Information Sciences 607 (2022) 758–782

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A computational trust model for social IoT based on interval neutrosophic numbers

Sajad Pourmohseni, Mehrdad Ashtiani, Ahmad Akbari Azirani *

School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran

ARTICLE INFO

Article history:
Received 16 April 2020
Received in revised form 29 May 2022
Accepted 31 May 2022
Available online 8 June 2022

Keywords:
Social internet of things (SIoT)
Trust management
Uncertainty
Honesty
Context awareness
Interval neutrosophic numbers

ABSTRACT

Nowadays, the trend of evolution of connected devices, communication networks, and cloud services towards the internet of things (IoT) has facilitated the interaction between smart objects with minimal human mediation. Considering IoT, where smart objects can be clients and providers of services for each other, trust between objects is a significant concern for selecting the most appropriate service providers. Trust is an uncertain concept, and its uncertainty originates from different sources, including context conditions, social relationships, and the accuracy of quantitative evaluations. Modeling and considering uncertainty in trust management for the IoT is the principal objective of this research. To this aim, several sources of uncertainty are modeled in trust calculations where interval neutrosophic numbers are used for modeling imprecision, indeterminacy, and inconsistency of the trustworthiness data. In the proposed model, trust in the quality of the provided services (QoS trust), as well as trust in the honesty of the socially related entities providing trust-related information (i.e. social trust), and trust in the suitability of context conditions (i.e. context-trust) are considered to calculate the overall trust used for the decision-making process. The impact of each of these dimensions on the final calculated trust has been evaluated in different scenarios.

1. Introduction

With the growing trend of using wireless objects and providing communication facilities for a large number of smart objects connected through the internet of things (IoT), various types of interactions have been made possible [1]. In the service-oriented architecture (SOA)-based IoT, smart things can be service providers (SPs) or service requesters (SRs), interacting with each other for receiving or providing different services [1,2]. With the introduction of social IoT (SIoT) [3], selecting a trustworthy object for the service has faced many challenges over the past decade. In such situations, recognizing the most appropriate objects for interaction and obtaining the most accurate information require establishing and managing relative trust among objects.

Trust management has a special place in IoT, which acts as an enabler to meet the quality of service satisfaction, allocation of secure and trustworthy computational resources [4], privacy [5], and several other factors such as reliability [6], honesty [7], and cooperativeness [8]. Without trust management, malicious or malfunctioning objects providing inappropriate services or incorrect information about other services will significantly increase the disadvantages of using IoT, making it prac-

* Corresponding author at: School of Computer Engineering, Iran University of Science and Technology, Hengam St., Resalat Sq., Tehran, Iran. Postal Code: 16846-13114; Fax: +98-21-73021480.

E-mail addresses: spurmohseni@gmail.com (S. Pourmohseni), m_ashtiani@iust.ac.ir (M. Ashtiani), akbari@iust.ac.ir (A. Akbari Azirani).

https://doi.org/10.1016/j.ins.2022.05.124
0020-0255/

tically unusable [9]. Trust management incorporates several objectives, including providing a measure for IoT entities to decide their interactions as well as organizing their relationships with other entities [8], while preserving their privacy [5]. Although not being the focus of this paper, in addition to maintaining the QoS, privacy preservation must also be considered in designing IoT applications [10]. Privacy preservation is a challenge that IoT trust management systems must address [5].

Considering QoS as the determining factor for selecting the best SP, several properties influence the estimated trust in the decision-making process. These properties may be subjective or objective characteristics of SPs or SRs as well as context conditions [8,2]. Previous studies have examined the effects of social aspects on trust, including the community of interest (CoI) [6,1], honesty [6,1,7], cooperativeness [6,1], and subjective trustworthiness [8]. Context conditions as another important aspect of trust calculation have been considered in various studies [2,11]. It has been shown that an object might have a certain behavior in a specific context, where the quality of context influences the expectations regarding the experienced QoS.

In this study, trust is not assumed a definite number, and the level of trust between two entities is considered as an uncertain value. Based on this viewpoint, uncertainty is an essential component of trust [12,13]. Thus, quantifying the uncertainty level and its application in evaluating the trust value can improve the accuracy and validity of the evaluated trust. To date, several studies have been performed regarding uncertainty modeling in the trust computation in various application domains [13–15]. However, there are very few works that have examined the effect of uncertainty in IoT trust computation [16,17,2,18]. Most of these studies state that investigating sources of uncertainty was not their principal concern. As such, the impact of uncertainty in IoT trust management has received less attention.

The model proposed in this research considers uncertainty as a key factor in trust calculations, considering various sources of uncertainty in the evaluation of input data, lack of knowledge, and context conditions. In the proposed model, trust in the quality of the provided services by the SPs (i.e. QoS Trust) is considered along with trust in the honesty of IoT entities providing trust-related information (i.e. social trust), and the trust of context conditions suitability (i.e. context trust) to calculate the overall trust. The quality of context conditions can influence the quality of services provided by SPs. This is also investigated by several works demonstrating the relationship between the quality of context and the services presented by SPs [11,2].

Additionally, confidence in the correctness of the trust-related information received from other entities, i.e., the fairness of recommendations, affects the calculated trust [19]. Generally, the proposed model considers context conditions and the honesty of entities as parameters for uncertainty modeling in the trustworthiness calculations. So far, different studies have been performed on the sources of uncertainty, and it has been concluded that these factors can be known or unknown [20]. Thus, uncertainties may be due to a lack of knowledge about the factors for determining the true value or because of measurement errors. Based on this viewpoint, the proposed model considers two types of uncertainty: (1) uncertainty caused by a lack of knowledge about the true values of the quantitative evaluations and (2) uncertainty resulted from a set of unspecific factors influencing the expected QoS. Each set of unspecific factors that cannot be considered separately is modeled as a high-level context condition, affecting the total QoS of the SP entity. However, if the influencing factors are known, their effect is regarded separately on their relevant trust evaluation criteria.

The proposed approach adopts a two-level view of QoS trust. The first one is a detailed view coming from a multi-criteria view toward trust. In this view, trust is considered as a combination of several criteria specified by the expert or the users of IoT services. In addition, the influencing factors in the context conditions of the service are known, and experts can specify their impact on the QoS. The second viewpoint is a coarse-grained view of the QoS in different contexts. The importance of this high-level aggregated view is that the complete functionality of the entity is examined under a set of conditions that cannot be investigated one by one. Also, there is a lack of knowledge about the impact of each individual criterion.

The possibility of contradiction between the received information is recognized as one of the factors causing uncertainty in the proposed model. Then, for representing the trust data model, the information specifying the suitability of the input data is evaluated besides other information about the security or physical safety violations as deterrents. Additionally, an aggregation of the known uncertainty factors is also performed. To satisfy the need for modeling inconsistency and indeterminacy about the input data and as well as the evaluated trust of entities, neutrosophic sets and numbers were used. The rationale behind using this mathematical framework is that neutrosophic numbers provide an appropriate mathematical mechanism for processing data with multiple sources of uncertainty in decision-making problems [21–23].

By reviewing the works performed so far in the domain of computational trust modeling in SIoT, we have inferred that although uncertainty is an essential aspect of the trust nature, modeling different sources of uncertainty in the SIoT trust management schemes deserves more attention. In this regard, we investigated the capabilities of neutrosophic sets and numbers and concluded that this mathematical tool can model several aspects of uncertainty in IoT environments. Consideration of truth, falsity, and indeterminacy for each data block can create more flexibility in uncertainty propagation in trust calculations. Additionally, we can model the primary influential factors in IoT environments based on these three neutrosophic components. Having these motivations, the purpose of this study is to experiment with the use of neutrosophic numbers to model different uncertainty factors in SIoT environments and then develop a logical relationship between this information and the expected level of trust. To tackle this problem, we aimed to develop a computational model for IoT trust management considering different sources of uncertainty using quantitative evaluations, context, as well as preferences of users. The proposed work incorporates the following innovations:

1. Modeling uncertainty in an SOA-based social IoT ecosystem considering the known and unknown sources of uncertainty, the inconsistency between the received information, and the indeterminacy of the input data evaluations.
2. Modeling the context of IoT entities as two sets: (1) a set of known factors influencing certainty and the suitability of trust evaluation criteria; and (2) a set of unknown factors where their impact on the QoS cannot be investigated separately.
3. Using social factors to determine honesty relationships between IoT entities in addition to the QoS trust.
4. Representing a trust computation model combining trust toward the honesty and QoS of IoT entities as well as the appropriateness of the corresponding context conditions for the SP selection.

The remainder of this paper is organized as follows. In Section 2, the background knowledge about trust in the SOA-based social IoT ecosystems is discussed. Also, the mathematical basis for the neutrosophic numbers is presented which is fundamental for understanding the uncertainty modeling in the proposed approach. Section 3 outlines the related work of the proposed approach. In Section 4, the framework and the respective computational model of the proposed approach are introduced. In Section 5, the series of evaluations performed to demonstrate the accuracy of the proposed model, its sensitivity to various parameters, and its comparison with existing similar approaches are presented. Finally, Section 6 concludes the paper.

1.1. Background knowledge

The basic notions of neutrosophic sets and numbers as a mathematical tool for modeling uncertainty and inconsistency in the input data are presented in this section. First, basic concepts related to neutrosophic sets and interval neutrosophic sets as well as numbers are reviewed. The basic notations used in this section are introduced in Table 2. The concept of neutrosophic sets has been introduced by Smarandache in [24], which means exploiting three independent functions for specifying truth, falsity, and indeterminacy for the elements' membership to a set. Assuming X is a space of points, and a generic element x in X exists, the neutrosophic set A defined in X is specified by a truth-membership function $T_A(x)$, an indeterminacy-membership function $I_A(x)$, and a falsity-membership function $F_A(x)$. All these functions map the element x to a real number within $[0^-.1^+]$.

There are several types of neutrosophic sets namely simplified neutrosophic sets (SNS) [25], single-valued neutrosophic sets (SVNS) [26], trapezoidal interval-valued [27], and interval neutrosophic sets (INS) [21]. All of these variations have made different assumptions about the T, I, and F membership functions. The model proposed in this research exploits INSs because of their capability and flexibility to take into account multiple sources of uncertainty. Below, the definitions and some important operations for INS are presented. Assuming X is a space of points, with a generic element X denoted by x, the INS $\tilde{A}$ in X is specified by truth, indeterminacy, and falsity membership functions named $\tilde{T}_{\tilde{A}}(x)$, $\tilde{I}_{\tilde{A}}(x)$, and $\tilde{F}_{\tilde{A}}(x)$ such that $\tilde{T}_{\tilde{A}}(x)$, $\tilde{I}_{\tilde{A}}(x)$, $\tilde{F}_{\tilde{A}}(x) \subseteq [0,1]$. Then, the INS $\tilde{A}$ could be formulated as follows [24]:

$$\begin{aligned}\tilde{A} &= \left\{\langle x, \tilde{T}_{A^\sim}(x), \tilde{I}_{A^\sim}(x), \tilde{F}_{A^\sim}(x)\rangle | x \in X\right\} \\ &= \left\{\langle x, \left[\inf_T\left(\tilde{A}\right), \sup_T\left(\tilde{A}\right)\right], \left[\inf_I\left(\tilde{A}\right), \sup_I\left(\tilde{A}\right)\right], \left[\inf_F\left(\tilde{A}\right), \sup_F\left(\tilde{A}\right)\right]\rangle | x \in X\right\}\end{aligned} \tag{1}$$

If X is assumed as the set of real numbers and x as a real number, $\tilde{T}_{\tilde{A}}(x)$, $\tilde{I}_{\tilde{A}}(x)$, and $\tilde{F}_{\tilde{A}}(x)$ represent the membership of the number x to a neutrosophic set of numbers S. Then, $\tilde{A}$ is called an interval neutrosophic number (INN) which specifies the neutrosophic membership degree for any real number x to the set S. Assuming A and B to be two INNs, the addition and multiplication of two INNs as well as multiplication of one INN by a real number are defined as below [21]:

$$\begin{aligned}A \oplus B = \langle &[inf_T(A) + inf_T(B) - inf_T(A) \times inf_T(B), sup_T(A) + sup_T(B) - sup_T(A) \times sup_T(B)], \\ &[inf_I(A) \times inf_I(A), sup_I(A) \times sup_I(A)], [inf_F(A) \times inf_F(B), sup_F(A) \times sup_F(B)]\rangle\end{aligned}$$

$$\begin{aligned}A \otimes B = \langle &[inf_T(A) + inf_T(B), sup_T(A) \times sup_T(B)], [inf_I(A) \times inf_I(A) - inf_I(A) \times inf_I(A), sup_I(A) \times sup_I(A)], \\ &[inf_F(A) \times inf_F(B), sup_F(A) \times sup_F(B)]\rangle\end{aligned}$$

$$\lambda \times A = \langle \left[1 - (1 - inf_T(A))^\lambda, 1 - (1 - sup_T(A))^\lambda\right], \left[inf_I(A)^\lambda, sup_I(A)^\lambda\right], \left[inf_F(A)^\lambda, sup_F(A)^\lambda\right]\rangle \tag{4}$$

The addition and multiplication operations ($\oplus$ and $\otimes$) have commutative and associative properties. Also, there is a distributive property of neutrosophic multiplication over neutrosophic addition [21]. For ranking INNs, a score index is defined which demonstrates the level of truth and certainty of an INN [21,22]:

$$Sc_{inn}(A) = (2 + inf_T(A) + sup_T(A) - inf_I(A) - sup_I(A) - inf_F(A) - sup_F(A))/4 \tag{5}$$

As the definition demonstrates, the larger the truth term of an INN is, and the lower indeterminacy and falsity terms are, the greater the score function would be. For comparing the accuracy of INNs, an accuracy index is defined which demonstrates how accurate the INN is [21,22]:

$$Acc_{inn}(A) = \frac{1}{2}(inf_T(A) + sup_T(A) - inf_I(A) \times (1 - inf_T(A)) - sup_I(A) \times (1 - sup_T(A)) - inf_F(A) \times (1 - sup_I(A)) - sup_F(A) \times (1 - inf_I(A)))$$

For calculating the similarity of two INNs A and B, a distance measure must be proposed that specifies to what extent the INNs are similar. There are several similarity measures, such as cosine similarity [28], algebraic similarity [29], Euclidean, and Hamming distance measures [23]. In the proposed approach, a Hamming distance measure based on [23] is used and calculated as follows:

$$Dis_{hamming}(A,B) = \frac{1}{6}[|\inf_T(A) - \inf_T(B)| + |\sup_T(A) - \sup_T(B)| + |\inf_I(A) - \inf_I(B)| + |\sup_I(A) - \sup_I(B)| + |\inf_F(A) - \inf_F(B)| + |\sup_F(A) - \sup_F(B)|] \quad (7)$$

Neutrosophic Hamming distance specifies the total value in T, I, and F terms that must change to convert an INN to another one [30]. It can be used as a measure to specify the distance of a set of neutrosophic points from the ideal point where the point with the smallest distance from the ideal point is the preferred one [30]. It is a typical and simple similarity measure that has been used in MCDM models for different applications [30–32].

2. Related work

In recent years, several trust computation models have been proposed for the IoT. These works have primarily focused on different aspects of trust management in IoT, such as architecture, context awareness, uncertainty, and social aspects. Chen et al. surveyed the trust computation models for IoT and classified trust computation models based on five design dimensions: (1) trust composition, (2) trust propagation, (3) trust aggregation, (4) trust updating, and (5) trust formation [33]. Yan et al. suggested a system model for IoT and concluded that a trustworthy IoT system should apply trustworthiness in ten different parts of the IoT system, including trusted relationships between IoT entities in each layer (e.g., objects, services), quality of IoT services (to ensure the right conditions considering the service context), and data perception considered in the proposed framework [8]. In another survey [34], the authors categorized innovations according to four layers of IoT given by ITU-T Y.2060 recommendations. They considered the information collection, computation, propagation, and updating as the four primary phases in trust computation models. In the following, some notable studies are reviewed that are related to essential aspects of the proposed model.

The use of innovative combinations for trust in IoT has been addressed in various works. Truong et al. considered IoT trust as a combination of several trust metrics, each of which derived from some technical attributes of the objects [35]. They suggest reputation, knowledge, and recommendation as the three main components of trust. In [6] and [7], Jayasinghe et al. used this trust combination method. From their point of view, knowledge could present subjective trust criteria such as honesty and CoI, while recommendation and reputation could be considered as numerical data received from the friends and non-friends objects. They used the concept of honesty as an essential trust attribute for evaluating the social trustworthiness of things, and further defined several subjective criteria for its evaluation. Jayasinghe et al. continued their research, introducing a machine-learning-based trust computation model which labels trust evaluation criteria using a clustering algorithm [36]. The model then combines the criteria based on the thresholds adjusted by a classification algorithm. Despite their notable advantages, these works did not consider uncertainty factors in trust modeling, nor did they consider context as a determining factor for specifying trust evaluation criteria. Bernabe et al. presented a multidimensional trust model for IoT which assumes four dimensions for trust [16]: (1) quality of service, (2) security, (3) reputation, and (4) social relationship. The trust dimensions consist of a hierarchy of trust criteria composed together while applying certainty and weight factors for each of them. The certainty is modeled as the fraction of the number of evidence to all of the previous interactions.

The social dimension of trust in IoT has been explored by introducing new concepts and using social relations in trust distribution. Nitti et al. used indirect social relations between nodes to distribute recommendation data by considering a chain of trustworthiness between recommenders and the trustor [9]. They divided trust into two parts: (1) the objective part for modeling the global reputation of each object, and (2) the subjective part for modeling trust evaluation between nodes. In [37], Din et al. proposed a lightweight trust management scheme, where cooperativeness is formulated as a social aspect of trust in their trust combination. They considered cooperativeness as the social cooperation of a node with others in the IoT network. In [38], the authors presented a trust management framework for heterogeneous IoT devices evaluating tie strength between them and using human intelligence in addition to device intelligence. Using social trust to control access to IoT devices has been demonstrated in [39] to prevent Sybil attacks in SIoT environments. The IoT devices were grouped into communities according to their social similarity, with malicious nodes being detected and prevented from accessing the social network and launching Sybil attacks.

As a concept in SIoT, Chen et al. defined a similarity measure based on a set of social criteria and used it for weighting recommendations from different nodes [1]. They defined an adaptive coefficient for combining direct observations and indi-

rect recommended trust from recommenders employed to resolve the issue of malicious recommendations. Chen et al. used cooperativeness, CoI, and honesty as the three primary social criteria for evaluating the trustworthiness of social nodes [40]. They used the concept of similarity, defined in their other work [1], to determine how much the recommendation of an object may be useful for the other one. They modeled the satisfaction result of any service experiment as a binary value, but they did not include uncertainty and context information in their trust management model.

Context, as one of the factors affecting the quality of services in IoT, has been studied from different viewpoints. Wang et al. proposed a context-aware trust management model for calculating the trustworthiness of IoT SPs in service-oriented ad hoc networks [2]. They used logit regression to estimate the behavior of service providers in response to context changes. They modeled the behavior of users by a single binary number and did not consider trust as a combination of multiple criteria. They still did not capture uncertainty sources in their work except for an error term for simulating noise tolerance in the recommendations. Saied et al. defined and used the concept of service similarity plus context similarity for selecting more relevant reports from recommenders in the process of trust aggregation [11]. They assumed that a set of criteria could be used for estimating context and service similarity, but they did not specify any practical criteria for quantifying service and context values. Adewuyi et al. [41] referred to context as an influencing factor for determining the trust aggregation method and assumed that the method must be an input parameter for any specific application. They modeled the trust decay and maturity for updating trust values during a time window as their primary contribution. Elsewhere, using a context-based IoT trust model, Altaf et al. represented a method for detecting IoT nodes performing Sybil or on-off attacks [42]. They created a trust score by combining information from IoT nodes and recommendations from peers. For filtering malicious nodes that performed Sybil attacks, they used a contextual similarity measure. In general, in the reviewed works about trust management in IoT, the context as a factor for uncertainty has not been addressed.

Uncertainty in IoT-based trust computational models has been studied in some works. Tissaoui et al. [43] studied the uncertainty phenomenon in IoT healthcare applications. They distinguished various types of uncertainty including structural, methodological, and decision uncertainty. Based on their research, several factors can be considered as the sources of uncertainty in the IoT context, including devices' resource constraints, the scale of IoT devices, and network effects. In addition, they mentioned several issues with data including inconsistency, incompatibility, ambiguity, and redundancy. Dong et al. used a fuzzy composition function for aggregating some network metrics proposed for evaluating the behavior of distributed nodes [17]. Alshehri et al. used a fuzzy-logic-based approach for detecting malicious SPs and recommenders [18]. They employed fuzzy membership functions to classify the IoT nodes into different performance classes based on their trust value. Although they used uncertain attributes for describing the behavior of the IoT nodes, they did not investigate the reasons for uncertainty, and the uncertainty originated from the context of interactions.

Neutrosophic sets and numbers have been used as a mathematical tool for modeling uncertainty in multi-criteria decision-making (MCDM) problems over the past years. An interesting example is the work of Ma et al. [14], which formulated the problem of selecting the most trustworthy cloud SPs using INSs. They modeled the potential risks as the falsity, the performance-cost ratio as the truthfulness, and uncertainty about the values of truthfulness plus falsity terms as the indeterminacy terms of the neutrosophic numbers. In the field of IoT, Nabeeh et al. [44] combined neutrosophic techniques with the analytical hierarchy process (AHP) MCDM model for IoT applications. They considered five influential factors for IoT applications and used a combination of AHP plus neutrosophic techniques for selecting the most appropriate alternative. In another example, Grida et al. [45], addressed the decision-making challenges in IoT-based supply chain management systems. They considered 23 evaluation criteria and utilized a combination of VIKOR and the best-worst method (BWM) for MCDM in their proposed framework. Additionally, they used neutrosophic sets theory to model vague, uncertain, inconsistent, and incomplete information in data evaluations. In [46], the authors applied multi-criteria decision analysis (MCDA) and AHP in combination with interval-valued neutrosophic numbers to perform a comparative analysis of IoT supply chains. In that study, expert opinions were analyzed using MCDA and AHP processes, in which uncertainty was considered using neutrosophic numbers.

3. Proposed method

In this section, the proposed trust management approach will be introduced. First, a general overview of the proposed framework and the steps required for trust processing are presented. Then, the core computational model of the proposed approach, which is based on the neutrosophic numbers, is outlined. The trust preprocessing subsection discusses how the quantitative data and the qualitative comments are preprocessed and converted to neutrosophic numbers. In addition, the approach for considering the sources of uncertainty is presented, and its influence on the calculation scheme is described. The combination of the preprocessed data is given in the trust calculation subsection, and finally, the trust history updating procedure is presented.

3.1. Preliminaries

We consider an SOA-based social IoT model [1,40], as illustrated in Fig. 1, where objects are SRs and SPs. The objects are owned either by real users (i.e., personal property) or legal users such as the municipality, legal offices, hotels, etc. Users and devices have unique identities in IoT cloud services and can be authenticated by each other. The IoT cloud services can per-

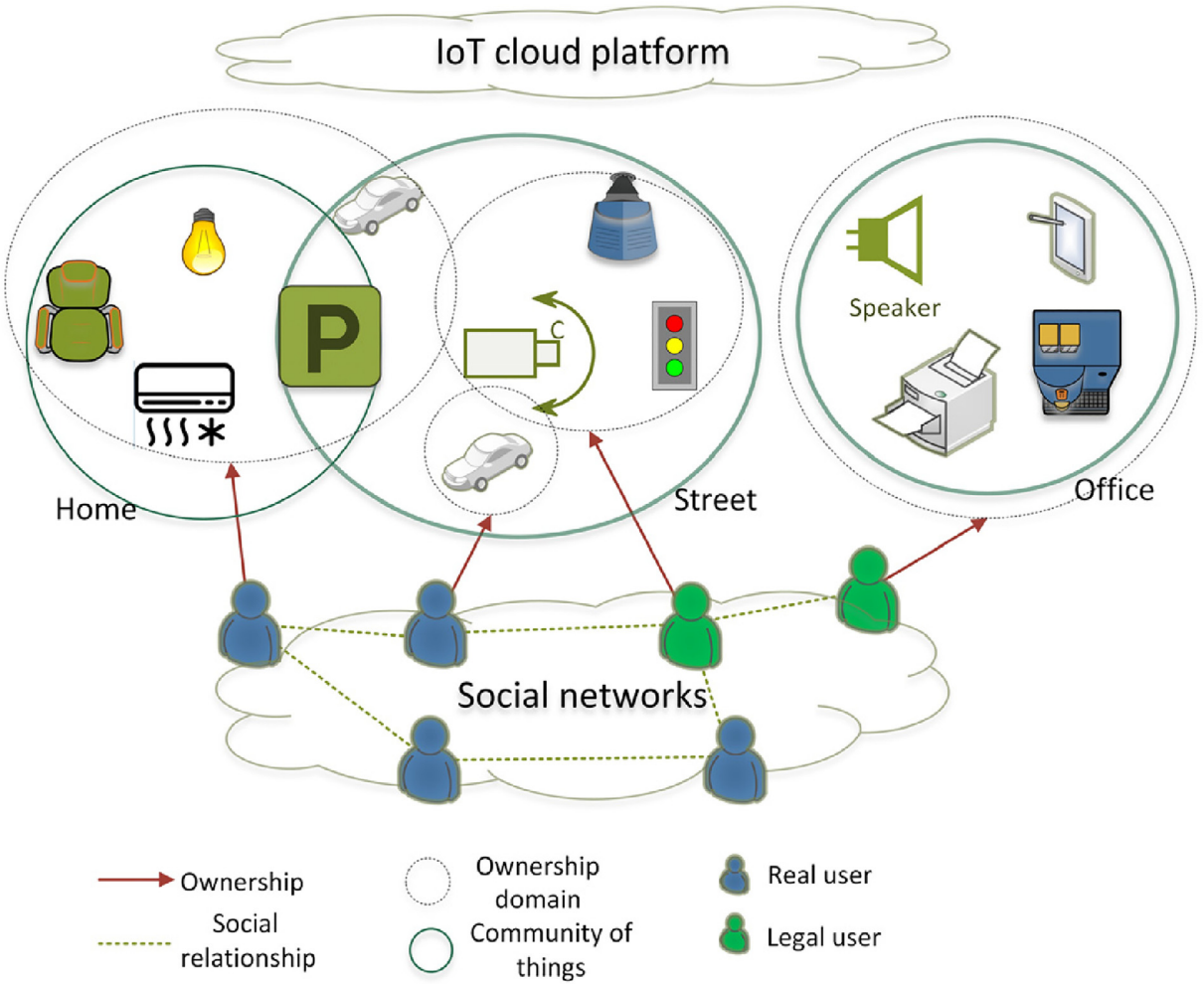

Fig. 1. The system model of SOA-based social IoT.

form service discovery for suggesting the service interaction alternatives (SIA) to the SRs. Social networks connect the users, where they can be friends or members of the same groups. Objects can be members of the same CoIs [6], where they can have more frequent interactions. In addition, two objects owned by the users having social relationships are also considered to have a relationship at the object level. It is assumed that there is an existing trust between the users and their devices. Hence, it is assumed that the trustor and the trustees are the SP and the SR devices of two users respectively. Objects can request services autonomously or through the intention of their owners. Thereafter, they can select between the suggested SIAs to provide the requested service. The SR's device calculates the trustworthiness level of each SIA and selects the best one for the interaction. The trustor's device calculates the trustworthiness of SIAs based on their assertions, recommendations received from social connections, and history records.

3.2. Problem definition

In the proposed system model presented in Fig. 1, some problems may cause lousy service experiences. In an IoT environment, there could be misbehaving SPs that, intentionally or not, provide inappropriate or low-quality services. Additionally, some objects may provide incorrect trust-related information about themselves or other objects. It would be very important for a trust management system to select an appropriate SP in every service request based on available information. This information may be uncertain because of different sources of uncertainty such as ambient noise, inappropriate context conditions, or measurement errors. Considering these problems, we aim to design a trust management system that addresses the following challenges:

1- The problem of misbehaving SPs: Some SPs may provide inadequate services, whether they are aware or not. These SPs should be quickly and correctly identified, and users should be notified of the nature of such misbehaving SPs in case such an entity exists in the environment.

2- The problem of incorrect recommendations: The recommender objects may be honest and provide correct recommendations. However, some recommenders may intentionally provide bad or incorrect recommendations, and try to perform *self-promoting, whitewashing, discriminatory, bad-mouthing, ballot-stuffing,* and *opportunistic service* attacks [1]. Such recommenders should be identified and their opinions should be ignored over time.

3- The problem of uncertainty in data and context: In an IoT environment, multiple sources of uncertainty always exist. In addition, uncertainty is an essential parameter in trust modeling and calculation [12,13]. Consideration of uncertainty sources in IoT trust calculations can enhance the accuracy of the results even further.

3.3. A general overview of the proposed model

In the following subsections, the general specifications of the proposed model are presented:

A. Trust combination

The proposed model considers trust as a combination of three main components that provide pieces of information required for trust calculation as follows:

1. **Assertion:** it refers to the assertions by the SIAs about their capabilities and contains self-evaluations about different trustworthiness criteria.
2. **History:** it refers to the evaluated trust based on experiences of previous interactions that the trustor has performed with SIAs.
3. **Recommendation:** it refers to the trustworthiness evaluations provided by other entities such as friends about their previous experiences with SIAs.

B. Trust aggregation

The trust information aggregation is performed in two ways in the proposed model as follows. These two views are related to the type of uncertainty described in the *Uncertainty* representation subsection.

1. **Detailed trust aggregation (DTAg)**: inspired by the multi-criteria decision-making view toward trust, this type of aggregation assigns a level of trust for each SIA's trustworthiness criterion and aggregates these values based on a weight vector specifying their importance.
2. **General trust aggregation (GTAg)**: this form of aggregation comes from a general viewpoint toward the trustworthiness of an entity.

C. The proposed computation framework

The trust computation framework for the trustor entity is displayed in Fig. 2. The main components are described below:

1. **Preprocessing:** Data preprocessing is a set of operations designed to transform the input trust-related data to INNs, used in the core of the trust computation model. These operations are performed by two components that are responsible for transforming the quantitative data and the linguistic opinions of the users:
   a. **Trust and context evaluation criteria preprocessing**: This component transforms the quantitative evaluations to INNs, considering sources of uncertainty and inconsistency.
   b. **Criteria weight specification:** User preferences about the importance of trust evaluation criteria are received as linguistic terms, then preprocessed, and presented further in the form of real numbers.
2. **Trust aggregation**: This unit aggregates the preprocessed trust information using history and recommendation data along with the context evaluations to calculate trust for interacting with each SIA. This trust value is used to rank SIAs and select the best option for the interaction.
3. **Trust updating:** After performing the interaction with the selected SIA, the actual outcome experienced about the QoS criteria is observed and evaluated. This information is processed and used to update the history information as follows:
   a. **The QoS of the selected SIA:** this parameter is updated based on the difference between the QoS asserted by the SIA and the experienced QoS of the performed interaction.
   b. **The honesty of recommenders:** This is calculated based on the similarity of the recommended values by any of the SIAs and the actual experienced value.

3.4. Computational aspects of the proposed model

This section presents the formal and mathematical notations of the proposed trust model. Table 1 reports all inputs required in the computational model. Table 2 also provides other notations used in calculations. Data types for each of the parameters have also been identified, which can be a non-negative integer (NNI), interval neutrosophic number (INN), real number (RN), or triangular fuzzy number (TFN). The TFNs are used for presentation simplicity. Meanwhile, the model can be extended to use other types of fuzzy numbers as well.

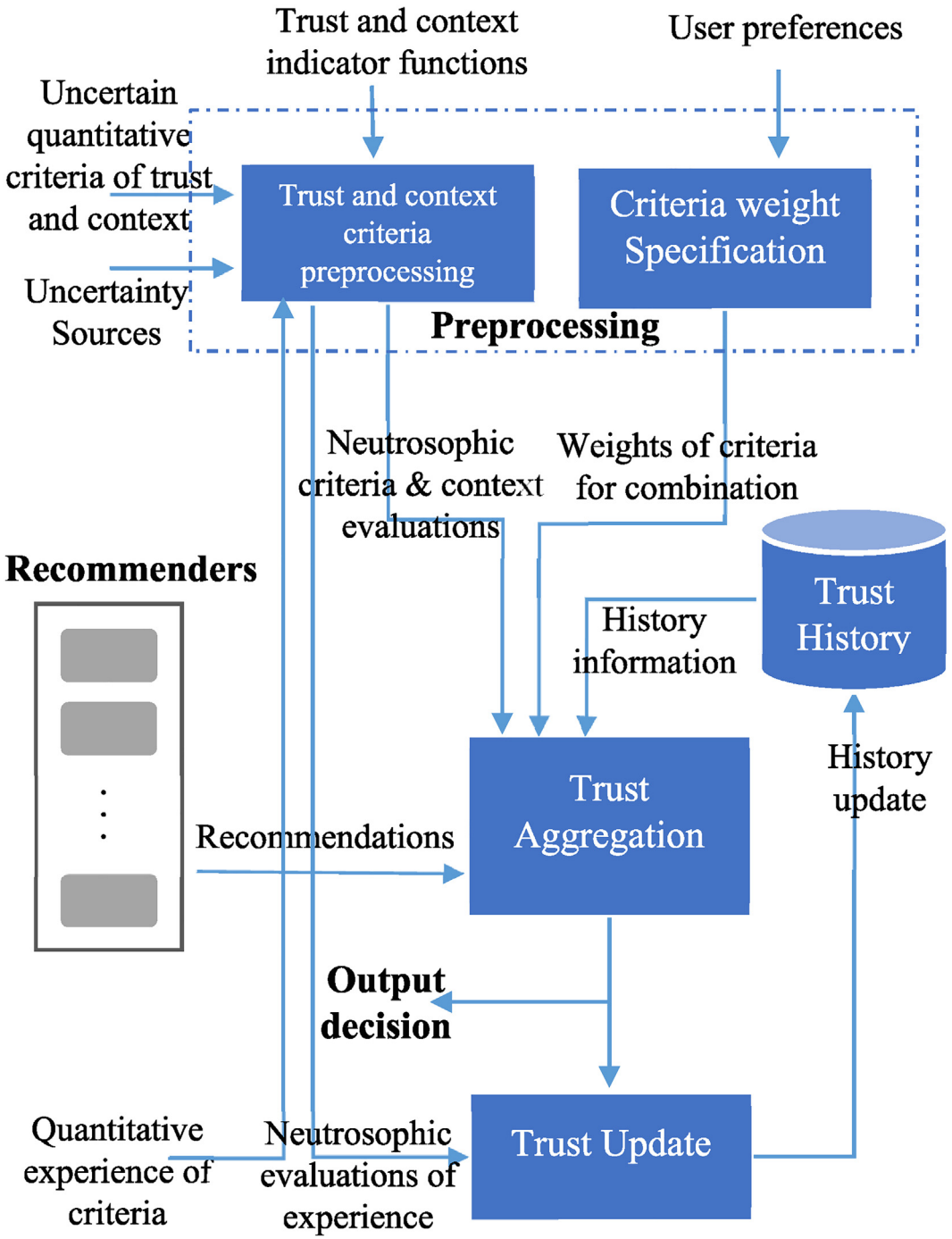

Fig. 2. The general framework of the proposed model.

The proposed model is based on calculation over INNs, and the trust relationship is modeled using these numbers. The overall trust of entity i toward the entity j, which is used to decide whether to receive the service s, is expressed as an INN such as $Trust_s^{i,j} = \left[T^{i,j}, I^{i,j}, F^{i,j}\right]$. Here, $T^{i,j}$, $I^{i,j}$, and $F^{i,j}$ are interval numbers, and as explained in the background section, they are the truth, indeterminacy, and falsity terms of the INN.

A. Context model

The trustor evaluates the interaction context with each SIA. This evaluation is used as an influential factor for determining the quality of interactions. The context modeling in the proposed model is based on the fact that the proposed model utilizes

Table 1
Input parameters used in the proposed model.

Symbol	Data type / Interval	Definition
$\boldsymbol{M_s}$	NNI $1 < M$	Number of detailed criteria for providing service s
$\boldsymbol{N}$	NNI $1 < N$	Number of SIAs
$\boldsymbol{R}$	NNI $0 \leq R$	Number of detailed recommenders
$\boldsymbol{R'}$	NNI $0 \leq R'$	Number of general recommenders
$\boldsymbol{S_{cr_m}}$	TFN	Satisfaction function of the m^{th} trust criterion
$\boldsymbol{D_{cr_m}}$	TFN	Dissatisfaction function of the i^{th} trust criterion
$\boldsymbol{v_{cr_{m,n}}}$	TFN	Fuzzy value of the m^{th} trust criterion asserted by the n^{th} SIA
$lincr_{m_1,m_2}$	Linguistic term	Linguistic term defining the importance of the ${m_1}^{th}$ trust criterion relative to the ${m_2}^{th}$ index
$Cov_{cn_c^d}\left(v_{cn_c^d}\right)$	TFN	Coverage function of high-level context named cn_c^d based on the $v_{cn_c^d}$ quantity
$\boldsymbol{V^n_{cn_c^d}}$	TFN	Fuzzy evaluation of the $v_{cn_c^d}$ quantity for the n^{th} SIA

Table 2
Basic notations used in the proposed model.

Symbol	Data type/Interval	Definition
$\boldsymbol{X}$	Set	A space of points.
$\boldsymbol{X}$	RN	A generic element x in X.
A, B	INN	Interval neutrosophic numbers (INNs).
$\boldsymbol{T_A(x)}$, $\boldsymbol{I_A(x)}$, $\boldsymbol{F_A(x)}$	Intervals in the range $[0^-, 1^+]$	$T_A(x)$: Truth interval of INN A. $I_A(x)$: Indeterminacy interval of INN A. $F_A(x)$: Falsity interval of INN A.
$\boldsymbol{inf}_T(A), \boldsymbol{sup}_T(A)$	RN	Infimum and supremum values of truth membership interval of INN A.
$\boldsymbol{inf}_I(A), \boldsymbol{sup}_I(A)$	RN	Infimum and supremum values of indeterminacy membership interval of INN A.
$\boldsymbol{inf}_F(A), \boldsymbol{sup}_F(A)$	RN	Infimum and supremum values of falsity membership interval of INN A.
$\boldsymbol{Trust_s^{i,j}}$	INN	Trust value of node i to node j to receive service s
$\boldsymbol{m}$	NNI $1 \leq m \leq M$	Commonly referring to the m^{th} trust criterion
$\boldsymbol{n}$	NNI $1 \leq n \leq N$	Commonly referring to the n^{th} SIA
$\boldsymbol{ev_{cr_{m,n}}}$	INN	QoS evaluation of the m^{th} criterion of the n^{th} SIA based on its claim
$\boldsymbol{ev^r_{cr_{i,j}}}$	INN	QoS evaluation of the m^{th} criterion of the n^{th} SIA by the r^{th} recommender
$\boldsymbol{ev_{cn_{m,n}}}$	INN	Evaluation of the m^{th} context criterion of the n th SIA
$\boldsymbol{ev^k_{cr_{m,n}}}$	TFN	QoS evaluation of the m^{th} criterion of the n th SIA by the k^{th} detailed recommender
$\boldsymbol{w_{cr_m}}$	RN $0 < w_{cr_m} \leq 1$	Weight of the m^{th} trust criterion
$\boldsymbol{his^{i,j,s}_{cn_c^d}}$	INN	History of node j providing service s evaluated by node i
$\boldsymbol{n^{i,j,s}_{cn_c^d}}$	NNI	Number of transactions by node i for receiving service a from node j
$\boldsymbol{cov^n_{cn_c^d}}$	RN $0 \leq cov^n_{cn_c^d} \leq 1$	Coverage of the high-level context cn_c^d by the n th SIA
$\boldsymbol{Set^s_{cn}}$	Set	Set of high-level contexts of service s
$\boldsymbol{N^d_{cn_s}}$	NNI	Number of high-level contexts from dimension d defined for service s
$\boldsymbol{N_{cn_s}}$	NNI $0 \leq N_{cn_s} \leq 5$	Number of high-level context diminutions considered in trust calculations
$\boldsymbol{d}$	NNI $0 \leq d \leq N_{cn_s}$	Typically referring to the d^{th} high-level context dimension
$\boldsymbol{hon^i_j}$	RN	The honesty of node j evaluated by node i
$\boldsymbol{n^i_{trans_j}}$	NNI	Number of transactions that node i has requested from node j
$\boldsymbol{v^{ex}_{cr_{m,n}}}$	TFN	Fuzzy value of the m^{th} trust criterion experienced by the selected SIA with ID n
$\boldsymbol{ex_{cr_{m,n}}}$	INN	QoS experienced about the m^{th} criterion of the selected SIA with ID n

context as an enabler for expressing uncertainty. The uncertainty may be from some known factors influencing each trust evaluating criterion or a set of unknown factors where their impact on the QoS of the SIA is not undividedly known. Accordingly, the context quality is modeled as described below:

1. Detailed context (DCn): The context at this level is a factor that influences the effectiveness of each trust assessment criterion. For example, the accuracy of a sensor can be assumed as a trust assessment criterion where its corresponding context criterion is the ambient noise. Here, noise as a background parameter influences the effect of precision measurement thus affecting the degree of trust in the value measured by the sensor. Considering $\boldsymbol{M_s}$ trust evaluation criteria and $\boldsymbol{N}$ SIAs for the interaction, the quality of context of the $\boldsymbol{m}$ th trust assessment criterion for interacting with the $\boldsymbol{n}$ th SIA is an INN denoted by $\boldsymbol{ev_{cn_{m,n}}}$.

2. High-level context (HLC): At a higher level, context is modeled as an influential factor for the complete functionality of a particular service for an object. The object's performance at different times, locations, and by different users can have a quality associated with that context. For example, at night time, a camera designed for night vision works more suitably. For the HLC identification, we have used the five W's understanding of context offered by Abowd et al. [47]. The proposed model uses the five W's as five potential dimensions for classifying HLCs. For any dimension, the service expert can designate

several HLCs and define fuzzy membership functions that specify their coverage on their relevant quantities. For a service s considering N_{cn_s} HLC dimensions, the set of HLCs can be defined as follow:

$$Set_{cn}^{s} = \{cn_c^d | 1 \le d \le N_{cn_s}, 1 \le c \le N_{cn_s}^d, d \in \{Where, When, Who, What, Why\}\} \tag{8}$$

Here, d denotes an HLC dimension containing $\boldsymbol{N_{cn_s}^d}$ HLCs and $\boldsymbol{cn_c^d}$ indicates an HLC with index c from dimension d. For any HLC $\boldsymbol{cn_c^d}$, a fuzzy membership function $Co\upsilon_{cn_c^d}\left(\upsilon_{cn_c^d}\right)$ is defined that specifies its fuzzy coverage. Its input variable $\upsilon_{cn_c^d}$ is the measured value of the quantitative parameter relevant to $\boldsymbol{cn_c^d}$ while its output is a real number within $[0, 1]$ specifying the coverage of the HLC.

As an example, a fuzzy coverage function can be defined to specify day-time based on the clock time, as the input variable. The input variable $\upsilon_{cn_c^d}$. is a measured value for the $\boldsymbol{n}$ th SIA as a fuzzy number, referred to as. This value must be combined with the HLC coverage function $Co\upsilon_{cn_c^d}\left(\upsilon_{cn_c^d}\right)$ to specify how much the $\boldsymbol{n}$ th SIA is under the coverage of $\boldsymbol{cn_c^d}$. The output of this combination is the effective coverage of HLC $\boldsymbol{cn_c^d}$ for the SIA $\boldsymbol{j}$, displayed by $\boldsymbol{co\upsilon_{cn_c^d}^j}$. The details of these calculations are described in the trust preprocessing section. In any interaction, the effective coverage and the aggregation of previous experiences in that HLC are combined to specify the QoS prediction. The details of this process are described in the trust aggregation section.

B. History model

The proposed model considers two types of history information about the entities: (1) honesty and (2) QoS records. The history of honesty represents social trust toward an entity demonstrating its trustworthiness in providing trust-related information, while QoS specifies its performance quality. Then, the proposed model can distinguish between dishonest entities and those that are malfunctioning because of their physical limitations or disruptions. Such differentiation is very important for the decision-making about service selection and filtering of malicious recommendations. QoS history is preserved in two models: (1) detailed and (2) aggregated. The detailed history of an object demonstrates the quality of each trust composition criterion of the SP, while aggregated history demonstrates its complete functionality for providing specific services in different contexts. The detailed history is necessary because an entity (the entity itself or the recommendation receiver) can specify the importance of each trust criterion during trust aggregation. On the other hand, aggregated history specifies the overall functionality of the SP in relevant HLCs. The formal expressions of the history models are presented below:

1. Aggregated QoS history (AgQH): The AgQH of an object with index i represented as $His_{al_i}^{general}$ is a set of records specifying the QoS provided by any SP with index n providing the service s.

$$\boldsymbol{His_{al_i}^{general}} = \left\{ (\boldsymbol{his_{cn_c^d}^{i,n,s}}, \boldsymbol{n_{cn_c^d}^{i,n,s}}) \middle| \boldsymbol{cn_c^d} \in \boldsymbol{Set_{cn_s}^h} \right\} \tag{9}$$

where $Set_{cn_s}^h$ is the set of HLCs of the service s, $his_{cn_c^d}^{i,n,s}$ denotes an INN representing the aggregated QoS of the entity n providing the service s to the SIA i in the HLC cn_c^d, and $n_{cn_c^d}^{i,n,s}$ is the number of times the object i has received the service s from the object n in the HLC cn_c^d.

2. Detailed QoS history (DtQH): The DtQH of an object with index i represented as $His_{al_i}^{detail}$ is a set of records specifying the criterion level QoS of a service s that has been received from any SP with index n.

$$His_{al_i}^{detail} = \left\{ \left(H_{al_{i,n}}^{det}, n_{his_{i,n}}^{det} \right) | 0 < i, n \right\} \tag{10}$$

where $n_{his_{i,j}}^{det}$ is the number of times that the entity i has received service from the SP with ID n, $H_{al_{i,n}}^{det}$ is a $1 \times M$ vector containing its evaluations of the detailed criteria, and M is the number of all detailed criteria from all of the services provided by the entity n.

3. Honesty history (HonH): The HonH of an object with index i is a set of records represented as $His_i^{honesty}$, indicating the rightness and accuracy of the recommendations received from any object j. This accuracy is obtained from comparing the recommended values and the real experienced values of the criteria, specified after the interaction.

$$His_i^{honesty} = \left\{ \left(n_{trans_j}^i, hon_j^i \right) \middle| 0 \le hon_j^i \le 1, 1 < n_{trans_j}^i \right\} \tag{11}$$

where $n_{trans_j}^i$ is the number of times the entity i has received recommendations from the entity j and hon_j^i reflects a real number specifying the belief of the entity i to the honesty of node j.

C. Recommendation model

QoS recommendation is an essential operation in the trust distribution model. All entities can share their knowledge stored in QoS history records about other entities to the entities requesting recommendations. This knowledge is the information aggregated inside the history records of the entity based on previous experiences with other objects. As explained in the previous subsection, the QoS history records are preserved as detailed and aggregated history records. Thus, the recommender can provide the recommendations in two ways:

1. Detailed recommendation (DetR): In this type of recommendation, the recommender provides detailed information about the SIAs based on its DtQH records. The recommendations of an entity with the index r about N SIAs are presented as an $N \times M_s$ matrix named Rec^{r}_{cr}; each of its elements as $rec^{r}_{cr_{m,n}}$ demonstrates the evaluation of the entity k about the m th detailed criterion of the n th SIA.

2. Aggregated recommendation (AggR): In this type of recommendation, the recommenders provide their knowledge about the SIAs as aggregated INNs in relevant HLCs. For this purpose, any recommender considers its AgQH records for the aggregated history of alternatives and the relevant HLC. Then, the AggR of the recommender with index r' about the SIA n is retrieved from its AgQH $His^{general}_{al_i}$ as a set of recommendations called $Rec^{r'}_{gen_{n,s}}$ as below:

$$Rec^{r'}_{gen_{n,s}} = \left\{ rec^{cn^d_c}_{al^{r'}_{n,s}} \middle| rec^{cn^d_c}_{al^{r'}_{n,s}} = his^{n,r',s}_{cn^d_c}, \left(his^{n,r',s}_{cn^d_c}, n^{n,r',s}_{cn^d_c} \right) \in His^{general}_{al_{r'}}, cn^d_c \in Set^h_{cn_s} \right\} \tag{12}$$

Here, $rec^{cn^d_c}_{al^{r'}_{n,s}}$ is the aggregated evaluation of SIA n for providing service s which is evaluated by the recommender entity r in the HLC cn^d_c.

D. Trust aggregation model

As stated earlier, the proposed model uses two types of trust aggregation, which are GTAg and DTAg models which are used for the aggregation of three main trust components, namely: (1) assertation, (2) history, and (3) recommendation. The DTAg model is utilized for aggregating detailed trust-related information, including DetQH, DetR, and the assertation trust information. The GTAg is used for comprehensive trust-related information, including AgQH and AggR aggregation. The formal representation of the trust aggregation models is provided below:

1. Detailed trust aggregation: In this trust aggregation model, the detailed evaluation of trust composition criteria from different sources is combined. The detailed trust of an entity with the ID n calculated by the entity i providing the intended service s is calculated as follows:

$$Trust^{i,n,s}_{detailed} = \sum_{m=1}^{M_s} \sum_{r=1}^{R} \left(w_{cr_m} \times hon^i_r \right) \times \left(ev^r_{cr_{m,n}} \otimes ev_{cn_{m,n}} \right) \tag{13}$$

where hon^i_r is the entity r in the HonH of entity i and $ev^r_{cr_{m,j}}$ denotes an INN representing the evaluation of trust combination criterion with index m evaluated by the entity r. It is assumed that R different sources provide information about M_s detailed criteria and $ev_{cn_{m,j}}$ is the DCn of the m th detailed criteria of the entity j. The parameter w_{cr_m} is a real number within $[0, 1]$, representing the weight of criteria with index m in the trust combination of the service.

2. General trust aggregation: In this trust aggregation model, the comprehensive trust-related information from different sources is aggregated using HLCs. For this purpose, the first step of calculating the general aggregated trust evaluation (GAE) of any SIA with ID n providing the intended service s in the HLC cn^d_c is performed by the trust calculator i as follows:

$$gae^{cn^d_c}_{i,n,s} = \sum_{r'=1}^{R'} \left(hon^i_{r'} \otimes ev^{cn^d_c}_{al^{r'}_{n,s}} \right) \tag{14}$$

It is assumed that R' sources of general trust evaluation provide their information to the trust calculator entity. The $ev^{cn^d_c}_{al^{r'}_{j,s}}$ is an INN representing the GAE of the alternative n providing the service s in the HLC cn^d_c, which is evaluated by the entity r' having the honesty $hon^i_{r'}$ in the HonH of the trust calculator i. The second step is to specify GAE of the most relevant HLC in any of the dimensions d, which is calculated based on the formula below:

$$gae^d_{i,n,s} = \max_{score} \left(\left\{ gae^d_{al_i} | gae^d_{al_{i,s}} = cov^j_{cn^d_c} \otimes gae^{cn^d_c}_{i,n,s}, 1 \leqslant c \leqslant N^d_{cn}, cn^d_c \in Set^h_{cn_s} \right\} \right) \tag{15}$$

where the max_{score} function returns the INN with the minimum neutrosophic score value from its input set. The combination of certainty for being within the domain of HLC ($cov^j_{cn^d_c}$) and the certainty of the HLC to be sufficient for the service ($gae^{cn^d_c}_{i,j,s}$) is calculated to predict the QoS. The final step is to evaluate the final general trust that is an INN with the minimum score, among all $gae^d_{i,j,s}$ values in all HLC dimensions:

$$Trust^{i,n,s}_{geteral} = min_{score} \left\{ gae^d_{i,n,s} | 1 \leq d \leq N_{cn} \right\} \tag{16}$$

3.5. Trust preprocessing

At the core of the proposed model, calculations are based on the INNs. However, as outlined in Table 1, the input data of trust and context criteria evaluations are fuzzy quantitative values. In addition, the user preferences about the importance of trust and context criteria are linguistic terms that must be transformed into real values. Thus, it is necessary to preprocess these types of data, considering the sources of uncertainty to prepare suitable information used by the trust calculation unit.

A. Converting the evaluation criteria to INNs

In order to convert quantitative data for the trust and context evaluation criteria into INNs, it is necessary to identify the interval numbers for each of their '*T*', '*I*', and '*F*' terms. This part of the calculations is performed to determine the '*T*' and '*F*' terms, with the specification for the '*I*' term presented in Section 4.6. The input parameters of this section are as follows:

1. **Fuzzy evaluations of quantitative data:** In the proposed model, the evaluations of the input quantities are presented as fuzzy numbers. In this regard, TFNs have been used for the simplicity and consistency of the calculations. These inputs, described in Table 1, are $v_{cr_{m,n}}$, $v_{cn^k_{m,n}}$, and $V^n_{cn^d_c}$.
2. **Indicator functions**: These fuzzy functions are used as indicators mapped into quantitative evaluations of trust and context criteria to specify how much the values are appropriate or unsuitable for the quality of the presented service. Two types of indicator functions are offered for preprocessing any quantitative trust or context evaluation criteria which are described below:
   a. *Satisfaction indicator functions:* These fuzzy functions specify the appropriateness of trust and context criteria for providing a high level of QoS. The S_{cr_m} and S_{cn_m} are the two satisfaction functions used to designate the suitability of the quantitative evaluations of m th trust criterion ($v_{cr_{m,n}}$) and the corresponding detailed context criterion ($v_{cn_{m,n}}$). The result of this designation is generating the '*T*' terms of the output INN evaluations which are $ev_{cr_{m,n}}$ and$ev_{cn_{m,n}}$.
   b. *Dissatisfaction indicator functions:* These fuzzy functions represent the possibility of hazard, based on the quantitative values of trust and context evaluation criteria. In this way, the hazard and safety indicators of any criterion are modeled independently from the appropriateness. The D_{cr_m} and D_{cn_m} are the two dissatisfaction functions that are used to generate the '*F*' terms of $ev_{cr_{m,n}}$ and$ev_{cn_{m,n}}$.
3. **HLC coverage function:** The function $Cov_{cn^d_c}\left(v_{cn^d_c}\right)$ is combined with its related quantitative evaluation $V^n_{cn^d_c}$ to determine the effective coverage of HLC cn^d_c on the service interaction. This combination is performed similarly to the mapping of indicator functions to their respective quantitative evaluation.

The core of quantitative data preprocessing is a combination function that maps the quantitative data into indicator functions to achieve an interval number, indicating how much the quantitative evaluation is sufficient or insufficient. This mapping function $In_{QI}(t)$ receives the indicator function $Id(t)$ and the quantitative evaluation $Qu(t)$ as inputs, and then generates an interval number:

$$[l, r] = In_{QI}(Id(t), Qu(t)) \tag{17}$$

Here, l and r are the left and right values of the output interval number, and t denotes the parameter referring to the evaluated quantity. Fig. 3 demonstrates the steps required for calculating l and r.

The first step of the calculations is to find the intersection points between two functions $Id(t)$ and $Qu(t)$. The parameters j^r_{col} and j^l_{col} are assumed to be the right and left intersection points of the $Id(t)$ and $Qu(t)$ curves on the t axis. Furthermore, if they do not reach each other from one side, the infinite is assumed as the contact point on that side. The second step is to calculate an overlapping set within $j^l_{col} < t < j^r_{col}$.

$$Set_{overlap}(Id(t), Qu(t)) = \{Id(t) * Qu(t) Id(t) * Qu(t) | j^l_{col} < t < j^r_{col}, Id\left(j^l_{col}\right) = Qu\left(j^l_{col}\right), Id\left(j^r_{col}\right) = Qu\left(j^r_{col}\right)\} \tag{18}$$

Finally, the l and r parameters are considered as the minimum and maximum values of the overlapping set$Set_{overlap}$:

$$[l, r] = \left[\min\left(Set_{overlap}\right), \max\left(Set_{overlap}\right)\right] \tag{19}$$

As an example, suppose that $Id(t) = trimf(-1, 0, 1)$ and $Qu(t) = trimf(-2, 0, 2)$. Then, the calculation steps are as follows:

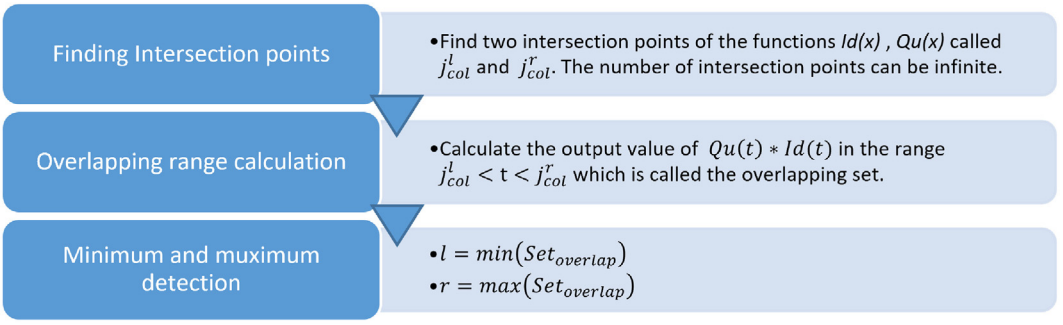

Fig. 3. The required steps for converting the evaluation criteria to INNs.

Step 1: The left and right intersection points of the two functions $Qu(t)$ and $Id(t)$ are detected as $j_{col}^{l} = -2$ and $j_{col}^{r} = 0$; the value of t within [-2, 0] is considered in the next step.

Step 2: The value of $Qu(t) * Id(t)$ must be calculated within $-2 < t < 0$:

$$Qu(t) * Id(t) = \begin{cases} 0 & -2 \le t < -1 \\ \left(\frac{t}{2} + 1\right) * (t+1) & -1 \le t \le 0 \end{cases} \tag{20}$$

Step 3: The minimum and maximum values of $Qu(t) * Id(t)$ within this range are 0 and 1. These values are obtained by setting t equal to -1 and 0. Then, the output interval number would be [0,1].

Using the mapping function $In_{QI}(t)$, the quantitative data preprocessing is computed to generate the following outputs described in Table 2:

1. INN evaluations of trust criteria: Assuming any $ev_{cr_{i,j}}$ presented as a triple of '*T*', '*I*', and '*F*' terms, the '*T*' and '*F*' terms are calculated using the $S_{cr_m}(t)$ and $D_{cr_m}(t)$ indicator functions as follows:

$$ev_{cr_{m,n}} = \left[T_{ev_{cr_{m,n}}}, I_{ev_{cr_{m,n}}}, F_{ev_{cr_{m,n}}}\right] \tag{21}$$

$$T_{ev_{cr_{m,n}}} = In_{QI}\left(S_{cr_m}(t), v_{cr_{m,n}}(t)\right) \tag{22}$$

$$F_{ev_{cr_{m,n}}} = In_{QI}\left(D_{cr_m}(t), v_{cr_{m,n}}(t)\right) \tag{23}$$

2. INN evaluation of detailed context criteria: As with the evaluation of trust criteria, the '*T*' and '*F*' terms of any $ev_{cn_{m,n}^{k}}$ can be calculated as follows:

$$ev_{cn_{m,n}} = \left[T_{ev_{cn_{m,n}}}, I_{ev_{cn_{m,n}}}, F_{ev_{cn_{m,n}}}\right] \tag{24}$$

$$T_{ev_{cn_{m,n}}} = In_{QI}\left(S_{cn_m}(t), v_{cn_{m,n}}(t)\right) \tag{25}$$

$$F_{ev_{cn_{m,n}}} = In_{QI}\left(D_{cn_m}(t), v_{cn_{m,n}}(t)\right) \tag{26}$$

The calculation of the '*I*' term in INN evaluation of trust and detailed context criteria is based on combining several uncertainty sources explained in the *Uncertainty representation* section.

3. Effective coverage of HLC: The combination of the context coverage function $Cov_{cn_c^d}(t)$ and the fuzzy value of the quantity $V_{cn_c^d}^{n}(t)$ is performed as follows:

$$[x, y] = In_{QI}(Cov_{cn_c^d}(t), V_{cn_c^d}^{n}(t)) \tag{27}$$

$$cov_{cn_c^d}^{n} = (x + y)/2 \tag{28}$$

B. Specifying criteria weights

The importance of trust and context evaluation criteria is specified as linguistic terms by the service user or expert. Users specify the importance of any criterion relative to another criterion and use linguistic terms that simplify comparison for human users. In Table 1, an input type called $lincr_{m_1,m_2}$ is described, which is the linguistic term for the weights of trust evaluation criteria.

The linguistic terms are mapped to the real numbers specifying the weight of each criterion using the fuzzy-AHP method proposed in [48]. In this method, initially, the linguistic terms demonstrating the importance of a criterion compared to another one are converted to fuzzy numbers. Then, the fuzzy weights of the criteria are specified utilizing AHP analysis. Finally, the output of this section is the w_{cr_m} weights for all values of m.

3.6. Uncertainty representation

The proposed model considers uncertainty in two main aspects: (1) context uncertainty (explained in the context model) and (2) measurement uncertainty. Measurement uncertainty is due to the inaccurate measurements of quantities as well as a lack of knowledge about their actual and accurate values. In the proposed model, different factors causing the knowledge insufficiency in evaluations are aggregated to form the indeterminacy term of INN trust and detailed context criteria evaluations denoted as $I_{ev_{cr_{m,n}}}$ and$I_{ev_{cn_{m,n}}}$ respectively. Additionally, the inaccuracy of calculations is modeled by fuzzy and neutrosophic interval numbers propagating uncertainty in the calculations.

The indeterminacy terms in the trust calculation process are a combination of the discussed uncertainty factors affecting the certainty of the quantitative data. For any othese factors influencing trust or detailed context evaluation criteria, an evaluation function is defined as follows:

$$unc_p^{cn_{m,n}} = Unc_p\left(u_p^{cn_{m,n}}\right), unc_p^{cr_{m,n}} = Unc_p\left(u_p^{cr_{m,n}}\right) \tag{29}$$

where Unc_p is the function that quantifies the amount of uncertainty caused by the uncertainty factor p based on its input values $u_p^{cn_{m,n}}$ and$u_p^{cr_{m,n}}$. The resulting values $unc_p^{cn_{m,n}^k}$ and $unc_p^{cr_{m,n}}$ are the quantified uncertainty values defined within [0,1], induced by p for the detailed context criterion $cn_{m,n}$ and the trust evaluation criterion$cr_{m,n}$. Eventually, the indeterminacy terms, defined as interval numbers, are calculated as follows:

$$I_{ev_{cr_{i,j}}} = [\min(S_{cr}), \max(S_{cr})], S_{cr} = \left\{ Unc_p^{cr}\left(u_p^{cr}\right) \middle| \text{forallvaluesof} p \right\} \tag{30}$$

$$I_{ev_{cn_{i,j}}} = [\min(S_{cn}), \max(S_{cn})], S_{cn} = \left\{ Unc_p^{cn}\left(u_p^{cn}\right) \middle| \text{forallvaluesof} p \right\} \tag{31}$$

Several uncertainty factors can be assumed to contribute to the measurement uncertainty, but the most relevant ones are as follows:

1. The elapsed time from the measurements: The more recent the measurements, the more reliable they are supposed to be.

2. Insufficiency of data samples: Any entity evaluates the quantitative trustworthiness criteria along with context based on a different number of samples. The larger the number of samples, the higher the certainty about the criteria would be.

3. Noise and fault: These factors can be acknowledged as significant sources of uncertainty. Different types of noise can affect the certainty of the evaluated data, which can be investigated in future works. Additionally, fault can be regarded as an influential factor in the functionality of IoT devices. The consideration of fault requires deeper analysis in future works.

3.7. Trust aggregation

In the previous section, the data necessary for trust calculation have been identified. In this section, the trust aggregation steps are explained. The trust aggregation in the proposed model involves aggregating the following data:

1. Trust information by asserted SIAs.
2. Trust information recommended by the recommenders.
3. Historical trust information from the database of the trustworthiness calculator agent.
4. Total data from the previous items.

The following subsections describe the aggregation of the data mentioned above. These data can be detailed or general, aggregated based on the detailed or general trust aggregation models presented in Section 4.2.

A. Asserted trust aggregation

The evaluations asserted by SIAs about their trust evaluation criteria are aggregated to specify the total self-evaluations of SIAs. Any SIA preprocesses the quantitative evaluation of the trust plus context evaluation criteria and provides their evaluation as INNs $ev_{cn_{m,n}}$ and$ev_{cr_{m,n}}$. The detailed aggregated evaluation of trust, based on the assertions of the SIA n denoted as $dae_{assertion\ n}$ is calculated based on the detailed trust aggregation formula, i.e. Equation (13).

B. Trust recommendations aggregation

This part of the calculations deals with aggregating recommended trust information from the recommenders, leading to the generation of the recommendation part of the total trust. Having two types of recommendation models, the proposed model aggregates the information from each type of recommendation separately and then aggregates the results to generate the total recommendation part of the trust.

1. Aggregation of detailed recommendations: Here, the detailed trust aggregation in Equation (12) is used for trust aggregation. In this formula, considering R recommenders providing their recommendations in a detailed model, and the detailed recommendations $rec^r_{cr_{m,n}}$ as the $ev^r_{cr_{m,n}}$ evaluations, the aggregated evaluation of the detailed recommendations about the alternative n is calculated as the result of the Equation (13), denoted asdae_{al_n}.

2. Aggregation of general recommendations: The general trust aggregation model, calculated based on Equations (14), 15, and 16, is used to aggregate the recommendation of R' recommenders providing general recommendations as specified in Equation (12). Considering the recommendation $rec^{cn^d_c}_{al^{r'}_{n,s}}$ as the evaluation $ev^{cn^d_c}_{al^{r'}_{n,s}}$ in the mentioned formulas, the aggregated evaluation of the general recommendations about the alternative n is calculated as the result of the Equation (16) which is named gae_{al_n}.

3. Total Aggregation of recommendations: For any SIA with ID n, the general and detailed recommendation aggregations (dae_{al_n} and gae_{al_n}) are combined based on a weighted sum model as given in Equation (32) to generate the recommended trust evaluation of the SIA. The weights of the combination are proportional to the number of detailed and general recommenders (R and R').

$$rec_n = \left(\frac{R}{R+R'} \otimes dae_{rec_i}\right) \oplus \left(\frac{R'}{R+R'} \otimes gae_{rec_n}\right) \tag{32}$$

C. Trust history aggregation

The history aggregation process is similar to the recommendation aggregation process, assuming only one source of trust information which is the AgQH and DtQH records of the trustworthiness calculator entity. This entity provides recommendations based on historical data about SIAs for the requesting entities. Aggregation of detailed QoS history records using Equation (13) and assuming self-honesty hon_i equal to 1, generate the detailed aggregated evaluation of history for any of the alternatives n displayed by dae_{his_n}. Similarly, using Equations (14), 15, and 16, the general aggregated evaluation of history for any of the alternatives n is calculated and denoted by gae_{his_n}. As with the total recommendation aggregation, the general and aggregated evaluations of history are combined using a weighted sum model presented below:

$$his_n = \left(\frac{n^{i.n.s}_{cn^d_c}}{n^{i.n.s}_{cn^d_c} + n^{\det}_{his_{i.n}}} \times dae_{his_n}\right) \oplus \left(\frac{n^{\det}_{his_{i.n}}}{n^{i.n.s}_{cn^d_c} + n^{\det}_{his_{i.n}}} \times gae_{his_n}\right) \tag{33}$$

The generated value his_n is the historical part of the total trust toward the SIA_n.

D. Total trust aggregation

Following the aggregation of the assertation, recommendation, and historical parts of trust, the resulting values are aggregated to generate the total trust. For any SIA_n, the total aggregated trust t_{total_n} is calculated using a weighted sum model as follows:

$$t_{total_n} = \left(w^{assertation}_n \times dae_{assertation\,n}\right) \oplus \left(w^{his}_n \times his_n\right) \oplus \left(w^{rec}_n \times rec_n\right) \tag{34}$$

where the real numbers $w^{assertation}_n$, w^{his}_n, and w^{rec}_n are the regular aggregation weights and their sum is equal to one.

To calculate the regular weights, three equivalent non-regular weights are calculated and then normalized within the interval [0,1]. In this weighting, the neutrosophic accuracy of the assertation, recommendation, and the historical parts of trust is used as a determinant of its importance for trust aggregation. Additionally, for the recommendation, the total number of recommenders and for the history part, the total number of interactions is used as an incremental factor. However, this increase is intended with a logarithmic rate to limit its impact. Then, the non-regular weights are calculated as follows:

$$\tilde{w}^{assertation}_n = Acc_{inn}(dae_{assertation\,n}) \tag{35}$$

$$\tilde{w}^{his}_n = \left(Acc_{inn}(his_n) \times log\left(n^{i.n.s}_{cn^d_c} + n^{det}_{his_{i.n}} + 1\right)\right) \tag{36}$$

$$\tilde{w}^{rec}_i = Acc_{inn}(rec_i) \times log\left(R + R^{'} + 1\right) \tag{37}$$

After that, the regular weights are calculated using the non-regular weights as follows:

$$w^{assertation}_n = \frac{\tilde{w}^{assertation}_n}{sum_w}, w^{rec}_n = \frac{\tilde{w}^{rec}_n}{sum_w}, w^{his}_n = \frac{\tilde{w}^{his}_n}{sum_w} \tag{38}$$

$$sum_w = \left(\tilde{w}^{assertation}_n + \tilde{w}^{rec}_n + \tilde{w}^{his}_n\right)$$

After identifying the regular weights, the total trust of any SIA can be calculated based on Equation (34), which is an INN. This total trust is cumulative of all evaluation data, context conditions, and user preferences, which indicates the total expectation about the QoS experience with any SIA and is used for selecting the most appropriate SIA for the interaction. For this purpose, it is necessary to sort SIAs based on their total trust. Thus, there is a need for a measure to map INNs to real numbers. The neutrosophic score function is an appropriate measure for this purpose, given its definition and characteristics, which include its direct relationship to the truth of the INN and its inverse relation to uncertainty and falsity. As such, for any SIA, trust decision making denoted as t_{dec_n} is performed using the score function, and the SIA with the highest t_{dec_n} is selected for the service.

$$t_{dec_n} = Sc_{inn}(t_{total_n}) \tag{39}$$

3.8. Trust updating

In this stage of trust calculations, the trust calculator entity updates its history records based on its real experience with the selected SIA. This update is performed on the QoS history record of the selected SIA as well as the honesty history record of the recommenders. For the selected SIA, the experienced QoS is considered as the basis for updating its QoS history record. Likewise, the difference between the experienced QoS and the recommendation by any recommender which indicates the correctness and precision of the recommendation is used to update its honesty history.

To evaluate the recommenders and the selected SIA, it is necessary to evaluate the real QoS, experienced by the selected SIA. The quantitative evaluation of the m th trust criterion experienced by the selected SIA with ID n is referred to as $v^{ex}_{cr_{m,\tilde{n}}}$. As displayed in Fig. 2, the experienced quantitative values are preprocessed similar to the assertation values of the alternatives

and are transformed to INNs. The equivalent INN (denoted as $ex_{cr_{m,\tilde{n}}}$), is the evaluation of the m th criterion for the selected SIA with ID $\tilde{n}$. Then, the total QoS, experienced by the selected SIA, is calculated as follows:

$$ex_{total}^{\tilde{n},s} = \sum_{m=1}^{M_s} (w_{cr_m} \otimes ex_{cr_m}^{\tilde{n},s}) \tag{40}$$

In the proposed model, trust updates about the recommenders and the selected SIA are performed considering the quality of the transaction context. As the trust aggregation Equations (13) and (16) represent, the quality of context influences the calculated trust of an entity. Thus, the quality of context affects the expectation of the accuracy of recommenders' opinions, and the self-assertions of SIAs. The total quality of context for the selected SIA with ID $\tilde{n}$ offering service s is calculated using the following formula:

$$ex_{context}^{\tilde{n},s} = \sum_{m=1}^{M_s} (w_{cr_m} \otimes ex_{cn_m}^{\tilde{n},s}) \tag{41}$$

In the following subsections, the trust updating model of the selected SIA and the recommenders is presented.

A. Alternatives trust updating

The trust updating for the selected SIA is performed on general and history records. The following formula represents the approach to updating the general history using an exponential moving average with a coefficient named α:

$$his_{cn_c^d}^{i,\tilde{n},s}(t+\Delta t) = (\alpha * ex_{total}^{\tilde{n},s}) \oplus \left((1-\alpha) * his_{cn_c^d}^{i,\tilde{n},s}(t)\right), \left(his_{cn_c^d}^{i,n,s}, n_{cn_c^d}^{i,\tilde{n},s}\right) \in His_{al_{\tilde{n}}}^{general} \tag{42}$$

where α is a real number within [0,1] specifying the weight of the recent experience. Note that the recent experiences are considered with a higher importance in trust updating. Also, if the real experience $ex_{total}^{n,s}$ is more accurate and has less uncertainty, it is considered a more reliable experience and will have more impact on the updated trust value. The α coefficient is calculated using the following formula:

$$\alpha = Acc_{inn}(ex_{total}^{\tilde{n},s}) \times Sc_{inn}(ex_{context}^{\tilde{n},s}) \tag{43}$$

Similar to the general history update, the detailed history update is performed using the exponential moving average with the coefficient named β_m. However, the update is individually performed for any trust evaluation criteria:

$$his_{al_{\tilde{n}},m}^{i}(t+\Delta t) = (\beta_m * ex_{cr_m}^{\tilde{n},s}) \oplus \left((1-\beta_m) * his_{al_{\tilde{n}},m}^{i}(t)\right) \tag{44}$$

where β_m is a real number like α and within the same range, specifying the weight for updating criteria m and is calculated as below:

$$\beta_m = Acc_{inn}(ex_{cr_m}^{\tilde{n},s}) \times Sc_{inn}(ex_{context}^{\tilde{n},s}) \tag{45}$$

B. Recommenders' trust updating

This update is performed for detailed and general recommenders separately. For a detailed recommender with ID r, the distance between the detailed recommendations for all service s' criteria and the experienced value for any criterion is aggregated using the weight of each criterion as below:

$$dis_r^{\tilde{n},s} = \sum_{m=1}^{M_s} w_{cr_i} \times Dis_{hamming}(rec_{cr_{m,\tilde{n}}}^{r}, ex_{cr_m}^{\tilde{n},s}) \tag{46}$$

Here, the resulting value $\tilde{dis}_r^{n,s}$ is the total distance between the recommendation of recommender r about the selected SIA $\tilde{n}$ and the experienced values for different service evaluation criteria. The respective distance for the general recommendations is considered as the Hamming distance between the general recommendation and the total experience as follows:

$$\tilde{dis}_x^{n,s} = Dis_{hamming}(rec_{al_{\tilde{n}},s}^{gen}, ex_{total}^{k,s}) \tag{47}$$

Hamming distance is used because we want to evaluate the distance of the received recommendations to an ideal point which is the real experienced QoS. That means, ideally, the SR expects recommenders to provide the real experienced QoS as their recommendations. Thus, based on this natural mapping and also due to its simplicity, we chose to use Hamming distance instead of other distance measures, as it has been used in other approaches such as the work presented in [30].

Similar to the QoS history updating, the honesty history updating is performed using an exponential moving average formula, as follows:

$$hon_r^i(t+\Delta t) = w_{rec_r}^{update} \times \left(1 - dis_x^{k,s}\right) + \left(1 - w_{rec_r}^{update}\right) \times hon_j^i(t) \tag{48}$$

Similar to the α and β_m coefficients, the update coefficient $w_{rec_r}^{update}$ has a direct relationship with the quality of context. Furthermore, the number of previous recommendations $n_{trans_r}^{i}$ represents the certainty of the recommendation corresponding to the previous honesty value of recommender r. Thus, it must have an inverse relationship with $w_{rec_r}^{update}$ which can be calculated by the following formula:

$$w_{rec_r}^{update} = \frac{Sc_{inn}\left(\widetilde{ex}_{context}^{n.s}\right)}{\log\left(n_{trans_r}^{i}+1\right)} \tag{49}$$

Here, the use of the logarithmic rate limits the impact of the number of transactions for large values of $n_{trans_r}^{i}$.

4. Evaluations

In this section, the performance of the proposed model is validated, and the impact of various factors on its performance is investigated.

4.1. Evaluation assumptions

The devised simulation scenarios are selected in a way to be similar to the related approaches of the current research, such as the studies performed by Chen et al. [1] and Wang et al. [2]. For the scenarios, a service-oriented environment has been assumed to contain N IoT nodes. In the simulations, P_b percent of the nodes has been considered as the bad nodes. It is assumed that the nodes receive recommendations from peers with whom their owners have a social relationship. Two types of social relations have been considered between the owners of the IoT nodes: (1) friendship and (2) membership in the same group. It is supposed that any node on average has N_{friend} friends and is a member of N_{group} groups. It is assumed that for any node, the friends provide detailed recommendations, and the nodes in the same group provide a general recommendation.

The simulation scenarios are performed in several iterations, in each of which one node is selected randomly as the SR. Then, N_c nodes are selected randomly as candidates for providing the requested service. These parameters are summarized in Table 3. The specified value or range of values is used in different simulation scenarios. In the evaluation scenarios, several types of IoT nodes have been considered to have different behaviors and operations in various contexts.

In this section, the behavioral model of the IoT nodes and the context models are described. For the sake of simplicity, one type of service has been assumed in the simulations. Table 4 reports the trustworthiness criteria and the related indicator functions for the service named S. The weights of the criteria are specified by the linguistic terms *important* and *very important* which are mapped to the real values 0.7 and 0.9. The detailed context criteria for the two trustworthiness criteria, their indicator functions, and their importance are parameterized in Table 5. In Table 6, QoS service behavior is designated for three types of IoT nodes, specifying the asserted and real experienced behavior about the service evaluation criteria. These three models are used in the evaluation scenarios in the detailed contexts parameterized in Table 7 as well as the HLCs in Table 8. These two tables specify two models for the detailed context and two models for HLC, both used in the simulation scenarios.

4.2. Simulation scenarios

To validate the proposed method, three categories of evaluations have been performed, which are discussed in this section. In the performed evaluations, three criteria were evaluated in a window W of the simulation's iterations. This window

Table 3
Simulation parameters' values.

Parameter	Description	Value range	Default value
N	Number of nodes	100	100
P_b	The percentage of bad nodes	[10–90%]	30
F	The average number of friends for each node	10	10
G	The average number of social groups each node is a member of	10	10
N_c	Number of candidate nodes for the interaction	3	3

Table 4
Trustworthiness criteria specifications for the service S.

Trustworthiness criteria	Variation	Satisfaction	Dissatisfaction	The default weight of criteria
Delay (Seconds)	$0 < x < inf$	$S_{cr_{delay}}(t) = trimf(0,0,120)$	$D_{cr_{delay}}(t) = trimf(200,250,inf)$	Very important
Accuracy (%)	$0 < e < inf$	$S_{cr_{accuracy}}(e) = trimf(0,0,10)$	$D_{cr_{accuracy}}(e) = trimf(40,40,100)$	Important

Table 5
Detailed context specification of the service *S*.

Trustworthiness criteria	detailed context criteria	Variation	Satisfaction indicator function	Dissatisfaction indicator function	The default weight of criteria
Network delay	Network utilization	$0 < x < 100$	$S_{cn_{net\_util}}(x) = trimf(0,0,40)$	$D_{cn_{net\_util}}(x) = trimf(50,100,100)$	Important
Accuracy	White noise	$0 < e < inf$	$S_{cn_{accuracy}}(e) = trimf(0,0,100)$	$D_{cn_{accuracy}}(e) = trimf(100,120,inf)$	Important

Table 6
Quantitative evaluation of trustworthiness criteria for three models of IoT nodes.

Trustworthiness Criteria	Evaluation of data source	Node type 1 (Good)	Node type 2 (Middle)	Node type 3 (Bad)
Delay	Asserted by the SIA	$V_{cr_{delay,Alt\#1}} = trimf(10,20,30)$	$V_{cr_{delay,Alt\#2}} = trimf(50,60,70)$	$\boldsymbol{V_{cr_{delay,Alt\#3}} = trimf}(10,20,30)$
	Experienced by trustor	$ex^{Alt\#1,s}_{cr_{delay}} = trimf(10,20,30)$	$ex^{Alt\#2,s}_{cr_{delay}} = trimf(50,60,70)$	$\boldsymbol{ex^{Alt\#1,s}_{cr_{delay}} = trimf}(200,300,700)$
Accuracy	Asserted by the SIA	$V_{cr_{accuracy,Alt\#1}} = trimf(0,1,2)$	$V_{cr_{accuracy,Alt\#2}} = trimf(15,20,25)$	$\boldsymbol{V_{cr_{accuracy,Alt\#3}} = trimf}(0,1,2)$
	Experienced by trustor	$ex^{Alt\#1,s}_{cr_{accuracy}} = trimf(0,1,2)$	$ex^{Alt\#2,s}_{cr_{delay}} = trimf(15,\ 20,25)$	$ex^{Alt\#3,s}_{cr_{delay}} = trimf(50,60,90)$

Table 7
Quantitative evaluations of context criteria for two models of detailed context.

Quantity	Detailed context 1 (Good)	Detailed context 2 (Bad)
Network utilization	$V_{cn_{net\_util,Alt}}(x) = trimf(0,0,40)$	$V_{cn_{net\_util,Alt\#}}(x) = trimf(50,0,0)$
accuracy	$V_{cn_{accuracy,Alt}}(e) = trimf(10,11,12)$	$V_{cn_{accuracy,Alt}}(e) = trimf(10,11,12)$

Table 8
Quantitative evaluations concerning the coverage and membership functions of two models of HLC.

High-level context	variation	Coverage function	HLC 1 (High coverage)	HLC 2 (Pure coverage)
Day time (When)	$0 < t < 24$	$Cov_{cn^{when}_{dayTime}}(t) = trapmf(\ 4,7,18,20)$	$Mem^{al_1}_{cn^{when}_{dayTime}}(t) = trimf(10,10,10)$	$Mem^{al_2}_{cn^{when}_{dayTime}}(t) = trimf(2,2,2)$
Home distance (Where)	$0 < l$	$Cov_{cn^{where}_{nearHome}}(l) = trimf(l,0,0,1000)$	$Mem^{al_1}_{cn^{where}_{nearHome}}(l) = trimf(l,100,101,102)$	$Mem^{al_2}_{cn^{where}_{nearHome}}(l) = trimf$ $(l,1200,1201,1202)$

is used for the smoothness of the outcome diagrams, with its value assumed to be 500. The evaluation criteria presented in their respective diagram are described below:

a) **QoS-T diagram**: The average value of QoS trust, calculated by the IoT nodes, is demonstrated in this diagram. The values are calculated for the *good*, *bad*, or *specific* nodes as the output of Equation (39). The value of this criterion is used to decide the best SIA for interaction and is affected by several factors, including QoS evaluations, sources of uncertainty, recommendations, and quality of context.
b) **Honesty diagram**: The average value of honesty calculated for different types of IoT nodes is displayed in this diagram. The value of this criterion specifies how honest different IoT entities view other nodes. This parameter is calculated using Equation (48).
c) **CDR diagram**: The correct decisions ratio (CDR) specifies in what fraction of decisions made by SRs, the best SP is selected. This ratio is calculated by dividing the number of decisions made, in which the best SP node has been selected in the recent W iterations (denoted by $N_{correct}$) by the value of w, as represented by Equation (50). This criterion somehow represents the satisfaction of nodes with the services received.

$$CDR = N_{correct}/w \tag{50}$$

A. Coverage and accuracy evaluations

These experiments are performed to determine the accuracy and rationality of the results as well as to designate how consistent the estimates are with the reality and expectations about the output.

1. The impact of the percentage of bad nodes

The purpose of this evaluation is to estimate the convergence speed of the calculated trust for good and bad nodes when the percentage of bad nodes (P_b) changes. In these experiments, the bad nodes provide reverse recommendations and services with bad qualities. The simulations have been performed considering 10, 30, 60, and 90% for the parameter P_b. As illustrated in Fig. 4.a, the CDR value for all simulations coverages to a value close to 1. Further, this convergence occurs faster for

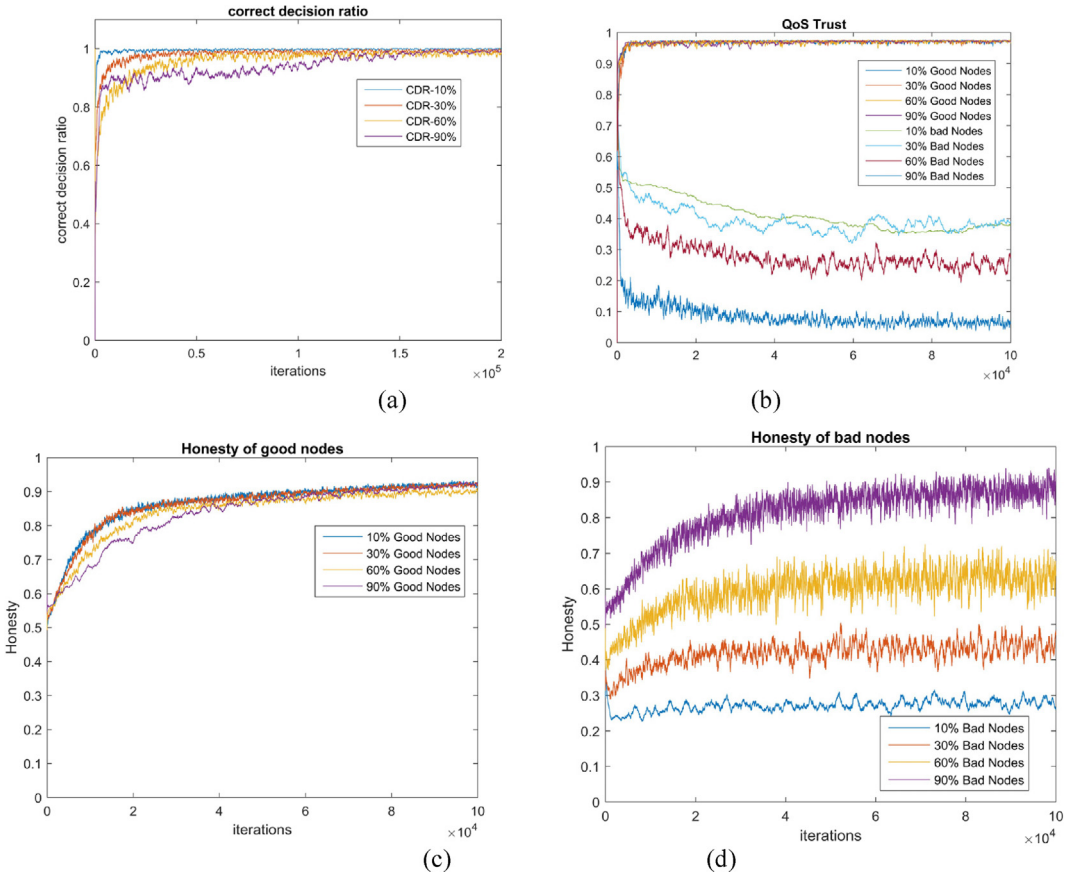

Fig. 4. The impact of the bad node percentage.

the simulations with greater P_b. That is because the QoS trust is calculated and maintained by the distributed nodes, and when the percentage of bad nodes is higher, it takes a longer time for the good nodes to form trust between each other and to receive services and recommendations. In these simulations, as demonstrated in Fig. 4.b, the convergence speed of the QoS-Trust criterion for good nodes to its final value is almost similar. However, for the bad nodes, the convergence is slower when P_b is larger. The reason is, when the percentage of bad nodes is lower, due to their scarcity, their probability of being selected as an SIA is reduced. Thus, the convergence of their trust toward the final value will occur at a slower rate.

The honesty diagrams in Fig. 4.c and Fig. 4.d reveal that if the value of P_b is larger, the honesty of bad nodes converges to a higher value. That is because when the number of bad nodes is larger, their positive recommendations about each other would promote their honesty. However, since the good nodes recognize each other due to correct recommendations and increase honesty in their history, the honesty of good nodes converges to its desired value.

2. Honesty impact

The recommendation behavior of the evaluated nodes has a significant impact on the trust convergence, which is examined in this part. A bad node's behavior can be due to low QoS. However, even this node can be honest in providing recommendations about other nodes. In this part, two models of bad nodes' behavior are considered, and two experiments have been performed regarding these two types of nodes:

1. Providing improper QoS while correct recommendations about other nodes are given.
2. Providing improper QoS while the recommendations about the other nodes are incorrect as well.

Experiments indicate that if bad nodes present honest recommendations, the speed of convergence to the final trust would be faster. The reason for this is the positive effect of the honest recommendations provided by all nodes, improving the trust distribution between nodes. In Fig. 5.c, the CDR is always higher when all nodes are honest. The honesty diagram in Fig. 5.a demonstrates that if bad nodes make honest recommendations, their honesty converges to the final value along with good nodes, and if they provide incorrect recommendations, their honesty converges to a low number. The QoS-T diagram in Fig. 5.b reveals that providing malicious recommendations by bad nodes causes their QoS-T to be high at the beginning of the experiment. However, as the simulation progress forward and the history information is gradually completed, the QoS trust

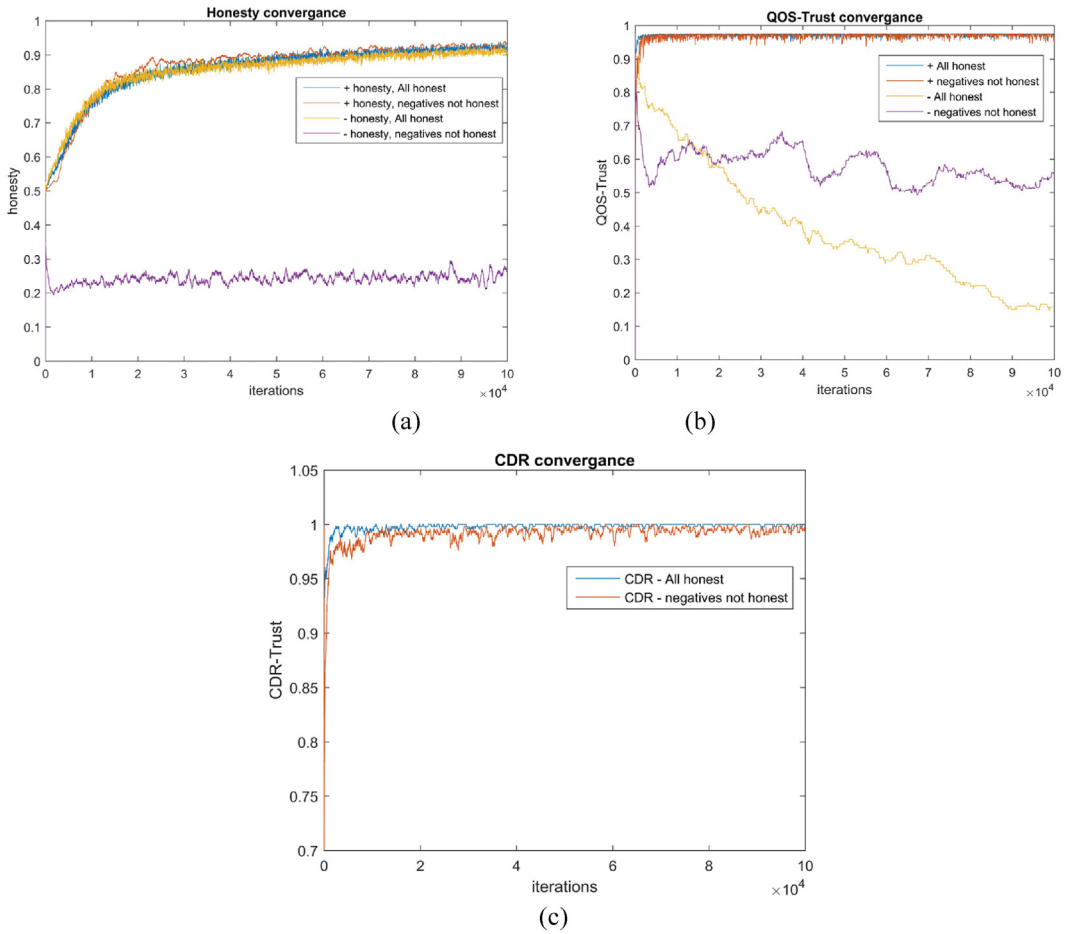

Fig. 5. Impact of bad nodes' honesty on the coverage of QoS trust.

and honesty of bad nodes converge to the low-value range. The converged value of QoS in this state is higher than in the other simulations where the bad nodes provide correct recommendations. This is because the correct recommendations facilitate the distribution of trust-related information between objects and create a faster convergence.

B. Sensitivity analysis

The simulations performed in this section aim to demonstrate the effectiveness of different components in the proposed model. The main approach of these simulations is that in each scenario, N_s IoT nodes are selected randomly. Then, during the simulation process, various parameters are changed in the selected nodes at the iteration I_{ch1} and are returned to their initial state at the iteration I_{ch2}. Next, the effect of this variation is analyzed on this interval, called transition interval (TrI),. In the performed simulations, the number N_s is assumed 5, with I_{ch1} and I_{ch2} being 15,000 and 75,000 respectively.

1. QoS changes sensitivity

Two forms of QoS changes in the selected nodes have been investigated: (1) QoS change of only one criterion and (2) QoS change of all criteria to the middle node, outlined in Table 6. In the first evaluation scenario, the $ex_{cr_{accuracy}}^{specifics,s}$ criterion for the specific nodes is assumed to have the value stated for the bad IoT nodes presented in Table 6. In the second scenario, the specific nodes provide services with middle node quality. In both scenarios, the selected nodes truly represent their QoS assertions and the correctness of recommendations about the others.

As depicted in Fig. 6, the QoS trust for both scenarios diminishes to about the average value for QoS. These tests suggest that the value of any trustworthiness criterion can influence the overall trust based on its corresponding weight. Because in both scenarios the selected nodes did not change their honesty behavior, the honesty diagram for both is almost the same as displayed in Fig. 5. The honesty of all nodes ensures correct trust distribution between IoT nodes. Thus, the CDR factor in both scenarios was almost the same, converging to its maximum value as depicted in Fig. 5.

2. Sensitivity to context uncertainty

In this part, the effect of context changes on the QoS trust of the selected nodes is examined. As explained in Section 4.3, two types of context models, named DTC and HLC, have been considered. The impact of DTC is examined by setting the inap-

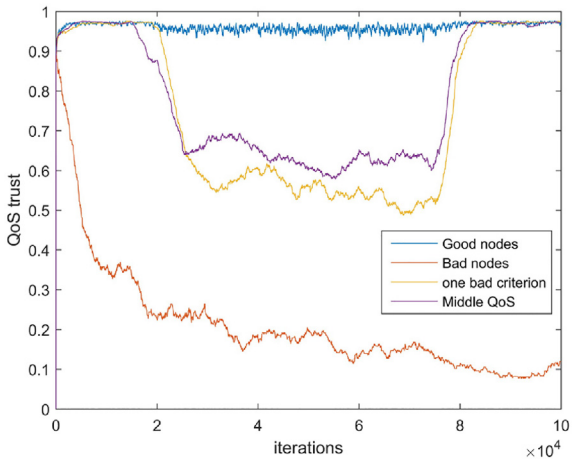

Fig. 6. QoS diagram for the QoS change scenario.

propriate detailed context for all criteria, as specified in Table 7. Accordingly, as indicated in Fig. 7, the QoS trust of the selected nodes is diminished in the transition interval. The reason is that the inconsistent detailed context in Equation (13) lowers the level of detailed QoS trust, affecting the final level of QoS trust. The effect of HLC is considered by reducing the coverage of the general contexts in which the service functionality of the SIAs has been identified as appropriate. As the IoT nodes perform well during the simulation, in the case of high coverage for the HLCs listed in Table 8, the coverage of both HLCs is reduced to the pure coverage specified in Table 8. As exhibited in Fig. 7, the QoS trust of the selected nodes is diminished. As seen, the decline caused by the HLC changes is higher than the effect of DTC. In these simulations, since the number of aggregated recommenders is higher than that of the detailed recommenders (noted in Table 3), the impact of HLC would be greater.

In the final experiment, both the DTC and HLC changes are performed in the transition interval for the selected nodes. Hence, the QoS trust curve of this experiment is lower compared to the results of the previous simulations. That is because the effects of both detailed and high-level contexts are considered.

C. Comparative evaluations

In this section, the comparisons of the proposed approach with similar existing approaches are presented. The selection of neutrosophic numbers as the data type for trust modeling is an important aspect of the current study. Thus, we have first demonstrated the effectiveness of this data type in comparison with two other data types. Furthermore, the proposed approach is compared with two state-of-the-art approaches.

1. Effectiveness of using neutrosophic numbers

In this part, we demonstrate the effectiveness of using neutrosophic numbers on the accuracy of the estimated trust. In the performed simulations, we demonstrate how much the INNs' capabilities for modeling trust have improved the accuracy of the calculated trust compared to other similar representation models. Here, three data models are compared: (1) INN, (2)

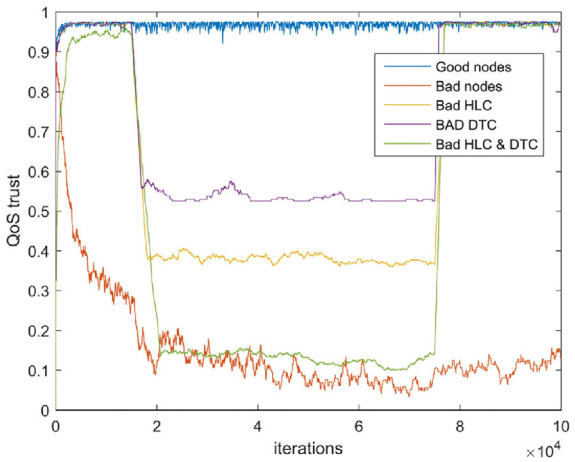

Fig. 7. QoS trust values with respect to the context changes.

interval-valued intuitionistic fuzzy numbers (IIFNs) [49,50], and (3) simple real numbers (RNs). The simulations are done for the model of the IoT node described in Table 6 denoted as the *good* node model. A major distinction is that for this case, it is assumed that the evaluation uncertainty modeled as the indeterminacy part of INNs has its maximum value. This is due to the existence of multiple sources of uncertainty in the evaluated quantitative values. The scenarios are described below:

a) **Simple real numbers:** By using this representation model, the QoS-trust, context trust, and honesty trust are modeled as RNs within [0.1]. This trust model only represents the truth part of the trust. Then, the mean for the interval number is set as the truth part of the INNs and is considered as the trust, while the indeterminacy and falsity parts are ignored.
b) **Interval-valued intuitionistic fuzzy numbers:** This trust model represents the truth and falsity parts of the trust, while the indeterminacy part is ignored. The score function used for calculating trust in Equation (39) is assumed to be the score function proposed in [50].
c) **Interval-valued neutrosophic numbers:** This is the main mathematical representation for the proposed model in this research.

Fig. 8 demonstrates the QoS diagram for the described scenarios. As shown, the trust evaluated by the RN model starts converging to the maximum value for trust, but its convergence occurs more slowly compared to the IIFN model. This is because the IIFN model considers falsity and truth terms together, and the evaluated trust values are more likely to converge to their final values. The indeterminacy term is ignored in the IIFN model, and its value converges more rapidly to the maximum trust value. This is despite the existence of indeterminacy. The trust evaluated using the INN model converges to a value close to 0.5 which is the value of INN (1,1,0). This is because the uncertainty term has been considered, and the evaluated trust converges to its real value. At the start of the simulation, there is a limited upward trend. The reason for such a trend at the start of the simulation is that all nodes have introduced themselves as ideal nodes without uncertainty in providing services. However, after the simulation progresses, their real behavior is identified, and their trust converges to its real value.

2. Comparative analysis with similar works

We have selected the works performed by Chen et al. [1] and Alshehri et al. [18] as they are amongst the most notable works in this domain, and their overall scheme can be appropriately compared with the proposed approach. For the comparative testing scenario, we have chosen the sensitivity to context uncertainty, explained in section 5.2. The simulation parameters are assumed to have the default values mentioned in section 5.1. The compared works have not modeled trust using a multi-criteria approach. Thus, the behavior of *good* and *bad* nodes is specified by 1 and 0 values for their overall experience quality.

In the comparative test scenario, we have assumed that 30% of the randomly selected nodes are under inadequate high-level context (HLC) conditions during the transition interval of each service interaction. The dynamic context change assumption is based on the mobility of nodes in a natural IoT environment. By sensing the context criteria as uncertainty parameters and including them in trust calculations, the proposed method can detect SIAs that are not suitable for interaction due to bad context conditions. Accordingly, as shown in Fig. 9(a), the CDR graphs of compared works drop by over 30% (as 30% of nodes are in bad HLC) during the transition interval, but the results of the proposed approach remain at the same level.

Fig. 9(b) illustrates the mean QoS Trust for the nodes that have poor HLC conditions. As the proposed approach considers context uncertainty, the trust calculated for these nodes diminishes same as in Fig. 7. However, in similar works, since they

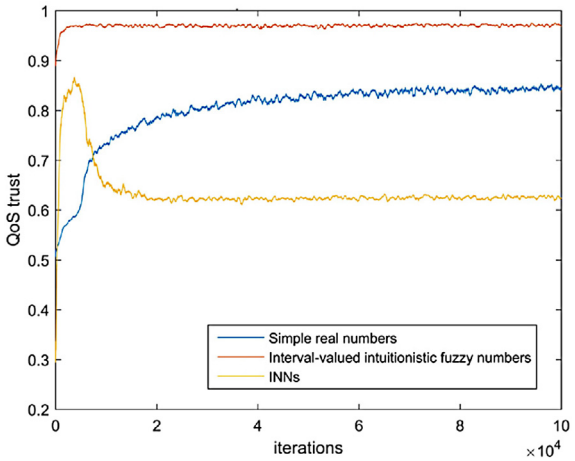

Fig. 8. The QoS trust calculated for the proposed INN model compared to the QoS trust for the RN and IIFN models.

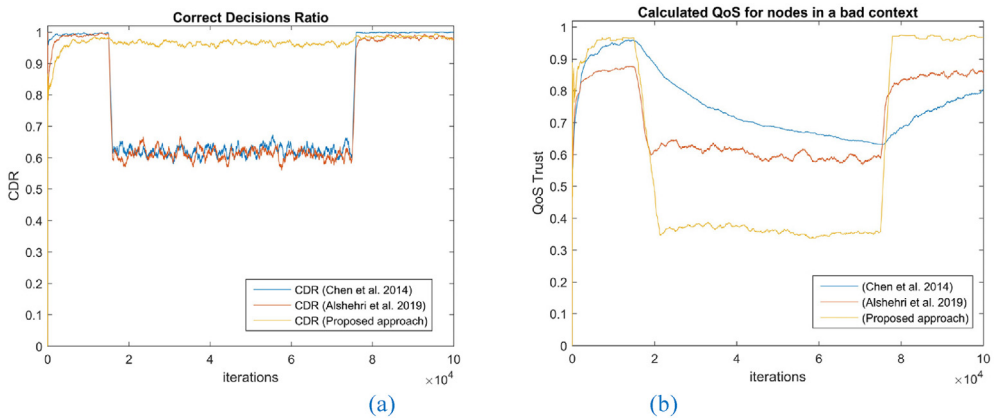

Fig. 9. (a)Comparison of the Correct Decision ratio (CDR) for the proposed method with the works of Chen et al. [1] and Alshehri et al. [18]; (b) Comparison of the QoS trust for the proposed method with the works of Chen et al. [1] and Alshehri et al. [18].

do not consider context, the calculated trust diminishes by only about 30%, which is the percentage of nodes that are in a bad HLC. In these works, the overall calculated trust decreases by around 30% for all nodes.

5. Conclusion

In this research, a computational trust model was proposed for the decision-making in SOA-based SIoT environments where uncertainty is considered a primary concern. To this aim, several specific and unspecific sources of uncertainty in the context conditions of IoT interactions and data evaluation were modeled and applied. In this model, the certainty toward the QoS of service interaction alternatives, the honesty of recommenders, and the appropriateness of context conditions were evaluated separately and merged to form the final trust. In the proposed model, INNs as a beneficial mathematical tool for considering uncertainty were leveraged. The proposed model was applied in a social environment, where the average QoS trust and honesty were selected as the evaluation criteria for the IoT nodes. It was shown that these evaluation criteria would converge to their expected values based on the behavior of the considered nodes. In the evaluation scenarios, the effect of QoS and honesty changes for IoT nodes, the indeterminacy of the data, and uncertainty in specific or unspecific context conditions, as well as the recommendation attacks by malicious IoT nodes were examined. The results of simulations indicated that the rate of correct decisions for selecting the best SP was not affected significantly, and the model generated accurate results.

As for future works in this area, we are working to apply uncertainty modeling at the IoT's cloud service level. Cloud services can provide trust management as a service for the IoT nodes, and they do not have restrictions such as low computational power and storage resources. In addition, the distributed architecture of the 5G networks can be used as a computational platform for evaluating trust for different applications. The capabilities of these distributed resources in conjunction with the centralized cloud resources can be studied for trust calculations. As a result, the proposed trust model can be adapted for operation at the cloud service level, where uncertainty modeling can be useful for IoT cloud applications. Another possible extension of the proposed approach is the consideration of the service requestor's feedback about the quality of the experienced service to the selected service provider. This way, the SP can adjust the criteria for the offered service based on the preferences of any SR in its community of interest. These adjustments can be performed based on the trade-offs between the speed and the quality preferences of the offered service. Another potential extension to the current work is to use a trapezoidal interval-valued neutrosophic model instead of the currently used interval-valued model. Trapezoidal interval-valued neutrosophic numbers can be the basis for more accurate calculations resulting in a better computational trust model. Finally, extending the model in a way to capture the privacy-preservation concerns of the users as addressed in similar approaches such as [48] can be another interesting direction.

CRediT authorship contribution statement

Sajad Pourmohseni: Conceptualization, Methodology, Software, Validation, Writing – original draft. **Mehrdad Ashtiani:** Writing – review & editing. **Ahmad Akbari Azirani:** Supervision, Writing – review & editing, Project administration.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] I.R. Chen, J. Guo, F. Bao, Trust management for soa-based iot and its application to service composition, IEEE Trans. Serv. Comput. 9 (3) (2014) 482–495.
[2] Y. Wang, I.R. Chen, J.H. Cho, A. Swami, Y.C. Lu, C.T. Lu, J.J.P. Tsai, CATrust: context-aware trust management for service-oriented ad hoc networks, IEEE Trans. Serv. Comput. 11 (6) (2016) 908–921.
[3] M. Roopa, S. Pattar, R. Buyya, K. Venugopal, S. Iyengar, L. Patnaik, Social Internet of Things (SIoT): foundations, thrust areas, systematic review and future directions, Comput. Commun. 139 (2019) 32–57.
[4] J. Guo, G. Huang, Q. Li, N. Xiong, S. Zhang, T. Wang, STMTO: A smart and trust multi-UAV task offloading system, Inf. Sci. 573 (2021) 519–540.
[5] M.A. Azad, S. Bag, F. Hao, A. Shalaginov, Decentralized self-enforcing trust management system for social Internet of Things, IEEE Internet Things J. 7 (4) (2020) 2690–2703.
[6] U. Jayasinghe, N.B. Truong, G.M. Lee, T.W. Um, RpR: A trust computation model for social Internet of Things, 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, 2016.
[7] U. Jayasinghe, H.W. Lee, G.M. Lee, A computational model to evaluate honesty in social internet of things, The Proceedings of Symposium on Applied Computing, Marrakech, Morocco, 2017.
[8] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of Things, J. Network Comp. Appl. 42 (2014) 120–134.
[9] M. Nitti, R. Girau, L. Atzori, Trustworthiness management in the social internet of things, IEEE Trans. Knowl. Data Eng. 26 (5) (2013) 1253–1266.
[10] C. Perera, M. Barhamgi, A.K. Bandara, M. Ajmal, B. Price, B. Nuseibeh, Designing privacy-aware internet of things applications, Inf. Sci. 512 (2020) 238–257.
[11] S.Y. Ben, A. Olivereau, D. Zeghlache, M. Laurent, Trust management system design for the Internet of Things: a context-aware and multi-service approach, Comput. Security 39 (2013) 351–365.
[12] Y.L. Sun, W. Yu, Z. Han, K.R. Liu, Information theoretic framework of trust modeling and evaluation for ad hoc networks, IEEE J. Sel. Areas Commun. 24 (2) (2006) 305–317.
[13] Z. Gonga, H. Wanga, W. Guoa, Z. Gong, G. Wei, Measuring trust in social networks based on linear uncertainty theory, Inf. Sci. 508 (2020) 154–172.
[14] H. Ma, Z. Haibin, H. Zhigang, L. Keqin, W. Tang, Time-aware trustworthiness ranking prediction for cloud services using interval neutrosophic set and ELECTRE, Knowl.-Based Syst. 138 (2017) 27–45.
[15] N.H. Aghdam, M. Ashtiani, M.A. Azgomi, An uncertainty-aware computational trust model considering the co-existence of trust and distrust in social networks, Inf. Sci. 513 (2020) 465–503.
[16] J. Bernabe, J. Ramos, AFGomez, TACIoT: multidimensional trust-aware access control system for the Internet of Things, Soft. Comput. 20 (9) (2016) 1763–1779.
[17] C. Dong, C. Guiran, S. Dawei, L. Jiajia, J. Jie, W. Xingwei, TRM-IoT: A trust management model based on fuzzy reputation for internet of things, Comput. Sci. Inf. Syst. 8 (4) (2011) 1207–1228.
[18] M.D. Alshehri, F.K. Hussain, A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT), Computing 101 (7) (2019) 791–818.
[19] "Detecting unfair recommendations in trust-based pervasive environments," *Information Sciences*, vol. 486, pp. 31-51, 2019.
[20] F.O. Hoffman, J.S. Hammonds, Propagation of uncertainty in risk assessments: the need to distinguish between uncertainty due to lack of knowledge and uncertainty due to variability, Risk Anal. 14 (5) (1994) 707–712.
[21] H.y. Zhang, J.q. Wang, X.-h. Chen, Interval neutrosophic sets and their application in multicriteria decision making problems, Sci. World J 2014 (2014).
[22] R. Sahin, "Multi-criteria neutrosophic decision making method based on score and accuracy functions under neutrosophic environment," arXiv preprint, arXiv:1412.5202, 2014.
[23] J. Ye, Similarity measures between interval neutrosophic sets and their applications in multicriteria decision-making, J. Intell. Fuzzy Syst. 26 (1) (2014) 165–172.
[24] F. Smarandache, A Unifying Field in Logics. Neutrosophy: Neutrosophic Probability, Set and Logic, American Research Press, Rehoboth, USA, 1999, pp. 1–141.
[25] J. Ye, A multicriteria decision-making method using aggregation operators for simplified neutrosophic sets, J. Intell. Fuzzy Syst. 26 (5) (2014) 2459–2466.
[26] W. Haibin, F. Smarandache, Y. Zhang, R. Sunderraman, Single valued neutrosophic sets, in *Review of the Air Force Academy, The Scientific Informative Review, No 1(16)/2010* , Brasov, Romania, "Henri Coanda" Air Force Academy Printed House, 2010, pp. 10-14.
[27] S. Broumi, D. Nagarajan, M. Lathamaheswari, M. Talea, A. Bakali, F. Smarandache, Intelligent algorithm for trapezoidal interval valued neutrosophic network analysis, CAAI Trans. Intel. Technol. 5 (2) (2020) 88–93.
[28] J. Ye, Improved cosine similarity measures of simplified neutrosophic sets for medical diagnoses, Artif. Intell. Med. 63 (3) (2015) 171–179.
[29] N.D. Thanh, L.H. Son, M. Ali, Neutrosophic recommender system for medical diagnosis based on algebraic similarity measure and clustering, in *in the proceedings of Fuzzy Systems (FUZZ-IEEE), IEEE International Conference*, Naples, Italy, 2017.
[30] D. Stanujkic, D. Karabasevic, F. Smarandache, E. Kazimieras, M. Maksimovic, An innovative approach to evaluation of the quality of websites in the tourism industry: a novel MCDM approach based on bipolar neutrosophic numbers and the Hamming distance, Transf. Busi. Econ. 18 (1) (2019) 149–162.
[31] A. Mukherjee, S. Sarkar, Several similarity measures of neutrosophic soft sets and its application in real life problems, Ann. Pure Appl. Math. 7 (1) (2014) 1–6.
[32] D. Karabašević, D. Stanujkić, E.K. Zavadskas, P. Stanimirović, G. Popović, B. Predić, A. Ulutaş, A novel extension of the TOPSIS method adapted for the use of single-valued neutrosophic sets and hamming distance for e-commerce development strategies selection, Symmetry 8 (1263) (2020) 12.
[33] J. Guo, I.R. Chen, J.J. Tsai, A survey of trust computation models for service management in internet of things systems, Comput. Commun. 97 (2017) 1–14.
[34] A. Sharma, E.S. Pilli, A.P. Mazumdar, P. Gera, Towards trustworthy Internet of Things: a survey on Trust Management applications and schemes, Comput. Commun. 160 (2020) 475–493.
[35] G. Lee, N. Truong, A reputation and knowledge based trust service platform for trustworthy social internet of things, In the proceedings of Innovations in Clouds, Internet and Networks (ICIN), Paris, France, 2016.
[36] U. Jayasinghe, G.M. Lee, T.W. Um, Q. Shi, Machine learning based trust computational model for IoT services, IEEE Trans. Sustainable Comput. 4 (1) (2018) 39–52.
[37] I.U. Din, A. Bano, K. A. Awan, A. Almogren, A. Altameem, M. Guizani, "LightTrust: lightweight trust management for edge devices in industrial Internet of things," *IEEE Internet Things J. (Early Access),* pp. 1-1, 2021.
[38] N. Narang, S. Kar, A hybrid trust management framework for a multi-service social IoT network, Comput. Commun. 171 (2021) 61–79.
[39] G.H.C. Oliveira, A.D.S. Batista, M. Nogueira, A. Santos, An access control for IoT based on network community perception and social trust against Sybil attacks, Int. J. Network Manage. (IJNM) 32 (1) (2022) e2181.
[40] I.R. Chen, F. Bao, J. Guo, Trust-based service management for social internet of things systems, IEEE Trans. Dependable Secure Comput. 16 (6) (2015) 684–696.
[41] A.A. Adewuyi, H. Cheng, Q. Shi, J. Cao, Á. MacDermott, X. Wang, CTRUST: A dynamic trust model for collaborative applications in the internet of things, IEEE Internet Things J. 6 (3) (2019) 5432–5445.
[42] A. Altaf, H. Abbas, F. Iqbal, M.M.Z.M. Khan, A. Rauf, T. Kanwal, Mitigating service-oriented attacks using context-based trust for smart cities in IoT networks, J. Syst. Archit. 115 (2021) 102028.

[43] A. Tissaoui, M. Saidi, Uncertainty in IoT for smart healthcare: challenges, and opportunities, International Conference on Smart Homes and Health Telematics, Cham, 2020.
[44] N.A. Nabeeh, M. Abdel-Basset, H.A. El-Ghareeb, A. Aboelfetouh, Neutrosophic multi-criteria decision making approach for iot-based enterprises, IEEE Access 7 (2019) 59559–59574.
[45] M. Grida, R. Mohamed, A.H. Zaid, A novel plithogenic MCDM framework for evaluating the performance of IoT based supply chain, in: Neutrosophic Sets and Systems, New Mexico, University of New Mexico, 2020, pp. 323–341.
[46] E. Eryarsoy, H.S. Kilic, S. Zaim, M. Doszhanova, Assessing IoT challenges in supply chain: A comparative study before and during- COVID-19 using interval valued neutrosophic analytical hierarchy process, J. Busi. Res. 147 (2022) 108–123.
[47] G.D. Abowd, E. D. Mynatt, Charting past, present, and future research in ubiquitous computing, *ACM Transactions on Computer-Human Interaction (TOCHI) - Special issue on human-computer interaction in the new millennium,* vol. 7, no. 1, pp. 29-58, 2000.
[48] M. Ashtiani, M. AbdollahiAzgomi, A hesitant fuzzy model of computational trust considering hesitancy, vagueness and uncertainty, Appl. Soft Comput. 42 (2016) 18–37.
[49] V.L.G. Nayagam, S. Muralikrishnan, G. Sivaraman, Multi-criteria decision-making method based on interval-valued intuitionistic fuzzy sets, Expert Syst. Appl. 38 (3) (2011) 1464–1467.
[50] J. Wu, F. Chiclana, A risk attitudinal ranking method for interval-valued intuitionistic fuzzy numbers based on novel attitudinal expected score and accuracy functions, Appl. Soft Comput. 22 (2014) 272–286.