electronics

MDPI

Article

Development of a Model for Trust Management in the Social Internet of Things

Mohammed Rizwanullah [1], Sunil Singh [2], Rajeev Kumar [3,*], Fatma S. Alrayes [4], Abdullah Alharbi [5], Mrim M. Alnfiai [6], Pawan Kumar Chaurasia [2] and Alka Agrawal [2]

[1] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam Bin Abdulaziz University, AlKharj 11942, Saudi Arabia
[2] Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, Uttar Pradesh, India
[3] Centre for Innovation and Technology, Administrative Staff College of India, Bella Vista, Raj Bhavan Road, Hyderabad 500082, Telangana, India
[4] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[5] Department of Computer Science, Community College, King Saud University, P.O. Box 28095, Riyadh 11437, Saudi Arabia
[6] Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
* Correspondence: rs0414@gmail.com

Abstract: The Internet of Things (IoT) has evolved at a revolutionary pace in the last two decades of computer science. It is becoming increasingly fashionable for the IoT to be rebranded as the "Social Internet of Things" (SIoT), and this is drawing the attention of the scientific community. Smart items in the Internet of Things (IoT) ecosystem can locate relevant services based on the social ties between neighbors. As a result, SIoT displays the interplay between various items as a problem in the context of the social IoT ecosystem. Navigating a network can be difficult because of the number of friends and the complexity of social ties. By identifying difficulties with standard SIoT devices' interaction with social objects, truthful friend computing (TFC) is a new paradigm for tracing such difficulties by utilising a relationship management component to improve network navigability. The concept of trust management can be useful as a strategy during collaborations among social IoT nodes. As a result, the trustor can use a variety of measures to evaluate a smart object's trustworthiness. Hence, this article demonstrates the need for the trustor to evaluate the extent to which a given metric has contributed to the overall trust score and illustrates profitability when engaging in a transaction with other nodes. With the help of the SIoT, this paper used a unified fuzzy-based computational technique and a multiple-criteria decision-making approach to evaluate the trust weights. The statistical findings show that the computing of "truthful friends" is the biggest challenge for successful SIoT implementation at the initial level.

Keywords: fuzzy; AHP; trust; Social Internet of Things; MCDM; truthful friend computing

check for updates

Citation: Rizwanullah, M.; Singh, S.; Kumar, R.; Alrayes, F.S.; Alharbi, A.; Alnfiai, M.M.; Chaurasia, P.K.; Agrawal, A. Development of a Model for Trust Management in the Social Internet of Things. *Electronics* **2023**, *12*, 41. https://doi.org/10.3390/electronics12010041

Academic Editors: Junaid Arshad, Jonathan Loo and Omair Shafiq

Received: 16 October 2022
Revised: 13 November 2022
Accepted: 15 November 2022
Published: 22 December 2022

1. Introduction

The Internet of Things (IoT) technology is the interconnection of numerous computing devices connected to the internet, distributed within the network environment in the form of homogeneous and heterogeneous nodes. Such devices tend to integrate environmental components and produce various services for the end user. These devices transform into smart devices because they generate a tremendous amount of data related to the physical world through sensors, actuators, and general-purpose multipurpose computers [1,2]. A recent survey found that the number of IoT devices connected to IoT networks would pass 30 million in 2020. So, it seems like it would be hard to get to a certain service in a busy IoT environment [3].

The IoT-based servers that are currently in use are swamped with a flood of requests that they are unable to handle and manage effectively. For solving real-world problems, this perspective introduces several algorithms. Algorithms with the same features are focused on centralised systems, which cannot handle large numbers of queries from multiple devices and cannot scale them appropriately by respective IoT servers. Hence, the term "Social Internet of Things" (SIoT) was coined to describe the scalability, mobility, heterogeneity, and truthful friend computing issues associated with such a centralised system. Social ties develop between social objects as a result of the adoption of the SIoT [4]. Consequently, social networking is a space where humans can communicate with smart things in the SIoT ecosystem, as well as between humans and other humans and between humans and other tangible items. Because of how these social institutions are built, the smart thing becomes socially important [5]. Due to the difference between the specific rules and regulations set by the owner of a device and the unknown and unfamiliar behaviour of such social objects, the SIoT environment may not provide the quality-based services and data format that were intended.

With the establishment of a social relationship bond, one friend (social object s1) can pose a query for another friend (social object s2) in a distributed SIoT environment. Such objects may act honestly or dishonestly because of their unpredictable behaviour while delivering services [6]. Therefore, determining the truthfulness of friends in the SIoT environment is quite a challenging task. By doing some tasks locally, true friend computing can help SIoT servers handle the large amount of work they have to perform. It provides positive exposure to the user experience through enhanced quality-based services and data, support for higher network navigation, mobility, and geographical distribution of SIoT nodes. However, the criteria of "truthful friend" computing make the problems of privacy and security more critical [7]. The conventional solutions in the SIoT are not appropriate for truthful friend computing because of their mobility, heterogeneity, and deceptive nature. Every node associated with SIoT networks communicates directly or indirectly with a stranger and shares sensitive information that must be received by the trusted ones. So, when the SIoT architecture is put into place, there needs to be a strong security-based solution.

Although there are various mechanisms to obtain better throughput for truthful friend computing like intrusion detection systems, encryption, decryption, access control, and authentication, these strategies are not appropriate for SIoT servers and the end users because they may be intruded upon by attackers or malfunction, resulting in misbehaviour and compromised data. Moreover, the available security-based solution cannot counter an attack within the SIoT network where a malevolent node has been previously an integral part of the system through an authentication process. SIoT networks consist of end devices, social objects, and services, followed by different social relationships, which may be obfuscated at the user's end [8]. Trust enables a client or end-user to judge the behaviour of social objects associated with SIoT networks and also helps in decision-making. Moreover, trust counts as an incumbent technique to obtain truthful friends, reliable interactions, and trustworthy nodes. It is essential to utilise trust in SIoT computing because a social object is the backbone of any SIoT-based application. A social network can be observed as a job pool where information related to nearby SIoT devices is processed, managed, and stored, such as healthcare and Facebook data.

The geographical distribution, mobility, different social relationships, and heterogeneity associated with SIoT networks further applaud the necessity of a trust management system in truthful friend computing. The social node or object called trustor depends upon the trust score to determine the trustworthiness of another social node called trustee and evaluate how beneficial the interaction and collaboration with concerned social objects have been. Truthful friend computing should be a two-way process within trust management. This signifies that truthful friends who can deliver services to the end social nodes (or devices) must be able to evaluate the veracity and honesty of the devices. In the end, the social nodes requesting services must be able to validate the level of trustworthiness and integrity. In a colluding SIoT network, trust management is very important because many different social nodes work together to provide services or resources to finish a specific task [9].

In a trust management system, the trustee's assessment by the trustor is performed through the critical information produced by the trust composition. The trustor analyses the trustworthiness of the trustee using subjective or objective-based metrics. Objective-based-trust metrics are those that are measurable and verifiable through quality-based services and quality-based data. On the other hand, subjective metrics are analysed on the basis of the decision of the trustor by exploring recommendations and honesty. Since no two trustors have the same social parameters, there is extensive variation in the subjective metric depending on the situation and network demand. In the SIoT environment, the two categories of interaction that exist are social object to social object collaboration and social object to thing collaboration [10]. To analyse the level of trustworthiness of social objects that have a calculable future and are capable of declining any uncertainty about the same, the trust management system uses effective metrics regarding the social object's present and past communication among its neighbours and receives recommendations. Hence, different trust metrics can be used in different situations to figure out how trustworthy a social object is.

These include QoS, QoD, recommendation, honesty, friendliness, cooperation, reputation, and community of interest. Based on trust metrics, the trustor computes the effective weight value of each metric. Therefore, associated weight evaluates the impactfulness of every metric that bears a resemblance to the trust scores. Trust metrics perform differently in different contexts when combined simultaneously. As a result, the trustee must adopt a metric to determine its relevance and range of levels, which metrics contribute to the trustee's collective trust [11]. At present, only a few studies demonstrate the trust management systems modelled for truthful friend computing. Some recommendation and reputation-based trust models have also been developed in dissimilar SIoT contexts for deployment, like mobile ad-hoc networks. However, the ranking of trust metrics could not be adopted as weights and was assigned randomly in the investigations undertaken in these studies. As a result, calculating trust and determining how much each metric and sub-metric matter as a weight is an important research endeavour. Multiple metrics are looked at at the same time during the multi-criteria decision-making (MCDM) process of figuring out weights for metrics.

A thorough analysis of the available literature in this context confirms that no positive action has been taken to propose a mechanism that performs a ranking of trust metrics related to truthful friend computing. Through this article, we aim to provide a hierarchy of trust metrics and help in developing an efficient trust management system (TMS) for truthful friend computing in a SIoT-based network. Additionally, the information regarding identified metrics and sub-metrics would also help in designing and developing an accurate and robust trust model that would be advantageous for both truthful friends and end-users. With this as a reason and the idea of building a trust model, our main goal is to look at a generalised and widely accepted framework for making decisions in truthful friend computing.

The present article intends three contributions that incorporate:

- Explaining the most important trust metric for a trustworthy, friendly computing environment.
- Performing further scaling by utilising the expert's opinion.
- Setting up the criteria for evaluating trust and how important it is to choose honest friends and the right nodes for communication in the SIoT environment.

According to the requirements, the authors have classified trust metrics for two application scenarios, namely client to social object and social object to social object. The investigated metric and associated sub-metric are graded by determining their weight values. Therefore, understanding the prioritisation and relevancy of different trust metrics and sub-metrics signifies an MCDM problem. Furthermore, the unified fuzzy Analytical

Hierarchy Process (fuzzy AHP) strategy has been employed to convert ambiguous human verdicts into more precise values. With this strategy, we rank the identified metrics and measure how much each metric and its sub-metrics contribute to the overall trust formation of the trustee.

The rest of the present article has been detailed as follows: Section 2 depicts a comprehensive revision of relevant articles, while Section 3 deals with the classification of identified trust metrics as the basis for research composition. The methodology and background knowledge of unified fuzzy AHP are discussed in Section 4. Furthermore, Section 5 shows the application of the fuzzy AHP mechanism in a SIoT-based environment for truthful friend computing. Section 6 elucidates the ranking of the trust metric and trust sub-metric using native and universal criteria. Section 6 tabulates our findings and shows the comparison of the trust metric and trust sub-metric through the ranking of trust scores. Section 7 concludes the study.

2. Related Work

The last decade saw the emergence of various wired and wireless communication technologies and protocols that are capable of performing global trust computation in the field of IoT. In this section, the development of the social aspect of the IoT takes place where smart devices create their social objects, which can establish social relationships with other social objects. To access the service through these social objects, trust among such nodes plays a vital role in a SIoT-based network. The subject of trust management in truthful-friend computing has only been the subject of a small amount of research. However, a mechanism, strategy, and solution for managing trust have started things off in a good way.

Kowshalaya et al. [12] suggested a trust management model for SIoT-based networks to judge the behaviour of social objects. They evaluated the trustworthiness of nodes by utilising trust metrics such as direct trust (first-hand information), indirect trust (second-hand recommendation), energy, centrality, a community of interest, and service score. The synchronisation of trust updates periodically makes the proposed scheme more effective and reliable. Further, they also analysed the performance of the SIoT network and established the reliability of the presented trust model under the presence of ON/OFF selective forwarding attacks. However, the low trust value needs more refinement to detect the patterns of an intruder. Xiao et al. [13] describe a trust management model based on reputation and guarantor that eventually computes trust by utilising the social behaviours of nodes to produce an instant response to a service request by the client object. They also assign a ranking to these social objects. Those that perform a good job are at the top, while those that do not are at the bottom, and are called *vindictive social objects*.

Awan et al. [14] visualised a model for a trust management system to manipulate trust, which deals with inter-domain communication while deploying services in IoT networks. The model presented concentrates on the centralised control of clients' service requests and performs storage for trust value and the generation of certificates that are not capable of ensuring the scalability of the system. However, the objects that have a lot of social connections and clients who are attacked in different ways are not considered to be part of the system. Alemneh et al. [15] wrote about a good way for smart nodes to figure out if they are telling the truth by using a trust management system as part of IoT-based fog computing services. This model lets service requesters check the reliability of service providers and helps service providers check how trustworthy service requesters are.

Ben Saied et al. [16] combine multiple functions to form new batches for all the previous interactions among social nodes according to a single criteria. After gathering the social nodes into a single format, the nodes may be unknown to each other. Talbi et al. [17] described an interest-based model for the formation of social relationships among social IoT nodes autonomously with regard to the virtual-based community. The presented model is sufficient for computing the trust of SIoT social nodes based on the preferences made by client users on an interest basis. Further, they have also depicted a new system based on recommendations indicating similarity between the service requester and the service provider to enhance the desired services. However, these studies have not focused on the classification and prioritisation of trust metrics or parameters in truthful friend computing in SIoT.

Several trust management techniques have been proposed in different applications of SIoT-based networks while considering the importance of social relationships. Chen et al. [18] proposed three types of relationships consisting of clients' communication through social friendship, social interrelation, and community of interest by utilising the social trust parameter. The problem with this work is that they have not considered various attack approaches on nodes. Nizamkari et al. [19] go along with a similar ideology as Chen; the clients utilise their prior communication and connected friend's exposure to calculate the trust data value of the service provider, i.e., the trustee. Therefore, if the client does not have sufficient exposure (trusted friends), then the recommendation of one's social object can be utilised to depict the same relationship.

Mendazoa et al. [20] changed the exposure of the client's nearby objects and QoS to evaluate the trust value between the trustor and the trustee. Each client can receive the information of each trustee and store all the details of the nodes and their experiences. The proposed model detects malicious nodes and stores the information in the form of a table for lightweight IoT devices. Chen et al. [21] describe a method for governing ATMP (adaptive trust management protocol) in SOA based on social IoT networks. This method is further divided into different parts based on user feedback, using similar friends and communities of interest. SIoT-based constraints have been associated with this protocol, like limited storage and behind-the-scenes update trust values. Troung et al. [22] proposed different scenarios for models that include the triad of reputation, experience, and knowledge-based for the application of mobile crowd sensing through a trust management system to compute trust for several parameters. Different criteria were used in these studies to focus on the social relationship part, but they were unable to figure out how it affected network navigation.

To address the weakness of the MCDM riddles-based analytical hierarchy process (AHP), the fuzzy AHP strategy has been integrated with fuzzy set theory to produce more effective and accurate results. Bharti et al. [23] utilised the technique of fuzzy AHP to optimise the process of friend selection within the SIoT environment through a novel framework called Optimal Resource Discovery and Selection (ORDS). To represent the knowledge parameter, the authors utilised the capability of ontology-based semantic description. Further, they used a fuzzy-based set of rules to decipher the results. This approach gave more accurate results than the outcomes obtained from the other algorithms. On the other hand, the study showed a poor aspect of scalability.

Cuka et al. [24] proposed a fuzzy-based mechanism for the smart selection of smart physical devices that are deployed in the SIoT environment by utilising a fuzzy logic model. They used device remaining energy, device interaction, contact time, device inter-distance, and device buffer occupancy as network parameters. Alshehri et al. [25] proposed a fuzzy logic-based protocol for detecting on-off attacks, contradicting behaviour attacks, and other malicious nodes. This protocol allowed nodes to transfer data securely from one cluster to another. Additionally, the protocol utilised fuzzy logic to identify bad nodes and limit their untrusted role in making erroneous recommendations regarding nodes in the network.

Baranwal et al. [26] proposed a framework that makes use of multi-criteria decision-making (MCDM) as a combination of known approaches under the names Analytic Hierarchy Process (AHP) and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) for conducting the selection process, where QoS parameters of various components of the IoT act as criteria. The effectiveness of the proposed approach is based on sensitivity analysis to compute the ratings of service providers. Because the parameter in the above framework is unique and has its own properties, it cannot be used for trust management in truthful friend computing. The summarization of different authors' work in the SIoT environment is depicted in Table 1.

Table 1. Summary of Related work.

Authors	Criteria for Trust Management	Methodology Adopted	Major Contribution
Kowshalaya et al.	Direct trust, Centrality, Cooperativeness, community of interest, Energy and Service score	Proposed dynamic trust management model based direct observation and indirect recommendation	Produce better results while comparing with three schemes namely, fuzzy trust, context-aware trust and SOA-based trust. The proposed model is also reliable against ONN/OFF selective forwarding attack
Xiao et al.	Direct trust, credit and reputation	Offered a novel trust evaluation model based on reputation guarantor. To test working of model an application was built on Microsoft visual studio	Presented model easily scalable to large networks. Credit and reputation are utilised for building trust and detecting malicious nodes depicts the reliability of model
Awan et al.	Direct and Indirect trust	Proposed Holistic Cross-domain (HCD) trust management model based on multilevel central authorities	HCD calculates the domain trust, manages the trust values, and distributes standard trust certificates to domains based on a degree of trust. Also compared the HoliTrust with the existing trust mechanisms
Alemneh et al.	Direct trust and Recommendation	Propose a two-way subjectivelogic-based trust management system that enables a service requester to verify whether a service provider can give reliable and secure services	Presented model based on subjective logic for trust management shows converges quickly and high accuracy as well as resilient to trust-related attacks
Ben Saied et al.	Context similarity in terms of type of sevice (x-axis) and node capabilities (y-axis)	Offered context-aware and multi-service trust management model for IoT-based system	Proposed model shows high accuracy to determine the class of common attacks designed for target trust management systems
Talbi et al.	Direct and Indirect trust	Proposed interest-based trust management scheme for SIoT systems to deal with u trustworthy nodes and enhance the cooperation between SIoT devices	Simulation results validate the convergence of the interest-based trust management scheme. High performance is observed while the trustee is assessed in subjective way according to the trustor's interest preferences when the two parties share a past
Chen et al.	Friendship, social contact, and community of interest	Proposed adaptive and scalable trust management (ASTM) model to support service composition applications and also develop novel adaptive filtering techniques to determine the best way to combine direct trust and indirect trust	The adaptive IoT trust protocol performs well in case of Eigen Trust and Peer Trust in trust convergence, accuracy and resiliency against malicious nodes. The proposed filtering technique is quite helpful in determining the combined value for direct and indirect trust
Nizamkari et al.	Centrality and trust level	Proposed scalable graph-based collaborative filtering recommendation algorithm, to solve service selection problem using trust score	The proposed method evaluates trust using scalable recommender and shows moderate performance by utilising RMSE and MAE and coverage as compared to traditional CF
Mendazoa et al.	Direct and Indirect Trust	Proposed a distributed trust management model for multi-service IoT using direct and indirect observations	The trust management scheme provided utilizes positive and negative scores for trust evaluation and also detects malicious behaviour in the network. Also shows positive response for ON/OFF and selective attacks
Chen et al.	Direct observations and indirect recommendations	Offered adaptive trust management for social IoT systems in which social relationships evolve dynamically	Convergence, accuracy, and resiliency are measured on proposed adaptive trust management model. Service composition scheme outperforms random service composition
Troung et al.	Direct and Indirect Observation	Propose a trust evaluation model based on triad trust indicators (TIs) Reputation, Experience and Knowledge considering muti-dimensional trust aspects in SIoT	Semantic-Web technologies are utilised to compute overall trust value received by different trust indicators. For effective ranking of Trust indicators Rep ranking produces more prominent result
Alshehri et al.	Trigger Outliers, Trigger Bad Mouths, Trigger Memory Thresholds, Trigger Balanced Node Distribution	Offered clustered-based trust management model for IoT-based network	The methodology addresses practical and pressing issues related to IoT trust management such as trust-based IoT clustering, intelligent methods for countering bad-mouthing attacks on trust systems
Baranwal et al.	QoS-Things, Communication and Computing	Propose a framework of multi-criteria decision making as a combination AHP and TOPSIS for conducting the selection process where QoS parameters of various components of IoT act as criteria	To measure the robustness of the method, IoT-based healthcare system is discussed followed by sensitivity Analysis. They also evaluated the performance and compared it with existing works

Evidently, very few studies have undertaken research on SIoT environments where MCDM techniques have been deployed in a different context. Moreover, no work has been carried out in the context of truthful friend computing. To address this research void, our study adopts the MCDM-based fuzzy AHP methodology to perform a rule-based ranking of the identified trust metrics. As discussed previously, truthful friend computing in SIoT networks is a two-way process, i.e., service requestor (SR) to service provider (SP); and service provider to service requestor. This shows that trust management must be bidirectional in truthful friendship computing. Hence, this article utilises two scenarios of trust management: *SR to SP* and *SP to SR*. This article also gives details about the trust metrics or criteria that have been found to be important for evaluating trust, as well as the relative importance of choosing honest friends and good nodes for communication on the SIoT network.

3. Research Composition

3.1. Trust Metrics

Trust metrics or parameters associated with SIoT networks are a knowledgeable criterion in the fuzzy expert system for locating the truthfulness of social objects. From the review of the literature cited above, we determined that trust can be evaluated on various metrics. In our article, we looked at the different trust metrics, such as quality of data (QoD), transaction time, latency, reliability, scalability, quality of service (QoS), intrinsics, accessibility, recommendation, contextual representational, and reputation.

- **Quality of Services**: The QoS metric is utilised to determine the performance of a social IoT node by successfully responding to an end-user request by following certain criteria of a service level agreement [26]. The QoS metrics include sub-metrics such as latency, transaction time scalability, and reliability. Transaction time is defined as the sum of request time and response-receiving time. Latency is the amount of time it takes the SIoT server to finish a client's request, which can be affected by different propagation delays. Scalability is responsible for a scalable system for reinforcement of QoS to produce maximum throughput under heavy workload in a SIoT-based environment. Reliability is the chance that an SP will give its client the services they want according to a set of rules for a certain amount of time without failing.
- **Quality of Data***:* It determines the level of accuracy and completeness offered by a smart social object while providing a service to a client or during collaboration with other nodes. It is the level of intrinsic, contextual, accessibility, and representational format of data provided by a smart social object. Intrinsic data is the functionality of data quality, which includes accuracy, objectivity, believability, and reputation dimensions while transmitting information among nodes. Accessibility depends on the extent of availability and obtainability of data by the client while accessing desired services from the SIoT server. Contextual data signifies the specific context of the task, considering timeliness and completeness, and to what extent it is applicable in delivering services. Representational is the format of the data that must be kept short and consistent so that it can be interpreted correctly and is easy to understand [27].
- **Social Relationship:** The social relationship responsible for social trust between owners and SIoT devices is measured by honesty, centrality, cooperativeness, community of interest, and connectivity. Social relationships like POR and CLOR represent the nature of bonding among social objects due to continuous interaction between the client (trustor) and SP (trustee). So, it lets the trustor keep an eye on the trustee's bad behaviour (dishonesty) for a certain amount of time when the SIoT network is working well [28]. Honesty signifies whether a particular social object is honest or not. In the SIoT, a malicious node can act dishonestly while providing services as well as recommendations. Cooperativeness is the characteristic that describes the extent of the social objects' socially interactive behaviour towards the trustor. Community of Interest (CoI) is the property of the SIoT network, whether the trusted social object belongs to a socially similar group or community (same community, co-location, and

co-work) or not. Centrality is how important a social object i is in relation to another social object j, but it decreases for other social nodes in the SIoT network.

- **Past Reputation**: The client's (trustor's) previous trust value signifies the trust of the SP (trustee) and depends on earlier communication for a specific time frame between the client and SP. There is a significant impact of past interactions between the trustee and the trustor on computing the trustee's trustworthiness [29]. If the trustor and the trustee had direct interactions in the past, it may have hurt the trust score now.
- **Recommendation:** The trust score of a social object can be used to compute the trust of the SP, specifically when the client does not have any past interaction with the trustee. When a specific trustor cannot locate a trust score through direct observation, recommendations from a nearby social object are used for evaluation. Further, the recommendation must be honest and strong enough to prevent trust-related attacks [30].

The summary of trust metrics in truthful friend computing is depicted in Table 2.

Table 2. List of Sub-trust metrics for Truthful friend computing.

Metrics	Sub-Metrics	Description
QoS (M1)	Transaction Time (SM1)	A service request is defined as the minimal period associated with the SIoT server completing a service request between the two SIoT nodes within a specified time frame. If a transaction is not finished in the time allotted, it has to be started over to make sure everything is in sync [31].
	Latency (SM2)	It is the time taken by the SIoT server to complete the client's request that experiences various propagation delays like transmission and processing while providing the desired service to end-users through the utilisation of social virtual objects [32].
	Scalability (SM3)	Scalability signifies the capability of handling workload (several service requests) within the SIoT system. According to our scenario's scalability in terms of trust metrics, network throughput will gradually exceed the number of clients as the number of clients grows. The bulkiness of the SIoT network is observed in terms of service requests received by the server and the number of data streams produced. As a result, scalability is responsible in a SIoT-based environment for a scalable system for QoS reinforcement to produce maximum throughput under heavy workload [33].
	Reliability (SM4)	It is responsible for measuring the manner in which services are completed successfully without failure within a particular timeframe and under certain conditions. It can be seen in IoT systems that the number of client requests declines by SP at peak times following certain conditions. So, reliability is the chance that an SP will give its client the services they want according to a set of rules without failing for a certain amount of time [34].
QoD (M2)	Intrinsic (SM5)	The intrinsic data deals with the functionality of data quality, which includes accuracy, objectivity, believability, and reputation dimensions while transmitting information among nodes (SP to SR and SR to SP) to perform an integral transaction in SIoT-based services. Data is only reliable if it is both accurate and objective, but it also needs to be believable and have an effective dimension, which is the source of the data.
	Accessibility (SM6)	Accessibility of good-quality data depends on the extent of availability and obtainability of data by the client while accessing desired services from the SIOT server. Hence, the role of the SIoT system is to make the platform secure and accessible.
	Contextual (SM7)	The contextual data indicates the specific context of the task, considering timeliness and completeness, and to what extent the data is applicable in delivering services in SIOT using different social relationships among different smart devices. The client who used the services was more interested in the quality of contextual data (value added, relevance, and amount of data) than in how it was represented.
	Representational (SM8)	When information is shared between a client and a service provider, the format of the data must be kept short and consistent so that it can be interpreted correctly and is easy to understand.

Table 2. *Cont.*

Metrics	Sub-Metrics	Description
Social Relationships (M3)	Honesty (SM9)	The social relationship property named honesty signifies whether a particular social object is honest or not. In the SIoT, a malicious node can act dishonestly while providing services as well as recommendations. The selection of honesty as a trust sub-metric because of the dishonest social object may interrupt trust management and the continuity of desired services in SIoT-based applications. In a SIoT-based application scenario, a social object uses direct interaction and indirect evidence (like a node's past reputation and recommendations) to figure out how honest the connected node is [35].
	Cooperativeness (SM10)	The cooperativeness trust metric property describes how much social objects interact with the trustor in a social way. The social object may follow a set of rules when interacting with a trusted social object or friends with whom it has a strong social tie, but become uncooperative when interacting with another social object. A social object in SIoT applications can compute the cooperativeness characteristics of different social nodes using social tie-up and perform a selection of the socially active cooperative social objects to achieve high application performance [12].
	Community of Interest (SM11)	The CoI trust metric signifies the property of the SIoT network: whether the trusted social object belongs to a socially similar group or community (same community, co-location, and co-work) or not. The two social objects having a greater level of trust-based CoI can produce various interactions and positive experiences among other nodes, which can result in better performance of the application [36].
	Centrality (SM12)	The centrality of a social object, the trust sub-metric of social relationships among other social objects, represents its geographical position in the SIoT network. It indicates the importance of a specific social object (i) in relation to a social object (j) while declining the importance of other social nodes in the SIoT network. As a result, the primary goal of centrality is to prevent mean social objects from making more connections [37].
Past Reputation (M4)	-	Past reputation is defined as having a big effect on how the trustee and the trustor have worked together in the past. This affects how trustworthy the trustee is.
Recommendations (M5)	-	A recommendation is the property of a social object utilised for the evaluation of trust value when a particular trustor is not able to locate a trust score through direct observation.

3.2. Trust Management in SIoT

Trusted interactions are dynamically managed among smart social nodes by utilising the capabilities of the TMS in the social IoT network. Evaluation of trust is computed through a social object's trust score by following the criteria of profitability to assign a task, interact with, and collaborate with other social objects. The trust in the trustee acts as a function of the interaction data values (present and past) obtained from the different social objects. The calculation of trust is based on trust metrics, which tell the trustor how much weight is to be given to each parameter [38]. The social object's truthfulness is based on the direct trust value received from the direct communication of a client and the previous reputation data value with the SP, along with suggestions obtained from the social object. Notably, in SIoT computing, TMS follows two-way communication from SR to SP and SP to SR. As a result, we considered the two scenarios of SR to SP and SP to SR, where SP provides services to the end-user and SR requests social object collaboration with others in the same community or group to perform TFS. So, the trust management system (TMS) is split into two parts: direct trust (DT) and indirect trust (IDT).

- Direct trust: The DT evaluation of social object node SONk by the end-user depends on QoD and QoS in terms of SR and SP. It also computes the DT value of j utilising social bonding (centrality, community of interest, and cooperativeness) among social objects in the SIoT network. The SIoT smart SONi asks for a collaborative service request with SONk to compute a direct trust score SONk by utilising trust metrics QoS and QoD, while trust evaluation SONi is computed by SONk depending on social bonding (centrality, community of interest, and cooperativeness).
- Indirect Trust: The IDT computes the subjective trust value of the SP on the basis of suggestions and prior knowledge received by the client. In other words, the IDT data

value is the integration of recommendations and earlier experience of social objects in SIoT networks.

4. Fuzzy Set Theory and Unified Fuzzy AHP

We start our discussion by focusing on the inceptional background information needed in the ranking procedure of trust metrics.

4.1. Fuzzy Set Theory

Several researchers have used different types of membership functions in their corresponding work, like trapezoidal fuzzy numbers, Gaussian numbers, triangular fuzzy numbers, etc. In this paper, the authors consider the TFN numbers that lie between 0 and 1 [39]. It is easy to adapt, and compute with the TFN functions and affords the straightforwardness associated with the fuzziness dataset [40]. Moreover, a fuzzy digit N on F is known as TFN; its general membership function is represented by Equation (1).

$$u_N(x) = F \rightarrow [0,\ 1] \tag{1}$$

The possible definition related to the fuzzy set theory that has been discussed in these articles is given below [10,41,42].

Statement 1. *In a fuzzy system, the triangular fuzzy number (TFN) is depicted by 3 keywords lower (l), middle (m), and upper (u) as signified in Figure 1. The membership function $\mu_N(x)$ is defined in Equation (2).*

$$\mu\ _N(x) = \begin{cases} \frac{x-l}{m-l} & l \le x \le m \\ \frac{u-x}{u-m} & m \le x \le u \\ 0 & otherwise \end{cases} \tag{2}$$

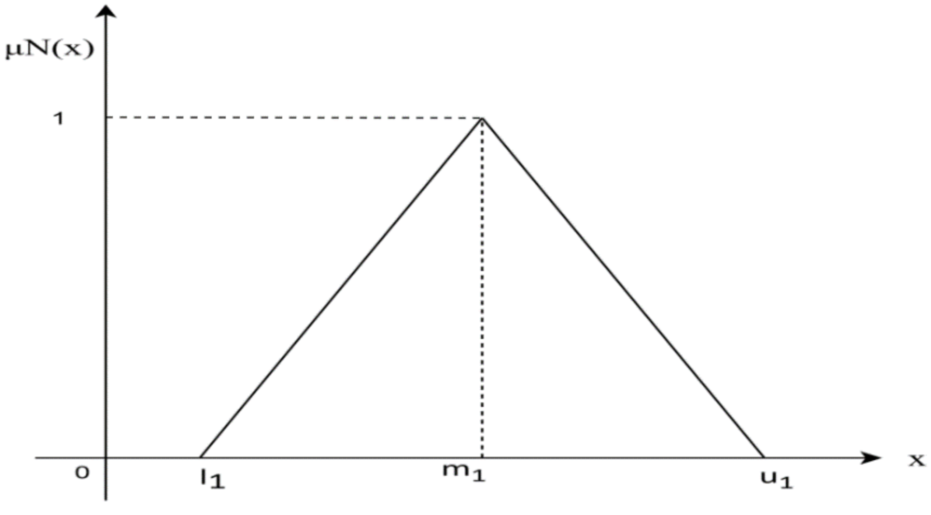

Figure 1. Triangular fuzzy numbers.

Statement 2. *Consider Ŷ and Ž are the two TFNs Ŷ = (Y^l, Y^m, Y^u) and Ž = (Z^l,Z^m,Z^u). The vertex approach is utilized to compute the distance between Ŷ and Ž as given by Equation (3).*

$$D(\hat{Y},\check{Z}) = \sqrt{\frac{1}{3}[(Y^l - Z^l)^2 + (Y^m - Z^m)^2 + (Y^u - Z^u)^2]} \tag{3}$$

Table 3 depicts the algebraic operation laws of two TFN.

Table 3. Fuzzy Operations.

Operation	Algebraic Expression
$Y \oplus Z$	$(Y^l + Z^l, Y^m + Z^m, Y^u + Z^u)$
$Y \ominus Z$	$(Y^l - Z^l, Y^m - Z^m, Y^u - Z^u)$
$\hat{Y} \otimes Z$	$(Y^l \times Z^l, Y^m \times Z^m, Y^u \times Z^u)$
$Y \oslash Z$	$(Y^l / Z^u, Y^m / Z^m, Y^u / Z^l)$
$\hat{Y}^{-1}$	$(1/Y^l, 1/Y^m, 1/Y^u)$
kY	(kY^l, kY^m, kY^u)

4.2. Unified Fuzzy Analytic Hierarchy Process Method

The fuzzy AHP proposed by Saaty is an effective approach that provides the solution to MCDM problems. This approach uses quantitative decision support to handle problems with multi-metrics by capturing expert opinion since it is unable to support uncertainty in human reasoning. Fuzzy AHP can compute more accurate results and appropriate judgments for real-time problems while uncertainty and imprecision are considered. Various researchers have proposed a number of fuzzy AHP techniques up to now. In this paper, the extent analysis mechanism is adapted to produce an accurate and consistent result and compared with traditional AHP [43]. The procedure followed regarding the fuzzy AHP strategy in eight phases is given below:

Phase 1. *The fuzzy scale of comparative significance between every element put together in the same pecking order defined in Table 4 signifies linguistic variables (Not Trusty, Very Less Trusty, Less Trusty, Strongly Trusty, Very Strongly Trusty, and Absolute Trusty) based on the comparative significance of a trust-based fuzzy scale.*

Table 4. Comparative significance of trust-based fuzzy scale.

Linguistic Value	TFN	TFN Reciprocal
Not Trusty	(1,1,1)	(1,1,1)
Very Less Trusty	(0.5,1,1.5)	(0.6,1,2)
Less Trusty	(1,1.5,2)	(0.5,0.6,1)
Strongly Trusty	(1.5,2,2.5)	(0.4,0.5,0.6)
Very Strongly Trusty	(2,2.5,3)	(0.3,0.4,0.5)
Absolute Trusty	(2.5,3,3.5)	(0.2,0.3,0.4)

Phase 2. *On the basis of expert opinion (see responses from an expert in Appendix A, Table A1), a fuzzy pair-wise comparison matrix is constructed by transforming linguistic variables into a fuzzy number using TFN. We used a trust-based fuzzy scale to convert lingual elements into a set depicting the fuzzy values, as shown in Table 4. An example of FPCM can be depicted as (Check sample responses from an expert in Appendix A, Table A1).*

$$T = \begin{bmatrix} t_{11} & \cdots & t_{1n} \\ \vdots & \ddots & \vdots \\ t_{n1} & \cdots & t_{nn} \end{bmatrix} \tag{4}$$

where $b_{ij} = 1$, for $i = j$ and $T_{ij} = (tij^l, tij^m, tij^u)$.

Phase 3. *In this phase, we constructed a single decision matrix (SDM) using a FPCM based on expert opinion about the trust metric for a social object in SIoT by utilising Equation (5).*

$$T_{ij} = (P_{ij}, Q_{ij}, R_{ij})$$

$$P_{ij} = min\ \{{P_{ij}}^k\} \tag{5}$$

$$Q_{ij} = \frac{1}{n} \sum\nolimits_{k=1}^{n} {Q_{ij}}^{k}$$

$$R_{ij} = max\{{R_{ij}}^{k}\}$$

where n represents the size of metrics and k signifies each member in SDM.

Phase 4. *The combined pair-wise matrix (CPM) acquired through Phase 3 is checked for consistency to gauge whether the expert's opinion regarding the trust metric of the SIoT system is consistent or not. First, the defuzzification of CPM is performed in crisp format [44,45]. For example, suppose V = (a, b, c) is a TFN. Its defuzzification into crisp format is depicted by the formula.*

$$T_{\text{crisp}} = \frac{l + 4m + u}{6} \tag{6}$$

After defuzzification, the pair-wise matrix is checked for consistency, and the matrix is normalised by dividing each element in a column by the sum of all its elements.

$$T_{ij} = \frac{t_{ij}}{\sum_{j=1}^{n} t_{ij}} \text{ for all } (i, j \in t) \tag{7}$$

where n represents the size of the metrics.

The eigen vector (EV) signifies the weight value of every trust metric depicted by

$$W_i = \frac{\sum_{j=1}^{n} t_{ij}}{n} \tag{8}$$

where W_i represents the EV in row i, and $\sum_{j=1}^{n} T_{ij}$ is the addition of every term in the row of the normalised pairwise matrix (NPM). The highest value of EV $\lambda_{\max}$ of the fuzzy crisp matrix is calculated by the multiplication of every term of the crisp matrix and EV. Therefore, $\lambda_{\max}$ is given by

$$\lambda_{\max} = \sum\nolimits_{i=1}^{n} \{ (\sum\nolimits_{j=1}^{n} T_{ij}) \times \ W_i \} \tag{9}$$

where $\sum_{j=1}^{n} T_{ij}$ represents the addition of all column terms of the crisp non-normalised values, W_i depicts the EV and n is the size of metrics.

The consistency ratio (CR) and consistency index are computed through Equations (10) and (11), respectively.

$$CI = \frac{\lambda_{\max}}{n - 1} \tag{10}$$

$$CR = \frac{CI}{RI} \tag{11}$$

In Table 5, RI depicts matrix sizes up to 10 metrics. In order to compute the consistency of the PCM, CR must be less than 0.10, otherwise, the procedure for the PCM has to be repeated. In other words, the expert's opinion about the identified trust metric for truthful friend computing is acceptable if CR < 0.10; otherwise, their judgment is incoherent.

Table 5. Random Index (RI).

Matrix Size	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Phase 5. *In this phase, we have to compute the fuzzy synthetic extent value (FSE) using a FPCM through Equation (12). The FSE for the ith value is expressed by*

$$S_i = \sum_{j=1}^{n} T_{ij} \ \otimes [\sum_{i=1}^{n} \sum_{j=1}^{n} T_{ij}]^{-1} \tag{12}$$

where S_i signifies FSE and $\sum_{j=1}^{n} T_{ij}$ is calculated by using fuzzy addition operational law, which is given by Equation (13)

$$\sum_{j=1}^{n} T_{ij}= (\sum_{j=1}^{n} T^{l}{}_{i}, \sum_{j=1}^{n} T^{m}{}_{i}, \sum_{j=1}^{n} T_{i}{}^{u}) \text{ for all } (I \ \epsilon \ [1,\ 2,\ 3 \ldots n]) \tag{13}$$

The expression is $\sum_{i=1}^{n} \times \sum_{j=1}^{n} T_{ij}$ evaluated by using fuzzy addition law on $\sum_{j=1}^{n} T_{ij}$. Further, each column element perform addition to compute $\sum_{i=1}^{n} \times \sum_{j=1}^{n} T_{ij}$ through Equation (14), that is,

$$\sum_{i=1}^{n} \times \sum_{j=1}^{n} T_{ij} = (\sum_{i=1}^{n} T_{j}{}^{l}, \sum_{i=1}^{n} T_{j}{}^{m}{}_{i}, \sum_{i=1}^{n} X_{j}{}^{u}) \text{ for all } (j \ \epsilon \ [1,\ 2,\ 3 \ldots n]) \tag{14}$$

The expression $[\sum_{i=1}^{n} \sum_{j=1}^{n} T_{ij}]^{-1}$ calculated by taking the transpose of the outcome (Equation (15)) which is given by

$$[\sum_{i=1}^{n} \sum_{j=1}^{n} T_{ij}]^{-1}= (\frac{1}{\sum_{i=1}^{n} t^{l}{}_{j}}, \frac{1}{\sum_{i=1}^{n} t^{m}{}_{j}}, \frac{1}{\sum_{i=1}^{n} t^{u}{}_{j}}) \tag{15}$$

Finally, the expression $\sum_{j=1}^{n} T_{ij} \otimes [\sum_{i=1}^{n} \sum_{j=1}^{n} T_{ij}]^{-1}$ is computed by applying fuzzy multiplication operation law using Equations (13) and (15) and is given by Equation (16)

$$S_i = (\sum_{j=1}^{n} T^{l}{}_{i} \times \frac{1}{\sum_{i=1}^{n} T^{l}{}_{j}}, \sum_{j=1}^{n} T^{m}{}_{i} \times \frac{1}{\sum_{i=1}^{n} T^{m}{}_{j}}, \sum_{i=1}^{n} T_{j}{}^{u} \times \frac{1}{\sum_{i=1}^{n} T^{u}{}_{j}}) \tag{16}$$

Phase 6. *The degree of possibility (DP) has to be calculated in this phase because there may be an existing TFN value between the two fuzzy numbers. Consider, there exist two triangular fuzzy numbers say H_1 = (l_1,m_1,u_1) and H_2 = (l_2,m_2, u_2), then their DP must be $H_1 \geq H_2$ is given by*

$$V\ (H_1 \geq H_2) = sup\ [min\ (\mu_{H1(y)}, \mu_{H2(z)})]. \tag{17}$$

The above expression can also be defined as given in Equation (17)

$$V\ (H_1 \geq H_2) = hgt\ (H_1 \cap H_2) = \mu_{H1}\ (d)$$

$$\mu_{\ N}(x) = \begin{cases} 1 & m_1 \ \geq m_2 \\ 0 & l_1 \geq u_1 \\ \frac{(l_2-u_2)}{(m_1-u_1)(m_2-l_2)} & otherwise \end{cases} \tag{18}$$

where, ordinate d is the highest point of intersection between μ_{H1}, μ_{H2}, and DP as depicted in Figure 2.

Phase 7. *Further, evaluate the degree of possibility (DP) using Equations (19) and (20) for convex fuzzy number i.e., greater than r CFNs.*

$$V\ (H \geq H_1, H_2.\ H_r) = minV(H \geq H_k)\ \forall k \in [1, 2, \ldots\ r] \tag{19}$$

$$d'(Gk) = minV(H_k \geq H_j)\ \forall j, k \in [1, 2, \ldots\ n], j \neq k \tag{20}$$

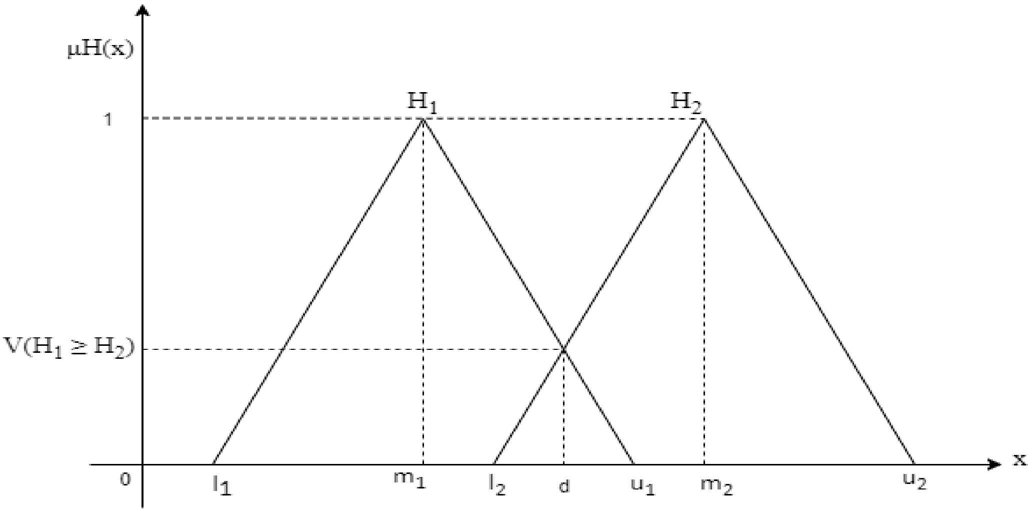

Figure 2. Degree of the possibility of two TFN.

Phase 8. *Compute the weight value and normalise it to again evaluate the non-fuzzy weight vector using Equations (19) and (20)*

$$\acute{W} = (d'\ (G_1), d'\ (G_2), \ldots, d'\ (G_n))^T \tag{21}$$

Finally, we obtain the weight computed through Equation (21) and further normalised to evaluate the non-fuzzy weight vector depicted by

$$W = (d(G_1), d(G_2), \ldots, d(G_n))^T \tag{22}$$

where $d\ (G_k)$, $\forall\ k \in [1, 2, 3, \ldots, n]$ represent the weight of metric k.

5. Ranking of Metrics and Sub-Metrics Based on Fuzzy AHP Application

The analytical hierarchy process has been utilised to perform a ranking of metrics in different environments [45,46]. We used a new fuzzy-AHP ranking method to do truthful friend (social IoT node) computing in the SIoT network (Appendices A and B), as described below:

5.1. Identification Metrics and Sub-Metrics for Determination of Trust in Truthful Friend Computing

To obtain the trust value of a social object for truthful friend computing, first, we have to perform a selection of trust-based metrics and sub-metrics. For the same reason, various metrics were identified from the literature in the SIoT environment. Further, the opinions of 15 experts belonging to academia and industry were used to collect data based on the discovered metrics. Hence, five metrics and twelve sub-metrics were selected as depicted in Table 1. Afterward, the hierarchy-based framework was constructed to compute the trust of a social object, which includes our goal, metrics, and sub-metrics, as shown in Figures 3 and 4. There are three levels in the proposed framework. The first level signifies our main goal, while the metric and sub-metric are ranked in levels 2 and 3, respectively. The ultimate aim of the present study is to perform a ranking of metrics and sub-metrics to evaluate the trust score of trustees through DT and IDT in SIoT. The use of fuzzy-AHP has been carried out to compute the weight value of every metric and sub-metric in this model.

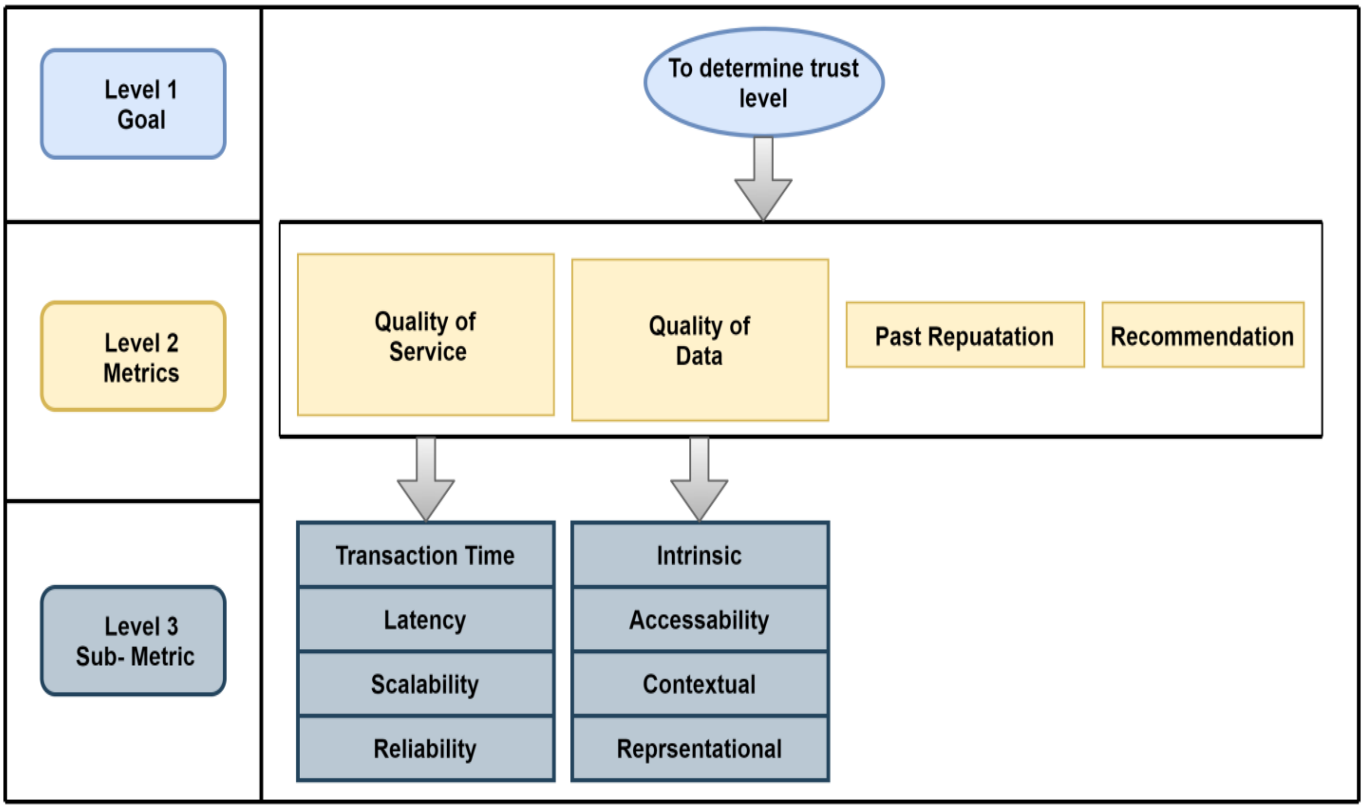

Figure 3. Trust-based computation hierarchy model (SR to SP) using fuzzy-AHP.

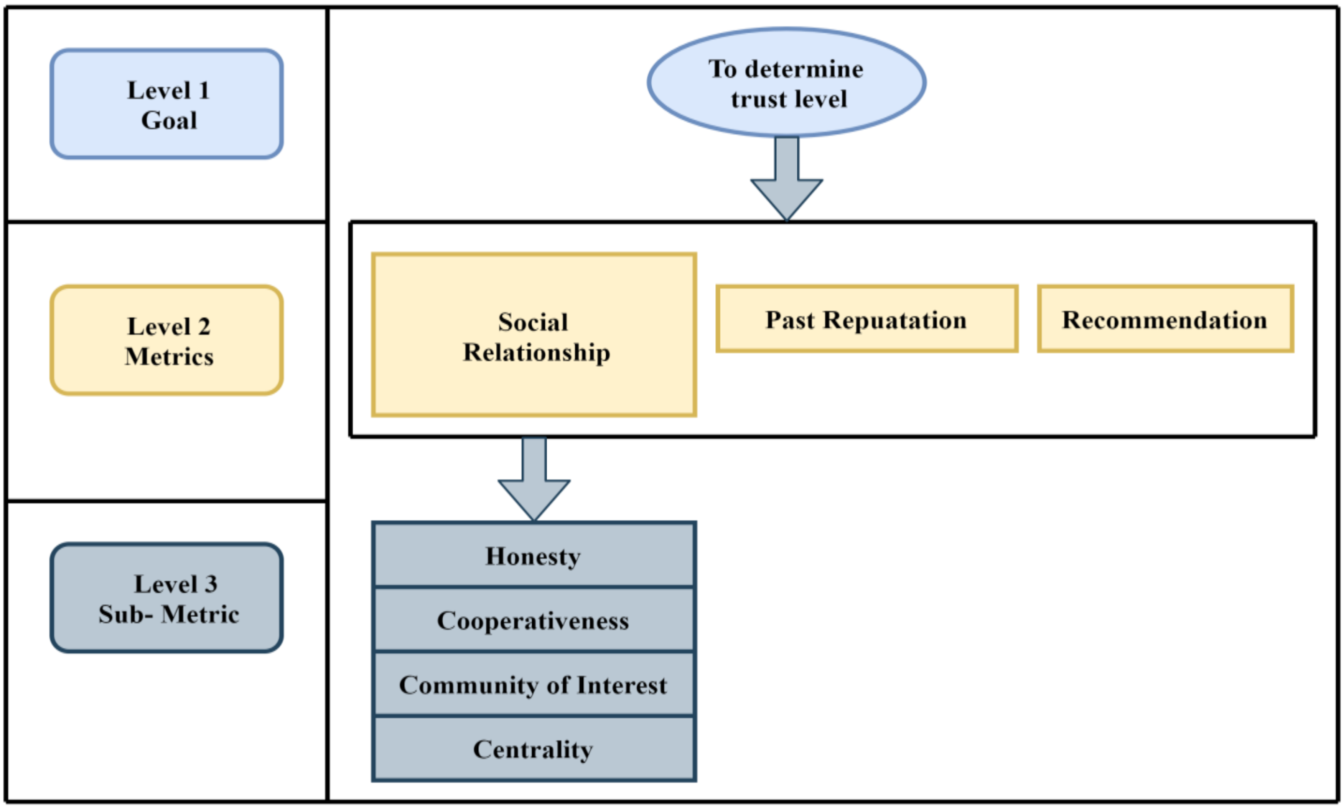

Figure 4. Trust-based Computation Hierarchy Model (SP to SR) using fuzzy-AHP.

5.2. Formation of Pair-Wise Comparison Matrix

The fuzzy AHP has been used to collate the opinions of fifteen experts and design trust metrics based on pair-wise comparisons. The sample size obtained from survey experts is quite small, and the fuzzy AHP is very subjective [47,48]. Various other researchers have also taken such a small dataset to produce effective results [49,50]. Therefore, utilising fifteen experts' suggestions to collect a dataset for fuzzy-AHP in our work is quite justifiable. Thereafter, a pair-wise comparison matrix is formed. The linguistic variables signify their corresponding triangular fuzzy number (TFN), as depicted in Table 4. After that, we obtained an aggregate FCM by combining fifteen matrixes through Equation (5). Finally, the obtained FPCM for scenario 1 and scenario 2 is depicted in Tables 6–10. For example, how the value of T_{ij} = (P_{ij}, Q_{ij}, R_{ij}) is calculated and sample data collected from the experts for the trust metric and sub-metric for levels 2 and 3 is given below:

Table 6. FPCM for Scenario 1.

	QoS	QoD	Reputation	Recommendation
QoS	1,1,1	0.4,1.45,2.5	1,1.89,2.5	1.5,2.16,3.5
QoD	0.4,0.97,2.5	1,1,1	1.5,2.29,3.5	1.5,2.42,3.5
Reputation	0.4,0.59,1.5	0.3,0.42,0.6	1,1,1	0.4,1.54,2.5
Recommendation	0.3,0.59,1.5	0.3,0.49,0.6	0.4,0.88,2.5	1,1,1

Table 7. Fuzzified Crisp Matrix for Scenario 1.

	QoS	QoD	Reputation	Recommendation
QoS	1	1.45	1.85	2.27
QoD	1.13	1	2.36	2.44
Reputation	0.71	0.43	1	1.51
Recommendation	0.68	0.47	1.07	1

Table 8. Normalised FCM for Scenario 1.

	QoS	QoD	Reputation	Recommendation
QoS	0.284	0.432	0.295	0.375
QoD	0.321	0.296	0.376	0.377
Reputation	0.201	0.128	0.159	0.209
Recommendation	0.193	0.14	0.171	0.138

$\lambda_{\max}$ = 4.165, CI = 0.06, CR = 0.06.

Table 9. EV on trust metrics for Scenario 1.

Trust Metrics	Eigenvector
QoS	0.345
QoD	0.343
Reputation	0.174
Recommendation	0.161

(1,1.5,2), (0.4,0.6,0.5), (1.5,2,2.5), (1,1.5,2), (1,1.5,2), (0.4,0.6,0.5), (1,1.5,2), (1,1.5,2), (0.4,0.6,0.5), (1,1.5,2), (1.5,2,2.5), (1,1.5,2), (1.5,2,2.5), (1,1.5,2), (1.5,2,2.5)

$$P_{ij} = min\ \{P_{ij}{}^{k}\}$$

$$= min\{1,\ 0.4,\ 1.5,\ 1,\ 1,\ 0.4,\ 1,\ 1,\ 0.4,\ 1,\ 1.5,\ 1{,}1,\ 1,\ 1.5\} = 0.4$$

$$\mathrm{Q_{ij}} = \frac{1}{n}\sum_{k=1}^{n} Q_{ij}{}^{k}$$

$$= \frac{1}{15}(1.5 + 0.6 + 2 + 1.5 + 1.5 + 0.6 + 1.5 + 1.5 + 0.6 + 1.5 + 2 + 1.5 + 2 + 1.5 + 2) = 1.45$$

$$R_{ij} = max\{R_{ij}{}^{k}\}$$

$$= max\{2, 0.5, 2.5, 2, 2, 0.5, 2, 2, 0.5, 2, 2.5, 2, 2.5, 2, 2.5\} = 2$$

Hence, T_{ij} = (0.4, 1.45, 2)

5.3. Validating the Consistency of the Pair-Wise Comparison Matrix

After the formation of PCM, the consistency ratio is computed. For example, we have evaluated the greatest EV for scenarios 1 and 2 of PCM. For the same, the TFN of a PCM is defuzzified, corresponding to crisp format, through Equation (6), and the obtained FCM is depicted in Tables 6–10. The fuzzified crisp matrix is further normalised through Equation (7), and the outcomes obtained are shown in Tables 8–12. Equation (8) is used to calculate the EV of the fuzzified crisp matrix. The outcomes of the EVs for two scenarios are depicted in Table 13.

Table 10. FPCM for scenario 2.

	Social Relationship	Reputation	Recommendation
Social relationship	1,1,1	1.5,2.234,3	1,2.26,3
Reputation	0.3,0.42,0.6	1,1,1	0.5,1.2,2
Recommendation	0.3,0.44,1	0.5,0.94,1	1,1,1

Table 11. Fuzzified crisp matrix for scenario 2.

	Social Relationship	Reputation	Recommendation
Social relationship	1	2.31	2.17
Reputation	0.444	1	1.21
Recommendation	0.514	0.89	1

Table 12. Normalised FCM for scenario 2.

	Social Relationship	Reputation	Recommendation
Social Relationship	0.511	0.549	0.499
Reputation	0.226	0.228	0.264
Recommendation	0.263	0.235	0.232

λ_{max} = 3.104, CI = 0.05, CR = 0.086.

Table 13. Eigenvector on trust metrics for scenario 2.

Trust Metrics	Eigen Vector
Social relationship	0.522
Reputation	0.239
Recommendation	0.234

We have computed the highest EV (max) of the fuzzified crisp matrix through Equation (9).

$$\Lambda\text{max} = (1 + 1.13 + 0.171 + 0.68) \times 0.345 + (1.45 + 1 + 0.43 + 0.47) \times 0.343 + (1.85 + 2.36 + 1 + 1.07) \times 0.174 + (2.27 + 2.44 + 1.51 + 1) \times 0.161 = 4.165$$

Since we have considered four metrics so the corresponding value of the RI is 0.90 using Table 5, hence CI is calculated using Equation (10).

$$\text{CI} = \frac{4.165 - 4}{4 - 1} = 0.06$$

Therefore, the consistency ratio (CR) is computed using Equation (11).

$$\mathrm{CR} = \frac{0.06}{0.90} = 0.05$$

Now, the CR value is 0.05 which is less than 0.10 so Table 5 representing PCM is acceptable and consistent.

For scenario 2,

$$\lambda_{\max} = (1 + 0.444 + 0.514) \times 0.522 + (2.31 + 1 + 0.89) \times 0.239 + (2.17 + 1.21 + 1) \times 0.234 = 3.104$$

Since we have considered three metrics so the corresponding value of RI is 0.058 using Table 5, hence the CI is calculated using Equation (10).

$$\mathrm{CI} = \frac{3.104 - 3}{3 - 1} = 0.05$$

Therefore, the consistency ratio (CR) is computed using Equation (11).

$$\mathrm{CR} = \frac{0.05}{0.58} = 0.086$$

Now, the CR value is 0.05, which is less than 0.10, so Table 10 representing PCM is acceptable and consistent. Using the same procedure, we have validated the CR for every metric and sub-metric, and the outcomes are depicted in Tables 14–16.

Table 14. FPCM for Quality of Service.

	SM1	**SM2**	**SM3**	**SM4**
SM1	1,1,1	1,1.64,2.5	0.5,1.42,2.5	0.5,1.4,2
SM2	0.4,0.55,1	1,1,1	0.5,1.07,2	0.4,0.7,2
SM3	0.4,0.73,2	0.5,0.95,2	1,1,1	0.4,0.9,2
SM4	0.5,0.71,2	0.5,1.17,2.5	0.1,1.17,2.5	1,1,1

$\lambda_{\max}$ = 4.109, CI = 0.03, CR = 0.04.

Table 15. FPCM for Quality of Data.

	SM5	**SM6**	**SM7**	**SM8**
SM5	1,1,1	0.5,1.39,2	0.5,1.19,2	1,1.69,2.5
SM6	0.5,0.67,2	1,1,1	0.5,1.04,2	0.5,1.39,2.5
SM7	0.5,0.85,2	0.5,1.03,2	1,1,1	0.5,1.3,2
SM8	0.4,0.55,1	0.4,0.73,2	0.5,0.77,2	1,1,1

$\lambda_{\max}$ = 4.106, CI = 0.035, CR = 0.038.

Table 16. FPCM for Social Relationships.

	SM9	**SM10**	**SM11**	**SM12**
SM9	1,1,1	0.5,1.32,2	1,1.44,2	0.5,1.34,2.5
SM10	0.5,0.72,2	1,1,1	0.5,1.09,2	1,1.05,2
SM11	0.50.84,2	0.4,0.56,0.6	1,1,1	0.5,1.3,2
SM12	0.4,0.58,1	0.4,0.72,2	0.4,0.47,2	1,1,1

$\lambda_{\max}$ = 4.175, CI = 0.058, CR = 0.064.

5.4. Evaluating the Priorities of Native Weights of Trust Metrics

We have computed the native weight (NW) of the trust metric and sub-metric and shown the description of our evaluation based on PCM in Table 6 for Scenario 1 of the main category. In this paper, we have utilised the extent analysis strategy [46], and the procedure for the same is given below:

The S_i of the PCM in Table 6 was calculated using Equation (12)

$$S_i = \sum_{j=1}^{n} T_{ij} \otimes \left[\sum_{i=1}^{n}\sum_{j=1}^{n} T_{ij}\right]^{-1}$$

$\sum_{j=1}^{n} T_{ij}$ is computed using Equation (13) and results are depicted in Table 17, and the value of $\sum_{i=1}^{n}\sum_{j=1}^{n} T_{ij}$ calculated by Equation (14) is given by

$$\sum_{i=1}^{n}\sum_{j=1}^{n} T_{ij} = (12.4,\ 19.67,\ 31.21)$$

Table 17. $\sum_{j=1}^{n} T_{ij}$ value for each metric.

Trust Metrics	$\sum\limits_{j=1}^{n} T_{ij}$
QoS	3.9,6.5,9.5
QoD	4.4,6.68,10.5
Reputation	2.1,3.55,5.6
Recommendation	2,2.94,5.6

Further, the inverse value of $\sum_{i=1}^{n}\sum_{j=1}^{n} T_{ij}$ computed using Equation (15) is given below:

$$[\sum_{i=1}^{n}\sum_{j=1}^{n} T_{ij}]^{-1} = [(\frac{1}{31.21}, \frac{1}{19.67}, \frac{1}{12.4})]$$

Therefore, the FSE value (S_i) is computed as

$$[S_i] = \begin{bmatrix} 3.9 & 6.5 & 9.5 \\ 4.4 & 6.68 & 10.5 \\ 2.1 & 3.55 & 3.52 \\ 1.7 & 2.94 & 5.6 \end{bmatrix} \otimes [0.032,\ 0.051,\ 0.082]$$

The result obtained for each value of S_i is depicted in Table 17. The degree of possibility (DP) for one TFN is higher than the other value computed by using Equations (17) and (18). The DP associated with convex fuzzy values (CFV) is also the highest compared to the other three, as shown in the following equations:

$$d'(S_1) = least\{WV(S_1 \geq S_2, S_3, S_4)\}$$

$$= least\ \{WV(1, 1, 1)\} = 1$$

$$d'(S_2) = least\{WV(S_2 \geq S_1, S_3, S_4)\}$$

$$= least\{WV(0.937, 1, 1)\} = 0.947$$

$$d'(S_3) = least\ \{W\ V(S_3 \geq S_1, S_2, S_4)\}$$

$$= least\{WV(0.529, 0.537, 1)\} = 0.585$$

$$d'(S_4) = least\{WV(S_4 \geq S_1, S_1, S_3)\}$$

$$= least\{WV(0.358, 0.322, 0.853)\} = 0.416$$

The WV is computed by utilising Equation (21)

$$W' = (1, 0.947, 0.585, 0.416)^T$$

Now, we can compute the normalised weight vector W by taking the transpose of W' utilising Equation (21)

$$W = (\frac{1}{2.948}, \frac{0.947}{2.948}, \frac{0.585}{2.948}, \frac{0.416}{2.948})^T$$

Therefore, as depicted in Table 18, the metric weights are computed. The outcomes show that the QoS metric has gained the highest weight value for trust evaluation in Scenario 1. In the same manner, the other metric and sub-metric can be prioritised for Scenario 2. Tables 17 and 18 show the results for metric and sub-metric measurements.

Table 18. FSE (S_i) value for trust metrics.

Trust Metrics	S_i
QoS	0.125,0.382,0.779
QoD	0.141,0.341,0.861
Past reputation	0.064,0.181,0.459
Recommendation	0.054,0.152,0,289

5.5. Evaluating the Priorities of Universal Weights of Trust Metrics

The trust metric for Scenario 1 and Scenario 2 are shown in Tables 19 and 20, which depict native and universal weights, respectively. The computed universal weight (UW) using fuzzy AHP of each trust metric reflects its priority over other metrics. The UW of every metric is the product of its native weight (NW) and level 1 metric weightage. The NW depicts each metric's impact on another metric in the same category. For instance, the LW of SM2 is 0.287, and it is the top graded metric in the class of QoS because of its weight vis-à-vis the others at the same level.

Table 19. Summary for the evaluation of trust metric for case 1.

Metric	Weight	Sub-Metric	Native Weight	Native Ranking	Universal Weight	Universal Ranking
QoS(M1)	0.342	SM1	0.280	2	0.0957	4
		SM2	0.287	1	0.0981	3
		SM3	0.183	4	0.0625	10
		SM4	0.251	3	0.0878	6
QoD(M2)	0.321	SM5	0.284	1	0.0911	5
		SM6	0.259	2	0.0831	7
		SM7	0.231	3	0.0741	8
		SM8	0.223	4	0.0715	9
Reputation(M4)	0.198	-	-	-	0.198	1
Recommendation(M5)	0.141	-	-	-	0.141	2

Table 20. Summarization for the evaluation of trust metric for case2.

Metric	Weight	Sub-Metric	Local Weight	Local Ranking	Global Weight	Global Ranking
Social Relationship(M3)	0.540	SM9	0.290	1	0.1566	3
		SM10	0.253	2	0.1366	4
		SM11	0.238	3	0.1285	5
		SM12	0.218	4	0.1177	6
Reputation(M4)	0.204	-	-	-	0.204	1
Recommendation(M5)	0.256	-	-	-	0.256	2

From the previous discussion, it is clear that recommendation and past reputation indicate IDT value, whereas QoD and QoS signify DT for scenario 1 and social relationship for scenario 2. Therefore, it can be observed that SM2 is the high-rank global metric for scenario 1, while past reputation gains the highest rank among all. In scenario 2, honesty (SM9) achieved the highest rank globally for the DT metric, while recommendation overall ranked high. Within level 1 for scenario 1, QoS is the top-rated metric whereas recommendation achieves the lowest rank (Table 19). In level 1 of the scenario, social relationships emerged as the highest prioritised metric because of their maximum weight from examining other metrics, whereas reputation seems to be the lowest one (Table 19).

6. Overall Impacts Assessment

The present research article ensures the identification, categorisation, and performance ranking of essential metrics for trust evaluation for truthful friend computing in SIoT. This social object can collaborate with other social objects to select a trustworthy and reliable social IoT object for delivering secure services. By investigating the literature, we have identified five metrics and twelve sub-metrics, and we then prioritise the metric and sub-metric by utilising the fuzzy AHP method. The application of a pair-wise comparison matrix depicts the importance of metrics and sub-metrics. The fuzzy AHP approach also determines the order in which each metric and sub-metric should be used.

6.1. Results

On the basis of the result depicted in Figure 5, latency is the top-graded metric locally, and it is rated as the higher metric globally for performing DT computation and achieves the third rank overall. This signifies that experts have taken latency as an important metric while computing direct trust for secure offloading and achieving TFS in the SIoT environment. The other most important metrics are transaction time, intrinsic data, accessibility, and reliability. Each of these has a natural weight of 0.280, 0.284, 0.259, and 0.251.

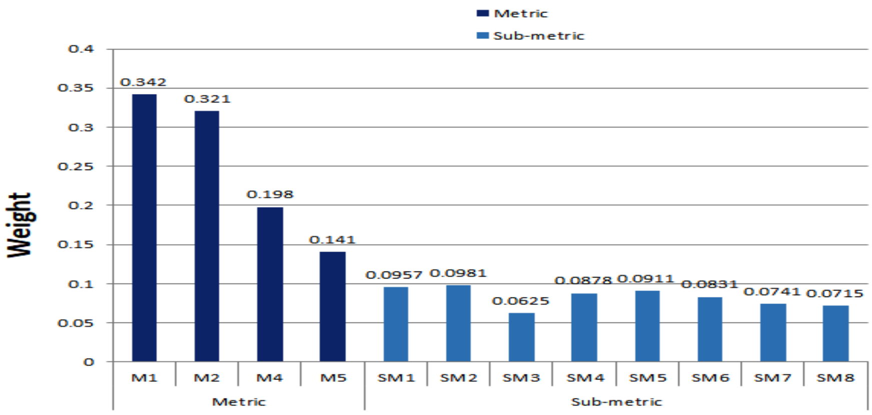

Figure 5. Ranking of Metric for scenario 1.

Moreover, in the case of indirect trust evaluation, past reputation performs better than the recommendation. This scenario points out that the experts considered the significance of past reputation over recommendation while receiving inputs from nearby nodes. In addition, recommendation and past reputation have no further sub-metric, so they obtained a higher rank among sub-metrics. So, reputation based on past communication obtained the top overall rank.

As depicted in Figure 6, locally honest has gained the highest rank and highest top-rated sub-metric for DT evaluation. This implies that experts recognise the importance of honesty in determining the trustee's trust in social objecttosocial object collaboration in TFS. Again, honesty is the highest-ranked sub-metric as compared to all others, with a UW of 0.1666. In the case of an IDT, the recommendation obtained a higher rank than the past reputation. This means that respondents agree that recommendations are more effective than reputation gained through past communication between social objects. Since there are no other factors for recommendation and reputation, they both have the highest values in the UW evaluation. Overall, recommendation received the highest rank.

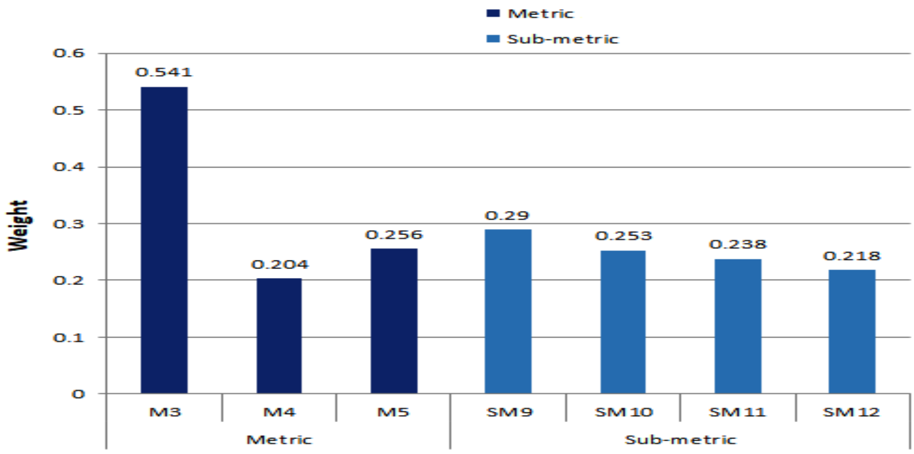

Figure 6. Ranking of Trust Metric for scenario 2.

6.2. Computation and Comparison

In order to compute the effectiveness of truth-friend computing in social IoT networks utilising TMS, five metrics and twelve sub-metrics were scrutinised for scenarios 1 and 2. To encapsulate the ambiguity and uncertainty involved in the human verdict, the fuzzy-AHP technique was used. To identify trusty nodes in a SIoT environment where the social IoT node is highly mobile and dynamic with a high degree of uncertainty, inaccuracy, and equivocation, fuzzy-AHP is most effective for imitation of numerous metrics for TMS since its throughput is quite impactful at reasonable MCDM. QoS and QoD are the most effective trust metrics in scenario 1. This signifies that the respondents have considered QoS and QoD to be protective metrics while performing friend computing among social objects by granting end-user access to desired services deployed in the SIoT network. In the category of QoS metrics, latency is the most desired parameter to obtain reliable services from a SIoT server.

For the SIoT server to compute the trustworthiness of a social object, social relationships appear to be the most significant parameter. The expert opinion relied on by the SIoT server must be focused on interaction and experiences related to the end-user rather than recommendations received from neighbouring SIoT objects. The social-object relationship between sub-metrically rated high honesty and then cooperativeness. To build a strong social relationship between two social objects, the degree to which they depend on each other is one of the most important factors. This is the highest weight factor.

In ref. [15], Alemneh et al. state that the contribution of an IDT score cannot exceed fifty percent as compared to the inclusive trust of the SP. According to the outcomes of our investigation, indirect trust contributes 31.5 percent for scenario 1 and 49.5 percent for scenario 2, respectively. The result says that the DT calculation of trust is more prominent than the IDT computation using past reputation and recommendation. The author in [47] considered that the weights of past reputation and recommendation are 0.3 and 0.4, respectively. In the same way, our results show that in Scenario 2, the IDT metric for past reputation is 0.204, which is exactly the same as what was seen for recommendation (0.256).

The maximum trust value escalates the speed of convergence by utilising recommendations through nearby social objects [48]. However, the weightage of the reputation based on prior interaction is 0.198, which is greater than the value observed for recommendation (0.141) in the case of service providers. The answer is that SR is more confined to SIoT servers to provide secure and efficient services, while SP is mostly associated with relationships among social objects. For instance, in [49], the weightage of 0.8 is given as a past trust value to an end-user, while 0.5 is associated with recommendations received from neighbour social objects and SIoT servers.

The computation of truthful friend computing in SIoT needs maximum data quality (QoD) as compared to QoS. The truthfulness of social objects emulates the criteria of QoS requirements despite affecting QoD protocols and service level agreements. Based on the result obtained in Table 18, the weight of QoD is 0.321, which is nearest to the value observed for QoS (0.342). When more weight is used in DT, the integrity and convergence of the trust value get better. It is clear from Tables 19 and 20 that the weight given to DT is greater as compared to IDT. The weight of the DT value for scenario 1 is 0.663, while scenario 2 has a weight of.540.

Since DT introspection and reputation based on prior communication using trust gradually influenced the presence of untrustworthy social objects in SIoT networks [46,49], a score represents a proper explanation of SP's (overall trust). As shown in Tables 18 and 19 and Figures 5 and 6, the results show that the self-observation trust scores for scenarios 1 and 2 are 0.861 and 0.744, respectively.

The QoD metric is responsible for delivering data quality services consisting of intrinsic, accessibility, contextual, and representational as the most important sub-metrics of a SIoT server, which must have the level of data quality to be transmitted since QoD revolves around these four criteria [50]. Based on what we found, the weights for intrinsic, accessibility, context, and representational are 0.284, 0.259, 0.231, and 0.223, respectively.

Furthermore, appropriate access control policies for SIoT servers should be enforced in order to detect anomalous social object behaviour and prevent unauthorised access. For the same reason, honesty is the highest-ranked sub-metric in the category of social relationship, which determines the QoS delivered by service providers, since it has merits like wrong recommendation detection and prevention, detection of a malicious social object, and prevention against trust attacks [35]. Table 19 shows that the weights of honesty (SM9) are higher than cooperativeness, the CoI, and centrality, which are 0.253, 238, and 0.218, respectively.

7. Conclusions

The authors used the fuzzy AHP technique to find and rank trust formation metrics in SIoT. This helped them perform "truthful friend" computing. The result shows that in the consideration of trust formation for scenario 1, QoS is the highly prioritised metric, having a weight value of 0.342, followed by QoD with a weight of 0.321, while recommendation gains the least weight. On the other hand, for scenario 2 regarding trust formations, social relationships are the top-ranked metric with a weight value of 0.540 while reputation is the least significant metric. In the QoS category, the sub-metrics make sure that latency has the highest rank with a weight of 0.287, followed by transaction time, and that scalability has the lowest rank. In the category of QoD, intrinsic has the highest-rated parameter weighting (0.284) by accessibility, while representational achieves the lowest rank in the same category. The outcomes of the findings of our work show that latency is the best metric for direct trust formation, with a UW of 0.0981 in scenario 1, while scalability is the lowest-ranked factor. In scenario 2, with a UW value of 0.1566 for DT formation, honesty is the best sub-metric for everyone, while centrality gets the least preference overall. In scenario 1 (SR to SP), the indirect trust score shows that reputation is more important than the recommendation from the nearby social object. In scenario 2 (SP to SR), the opposite is true.

The present research work shows that the fuzzy AHP mechanism in MCDM works well for choosing honest friends in a SIoT environment, and it can be used as an important tool for the social object in SIoT to find trust-building factors. In our work, we have utilised a limited number of trust metrics and have a small data sample size. So, including some other appropriate and effective trust metrics and a large sample data size that deals with the truthfulness of the social object can produce more refined results. Therefore, various strategies can be integrated with fuzzy logic for the identification and ranking of trust metrics for truthful friend computing in SIoT. So, in the future, researchers can think about using different MCDM techniques, like ANP, ELECTRA, TOPSIS, PROMETHEUS, etc., for comparing results.

Author Contributions: Conceptualization, M.R., S.S. and R.K.; Methodology, F.S.A., M.M.A., P.K.C. and A.A. (Alka Agrawal); Software, M.R., F.S.A. and A.A. (Alka Agrawal); Validation, M.R., F.S.A., A.A. (Abdullah Alharbi) and M.M.A.; Formal analysis, M.R., S.S. and M.M.A.; Investigation, A.A. (Abdullah Alharbi), P.K.C. and A.A. (Alka Agrawal); Resources, M.M.A. and A.A. (Alka Agrawal); Data curation, M.R., S.S., F.S.A. and M.M.A.; Writing—original draft, S.S.; Writing—review & editing, M.R., R.K., F.S.A., A.A. (Abdullah Alharbi), M.M.A., P.K.C. and A.A. (Alka Agrawal); Supervision, R.K. and A.A. (Alka Agrawal); Project administration, R.K. and A.A. (Abdullah Alharbi); Funding acquisition, M.R., F.S.A. and A.A. (Abdullah Alharbi). All authors have read and agreed to the published version of the manuscript.

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSP2022R444), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: Not applicable.

Acknowledgments: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSP2022R444), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Sample responses.

Responses from Experts								
Concerning goal			How much one trust metric is trusty over another					
Ques No.	Trust metrics	Not Trusty	Very Less Trusty	Less Trusty	Strongly Trusty	Very Strongly Trusty	Absolute Trusty	Trust metrics
1	M1				✓			M2
2	M1			✓				M4
3	M1					✓		M5
4	M2				✓			M4
5	M2					✓		M5
6	M4			✓				M5
			Responses from experts					
Concerning goal			How much one trust metric is trusty over another					
Ques No.	Trust metrics	Not Trusty	Very Less Trusty	Less Trusty	Strongly Trusty	Very Strongly Trusty	Absolute Trusty	Trust metrics
1	M3				✓			M4
2	M3					✓		M5
3	M4			✓				M5

Appendix B. Question and Sample Response

- Concerning goal- Determining trust score for secure offloading in truthful friend computing.

  (1) How trusty is quality of service (M1) compared with the quality of Data (M2)?
  (2) How trusty is quality of service (M1) compared with a past reputation (M4)?
  (3) How trusty is quality of service (M1) compared with recommendations (M5)?
  (4) How trusty is the quality of Data (M2) compared with M4?
  (5) How trusty is the quality of QoD compared to M5?
  (6) How trusty is past reputation compared with M5?

- Concerning goal -Determining trust score for a social object to social object collaboration in truthful friend computing.

  (1) How trusty is Social relationships (M3) compared with M4?
  (2) How trusty is M3 compared with past M5?
  (3) How trusty is past reputation compared with M5?

  See Table A1.

References

1. Nitti, M.; Atzori, L.; Cvijikj, I.P. Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies. *IEEE Internet Things J.* **2014**, *2*, 240–247. [CrossRef]
2. Singh, S.; Yadav, N.; Chuarasia, P.K. A Review on Cyber Physical System Attacks: Issues and Challenges. In Proceedings of the 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 28–30 July 2020; pp. 1133–1138.
3. Zhang, D.; Yang, L.T.; Huang, H. Searching in Internet of Things: Vision and Challenges. In Proceedings of the 2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications, Busan, Republic of Korea, 26–28 May 2011; pp. 201–206.
4. Amin, F.; Abbasi, R.; Rehman, A.; Choi, G.S. An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks. *Sensors* **2019**, *19*, 2007. [CrossRef] [PubMed]
5. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The Social Internet of Things (SIoT)—When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [CrossRef]
6. Han, G.; Zhou, L.; Wang, H.; Zhang, W.; Chan, S. A Source Location Protection Protocol Based on Dynamic Routing in WSNs for the Social Internet of Things. *Future Gener. Comput. Syst.* **2018**, *82*, 689–697. [CrossRef]
7. Yan, B.; Yu, J.; Yang, M.; Jiang, H.; Wan, Z.; Ni, L. A Novel Distributed Social Internet of Things Service Recommendation Scheme Based on LSH Forest. *Pers. Ubiquit. Comput.* **2021**, *25*, 1013–1026. [CrossRef]
8. Fortino, G.; Fotia, L.; Messina, F.; Rosaci, D.; Sarné, G.M.L. Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges. *IEEE Access* **2020**, *8*, 60117–60125. [CrossRef]
9. Chen, R.; Bao, F.; Guo, J. Trust-Based Service Management for Social Internet of Things Systems. *IEEE Trans. Dependable Secur. Comput.* **2015**, *13*, 684–696. [CrossRef]
10. Ogundoyin, S.O.; Kamil, I.A. A Fuzzy-AHP Based Prioritization of Trust Criteria in Fog Computing Services. *Appl. Soft Comput.* **2020**, *97*, 106789. [CrossRef]
11. Arjunasamy, A.; Ramasamy, T. A Proficient Heuristic for Selecting Friends in Social Internet of Things. In Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO), IEEE, Coimbatore, India, 7–8 January 2016; pp. 1–5.
12. Kowshalya, A.M.; Valarmathi, M.L. Trust Management in the Social Internet of Things. *Wirel. Pers. Commun.* **2017**, *96*, 2681–2691. [CrossRef]
13. Xiao, H.; Sidhu, N.; Christianson, B. Guarantor and Reputation Based Trust Model for Social Internet of Things. In Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 24–28 August 2015; pp. 600–605.
14. Awan, K.A.; Din, I.U.; Zareei, M.; Talha, M.; Guizani, M.; Jadoon, S.U. HoliTrust-A Holistic Cross-Domain Trust Management Mechanism for Service-Centric Internet of Things. *IEEE Access* **2019**, *7*, 52191–52201. [CrossRef]
15. Alemneh, E.; Senouci, S.-M.; Brunet, P.; Tegegne, T. A Two-Way Trust Management System for Fog Computing. *Future Gener. Comput. Syst.* **2020**, *106*, 206–220. [CrossRef]
16. Ben Saied, Y.; Olivereau, A.; Zeghlache, D.; Laurent, M. Trust Management System Design for the Internet of Things: A Context-Aware and Multi-Service Approach. *Comput. Secur.* **2013**, *39*, 351–365. [CrossRef]
17. Talbi, S.; Bouabdallah, A. Interest-Based Trust Management Scheme for Social Internet of Things. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1129–1140. [CrossRef]
18. Sahu, K.; Srivastava, R.K. Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective. *Adv. Math. Sci. J.* **2021**, *10*, 543–555. [CrossRef]
19. Nizamkari, N.S. A Graph-Based Trust-Enhanced Recommender System for Service Selection in IOT. In Proceedings of the 2017 International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 9–20 January 2017; pp. 1–5.
20. Mendoza, C.V.L.; Kleinschmidt, J.H. A Distributed Trust Management Mechanism for the Internet of Things Using a Multi-Service Approach. *Wirel. Pers. Commun.* **2018**, *103*, 2501–2513. [CrossRef]
21. Chen, I.-R.; Guo, J.; Bao, F. Trust Management for Service Composition in SOA-Based IoT Systems. In Proceedings of the 2014 IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, Turkey, 6–9 April 2014; pp. 3444–3449.
22. Truong, N.B.; Lee, H.; Askwith, B.; Lee, G.M. Toward a Trust Evaluation Mechanism in the Social Internet of Things. *Sensors* **2017**, *17*, 1346. [CrossRef]
23. Bharti, M.; Jindal, H. Optimized Clustering-Based Discovery Framework on Internet of Things. *J. Supercomput.* **2021**, *77*, 1739–1778. [CrossRef]
24. Cuka, M.; Elmazi, D.; Obukata, R.; Ozera, K.; Oda, T.; Barolli, L. An Integrated Intelligent System for IoT Device Selection and Placement in Opportunistic Networks Using Fuzzy Logic and Genetic Algorithm. In Proceedings of the 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 27–29 March 2017; pp. 201–207.
25. Alshehri, M.D.; Hussain, F.K.; Hussain, O.K. Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT). *Mob. Netw. Appl.* **2018**, *23*, 419–431. [CrossRef]
26. Singh, M.; Baranwal, G.; Tripathi, A.K. QoS-Aware Selection of IoT-Based Service. *Arab. J. Sci. Eng.* **2020**, *45*, 10033–10050. [CrossRef]
27. Wang, R.Y.; Strong, D.M. Beyond Accuracy: What Data Quality Means to Data Consumers. *J. Manag. Inf. Syst.* **1996**, *12*, 5–33. [CrossRef]

28. Rajendran, S.; Jebakumar, R. Friendliness Based Trustworthy Relationship Management (F-TRM) in Social Internet of Things. *Wirel. Pers. Commun.* **2022**, *123*, 2625–2647. [CrossRef]
29. Ahmed, A.I.A.; Ab Hamid, S.H.; Gani, A.; Khan, S.; Khan, M.K. Trust and Reputation for Internet of Things: Fundamentals, Taxonomy, and Open Research Challenges. *J. Netw. Comput. Appl.* **2019**, *145*, 102409. [CrossRef]
30. Mohammadi, V.; Rahmani, A.M.; Darwesh, A.M.; Sahafi, A. Trust-Based Recommendation Systems in Internet of Things: A Systematic Literature Review. *Hum. -Cent. Comput. Inf. Sci.* **2019**, *9*, 21. [CrossRef]
31. Vidyasankar, K. A Transaction Model for Executions of Compositions of Internet of Things Services. *Procedia Comput. Sci.* **2016**, *83*, 195–202. [CrossRef]
32. Ferrari, P.; Sisinni, E.; Brandão, D.; Rocha, M. Evaluation of Communication Latency in Industrial IoT Applications. In Proceedings of the 2017 IEEE International Workshop on Measurement and Networking (M&N), Naples, Italy, 27–29 September 2017; pp. 1–6.
33. Abdelghani, W.; Amous, I.; Zayani, C.A.; Sèdes, F.; Roman-Jimenez, G. *Dynamic and Scalable Multi-Level Trust Management Model for Social Internet of Things*; Springer: New York, NY, USA, 2022; Volume 78, ISBN 0-12-345678-9.
34. Kowshalya, A.M.; Valarmathi, M.L. Trust Management for Reliable Decision Making among Social Objects in the Social Internet of Things. *IET Netw.* **2017**, *6*, 75–80. [CrossRef]
35. Jayasinghe, U.; Lee, H.-W.; Lee, G.M. A Computational Model to Evaluate Honesty in Social Internet of Things. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017; pp. 1830–1835.
36. Bao, F.; Chen, I.-R.; Guo, J. Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems. In Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), Mexico City, Mexico, 6–8 March 2013.
37. Sahu, K.; Srivastava, K.R. Needs and importance of reliability prediction: An industrial perspective. *Inf. Sci. Lett.* **2020**, *9*, 5.
38. Adewuyi, A.A.; Cheng, H.; Shi, Q.; Cao, J.; MacDermott, Á.; Wang, X. CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 5432–5445. [CrossRef]
39. Rajak, M.; Shaw, K. Evaluation and Selection of Mobile Health (MHealth) Applications Using AHP and Fuzzy TOPSIS. *Technol. Soc.* **2019**, *59*, 101186. [CrossRef]
40. Saaty, T.L. How to Make a Decision: The Analytic Hierarchy Process. *Interfaces* **1994**, *24*, 19–43. [CrossRef]
41. Zadeh, L.A. Fuzzy Sets as a Basis for a Theory of Possibility. *Fuzzy Sets Syst.* **1978**, *1*, 3–28. [CrossRef]
42. Khan, A.A.; Shameem, M.; Kumar, R.R.; Hussain, S.; Yan, X. Fuzzy AHP Based Prioritization and Taxonomy of Software Process Improvement Success Factors in Global Software Development. *Appl. Soft Comput.* **2019**, *83*, 105648. [CrossRef]
43. Chang, D.-Y. Applications of the Extent Analysis Method on Fuzzy AHP. *Eur. J. Oper. Res.* **1996**, *95*, 649–655. [CrossRef]
44. Kahraman, C.; Cebeci, U.; Ruan, D. Multi-Attribute Comparison of Catering Service Companies Using Fuzzy AHP: The Case of Turkey. *Int. J. Prod. Econ.* **2004**, *87*, 171–184. [CrossRef]
45. Wong, J.K.W.; Li, H. Application of the Analytic Hierarchy Process (AHP) in Multi-Criteria Analysis of the Selection of Intelligent Building Systems. *Build. Environ.* **2008**, *43*, 108–125. [CrossRef]
46. Wang, Y.; Lu, Y.-C.; Chen, I.-R.; Cho, J.-H.; Swami, A.; Lu, C.-T. LogitTrust: A Logit Regression-Based Trust Model for Mobile Ad Hoc Networks. In Proceedings of the 6th ASE International Conference on Privacy, Security, Risk and Trust, Boston, MA, USA, 15–19 December 2014; 2014; pp. 1–10.
47. Gómez Mármol, F.; Martínez Pérez, G. TRIP, a Trust and Reputation Infrastructure-Based Proposal for Vehicular Ad Hoc Networks. *J. Netw. Comput. Appl.* **2012**, *35*, 934–941. [CrossRef]
48. Velloso, P.B.; Laufer, R.P.; de O. Cunha, D.; Duarte, O.C.M.B.; Pujolle, G. Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model. *IEEE Trans. Netw. Serv. Manag.* **2010**, *7*, 172–185. [CrossRef]
49. Hain, Y.; Huang, Z. TRFIoT: Trust and Reputation Model for Fog-Based IoT. In *Proceedings of the Cloud Computing and Security, London, UK, 15–17 August 2018*; Sun, X., Pan, Z., Bertino, E., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 187–198.
50. Byabazaire, J.; O'Hare, G.; Delaney, D. Data Quality and Trust: A Perception from Shared Data in IoT. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.