The Journal of Supercomputing
https://doi.org/10.1007/s11227-022-04674-2

A neutrosophic AHP-based computational technique for security management in a fog computing network

Jasleen Kaur[1] · Rajeev Kumar[2] · Alka Agrawal[1] · Raees Ahmad Khan[1]

Accepted: 7 June 2022

Abstract

Internet-enabled devices are deployed by individuals for almost every task. The concept of cloud computing has proven to be beneficial for users as the processing, storage and analysis of data are performed at the cloud level. However, in the case of latency-sensitive applications, the notion is called-off as the overall response time is high. In this situation, fog computing outperforms the cloud. With fog computing, the necessary computations are performed at the edge of the network, and thus, latency is highly reduced. In parallel, the increase in smart devices around the globe has led to a considerable increase in sensitive user data across the Web, which needs to be secured. Furthermore, multidimensional security depends on various factors whose prioritization plays an important role in addressing security issues. In this context, the authors identify various fog computing security factors and their corresponding subfactors. The identified factors are evaluated for their impact on security at the fog level through the neutrosophic-analytical hierarchy process. Moreover, to corroborate the effectiveness of the proposed technique, the results obtained are compared to the results from conventional approaches such as Fuzzy-AHP and Classical-AHP and are found to be statistically correlated. The proposed mechanism can be used by security practitioners to systematically manage fog computing security factors.

✉ Jasleen Kaur
jasleenkaur.lmp@gmail.com

[1] Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India

[2] Centre for Innovation and Technology, Administrative Staff College of India, Hyderabad, India

Published online: 08 July 2022

Keywords Fog computing · Security · Neutrosophic set · Single-valued neutrosophic set · Analytical hierarchy process

1 Introduction

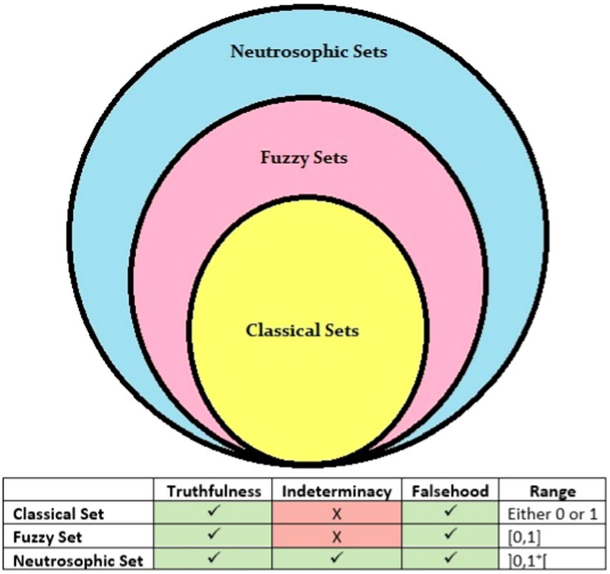
The prevalence of the Internet of things (IoT) in almost every field has led to the growth of smart devices across the globe. The International Data Corporation (IDC) estimated that by 2025, there will be approximately 41.6 billion IoT devices around the world [1]. However, these devices offer restricted computation power, battery, storage, etc., and consequently limit user experience. In this situation, cloud computing serves as an advantageous solution that delivers services to end users with regard to infrastructure, software and other platforms [2]. Cloud computing makes use of globally centralized data centers for data processing and storage. However, due to the large physical distance between the cloud data centers and the user devices, the response time increases. The increase in response time is not suitable for latency-sensitive applications, such as healthcare and banking. To resolve this issue, in 2014, the concept of fog computing was introduced [3]. In fog computing, cloud services occur at the edge of the network. In a typical three-tier IoT architecture, fog layer is placed between the cloud and the user's device. This layer acts as a mediator between the cloud and the users and regulates the latency-sensitive information to be processed locally, while the rest is sent to the cloud. This concept decentralizes the computing scenario and thus supports user mobility, location awareness and low latency [4].

Fog computing is very opportunistic in terms of real-time analysis. With its emergence, data processing occurs near the originator of the data, which accelerates the request and response cycle. However, despite its benefits, fog computing also has some crucial drawbacks. Fog is closer to the end devices and thus presents an increased attack surface area and is highly vulnerable to attacks [5–7]. With the immense increase in the usage of Internet-enabled devices and wide application areas of the IoT, an increasing amount of sensitive data floats at the fog level. Thus, security considerations at this layer cannot be overlooked. Despite being derived from the cloud concept, fog computing poses challenges in contrast to those presented by cloud computing due to the fundamental differences between both concepts [8]. Therefore, the solutions corresponding to cloud issues are not applicable to fog scenario. Hence, there is a need to address security issues at the fog level from a new foundation. Through the literature survey, it was found that very little work is done in the area of fog computing security [2, 6, 8]. Therefore, the authors addressed the security issue at the fog level in the proposed research work. In this context, the authors identified certain fog computing security factors and subfactors in the proposed research work.

The security of any system or platform is multidimensional in nature. Addressing security issues requires dealing with different security factors and aspects. With a wide range of security factors and subfactors, it becomes difficult for a security practitioner to decide which security factor is more essential than the other. In other words, which security factor should be priority? Thus, proper categorization of different security factors is critically important [10]. The empirical analysis of different security factors and subfactors pave the way for researchers to focus on high-priority factors for assured security in fog environments.

Currently, various security practitioners [11–14] are deploying multi-criteria decision-making (MCDM) techniques to rank security factors from different perspectives on the basis of expert opinions. However, expert opinions are often inconsistent, complex and vague in nature. Hence, using crisp values (0 or 1) is not very accurate due to indeterminacy and uncertainty in the responses. In addition, fuzzy set theory only focuses on the true or false degree of the response [15, 16]. However, neutrosophic logic measures the truth, indeterminacy and falsehood [17] and thus provides more accurate results through its ability to distinguish between the absolute truth and relative truth. The relation among classical, fuzzy and neutrosophic sets is shown in Fig. 1.

Neutrosophy is believed to handle real-world and scientific problems effectively because it considers all the aspects of a decision-making situation [49]. The presence of the indeterminacy degree helps experts present their opinion about uncertain preferences, which makes the technique highly accurate. Additionally, the integration of neutrosophic logic with the analytical hierarchy process (AHP) removes the need for consistent data to be obtained by experts. In the case of classical AHP (CAHP), if inconsistent data are received from the experts, they must be either modified by the expert or dropped, which may lead to inaccurate results. However, in the case of the neutrosophic analytical hierarchy process (NAHP) technique, the data are made consistent (Sect. 5) through various mathematical equations, which reduces the repetitive involvement of experts, thereby saving time and effort. Considering the benefits, the authors used the NAHP approach to analyze the collective decision of experts



	Truthfulness	Indeterminacy	Falsehood	Range
Classical Set	✓	X	✓	Either 0 or 1
Fuzzy Set	✓	X	✓	[0,1]
Neutrosophic Set	✓	✓	✓	$]0,1^{+}[$

Fig. 1 Relationship among classical, fuzzy and neutrosophic sets

about the priority of identified security factors, as AHP is believed to analyze the group decision effectively [12]. Thus, the major contributions of the research work are as follows:

1. Prioritization of the identified security factors and subfactors through the neutrosophic analytical hierarchy process.
2. Comparison of the results obtained by the neutrosophic analytical hierarchy process with the CAHP and fuzzy AHP (FAHP).

The rest of the paper is organized as follows: Sect. 2 discusses the related work. Section 3 presents the hierarchy of fog computing security factors, and Sect. 4 is the preliminary draft of neutrosophic operations. Furthermore, Sect. 5 describes the detailed NAHP methodology. The next section includes the implementation of the approach. Moreover, the obtained results are compared to those obtained from other classical approaches in Sect. 7, and the correlation between both techniques is determined. Section 8 discusses the advantages and limitations of the proposed research work. Finally, the paper concludes in Sect. 9.

2 Related work

The proposed study focuses on the deployment of NAHP methodology that ranks the fog computing security factors depending on the experts' opinions (such as academicians, industry professionals and security experts). The related work with respect to the proposed work can be categorized into three categories:

2.1 Literature related to fog computing security

Since the introduction of fog computing in 2014 [23], there has been a considerable amount of research in the area. Recently, the focus of the fog computing experts has shifted to the prevalent security issues in the area. This may be due to the large pool of sensitive user data, which can be processed anywhere between cloud-to-fog provinces. Fog computing security issues and challenges have been presented by various researchers [3–10, 28]. Among these, some studies focused on considering security during data transmission, while some experts stressed about its secure storage. Mukherjee et al. [24] listed several security and privacy challenges in a fog computing environment. Various malicious attacks, along with issues such as authentication, privacy, trust and intrusion detection, have been discussed in detail. Ni et al. [25] discussed the different security threats in a fog-IoT architecture, such as sybil, denial of service and man-in-the-middle. The security solutions have also been recommended by the authors. Singh et al. [26] conducted a survey of fog architectures and issues related to fog computing, including the security and privacy of the user's sensitive data. Similarly, Zhang et al. [27] elaborated on security and trust issues related to the area, while the authors explored various security and privacy challenges prevalent in the fog-IoT environment [5]. Thus, it may be concluded that the orientation of fog computing researchers is positive toward security.

2.2 Literature related to security estimation through MCDM methods

MCDM methods are extensively used by researchers for decision-making problems. When we discuss security estimation of a particular approach or application, many security factors need to be dealt with. The prioritization of security factors plays an important role in pinpointing security issues. Many researchers have worked to this end. For example, Erdogan et al. [29] estimated the risk of cybersecurity technologies using a fuzzy MCDM approach. The security features of IoT applications have been estimated by researchers through MCDM techniques [30]. An assessment of information about security risks has been performed by Turskis et al. [31]. Oh et al. [32] considered the privacy factor for usability estimation of a biometric system. An information security management framework based on MCDM has been proposed to estimate the suitability [33]. The cybersecurity estimation metrics have been evaluated by researchers [34]. Additionally, other similar approaches can be found in references [11–14]. The above studies clearly show that security estimation is possible through MCDM methods.

2.3 Literature related to neutrosophy

The main reason for the wide applicability of the neutrosophic set is its ability to provide accurate and consistent results. In 2014, this approach was deployed to select a suitable supplier depending on the choice of different decision-makers [35]. Similarly, Radwan et al. [18] used the NAHP approach for the selection of a learning management system, and Biswas et al. [36] used a single-valued neutrosophic environment for the analysis. Moreover, neutrosophic logic in MCDM problems is widely used to deal with uncertainties and falsehoods [19–22]. In 2018, Basset et al. [37, 38] presented an extension of NAHP for strategic planning and three-way decisions based on neutrosophic sets and AHP, respectively. A novel NAHP approach has been devised by Tey et al. [39], and the performance of law firms has been analyzed through a similar approach [40]. Researchers deployed a neutrosophic approach to select appropriate security services to meet the varying demands of mobile users [41]. Therefore, it may be concluded that the neutrosophic approach is widely used across the world for its consistent and accurate results.

The above discussion makes the following points evident:

- Researchers are positively working toward security in the fog computing environment.
- The security estimation and prioritization of security factors is performed through MCDM approaches.

- The NAHP approach is expected to provide the accurate results for the prioritization of fog computing security factors.

In addition, the prioritization of fog computing security factors and subfactors has still not been explored by researchers with reference to neutrosophic logic. Hence, the authors have deployed a neutrosophy-based computational technique to evaluate the impact of fog computing security factors.

3 Fog computing security

Due to the prevalent use of IoT devices, a massive amount of data (Big Data) is generated very quickly. According to the Digital 2022 Global Overview Report, the number of people using the internet globally has grown to 4.95 billion in 2022, with an increase of approximately 4% (192 million users) in 2021, which is 62.5% of the world's total population [42]. With this huge increase in the number of internet users and the widespread implementation of IoT devices in almost every field, the amount of data (sensitive data) generated across the web also increases exponentially. Thus, security at the fog level should be considered a priority.

The edge (or fog) network is a combination of several enabling technologies, viz., distributed systems, peer-to-peer systems, wireless networks, virtualization platforms, etc., which pose a great challenge for the maintenance of the security of a whole system. Additionally, the individual security of each of the mentioned technologies does not guarantee the overall security of the complete environment. This is another challenge in the scenario. As already known, in fog computing, cloud capabilities are provided to the end users at the network edge and the mutual operation of edge data centers and heterogeneous devices are other relevant security issues. Therefore, the migration of services at the local level needs to be thoroughly studied to determine if a secure fog environment is desired. For assured security, all the dimensions of security need to be studied at the basic level. If all the security-related factors and subfactors are keenly analyzed, then the researchers can guarantee overall security in the system. In light of the above discussion, the authors have identified fog computing security factors with their subfactors to systematically manage the security of fog scenarios [9]. Therefore, in this section, the authors present the hierarchical structure of fog computing security factors and subfactors based upon the available literature (Fig. 2). The involved factors and subfactors are initially identified through a systematic literature review [7] and discussion with security experts and academics. To this end, the different fog computing security factors and their subfactors are as follows:

3.1 Access control (C1)

In a classical access control mechanism, the user's sensitive data are stored in trusted servers. A login check is applied to these servers, and the authorized person has

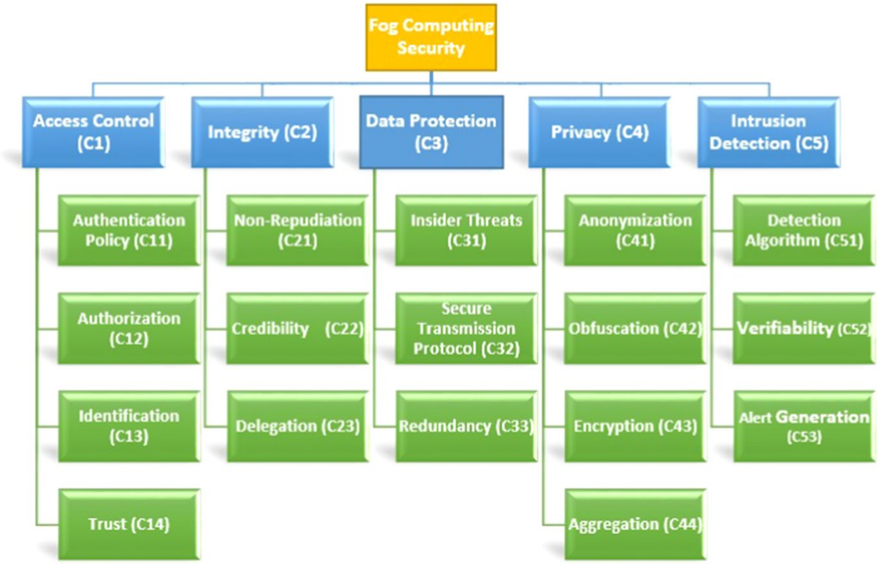


Fig. 2 Fog computing security factors

access to the information. However, in the fog-IoT scenario, users and servers exist in different trust domains and thus are mutually distrustful [43, 44]. The existing solutions for cloud scenarios cannot be directly applied to the fog due to the basic architectural differences between both concepts. Therefore, access control forms an integral factor in the fog security perspective. The different subfactors are as follows:

3.1.1 Authentication policy (C11)

The authentication mechanism based on authentication policy helps in checking whether someone is, in fact, who he declares to be by verifying the credentials prestored in the data authentication server [24].

3.1.2 Authorization (C12)

Authorization defines the access that any legitimate user has. It determines the user's permissions [24]. In a fog scenario, the development of an authorization mechanism is a task because of the single-hop distance between the user and the fog server.

3.1.3 Identification (C13)

Identification is defined as the degree to which the system recognizes (or identifies) the user before interacting with them through trusted login devices, access patterns, etc. [26].

3.1.4 Trust (C14)

Trust, in a network, may be defined as a method for estimating the legitimacy of nodes based upon past interactions and thus forms an integral subfactor of authentication [4]. It basically acts as a link between authorization and authentication.

3.2 Integrity (C2)

Integrity refers to the protection of the system or environment against unauthorized modification or tampering. With the deployment of fog computing in critical fields such as healthcare and banking, any tampering may lead to losses in terms of life and money [45]. In the case of data being modified on the basis of corrupted values, complete data may be damaged. As fog scenarios are mostly deployed in critical and latency-sensitive applications, real-time integrity checks are indispensable in fog-IoT scenarios. Its different subfactors are as follows:

3.2.1 Nonrepudiation (C21)

It may be defined as the non-allowance to the node of denying (or repudiating) any kind of interaction or modification [26]. Hence, integrity checks should consider nonrepudiation as an important factor.

3.2.2 Credibility (C22)

Credibility is defined as the degree to which the node's actions can be believed to be in agreement with the security of the system [27]. It plays a vital role in the detection of certain attacks in the fog scenario.

3.2.3 Delegation (C23)

This refers to the assignment of a privilege (or control) to a node by an authorized user. The degree of accountability of the modifications made by the delegated node computes the amount of delegation [24]. If any kind of update is being ordered to or by a node, it must check the delegation of the ordering node before making any sort of modification.

3.3 Data protection (C3)

The fog level may be visualized as a large pool of sensitive user data. This is because the fog level is the first set of processors through which the users' data are sent to the cloud after required processing. Thus, data protection is deemed a very important aspect when considering the security of a fog scenario [46]. The devices may request available resources for fast computation and may also pose a threat to data. Its subfactors are as follows:

3.3.1 Insider threats (C31)

Insider threats are difficult to detect and prevent in heterogeneous and mobile fog environments. For example, an attachment (file or link) believed to come from a reliable source may not be secure and may pose a threat to the environment [25].

3.3.2 Secure transmission protocol (C32)

The defined set of rules that govern the secure transmission of data from device to cloud via the fog is the transmission protocol [2]. If the transmission protocol has proper validations or checks to investigate the privileges and/or legitimacy of the communicating node, the security of the complete system may be greatly improved.

3.3.3 Redundancy (C33)

When stored at multiple locations, sensitive data need to be protected in every place [4]. The real-time computations by fog resources require regular redundancy checks for guaranteed data protection at the fog level.

3.4 Privacy (C4)

Privacy refers to the ability of fog nodes to prevent the user's personal information from being publicly available [47]. Privacy in the fog environment may be categorized into three types, viz., location privacy, data privacy and usage privacy. Various privacy subfactors are as follows:

3.4.1 Anonymization (C41)

This refers to the prevention of a user's identity from unauthorized disclosure or storage [3].

3.4.2 Obfuscation (C42)

This means that the user's exact information is not used for any processing but rather for the value nearest to the original value. The nearest value is obtained without the use of a key, which is the basic difference between obfuscation and encryption. It hides the user's exact information to safeguard their privacy [2]. The obfuscation technique is widely deployed in the case of location privacy [59].

3.4.3 Encryption (C43)

This refers to changing the users' private (or sensitive) data with the help of a key. The main requirement of any encryption mechanism for a fog environment is that it should be lightweight in nature to be easily applied to power constrained IoT devices [4].

3.4.4 Aggregation (C44)

Aggregation, in terms of fog privacy, means that the combination of two or more independent pieces of information about a person must not lead to the disclosure of their identity [10].

3.5 Intrusion detection (C5)

Intrusion detection, in general, may be defined as the process of detecting, recording and notifying attempted and successful attacks to a system or environment [48]. In the fog scenario, its different subfactors include the following.

3.5.1 Detection algorithm (C51)

The detection algorithm identifies the occurrence of any sort of intrusion to the fog system [47]. As an integral part of the intrusion detection system, the detection algorithm should be able to detect any intrusion in real-time.

3.5.2 Verifiability (C52)

Verifiability refers to the checking procedure that guarantees the proper functionalities of the complete system without being intruded [48]. Before generating an alert, it should verify its functionality and not be misleading.

3.5.3 Alert generation (C53)

Alert generation is the timely and accurate notification of any intrusion if the system is compromised [48]. At the fog level, it needs to be instantaneous.

The above section clearly specifies the different fog computing security factors. The NAHP methodology has been applied to these identified factors and subfactors. The detailed implementation of the methodology is described in Sect. 6.

4 Preliminaries

In this section, the preliminary information required for a proper understanding of this study is explained in detail. The main concept of neutrosophic sets and the arithmetic operations in the deployed scheme are discussed here. A neutrosophic set X is defined on universe U; $x=(T, I, F)$ in X with T, I and F being the real standard or nonstandard subsets of]0;1 + [. T, I and F are the degrees of the truth-membership function, the indeterminacy-membership function and the falsity-membership function in set X, respectively. The neutrosophic set generalizes the abovementioned set from a philosophical perspective. However, from a scientific or engineering perspective, the neutrosophic set and set-theoretic operators need to be made specific (not philosophical) in nature to increase the applicability of the concept. A single-valued neutrosophic set (SVNS) is an example of a neutrosophic set that can be used in real scientific and engineering applications [49].

An SVNS describes a variable 'p' by triple values where $p=(T, I, F)$, while T, I and F have their respective meanings [57]. Here, $0<T\leq 1$, $0 \ <I\leq 1$, $0 \ <F\leq 1$ and $0<T+I+F\leq 3$. Let P be an object space, and $p\varepsilon P$; then, the neutrosophic set P is defined by three membership functions, i.e., the truthfulness membership function $T_P(p)$, the indeterminacy membership function $I_P(p)$ and the falsehood membership function $F_P(p)$. As per [57], various operations on the SVNS are defined as:

Definition 1 Let $N_1=(T_1, I_1, F_1)$ and $N_2=(T_2, I_2, F_2)$ be two single-valued neutrosophic numbers, their addition is expressed as follows:

$$N_1 + N_2 = \left(T_1 + T_2 - T_1T_2,\ \ I_1I_2,\ \ F_1F_2\right) \tag{1}$$

Definition 2 Let $N_1=(T_1, I_1, F_1)$ and $N_2=(T_2, I_2, F_2)$ be two single-valued neutrosophic numbers, their multiplication is expressed as follows:

$$N_1 * N_2 = \left(T_1T_2,\ \ I_1 + I_2 - I_1I_2,\ \ F_1 + F_2 - F_1F_2\right) \tag{2}$$

Definition 3 Let $N_1=(T_1, I_1, F_1)$ and $N_2=(T_2, I_2, F_2)$ be two single-valued neutrosophic numbers, their division is expressed as follows:

$$\frac{N_2}{N_1} = \left(\frac{T_2}{T_1},\ \frac{I_2 - I_1}{1 - I_1},\ \frac{F_2 - F_1}{1 - F_1}\right) \tag{3}$$

Definition 4 Let $N_1=(T_1, I_1, F_1)$ be a single-valued neutrosophic number and A be an arbitrary positive real number, then the division of N_1 over A $(A>0)$ is expressed as follows:

$$\frac{N_1}{A} = \left(1 - \left(1 - T_1\right)^{1/A},\ I_1^{1/A},\ F_1^{1/A}\right) \tag{4}$$

Definition 5 Let $N_1=(T_1, I_1, F_1)$ be a single-valued neutrosophic number and A be an arbitrary positive real number, then the multiplication of N_1 and A $(A>0)$ is expressed as follows:

$$A * N_1 = \left(1 - \left(1 - T_1\right)^A,\ I_1^A,\ F_1^A\right) \tag{5}$$

Definition 6 *Deneutrosophication*-Let $N_1 = (T_1,\ I_1,\ F_1)$ be a single-valued neutrosophic number, a score function 'S' maps N_1 to a single crisp output (deneutrosophic number) is expressed as follows:

$$S\left(N_1\right) = \frac{\left(3 + T_1 - 2I_1 - F_1\right)}{4} \tag{6}$$

This section contains the different arithmetic operations as performed on single-valued neutrosophic numbers. The application of these operations in the proposed work is stated in Sects. 5 and 6 in detail.

5 Methodology

The term 'Neutrosophy' is derived from the Latin term 'Neuter' and the Greek term 'Sophia,' which mean 'Neutral' and 'Wisdom,' respectively. In this research work, the neutrosophic logic-based AHP methodology is utilized. The neutrosophic linguistic scale is adopted, as it is believed to provide more accurate results than the classical set. The basic reason behind deploying AHP is its comprehensive nature, with which it addresses different factors [12]. The AHP permits decision-makers (or experts) to convert a complex problem into a simple one. This is done by arranging the factors and subfactors into a hierarchical structure. Additionally, the application of neutrosophic logic makes it possible for the decision-maker to convert inconsistent inputs into consistent ones without the involvement of the experts. While deploying classical sets, the inconsistent values (if obtained) needed to be corrected or were dropped. This led to biased and inaccurate results. However, with neutrosophic sets, the inconsistent data (if obtained) are made consistent through various mathematical equations. This reduces the repetitive involvement of experts and thus saves time and effort.

Initially, the pairwise comparison matrix based upon the expert responses is made, and then an aggregated matrix is constructed using Eq. (7). The pairwise comparison matrix is preferred because of its unambiguity, consistency and efficiency. It provides an unbiased relative ranking indicating the degree of importance of each involved criterion. Furthermore, the consistent version of the obtained aggregated matrix is fabricated by deploying Eqs. (8–10). Then, the consistency ratio (CR) is calculated using Eq. (11). The detailed step-by-step description of the adopted methodology is as follows:

Step 1: Establishing a pairwise comparison matrix of the factors The factors, as identified in Sect. 4, were analyzed by a group of experts for each level and converted into numeric values using a neutrosophic scale [18] (Table 1). The results of the pairwise comparison of the five factors are summarized into a 5×5 matrix, R.

Table 1 Linguistic neutrosophic scale

Linguistic term	Value
Extremely highly preferred (EH)	[0.90, 0.10, 0.10]
Extremely preferred (E)	[0.85, 0.20, 0.15]
Very highly to extremely preferred (VSE)	[0.80, 0.25, 0.20]
Very highly preferred (VH)	[0.75, 0.25, 0.25]
Highly preferred (H)	[0.70, 0.30, 0.30]
Moderately highly to strongly preferred (MHS)	[0.65, 0.30, 0.35]
Moderately highly preferred (MH)	[0.60, 0.35, 0.40]
Equally to moderately preferred (EM)	[0.55, 0.40, 0.45]
Equally preferred (EE)	[0.50, 0.50, 0.50]
Moderately to equally preferred (ME)	[0.45, 0.60, 0.55]
Moderately lowly preferred (ML)	[0.40, 0.65, 0.60]
Moderately lowly to lowly preferred (MLL)	[0.35, 0.70, 0.65]
Lowly preferred (L)	[0.30, 0.70, 0.70]
Very lowly preferred (VL)	[0.25, 0.75, 0.75]
Mildly to very lowly preferred (VLE)	[0.20, 0.75, 0.80]
Mildly preferred (M)	[0.15, 0.80, 0.85]
Mildly lowly preferred (EL)	[0.10, 0.90, 0.90]

Step 2: Aggregating individual neutrosophic evaluation into group evaluation The neutrosophic arithmetic average aggregating operator [50] is calculated using Eq. (7). For a simple SVNS E_j; ($j = 1, 2, \ldots, n$), the aggregated value is obtained by:

$$F_w\left(E_1, E_2, \ldots\ldots, E_n\right) = \left\langle 1 - \prod_{j=1}^{n}\left(1 - T_{E_j}(x)\right)^{w_j}, 1 - \prod_{j=1}^{n}\left(1 - I_{E_j}(x)\right)^{w_j}, 1 - \prod_{j=1}^{n}\left(1 - F_{E_j}(x)\right)^{w_j} \right\rangle \tag{7}$$

where $W = (w_1, w_2 \ldots w_{\mathrm{n}})$ is the weight vector of E_j; ($j = 1,2,\ldots,n$); w_j ε[0; 1] and $\sum_{j=1}^{n} wj = 1$.

Step 3: Constructing a consistent pairwise comparison matrix Checking the consistency of the aggregated matrix is vital. The consistency can be checked in two ways [51, 52]. One method is by changing the neutrosophic values into corresponding crisp values using Eq. (6) and deploying the conventional method to calculate the consistency to be less than 0.1. The other method consists of modifying the obtained neutrosophic aggregated matrix into a consistent matrix. The authors adopt the second method because it decreases the experts' repetitive involvement and thus saves time and effort. The consistent matrix is then represented as ($T'_{\mathrm{xk}}; I'_{\mathrm{xk}}; F'_{\mathrm{xk}}$), and the involved steps are shown in Eqs. (8–10):

$$T'_{xk} = \frac{\sqrt[k-x-1]{T_{xy} * T_{yk} * T_{xk-1} * T_{k-1k}}}{\sqrt[k-x-1]{T_{xy} * T_{yk} * T_{xk-1} * T_{k-1k}} + \sqrt[k-x-1]{\left(1 - T_{xy}\right) * \left(1 - T_{yk}\right) * \left(1 - T_{xk-1}\right) * \left(1 - T_{k-1k}\right)}} \tag{8}$$

$$I'_{xk} = \frac{\sqrt[k-x-1]{I_{xy} * I_{yk} * I_{xk-1} * I_{k-1k}}}{\sqrt[k-x-1]{I_{xy} * I_{yk} * I_{xk-1} * I_{k-1k}} + \sqrt[k-x-1]{\left(1 - I_{xy}\right) * \left(1 - I_{yk}\right) * \left(1 - I_{xk-1}\right) * \left(1 - I_{k-1k}\right)}} \tag{9}$$

$$F'_{xk} = \frac{\sqrt[k-x-1]{F_{xy} * F_{yk} * F_{xk-1} * F_{k-1k}}}{\sqrt[k-x-1]{F_{xy} * F_{yk} * F_{xk-1} * F_{k-1k}} + \sqrt[k-x-1]{\left(1 - F_{xy}\right) * \left(1 - F_{yk}\right) * \left(1 - F_{xk-1}\right) * \left(1 - F_{k-1k}\right)}} \tag{10}$$

For $k > x + 1, \quad LetN_{xk} = \left(T'_{xk}, I'_{xk}, F'_{xk}\right), where\, y = x + 1$
For $k = x + 1, LetN_{xk} = \left(T_{xk}, I_{xk}, F_{xk}\right), where\, y = x + 1$
For $k < x, LetN_{xk} = \left(F'_{xk}, 1 - I'_{xk}, T'_{xk}\right),\ wherey = x + 1$

The above steps are repeated by the decision-maker until a consistent aggregated matrix is achieved. The consistency ratio represents the number of acceptable inconsistencies. It is calculated using Eq. (11) and should be less than 0.1. The value 0.1 is interpreted as 'the amount of inconsistent data being used is 10%.' Therefore, the acceptable value of CR is less than or equal to 0.1.

$$\mathrm{CR} = \frac{1}{2(n-1)(n-2)} \sum_{x=1}^{n} \sum_{k=1}^{n} \left(\left|T'_{xk} - T_{xk}\right| + \left|I'_{xk} - I_{xk}\right| + \left|F'_{xk} - F_{xk}\right| \right) \tag{11}$$

Step 4: Determining the neutrosophic relative weights of each preference relation After obtaining the consistent matrix R_0, the calculations are continued on R_0. An eigenvector process is employed to obtain the neutrosophic weights vector, $w = w_1; w_2; \ldots w_n$. Initially, the weights are normalized, and then the final weights are calculated.

Step 5: Calculating the final weight The rating of each factor is multiplied by the corresponding weights of the subfactor, and then, the local weights are obtained with respect to each main factor. These local ratings are further deployed to calculate the aggregated global ratings by multiplying them with the weights of the main factor.

Step 6: Converting neutrosophic numbers into crisp numbers Now, the obtained neutrosophic weights need to be converted into crisp numbers to obtain the overall ranking of the factor. This is done with the help of Eq. (6) and is known as the 'Deneutrosophication' phase.

The above steps define the overall methodology adopted by the researchers for prioritizing the fog computing security factors, as shown in Fig. 3. The implementation is described further.

6 Fog computing security assessment

The integrated methodology of NAHP has been utilized by researchers to address fog computing security more effectively and efficiently. The AHP is best known for its simple and efficient analysis [12], and the use of a neutrosophic scale compliments its functionalities and makes the integrated methodology well-suited for the

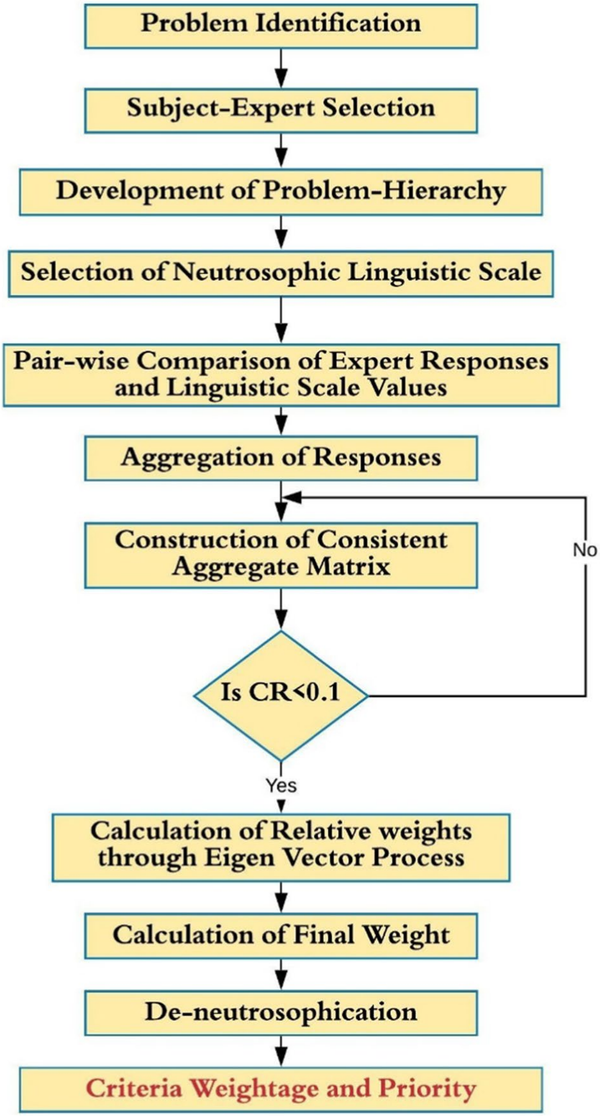

Problem Identification
Subject-Expert Selection
Development of Problem-Hierarchy
Selection of Neutrosophic Linguistic Scale
Pair-wise Comparison of Expert Responses and Linguistic Scale Values
Aggregation of Responses
Construction of Consistent Aggregate Matrix
No
Is CR<0.1
Yes
Calculation of Relative weights through Eigen Vector Process
Calculation of Final Weight
De-neutrosophication
Criteria Weightage and Priority

Fig. 3 Neutrosophic AHP methodology

Table 2 Response of expert '1' of level 1 factors

Expert '1'	C1	C2	C3	C4	C5
Access Control (C1)	EE	H	MH	ML	VH
Integrity (C2)	L	EE	EL	H	MH
Data Protection (C3)	ML	EH	EE	EL	L
Privacy (C4)	MH	L	EH	EE	H
Intrusion Detection (C5)	VL	ML	H	L	EE

Table 3 Neutrosophic value of response of expert ‘1’ of level 1 factors

Expert ‘1’	C1	C2	C3	C4	C5
C1	[0.50, 0.50, 0.50]	[0.70, 0.30, 0.30]	[0.60, 0.35, 0.40]	[0.40, 0.65, 0.60]	[0.75, 0.25, 0.25]
C2	[0.30, 0.70, 0.70]	[0.50, 0.50, 0.50]	[0.10, 0.90, 0.90]	[0.70, 0.30, 0.30]	[0.60, 0.35, 0.40]
C3	[0.40, 0.65, 0.60]	[0.90, 0.10, 0.10]	[0.50, 0.50, 0.50]	[0.10, 0.90, 0.90]	[0.30, 0.70, 0.70]
C4	[0.60, 0.35, 0.40]	[0.30, 0.70, 0.70]	[0.90, 0.10, 0.10]	[0.50, 0.50, 0.50]	[0.70, 0.30, 0.30]
C5	[0.25, 0.75, 0.75]	[0.40, 0.65, 0.60]	[0.70, 0.30, 0.30]	[0.30, 0.70, 0.70]	[0.50, 0.50, 0.50]

assessment of fog computing security by prioritizing the identified factors. Initially, a total of 50 experts were approached to comment on the prioritization of the identified fog computing security factors through a questionnaire. The experts included in the proposed work were from academia and industry (security and/or network specialists). Out of 50 responses, some were ambiguous or incomplete, and some of the experts did not even revert to the questionnaire. As a result, the authors were left with 42 appropriate responses that were included in this study. For a detailed explanation of the methodology, the response collected from Expert 1 is shown as an example in the following steps. All the steps (as seen through Expert 1 data) have been carried out over the data obtained from all the experts.

The step-by-step implementation of the methodology is as follows:

Step 1 The pairwise comparison matrix, as received by Expert ‘1,’ is mentioned in Table 2, and its corresponding neutrosophic values are given in Table 3. Similarly,

Table 4 Aggregated matrix of level 1 factors

R	C1	C2	C3	C4	C5
C1	[0.50, 0.50, 0.50]	[0.72, 0.33, 0.34]	[0.67, 0.38, 0.39]	[0.41, 0.67, 0.66]	[0.71, 0.43, 0.43]
C2	[0.28, 0.67, 0.66]	[0.50, 0.50, 0.50]	[0.60, 0.52, 0.52]	[0.39, 0.67, 0.67]	[0.62, 0.45, 0.45]
C3	[0.33, 0.62, 0.61]	[0.40, 0.48, 0.48]	[0.50, 0.50, 0.50]	[0.29, 0.78, 0.77]	[0.63, 0.45, 0.45]
C4	[0.59, 0.33, 0.34]	[0.61, 0.33, 0.33]	[0.71, 0.22, 0.23]	[0.50, 0.50, 0.50]	[0.74, 0.31, 0.32]
C5	[0.29, 0.57, 0.57]	[0.38, 0.55, 0.55]	[0.37, 0.55, 0.55]	[0.26, 0.69, 0.68]	[0.50, 0.50, 0.50]

Table 5 Consistent aggregated matrix of level 1 factors

R′	C1	C2	C3	C4	C5
C1	[0.500,0.500,0.500]	[0.720,0.330,0.340]	[0.794,0.348,0.358]	[0.538,0.595,0.599]	[0.670,0.417,0.421]
C2	[0.340,0.670, 0.720]	[0.500,0.500,0.500]	[0.600,0.520,0.520]	[0.379,0.793,0.783]	[0.683,0.473,0.479]
C3	[0.358,0.652,0.794]	[0.520,0.480,0.600]	[0.500,0.500,0.500]	[0.290,0.780,0.770]	[0.537,0.614,0.612]
C4	[0.599,0.405,0.538]	[0.783,0.207,0.379]	[0.770,0.220,0.290]	[0.500,0.500,0.500]	[0.740,0.310,0.320]
C5	[0.421,0.583,0.670]	[0.479,0.527,0.683]	[0.612,0.386,0.537]	[0.320,0.690,0.740]	[0.500,0.500,0.500]

Table 6 Relative weights of level 1 factors

	C1	C2	C3	C4	C5	Norm. Val	Rel. wt	Rank
C1	[0.520,0.473,0.443]	[0.726,0.325,0.323]	[0.796,0.343,0.351]	[0.578,0.536,0.537]	[0.675,0.406,0.409]	0.992	0.206	2
C2	[0.353,0.652,0.688]	[0.504,0.496,0.487]	[0.602,0.517,0.515]	[0.407,0.763,0.750]	[0.688,0.463,0.468]	0.950	0.197	4
C3	[0.372,0.633,0.770]	[0.524,0.476,0.590]	[0.502,0.496,0.494]	[0.311,0.748,0.735]	[0.541,0.607,0.604]	0.929	0.193	5
C4	[0.623,0.373,0.486]	[0.789,0.201,0.363]	[0.772,0.215,0.282]	[0.537,0.427,0.423]	[0.745,0.297,0.306]	0.996	0.207	1
C5	[0.438,0.561,0.633]	[0.483,0.523,0.675]	[0.614,0.382,0.532]	[0.344,0.645,0.700]	[0.504,0.490,0.490]	0.953	0.198	3

the responses of all the experts were converted into corresponding neutrosophic values.

Step 2 The aggregated neutrosophic matrix of the responses of all the experts was obtained through Eq. (7), as shown in Table 4.

Step 3 The consistent matrix R_0 corresponding to R obtained by Eqs. (8–10) is shown in Table 5. The CR value of R_0 is calculated by Eq. (11) and is 0.095, which is less than 0.1. Thus, it is concluded that the values obtained are consistent in nature, and further calculations are carried out on R_0.

Step 4 At this step, the neutrosophic relative weights are calculated by deploying a general eigenvector process on a consistent aggregated matrix. The final matrix with the ranks obtained after the process is shown in Table 6.

Step 5 At this step, the weights of the main factor(s) and the corresponding subfactors are multiplied together to obtain the global weights.

Table 7 Final level 2 weights of access control (C1)

Subfactor	Deneutrosophic value	Relative weight	Percentage	Rank
Authentication policy (C11)	0.8418	0.224	22.4	4
Authorization (C12)	0.9893	0.264	26.4	1
Identification (C13)	0.9468	0.252	25.2	3
Trust (C14)	0.9763	0.260	26.0	2

Table 8 Final level 2 weights of integrity (C2)

Subfactor	Deneutrosophic value	Relative weight	Percentage	Rank
Non-repudiation (C21)	0.9785	0.365	36.5	1
Credibility (C22)	0.7373	0.275	27.5	3
Delegation (C23)	0.9645	0.360	36.0	2

Table 9 Final level 2 weights of data protection (C3)

Subfactor	Deneutrosophic value	Relative weight	Percentage	Rank
Insider threats (C31)	0.9203	0.343	34.3	2
Secure transmission protocol (C32)	0.9888	0.368	36.8	1
Redundancy (C33)	0.7765	0.289	28.9	3

Step 6 Finally, the obtained values are converted into crisp numbers, and the global ranking is obtained.

It should be noted that Steps (1–6) are repeated, and the weights for the second-level factors with the deneutrosophied corresponding numbers are also

Table 10 Final level 2 weights of privacy (C4)

Subfactor	Deneutrosophic value	Relative weight	Percentage	Rank
Anonymization (C41)	0.9257	0.244	24.4	3
Obfuscation (C42)	0.9883	0.260	26.0	1
Encryption (C43)	0.9633	0.254	25.4	2
Aggregation (C44)	0.9189	0.242	24.2	4

Table 11 Final level 2 weights of intrusion detection (C5)

Subfactor	Deneutrosophic value	Relative weight	Percentage	Rank
Detection algorithm (C51)	0.9725	0.361	36.1	1
Verifiability (C52)	0.7602	0.282	28.2	3
Alert generation (C53)	0.9633	0.357	35.7	2

Table 12 The deneutrosophied global weights of factors and subfactors

Factor	Factor weight	Subfactor (SF)	SF local weight	Global weight	Rank
C1	0.206	C11	0.224	0.0461	17
		C12	0.264	0.0543	9
		C13	0.252	0.0519	14
		C14	0.260	0.0535	12
C2	0.197	C21	0.365	0.0719	1
		C22	0.275	0.0541	10
		C23	0.360	0.0709	4
C3	0.193	C31	0.343	0.0662	6
		C32	0.368	0.0710	3
		C33	0.289	0.0557	8
C4	0.207	C41	0.244	0.0505	15
		C42	0.260	0.0538	11
		C43	0.254	0.0525	13
		C44	0.242	0.0500	16
C5	0.198	C51	0.361	0.0714	2
		C52	0.282	0.0558	7
		C53	0.357	0.0706	5

calculated and represented in Tables 7, 8, 9, 10 and 11. Table 12 contains the global weights of the factors and the subfactors. The graphical representation of Level 1 and Level 2 factors is presented in Figs. 4 and 5, respectively. In the next

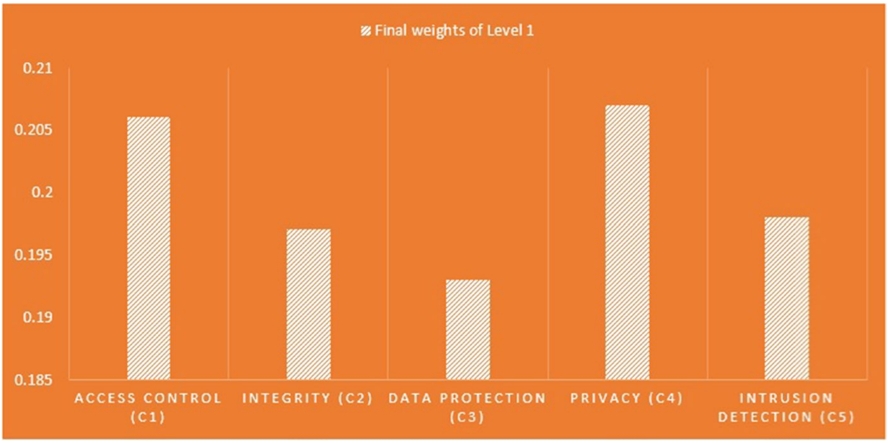


Fig. 4 Final weights of level 1

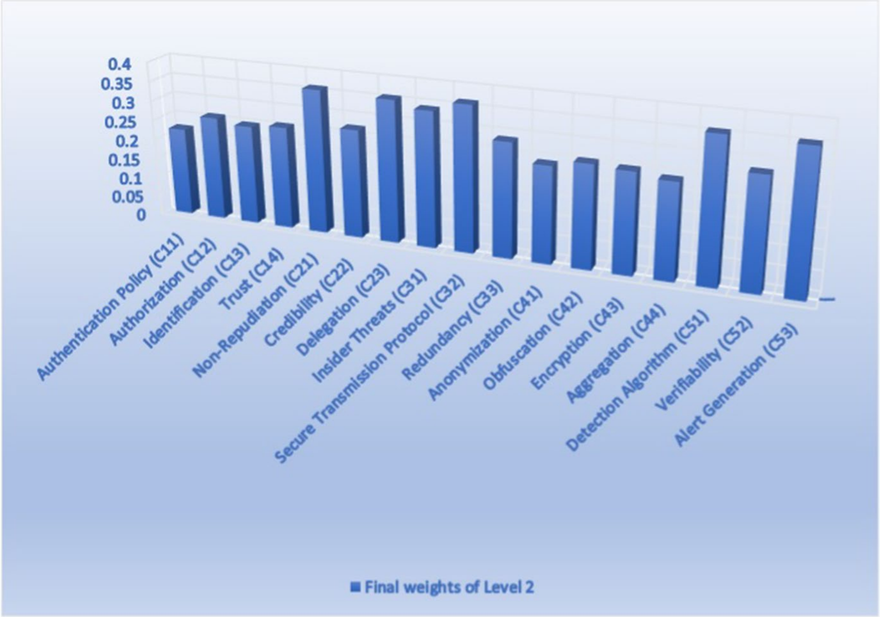


Fig. 5 Final weights of level 2

section, the comparison of the proposed technique with traditional approaches, such as FAHP and CAHP, is described in detail.

Table 13 Range and interpretation of spearman rank correlation coefficient

Range	Interpretation
$0.8 < \rho \leq 1.0$	Very strong relationship
$0.6 < \rho \leq 0.8$	Strong relationship
$0.4 < \rho \leq 0.6$	Average relationship
$0.2 < \rho \leq 0.4$	Weak relationship
$\rho \leq 0.2$	Very weak relationship

Table 14 Comparative analysis

	NAHP	FAHP	CAHP
NAHP	1	0.9215	0.8848
FAHP	0.9215	1	–
CAHP	0.8848	–	1

7 Comparative analysis

In this section, the proposed NAHP methodology is compared to the CAHP [9] and FAHP [58] techniques to observe the relativity of the results obtained by the given approach. The responses of the experts are converted into respective formats to apply to both the techniques, and the global ranks of the security factors are determined in both cases. The authors used the Spearman rank correlation coefficient to determine the correlation among the three methodologies. The Spearman correlation coefficient was selected as the measure of estimating the correlation because it is most the apt for the case of ordinal data [53]. The major advantage of the Spearman correlation coefficient lies with the fact that it can be computed with any kind of variables, including independent or dependent variables, and is given by the formula:

$$\rho = 1 - \frac{6 * \Sigma_{i=1}^{n} d_i^2}{n\left(n^2 - 1\right)} \tag{12}$$

where '*d*' is the difference between the ranks and '*n*' is the number of elements. The range and interpretation of different values of 'ρ' are shown in Table 13 [54].

The value of 'ρ' as determined for the mentioned techniques is presented in Table 14. The obtained values clearly depict the correlation between the proposed NAHP and the other two techniques, which is high. The comparative analysis of the relative weights of the approaches is shown in Fig. 6. The figure clearly depicts the similarity among the approaches. Therefore, it is concluded that the results obtained through NAHP are close to those obtained from the traditional approaches. Additionally, as discussed earlier (Sect. 1), considering the benefits of NAHP over the traditional approaches, the application of NAHP is justified in this scenario. In the next section, the authors discuss the interpretations based on the obtained results. The pros and cons of the proposed technique are also discussed in detail.

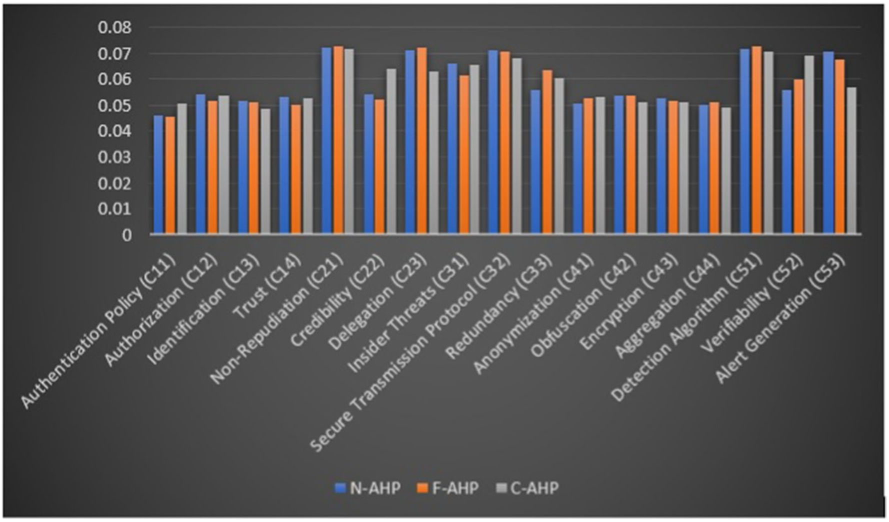


Fig. 6 Comparison of relative weights by NAHP, FAHP and CAHP

8 Discussion

In recent years, IoT data breaches have taken a toll on sensitive user data, posing a big question regarding the security of data flowing in the fog-IoT environment. It was reported by ZDNet in October 2019 that smart assistants, such as Google Assistant and Alexa, spy on user's personal data without any prior notification [55]. The security executive at Avast has recently stated that the identity and bank details of any individual can easily be stolen using a smart coffee machine [56]. Such incidents make the security of sensitive data flowing across the Internet a critical issue. Security is multidimensional in nature. The security of any software, system or platform is dependent on various factors. For proper and efficient security management, analysis of each factor and subfactor is needed. The order in which the different factors are assessed is another problem that needs to be considered. This makes security management a decision-making problem.

Fog computing security depends on factors such as access control, integrity and privacy. Finding an appropriate security solution is possible only when various factors and subfactors are efficiently managed at the earlier stages. Thus, the authors identified the different fog computing security factors and subfactors and organized them into a hierarchical structure. Furthermore, the identified factors and subfactors are ranked on the basis of their severity based on the experts' responses. The experts' responses are evaluated via a neutrosophic scale for accurate and consistent analysis. The weights of the factors at level-1 and the subfactors at level-2 are calculated by deploying the NAHP technique. The global weights of the factors are also estimated by the authors. Hence, the advantages of the presented NAHP approach are the following:

- It provides a systematic method to manage different security factors at earlier stages.
- Early management of security factors helps to properly estimate the overall fog security.
- The prioritization of the security factors at the fog level using the neutrosophic scale helps for accurate, consistent and unambiguous security analysis.
- The use of the neutrosophic scale reduces the experts' repetitive involvement by providing a way of constructing a consistent matrix from the inconsistent data if obtained. This saves time and effort.
- The proposed study can help industry professionals develop secure IoT applications to be deployed at the fog level.

However, the proposed research work also has some limitations:

- The opinions of only forty-two experts are considered for this research work. Including more expert responses may help achieve a more accurate security estimation.
- The fog computing security factors identified by the authors are not exhaustive in nature. Some factors may have been left unconsidered.

The main aim of this research study is to provide an efficient, consistent and accurate method for handling security factors at the fog level in a systematic manner. In the future, researchers are planning to address the identified security factors one-by-one on the basis of their priority to enhance security at the fog level.

9 Conclusion

Security cannot be incorporated only externally. It needs to be incorporated at each level. The categorization of fog computing security factors helps in maintaining the overall security of the Fog-IoT environment. As per the reviewed literature, the authors found no such mechanism in a fog environment that evaluates the severity of fog computing security factors using a neutrosophic approach. For proper estimation of fog computing security, the categorization of different factors and subfactors is very important.

The NAHP approach presents a quantitative method to estimate the weights of fog security factors and subfactors. The use of a neutrosophic linguistic scale adds to the accuracy and consistency of the obtained results. The results of the proposed NAHP approach are compared to those obtained from the FAHP and CAHP. NAHP is highly correlated with the mentioned techniques, which marks the applicability of the research work. Furthermore, this mechanism may be utilized by security practitioners to efficiently and systematically manage security at the fog level. On the basis of the ranking obtained in this study, researchers are planning to consider security factors in fog scenarios in the near future. For instance, the researchers may now first develop a privacy preservation approach through its highly ranked subfactor mechanism, e.g., obfuscation. Then, an access control mechanism will be developed.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare that there lies no conflict of interest.

References

1. "IDC: Analyze the Future". Available online at: https://www.idc.com/getdoc.jsp?containerld prUS45213219 [Accessed: 25/06/2021]
2. Mouradian C, Naboulsi D, Yangui S, Glitho RH, Morrow MJ, Polakos PA (2017) A comprehensive survey on fog computing state-of-the-art and research challenges. IEEE Commun Surv Tutorials 20(1):416–464
3. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on mobile cloud computing pp 13–16
4. Puthal D, Obaidat MS, Nanda P, Prasad M, Mohanty SP, Zomaya AY (2018) Secure and sustainable load balancing of edge data centers in fog computing. IEEE Commun Mag 56(5):60–65
5. Verma R, Chandra S (2019) Security and privacy Issues in fog driven IoT Environment. Int J Comput Sci Eng 7(5):367–370
6. Verma R, Chandra S (2020) A systematic survey on fog steered IoT: architecture, prevalent threats and trust models. Int J Wirel Inform Netw. https://doi.org/10.1007/s10776-020-00499-z
7. Kaur J, Agrawal A, Khan RA (2020) Security issues in fog environment: a systematic literature review. Int J Wirel Inf Networks 27:467483
8. Choo KKR, Lu R, Chen L, Yi X (2018) A foggy research future: advances and future opportunities in fog computing research. Future Gener Comput Syst. https://doi.org/10.1016/j.future.2017.09.014
9. Kaur J, Agrawal A, Khan RA (2020) Security assessment in foggy era through analytical hierarchy process. In: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) pp 1–6. IEEE
10. Pei S, Radovanovi M, Ivanovi M, Badica C, Toi M, Ikovi O, Bokovi D (2019) CAAVI-RICS model for analyzing the security of fog computing systems. International symposium on intelligent and distributed computing. Springer, Cham, pp 23–34
11. Ogundoyin SO, Kamil IA (2020) A Fuzzy-AHP based prioritization of trust criteria in fog computing services. Appl Soft Comput 97:106789
12. Singh V, Pandey D, Sahu K, Khan MW (2020) Optimizing the impact of security attributes in requirement elicitation techniques using FAHP. Communications 14:15
13. Alenei M, Pandey AK, Verma R, Faizan M, Chandra S, Agrawal A, Kumar R, Khan RA (2021) Evaluating the impact of software security tactics: a design perspective. CMC-Comput Mater Continua 66(3):2283–2299
14. Al-Zahrani FA (2020) Evaluating the usable-security of healthcare software through unified technique of fuzzy logic, ANP and TOPSIS. IEEE Access 8:109905–109916
15. Zadeh LA (1965) Fuzzy sets. Inform Control 8(3):338–353
16. Abdullah L (2013) Fuzzy multi criteria decision making and its applications: a brief review of category. Procedia Soc Behav Sci 97:131–136
17. Lupiez FG (2017) On neutrosophic sets and topology. Procodia Comput Sci 120:975–982
18. Radwan NM, Senousy MB, Alaa El Din MR (2016) Neutrosophic AHP multi criteria decision making method applied on the selection of learning management system. Infinite Study
19. Nabeeh NA, Abdel-Basset M, El-Ghareeb HA, Aboelfetouh A (2019) Neutrosophic multi-criteria decision-making approach for iot-based enterprises. IEEE Access 7:59559–59574
20. Kahraman C, Otay-stayi B, Onar S (2019) An integrated AHP & DEA methodology with neutrosophic sets. Fuzzy multi-criteria decision-making using neutrosophic sets. Springer, Cham, pp 623–645
21. Alava MV, Delgado Figueron SP, Blum Aleivar HM, Loyva Vazquez MY (2018) Single valued neutrosophic numbers and analytic hierarchy process for project selection. Neutrosophic Sets and Systems 21(1):13

22. Abdel-Basset M, Mohamed M, Zhou Y, Hezam L (2017) Multi-criteria group decision making based on neutrosophic analytic hierarchy process. J Intell Fuzzy Syst 33(6):4055–4066
23. Edge computing vs. fog computing: Definitions and enterprise uses. Available online at: https://www.cisco.com/c/en/us/solutions/enterprise-networks/edge-compating.html [Accessed: 28/07/2021]
24. Mukherjee M, Matam R, Shu L, Maglaras L, Ferrag MA, Choudhury N, Kumar V (2017) Security and privacy in fog computing: challenges. IEEE Access 5:19293–19304
25. Ni J, Zhang K, Lin X, Shen XS (2017) Securing fog computing for internet of things applications: challenges and solutions. IEEE Commun Surv Tutor 20(1):601–628
26. Singh SP, Nayyar A, Kumar R, Sharma A (2019) Fog computing: from architecture to edge computing and big data processing. J Supercomput 75(4):2070–2105
27. Zhang P, Zhou M, Fortino G (2018) Security and trust issues in fog computing A survey. Futur Gener Comput Syst 88:16–27
28. Kaur J, Verma R, Alharbe NR, Agrawal A, Khan RA (2020) Importance of fog computing in healthcare 4.0.7. In: Fog computing for healthcare 4.0 environments. Springer, Cham pp 79–101
29. Erdoan M, Karaan A, Kaya Budak A, olak M (2019) A fuzzy based MCDM methodology for risk evaluation of cyber security technologies. In: International Conference on Intelligent and Fuzzy Systems. Springer, Cham, pp 1042–1049
30. Hinduja A, Pandey M (2020) An ANP-GRA-based evaluation model for security features of loT systems. Intelligent communication, control and devices. Springer, Singapore, pp 243–253
31. Turkis Z, Goranin N, Nurusheva A, Boranbayev S (2019) Information security risk assessment in critical infrastructure: a hybrid MCDM approach. Informatica 30(1):187–211
32. Oh J, Lee U, Lee K (2019) Usability evaluation model for biometric system considering privacy concern based on MCDM model. Secur Commun Netw. https://doi.org/10.1155/2019/8715264
33. Kaušpadienė L, Ramanauskaitė S, Čenys A (2019) Information security management framework suitability estimation for small and medium enterprise. Infinite Study
34. Bhol SG, Mohanty JR, Pattoaik PK (2120) Cyber security metrics evaluation using multi-criteria decision-making approach in smart intelligent computing and applications. Springer, Singapore, pp 665–675
35. Sahin R, Yüder M (2014) A multi-criteria neutrosophic group decision making method based TOPSIS for supplier selection arXiv preprint arXiv:1112.5077
36. Biswas P, Pramatok S, Gin BC (2016) TOPSIS method for multi-attribute group decision-making under singh-valond neutrosophie environment. Neural Comput Appl 27(3):727–737
37. Abdel-Basset M, Mohamed M, Smarandache F (2018) An extension of neutrosophic AHPSWOT analysis for strategic planning and decision-making. Symmetry 10(4):116
38. Abdel-Basset M, Manogaran G, Mohamed M, Chilamkurti N (2018) Three-way decisions based on neutrosophic sets and AHP-QFD framework for supplier selection problem. Futur Gener Comput Syst 89:19–30
39. Tey DJY, Gan YF, Selvachandran G, Quek SG, Smarandache F, Abdel-Basset M, Long HV (2019) A novel neutrosophic data analytic hierarchy process for multi-criteria decision-making method: a case study in Kuala Lumpur stock exchange. IEEE Access 7:53687–53697
40. Kahraman C, Oztaysi B, Cevik Onar S (2020) Single & interval-valued neutrosophic AHP methods: Performance analysis of outsourcing law firms. J Intell Fuzzy Syst 38(1):749–759
41. Abdel-Basset M, Manogaran G, Mohamed M (2019) A neutrosophic theory-based security approach for fog and mobile-edge computing. Comput Netw 157:122–132
42. "Digital trends 2022: Every single stat you need to know about the Internet". Available online at: https://datareportal.com/reporta/digital-2022-global-overview-report [Accessed: 22/05/2022]
43. Xue K, Hong J, Ma Y, Wel DS, Hong P, Yu N (2018) Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing. IEEE Network 32(3):7–13
44. Fan K, Xu H, Gao L, Li H, Yang Y (2019) Efficient and privacy preserving access control scheme for fog-enabled loT. Futur Gener Comput Syst 99:134–142
45. Alazeb A, Panda B (2019) Ensuring data integrity in fog computing based health care systems. In: International Conference on Security, Privacy and Anonymity in Com putation, Communication and Storage. Springer, Cham, pp 63–77
46. Dang TD, Hoang D (2017) A data protection model for fog computing. In: 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC) pp 32–38. IEEE

47. Mukherjee M, Ferrag MA, Maglaras L, Derhab A, Anzam M (2020) Security and privacy issues and solutions for fog. In: Fog and fogonomics: challenges and practices of fog computing, communication, networking, strategy, and economics
48. Almogren AS (2020) Intrusion detection in edge-of-things computing. J Parallel Distrib Comput 137:259–265
49. Smarandache F (1998) Neutrosophy: neutrosophic probability, set, and logic: analytic synthesis & synthetic analysis
50. Ye J (2014) A multicriteria decision-making method using aggregation operators for simplified neutrosophic sets. Journal of Intelligent & Fuzzy Systems 26(5):2459–2466
51. Sahin R, Yigider M (2014) "A Multi-criteria neutrosophic group decision making method based TOPSIS for supplier selection" arXiv preprint arXiv:1412.5077
52. Ye J (2015) An extended TOPSIS method for multiple attribute group decision making based on single valued neutrosophic linguistic numbers. J Intell Fuzzy Syst 28(1):247–255
53. Correlation (Pearson, Kendall. Spearman Available online https://www.statisticssolutions.com/correlation-pearson-kendall-spearman/ (Accessed on: 09/08/2021)
54. Kline P (1999) The handbook of psychological testing, 2nd edn. Routledge, London, England
55. Alexa and Google Home Devices Have Been Eavesdropping on Us, Again! Available on line at: https://www.pentasecurity.com/blog/top-5-shocking-lot-security-breaches-2019/ (Accessed: 15/07/2021)
56. Hackers can Steal Your Identity and Bank Details from a Coffee Machine. Available online at: http://www.cisomag.com/10-iot-security incidents-that-make-you-feel-less-secure/ (Accessed: 15/07/2021)
57. Wang H, Smarandache F, Zhang Y, Sunderraman R (2010) Single valued neutrosophic sets. Infinite study
58. Kaur J, Agrawal A, Khan RA (2022) A fuzzy AHP approach for prioritizing fog computing security parameters. In: Proceedings of First International Conference on Computational Electronics for Wireless Communications. Springer, Singapore, pp 535–543
59. Kaur J, Agrawal A, Khan RA (2022) Encryfuscation: a model for preserving data and location privacy in Fog based IoT scenario. J King Saud Univ-Comput Inform Sci. https://doi.org/10.1016/j.jksuci.2022.03.003

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.