an outsourcing provider based on the combined MABAC–ELECTRE method using single-valued neutrosophic linguistic sets," *Computers & Industrial Engineering*, vol. 120, pp. 429–441, 2018.
[33] N. Rahim, L. Abdullah, and B. Yusoff, "A border approximation area approach considering bipolar neutrosophic linguistic variable for sustainable energy selection," *Sustainability*, vol. 12, no. 10, p. 3971, 2020.
[34] R. Şahin and F. Altun, "Decision making with MABAC method under probabilistic single-valued neutrosophic hesitant fuzzy environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 10, pp. 4195–4212, 2020.
[35] I. Irvanizam, N. N. Zi, R. Zuhra, A. Amrusi, and H. Sofyan, "An extended MABAC method based on triangular fuzzy neutrosophic numbers for multiple-criteria group decision making problems," *Axioms*, vol. 9, no. 3, p. 104, 2020.
[36] R. Verma and S. Chandra, "Interval-valued intuitionistic fuzzy-analytic hierarchy process for evaluating the impact of security attributes in fog based internet of things paradigm," *Computer Communications*, vol. 175, pp. 35–46, 2021.
[37] M. Abdel-Basset, M. Saleh, A. Gamal, and F. Smarandache, "An approach of TOPSIS technique for

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

developing supplier selection with group decision making under type-2 neutrosophic number," *Applied Soft Computing*, vol. 77, pp. 438–452, 2019.

[38] V. Simic, I. Gokasar, M. Deveci, and A. Karakurt, "An integrated CRITIC and MABAC based type-2 neutrosophic model for public transportation pricing system selection," *Socio-Economic Planning Sciences*, vol. 80, p. 101157, 2022.

Appendix

Table 1. Pairwise comparison matrix by the second expert.

	F_1	F_2	F_3	F_4	F_5
F_1	1	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>
F_2	1/<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	1	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>
F_3	1/<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	1/<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	1	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>
F_4	1/<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	1/<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	1/<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	1	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>
F_5	1/<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	1/<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	1/<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	1/<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	1

Table 2. Pairwise comparison matrix by the third expert.

	F_1	F_2	F_3	F_4	F_5
F_1	1	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>
F_2	1/<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	1	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>
F_3	1/<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	1/<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	1	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>
F_4	1/<(0.35, 0.35, 0.10), (0.50, 0.75,	1/<(0.60, 0.45, 0.50), (0.20, 0.15,	1/<(0.40, 0.30, 0.35), (0.50, 0.45,	1	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80),

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

	0.80), (0.50, 0.75, 0.65)>	0.25), (0.10, 0.25, 0.15)>	0.60), (0.45, 0.40, 0.60)>		(0.50, 0.75, 0.65)>
F_5	1/<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	1/<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	1/<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	1/<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	1

Table 3. Normalization pairwise comparison matrix.

	F_1	F_2	F_3	F_4	F_5
F_1	0.169773	0.150976	0.162135	0.174137	0.190121
F_2	0.208034	0.181777	0.168994	0.164229	0.195402
F_3	0.209706	0.213683	0.197525	0.175338	0.210624
F_4	0.211274	0.240579	0.243901	0.21617	0.18018
F_5	0.201213	0.212985	0.227445	0.270126	0.223672

Table 4. Pairwise comparison matrix by first experts to the first main criteria.

	$F_{1.1}$	$F_{1.2}$	$F_{1.3}$
$F_{1.1}$	1	0.695833	0.75
$F_{1.2}$	1.437126	1	0.9
$F_{1.3}$	1.333333	1.111111	1

Table 5. Aggregated pairwise comparison matrix to the first main criteria.

	$F_{1.1}$	$F_{1.2}$	$F_{1.3}$
$F_{1.1}$	1	0.830556	0.820833
$F_{1.2}$	1.225362	1	0.855556
$F_{1.3}$	1.235209	1.175523	1

Table 6. Normalization pairwise comparison matrix to the first main criteria.

	$F_{1.1}$	$F_{1.2}$	$F_{1.3}$
$F_{1.1}$	0.28897	0.276292	0.306694
$F_{1.2}$	0.354092	0.332659	0.319668
$F_{1.3}$	0.356938	0.391049	0.373638

Table 7. The decision matrix by the first expert.

	A_1	A_2	A_3	A_4	A_5
$F_{1.1}$	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>
$F_{1.2}$	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>
$F_{1.3}$	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>
$F_{2.1}$	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>
$F_{2.2}$	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>
$F_{2.3}$	<(0.95, 0.90, 0.95), (0.10, 0.10,	<(0.60, 0.45, 0.50), (0.20, 0.15,	<(0.95, 0.90, 0.95), (0.10, 0.10,	<(0.40, 0.30, 0.35), (0.50, 0.45,	<(0.95, 0.90, 0.95), (0.10, 0.10,

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

	0.05), (0.05, 0.05, 0.05)>	0.25), (0.10, 0.25, 0.15)>	0.05), (0.05, 0.05, 0.05)>	0.60), (0.45, 0.40, 0.60)>	0.05), (0.05, 0.05, 0.05)>
$F_{2.4}$	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>
$F_{3.1}$	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>
$F_{3.2}$	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>
$F_{3.3}$	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>
$F_{4.1}$	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>
$F_{4.2}$	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.60, 0.45, 0.50), (0.20, 0.15, 0.25), (0.10, 0.25, 0.15)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>
$F_{4.3}$	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>
$F_{5.1}$	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>
$F_{5.2}$	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>
$F_{5.3}$	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.35, 0.35, 0.10), (0.50, 0.75, 0.80), (0.50, 0.75, 0.65)>	<(0.20, 0.20, 0.10), (0.65, 0.80, 0.85), (0.45, 0.80, 0.70)>
$F_{5.4}$	<(0.95, 0.90, 0.95), (0.10, 0.10, 0.05), (0.05, 0.05, 0.05)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>	<(0.70, 0.75, 0.80), (0.15, 0.20, 0.25), (0.10, 0.15, 0.20)>	<(0.40, 0.30, 0.35), (0.50, 0.45, 0.60), (0.45, 0.40, 0.60)>

Table 8. The score values of the decision matrix by the first expert.

	A_1	**A_2**	**A_3**	**A_4**	**A_5**
$F_{1.1}$	0.6958	0.6958	0.8333	0.9	0.75
$F_{1.2}$	0.9	0.7667	0.9	0.6958	0.766667
$F_{1.3}$	0.7667	0.9	0.8333	0.8333	0.75
$F_{2.1}$	0.9	0.8333	0.8333	0.8333	0.75
$F_{2.2}$	0.6958	0.7667	0.7667	0.9625	0.766667
$F_{2.3}$	0.9625	0.8333	0.9625	0.7667	0.9625
$F_{2.4}$	0.9625	0.7667	0.9625	0.7667	0.766667
$F_{3.1}$	0.9	0.9625	0.9	0.6958	0.766667
$F_{3.2}$	0.9	0.6958	0.9625	0.6958	0.766667
$F_{3.3}$	0.8333	0.8333	0.6958	0.6958	0.695833

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

$F_{4.1}$	0.9	0.8333	0.9625	0.9625	0.695833
$F_{4.2}$	0.9625	0.9625	0.8333	0.8333	0.766667
$F_{4.3}$	0.9625	0.9	0.9625	0.9625	0.766667
$F_{5.1}$	0.9	0.9	0.9	0.9625	0.695833
$F_{5.2}$	0.75	0.75	0.9	0.7667	0.75
$F_{5.3}$	0.6958	0.75	0.9625	0.75	0.695833
$F_{5.4}$	0.9625	0.7667	0.7667	0.9	0.766667

Table 9. The aggregated decision matrix.

	A_1	**A_2**	**A_3**	**A_4**	**A_5**
$F_{1.1}$	0.763889	0.695833	0.855556	0.9	0.8
$F_{1.2}$	0.877778	0.766667	0.9	0.695833	0.833333
$F_{1.3}$	0.833333	0.9	0.833333	0.855556	0.827778
$F_{2.1}$	0.920833	0.833333	0.877778	0.833333	0.870833
$F_{2.2}$	0.873611	0.766667	0.854167	0.941667	0.831944
$F_{2.3}$	0.941667	0.833333	0.941667	0.831944	0.9625
$F_{2.4}$	0.9625	0.766667	0.941667	0.766667	0.766667
$F_{3.1}$	0.877778	0.941667	0.877778	0.695833	0.766667
$F_{3.2}$	0.9	0.763889	0.898611	0.763889	0.811111
$F_{3.3}$	0.876389	0.833333	0.852778	0.741667	0.741667
$F_{4.1}$	0.9	0.855556	0.941667	0.941667	0.763889
$F_{4.2}$	0.9625	0.9625	0.855556	0.876389	0.831944
$F_{4.3}$	0.941667	0.9	0.941667	0.9625	0.855556
$F_{5.1}$	0.877778	0.877778	0.920833	0.941667	0.7875
$F_{5.2}$	0.8	0.8	0.920833	0.788889	0.85
$F_{5.3}$	0.784722	0.820833	0.9625	0.8	0.873611
$F_{5.4}$	0.9625	0.766667	0.766667	0.920833	0.766667

Table 10. The weighted normalized decision matrix.

	A_1	**A_2**	**A_3**	**A_4**	**A_5**
$F_{1.1}$	0.117861	0.109951006	0.128516	0.133682	0.122059
$F_{1.2}$	0.063248	0.070580966	0.059353	0.066915	0.021087
$F_{1.3}$	0.089318	0.095174148	0.089318	0.09127	0.08883
$F_{2.1}$	0.011267	0.01356343	0.012397	0.013563	0.012579
$F_{2.2}$	0.065308	0.059092176	0.064177	0.069263	0.062886
$F_{2.3}$	0.102143	0.093350076	0.102143	0.046	0.103834
$F_{2.4}$	0.212844	0.172564385	0.208559	0.172564	0.172564
$F_{3.1}$	0.054977	0.058091364	0.054977	0.046108	0.049561
$F_{3.2}$	0.078503	0.067877442	0.078394	0.067877	0.071564
$F_{3.3}$	0.092146	0.089155457	0.090506	0.082788	0.082788
$F_{4.1}$	0.25365	0.245299986	0.261478	0.261478	0.228078
$F_{4.2}$	0.102589	0.10258857	0.094822	0.096335	0.093107
$F_{4.3}$	0.114569	0.110966545	0.114569	0.11637	0.107124
$F_{5.1}$	0.116496	0.116495709	0.12037	0.122245	0.108372
$F_{5.2}$	0.061019	0.061019192	0.068116	0.060367	0.031
$F_{5.3}$	0.099425	0.102332807	0.11374	0.100655	0.106582
$F_{5.4}$	0.069	0.131459447	0.131459	0.151613	0.131459

Table 11. The distance matrix.

	A_1	**A_2**	**A_3**	**A_4**	**A_5**
$F_{1.1}$	-0.8675	-0.87541	-0.85684	-0.85168	-0.8633
$F_{1.2}$	-0.87005	-0.86272	-0.87395	-0.86639	-0.91221
$F_{1.3}$	-0.86086	-0.85501	-0.86086	-0.85891	-0.86135
$F_{2.1}$	-0.85258	-0.85029	-0.85145	-0.85029	-0.85127
$F_{2.2}$	-0.86205	-0.86827	-0.86318	-0.8581	-0.86447
$F_{2.3}$	-0.86162	-0.87041	-0.86162	-0.91776	-0.85993

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023

$\mathbf{F_{2.4}}$	-0.8183	-0.85858	-0.82258	-0.85858	-0.85858
$\mathbf{F_{3.1}}$	-0.86259	-0.85948	-0.86259	-0.87146	-0.86801
$\mathbf{F_{3.2}}$	-0.8714	-0.88202	-0.87151	-0.88202	-0.87834
$\mathbf{F_{3.3}}$	-0.87003	-0.87302	-0.87167	-0.87939	-0.87939
$\mathbf{F_{4.1}}$	-0.8076	-0.81595	-0.79977	-0.79977	-0.83317
$\mathbf{F_{4.2}}$	-0.86896	-0.86896	-0.87673	-0.87522	-0.87844
$\mathbf{F_{4.3}}$	-0.86169	-0.86529	-0.86169	-0.85989	-0.86914
$\mathbf{F_{5.1}}$	-0.86961	-0.86961	-0.86574	-0.86386	-0.87774
$\mathbf{F_{5.2}}$	-0.87577	-0.87577	-0.86867	-0.87642	-0.90579
$\mathbf{F_{5.3}}$	-0.87425	-0.87135	-0.85994	-0.87302	-0.8671
$\mathbf{F_{5.4}}$	-0.93961	-0.87715	-0.87715	-0.85699	-0.87715

DOI: https://doi.org/10.54216/IJNS.200205
Received: June 11, 2022 Accepted: January 16, 2023