




Can we quantify trust? Towards a trust-based resilient SIoT network

Subhash Sagar^{1,3}  · Adnan Mahmood¹ · Quan Z. Sheng¹ · Munazza Zaib¹ · Farhan Sufyan²

Received: 17 May 2023 / Accepted: 28 October 2023 / Published online: 18 November 2023
© The Author(s), under exclusive licence to Springer-Verlag GmbH Austria, part of Springer Nature 2023

Abstract

The emerging yet promising paradigm of the Social Internet of Things (SIoT) integrates the notion of the Internet of Things with human social networks. In SIoT, objects, i.e., *things*, have the capability to socialize with the other objects in the SIoT network and can establish their social network autonomously by modeling human behaviour. The notion of trust is imperative in realizing these characteristics of socialization in order to assess the reliability of autonomous collaboration. The perception of trust is evolving in the era of SIoT as an extension to traditional security triads in an attempt to offer secure and reliable services, and is considered as an imperative aspect of any SIoT system for minimizing the probable risk of autonomous decision-making. This research investigates the idea of trust quantification by employing trust measurement in terms of direct trust, indirect trust as a recommendation, and the degree of the SIoT relationships in terms of social similarities (community-of-interest, friendship, and co-work relationships). A weighted sum approach is subsequently employed to synthesize all the trust features in order to ascertain a single trust score. The experimental evaluation demonstrates the effectiveness of the proposed model in segregating the trustworthy and the untrustworthy objects, and illustrates the superior performance of the proposed trust model over state-of-the-art trust models.

Keywords Trust quantification · Community-of-Interest · Friendship · Co-work relationships · Social Internet of Things

Mathematics Subject Classification 68M25 Computer Security

1 Introduction

The notion of the Internet of Things (IoT) refers to the billions of smart objects (e.g., gadgets, machines, and associated software) equipped with sensors and actuators, connected to the internet [1, 2]. This evolution of connected smart objects has led to

Extended author information available on the last page of the article

a number of promising real-world applications, having direct inference on our daily lives, and such applications include smart cities, smart healthcare, smart homes, etc [3]. It is anticipated by Statista¹ that by 2025, there will be around more than 30 billion smart objects, and as a result, scalability and navigability are some of the significant challenges to the adoption of the IoT ecosystem.

The paradigm of the Social Internet of Things (SIoT) is a promising solution to address such challenges. The notion of SIoT has augmented the idea of IoT by incorporating the concept of social networking in smart objects, wherein each object can establish social relationships with other objects autonomously based on the rules set out by their respective owners [4]. Some of the fundamental SIoT relationships can fall into the category of ownership object relationships, social object relationships, parental object relationships, co-location objects relationships, and co-work object relationships. The socialization of objects (via SIoT relationships) has paved the way for the next generation of IoT with an ability to accommodate trillions of smart objects (i.e., service requestors and providers), and has led to numerous benefits, including but not limited to assurance of effective service discovery and network navigability, network scalability similar to human beings, establishing trustworthy relationships among objects, and utilizing of social network architecture for SIoT system. Nevertheless, maintaining trustworthy relationships and providing seamless connectivity to a multitude of heterogeneous objects is always fraught with risk owing to the security and trust of these objects [5, 6]. Since SIoT services are expected to make the decision autonomously without any human intervention, it is imperative for the service requester (i.e., trustor) to determine the trustworthiness of the objects before relying on the information provided by a service provider (i.e., trustee). This kind of trust assessment is essential since there are malevolent objects inside the network that are primarily motivated by the intent to jeopardize the network resources for harmful goals, for instance, the dissemination of malware or false information.

Given the aforementioned insights, the motive for establishing trustworthiness management for SIoT is indisputable. Over the past few years, a number of studies have been proposed in an effort to address the challenges of trustworthiness management in a variety of disciplines including but not limited to mobile and vehicular ad hoc networks [7], peer-to-peer networks [8], online social networks (for the identification of malicious users and sometimes fake stories) [9], and e-commerce (wherein the credibility of a service provider (i.e., retailer) is shared by users by the means of transactions) [10]. The notion of trust in SIoT is characterized as the expectation of a trustor on a trustee to accomplish a well-defined objective in a particular domain within a specific time period. Trust assessment can be a value or a probability and is not the property of either trustor or a trustee, in fact, it is a correlation between the two within a particular environment. Moreover, trust assessment requires a substantial number of parameters owing to its complex dynamics that varies with environments and their respective contexts.

¹ <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>.

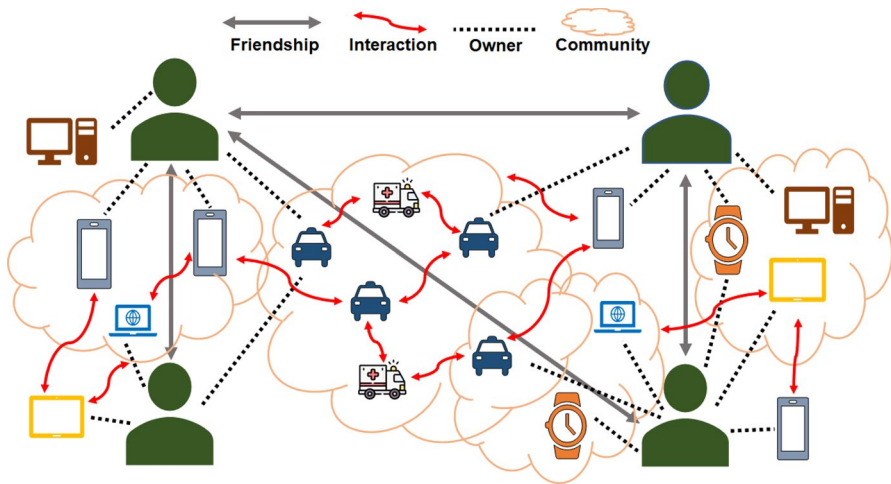


Fig. 1 A high-level view of similarity-based SIoT model

Accordingly, a SIoT-specific similarity-based trust quantification model is therefore proposed to measure the trust score of a SIoT object in this research. An illustration of the SIoT network encompassing a number of similarities is depicted in Fig. 1 [11], wherein objects interact with one another in a highly decentralized manner. In addition, objects are aligned to function in certain communities or at the workplace and have owners who keep a list of friends and communities-of-interest to symbolize social interactions in terms of social similarities. Direct and indirect (i.e., recommendations) interactions are necessary for building the trust of an object. Additionally, the perception or trust of one object for another object in the SIoT network is updated based on their interactions at any particular time instance. Furthermore, each object is accountable for independently carrying out the trust quantification process and defining its direct trust perception for other objects upon encounter by utilizing its owner's friendships, communities-of-interest, co-work relationships, and interactions amongst them. Finally, the main contributions of this study are as follows:

- A SIoT-specific similarity-based trust quantification model has been envisaged by employing direct perception (i.e., direct trust), indirect perception (i.e., recommendation/indirect trust), and the social characteristics in terms of social similarity of trustor-trustee pair in order to embark the misbehaving objects in the network whose status changes with varying interactions;
- A weighted sum scheme has been envisaged to aggregate the trust features for a unified trust score, wherein a combination of weight schemes are employed in order to efficiently aggregate the employed trust features and to analyze the suitable amalgamation of weights; and

- The experimental evaluation of the proposed model has been conducted in a simulation environment with different number of interactions to monitor the trust score of both the benevolent and the malevolent objects. Furthermore, we have analyzed the trust-based dynamically changing behaviour of objects throughout the interactions with varying weights' schemes. Conclusively, we have provided a comparative analysis of the proposed trust model vis-à-vis the state-of-the-art trust models so as to validate the reliability of the same.

The remainder of the paper is organized as follows. Section 2 presents the background of trust and an overview of the existing state-of-the-art trust computational model for SIIoT. Section 3 provides the detail of the employed trust quantification model for SIIoT. Section 4 reports the simulation setup and experimental results for the performance evaluation of the proposed model. Finally, Sect. 5 gives the concluding remarks.

2 Background and state-of-the-art

2.1 Background

The idea of trustworthiness management in SIIoT is evolving rapidly, and it is, therefore, indispensable to know the ideal trust parameter for any SIIoT system. This section delineates the notion of trust and its perspective in the SIIoT and the current state-of-the-art in trustworthiness management for the SIIoT.

2.1.1 Trust concept

The notion of trust is a fundamental aspect of human society and with the advancement in science (e.g., in terms of software and hardware), the concept of trust has been utilized in a number of disciplines (i.e., sociology, psychology, economics and computer science) [12, 13]. The concept of trust differs across disciplines and the fundamental definition of trust is "the confidence of a trustor in a trustee," and perceptions of trust depend on a variety of facets, including but not limited to, temporal factors, environmental factors, and human propensities [14]. In computer science, trust is considered as network and information security, and a system is believed to be trustworthy if it is secure and can categorize the individual accessing a particular system in order to guarantee the integrity and privacy of the information. The early variant of trust in computer science is characterized as a UNIX program free from Trojan horses [15].

2.1.2 Trust in SIIoT

The foundation of the SIIoT paradigm is focused on social interactions and is more inclined towards social science and trust is a crucial component of human social

interactions. According to a widely accepted definition in social science, trust is defined as “confidence” or “self-assurance”. As a result, trust in the context of the SIoT is often understood to be the confidence of a trustor in a trustee to achieve a goal within a certain context and within a specific time frame.

The measure of trust as confidence (also known as trust esteem) can be a probability or a value in the context of the SIoT. An object is also referred to as a trustor or trustee and can be a person, a machine, or an application. Furthermore, it’s crucial to comprehend that a trust is a relationship between the trustor and the trustee rather than being either of their possessions [16]. The overarching goal of the trust is understood as a trustee’s action, or it might be the information that the trustee provides based on the expectations of the trustor and the trustee’s personal characteristics [17, 18]. The key components in quantifying an SIoT object’s trust score are knowledge extraction (using social trust features or Quality-of-Service features), trust aggregation (using traditional weighted sum, fuzzy logic, machine learning, etc.), and finally, trust decision, which determines whether an object is trustworthy or not [19–21].

2.2 State-of-the-art

Recent years suggest the extensive utilization of the trust concept as an essential aspect of any IoT and/or SIoT system [22–24]. Accordingly, a context-aware socio-cognitive-based trust model for service delegation in service-oriented SIoT is proposed by Wei *et al.* [22], wherein two characteristics *competence quantification* and *willingness quantification* form the basis of the model. Furthermore, The degree of importance and the degree of social connections (DoSR) are used to quantify competence, and the degree of contribution (DoC) and the DoSR are also incorporated in the measurement of willingness. The DoC guarantees the service provider’s willingness, the DoI measures the competency of service providers in terms of processing power, storage, and communication capabilities, and the DoSR is used as the weighing criteria for both competence and willingness. In essence, the weighted sum approach is employed to aggregate the two trust parameters in order to provide the final trust score. Similarly, Pourmohseni *et al.* [25] delineated a trust model for SIoT by employing a variety of trust parameters, (i.e., QoS, social and context-based). Nevertheless, a new perspective for trust quantification is discussed which integrates the neutrosophic numbers with the trust-related data in order to deal with the uncertainty and inconsistency in trust-related data before quantifying the selected trust parameters. Finally, the weighted-sum aggregation is utilized to get the single trust score.

Furthermore, trustworthiness management systems are utilized for a number of applications including, but not limited to IoT, internet of vehicles (IoV), and blockchain. For instance, in [26], a trust evaluation mechanism is proposed for recruiting mobile nodes for crowdsourcing, wherein two trust parameters, namely experience and reputation are used and aggregated to compute the trust score of a node.

Similarly, a recommendation-based trust model for vehicle-to-everything (V2X) communication is provided in [27]. The suggestion from nearby nodes (i.e., automobiles and/or roadside units) determines how the weights are updated when combining direct trust and recommendation to determine the trust score of each vehicle. In addition, Mohammadi et al. [28] delineated a trust-based friends selection algorithm using an exhaustive search. The SIoT relationships (e.g., parental object relationships, social relationships, etc.) are employed to select trustworthy friends, wherein the data profiling, distance, and interactions are considered in terms of probability distribution to ascertain the degree of SIoT relationships. Finally, two types of trust scores (static and dynamic) are considered to quantify the trust score in order to eliminate the untrustworthy SIoT objects. More recently, the idea of the integration of the trust management systems with quantum computing has been employed. Shitharth et al. [29] proposed a quantum trust and consultative transaction-based blockchain cybersecurity model for a healthcare system. The proposed system encompasses three key blocks—the consultative transaction key generation and management for ensuring the security of data sharing in healthcare systems, storing of the data in discrete hash blocks by employing the blockchain technology, and integration of quantum trust-based agreement for trust estimation to guarantee a reliable transfer of data among the trusted users only. The extensive experimental analysis demonstrates the validity of the proposed framework when compared with state-of-the-art approaches.

A machine learning-based trust framework based on a node's social profile has been developed by Jayasinghe et al. [30], whereby various social characteristics are accumulated by utilising machine learning-based techniques to obtain the direct trust metric of any node in an IoT network. Similarly, a deep learning-based trust resilient model is proposed by Magdich et al. [31] in order to not only mitigate the trust-related attacks in terms of service provider's behaviour but also detect poor service providers. Furthermore, Xia et al. [32] delineate a trustworthiness inference framework by employing two trust measures, *similarity trust* and *familiarity trust*. Subsequently, a fuzzy logic-based aggregation technique is proposed to synthesize both trust metrics in order to get a single trust score. Most recently, an artificial neural network-based trustworthy object classification model for SIoT (referred to as "Trust-SIoT") is delineated that considers a number of trust features, i.e., direct trust, indirect trust as a recommendation, the credibility of the recommending objects in terms of their reliability and benevolence, and the social similarity, to classify the SIoT objects as trustworthy, untrustworthy or neutral [21]. As of late, a number of studies staged the idea to employ blockchain-based trust models [33–36], e.g., a lightweight blockchain-based trust evaluation mechanism is introduced [33], wherein the SIoT relationships among the objects are considered in the form of a social network. Moreover, an Ethereum platform is utilized to realize the validity of the model in detecting the untrustworthy SIoT object performing trust-related attacks. Nevertheless, the model still needs the fundamental trust metrics, i.e., direct trust, indirect trust, and social relationships to compute the trust score of SIoT devices. It is evident that the recent advancement in technology has the potential to be employed in the trustworthiness management system. however, integrating

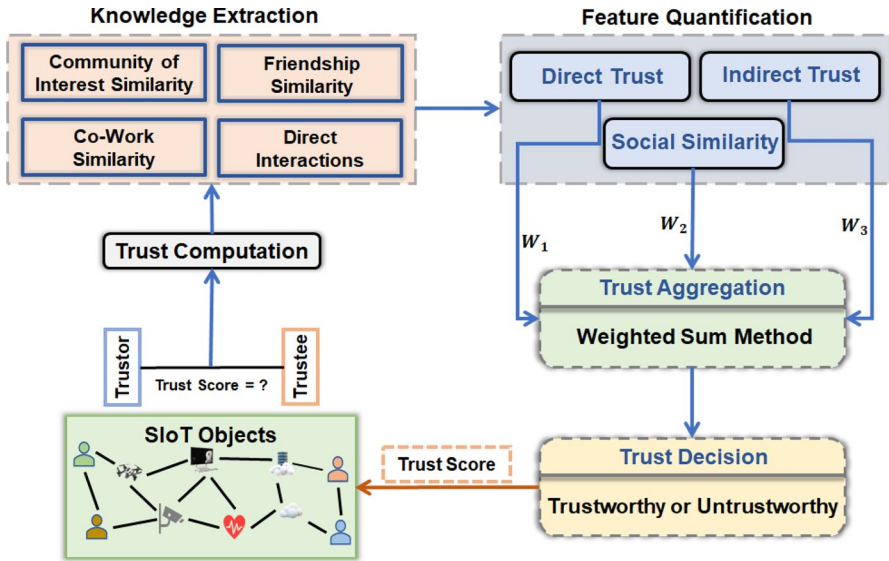


Fig. 2 A schematic diagram of the proposed trust computational model

the concept of context-awareness, the dynamic nature of SIoT application, and the computational latency are some of the challenges that need further exploration.

3 Trust quantification model

As depicted in Fig. 2, the envisaged trust quantification model considers all the characteristics of trustworthiness management, including but not limited to, knowledge extraction, quantification of trust features from the knowledge in terms of the direct trust (i.e., direct observation), indirect trust (i.e., recommendations), and the degree of social similarity, followed by trust aggregation, and finally, the trust decision. Knowledge extraction from the SIoT network is the first step in trustworthiness management, the proposed trust quantification model extracts the SIoT relationships in terms of social metrics (i.e., Community-of-interest, Friendship, and Co-work Similarity) and the information of direct interactions in terms of positive and negative interactions. Subsequently, the feature extraction step quantifies the extracted knowledge in terms of direct trust, indirect trust, and the degree of social similarity. A weighted sum approach is then employed to aggregate all the extracted trust features in order to obtain the single trust score. Finally, it is a trust decision step that is responsible for the classification of the SIoT object into trustworthy or untrustworthy groups via trust-threshold value (θ). The final trust score of an object (i.e., truster) i towards another object (i.e., trustee) j in the SIoT network is denoted by $Trust_{FT}^t(i, j)$ at time $t = [0, t]$. The final trust score encompasses three trust observations – (i)

Table 1 Summary of notations

Notations	Description
\mathcal{P}	Positive interactions
\mathcal{N}	Negative interactions
θ	Trust threshold
N	Number of neighbouring objects
C	Set of communities
F	Set of friends
M	Set of multicast interactions
Sim'_{CoI}	Community-of-interest similarity
Sim'_{FS}	Friendship similarity
Sim'_{CW}	Co-work similarity
$Trust'_{DT}$	Direct trust of a trustor-trustee pair at time t
$Trust'_{RT}$	Indirect trust or recommendation of a trustor-trustee pair at time t
$Trust'_{SS}$	Social similarity of a trustor-trustee pair at time t
$Trust'_{FT}$	Final trust score of a trustor-trustee pair at time t

Direct Trust ($Trust'_{DT}(i, j)$), (ii) Indirect Trust or Recommendations ($Trust'_{RT}(i, j)$), and (iii) Social Similarity ($Trust'_{SS}(i, j)$). The range of final trust score varies between [0, 1], wherein the score closer to 0 classifies the object as untrustworthy and the score closer to 1 classifies an object as trustworthy (Table 1).

3.1 Direct trust ($Trust'_{DT}$)

Direct trust represents the direct observation of a trustor i towards a trustee j . The proposed model quantifies the direct observations by employing both successful (positive) interactions and unsuccessful (negative) interactions between a trustor-trustee pair. We have considered the Bayesian inference with beta probability density function to quantify the direct trust [37]. The direct trust of a trustor towards a trustee is defined as:

$$Trust'_{DT}(i, j) = \frac{\mathcal{P}^t(i, j) + 1}{\mathcal{P}^t(i, j) + \mathcal{N}^t(i, j) + 2} \tag{1}$$

wherein, \mathcal{P} and \mathcal{N} represent positive and negative interactions respectively at any given time t . These positive and negative interactions represent the feedback provided by the trustor and are considered one of the key characteristics of the trust quantification process. In general, it is presumed that a trustor can perfectly rate the trustee (i.e., received service) after the service is fully realized.

3.2 Indirect trust–recommendation ($Trust_R^t$)

In contrast to direct trust, the idea of indirect trust is to provide the recommendation as a trust about a trustee to a trustor in the absence of direct observation vis-à-vis the trustor-trustee pair. Furthermore, the recommendation is an indispensable indicator if the trustor needs the recommendations from the neighbouring objects in the SIoT network and is effective in order to accurately quantify the trust score of a trustee. The proposed model employs the mean of the direct trust of neighbouring friends k towards the trustee j in order to ascertain the recommendations as a trust $Trust_R^t$ at time t as is computed as:

$$Trust_R^t(k, j) = \frac{1}{N} \sum_{N=1}^m Trust_{DT}^t(k_N, j) \quad (2)$$

wherein, N signifies the total number of neighbouring objects. Furthermore, the proposed model has taken into consideration the recommendations from the neighbouring friends of the trustor having a direct trust score of above the threshold (θ) to address the issues of a variety of trust-related attacks (i.e., bad-mouthing attacks and ballot-stuffing attacks) during the amalgamation of recommendations as a trust with the final trust score.

3.3 Social similarity ($Trust_{SS}^t$)

The social similarity feature $Trust_{SS}^t$ is employed to ascertain the social aspects of a trustee towards a trustor at any time t . In essence, the social aspects of a trustee could be assessed by utilizing a number of measures, the proposed model exploits three fundamental similarities metrics to assess a trustee and are described as follows:

3.3.1 Community-of-interest similarity (Sim_{Col}^t)

This trust feature determines the similarity in interests between a trustor i and a trustee j , by determining the degree of community-based similarity. It is achieved by comparing the common interests, such as memberships in similar online social networking and e-commerce groups, between the trustor and trustee. The community-based similarity is calculated by taking the ratio of common communities in which both trustor and trustee are active to the total number of communities in which both parties are involved. This community-of-interest similarity $Sim_{Col}(i, j)$ at time $t = [0, t]$ is ascertained as follows:

$$Sim_{Col}^t(i, j) = \frac{|C_i \cap C_j|}{|C_i \cup C_j|} \quad (3)$$

where, C_i and C_j represent the set of communities of a trustor and a trustee respectively, and $|.$ shows the cardinality of a set, i.e., count of the communities.

Table 2 Weight Schemes (WS)

Features	Weights		
	WS – 1	WS – 2	Mean
$Trust_{DT}^t(i, j)$	0.5	0.4	0.33
$Trust_{SS}^t(i, j)$	0.3	0.3	0.33
$Trust_R^t(i, j)$	0.2	0.3	0.33

3.3.2 Friendship similarity (Sim_{FS}^t)

The friendship similarity signifies the importance of an object in terms of its social relationships with other neighbouring objects (i.e., friends). The primary intent of friendship similarity is to assess the significance of an object to prohibit malicious objects from establishing forged relationships. In essence, the friendship similarity ($Sim_{CoI}^t(i, j)$) as the ratio of common friends between a trustor-trustee pair to the total number of friends a trustor i and a trustee j at time $t = [0, t]$ is ascertained as follows:

$$Sim_{FS}^t(i, j) = \frac{|F_i \cap F_j|}{|F_i \cup F_j|} \quad (4)$$

where, F_i and F_j represent the set of friends of a trustor and a trustee respectively.

3.3.3 Co-work similarity (Sim_{CW}^t)

The co-work similarity feature of an object is measured when the functionality of two or more objects is integrated to achieve a shared purpose by collaborating in a common IIoT application. In this case, the co-work relationships between the IIoT object are prioritized over their physical location. The cosine similarity between the multicast interactions of the trustor i and the trustee j is used to measure the degree of co-work relationships. In essence, the co-work similarity $Sim_{CW}^t(i, j)$ is considered as the ratio of common multicast interactions vis-à-vis trustor-trustee pair to the total number of multicast interactions and is computed as:

$$Sim_{CW}^t(i, j) = \frac{|M_i \cap M_j|}{\sqrt{|M_i| \cdot |M_j|}} \quad (5)$$

Finally, the social similarity ($Trust_{SS}^t(i, j)$) as the trust metric vis-à-vis trustor-trustee pair is thus computed as follows:

$$Trust_{SS}^t(i, j) = \frac{1}{n} \sum_{f=1}^n Sim_{\mathcal{X}}^t(i, j) \quad (6)$$

wherein, \mathcal{X} represents the degree of social similarity (i.e., CoI , FS , and CW) and n signifies the count of integrated similarity measures.

Table 3 Weights for each scenario to compute the final trust score

Scenario	$Trust_{DT}^t(i, j)$	$Trust_{SS}^t(i, j)$	$Trust_R^t(i, j)$
1	w_1	w_2	w_3
2	$w_1 + w_2$	0	w_3
3	$w_1 + w_3$	w_2	0
4	0	w_2	$w_3 + w_1$
5	$w_1 + w_2 + w_3$	0	0
6	0	0	$w_1 + w_2 + w_3$

3.4 Final trust score

Conclusively, a weighted sum method approach is employed to combine all the trust features in order to ascertain a single trust value and is depicted as:

$$Trust_{FT}^t(i, j) = w_1 * Trust_{DT}^t(i, j) + w_2 * Trust_{SS}^t(i, j) + w_3 * Trust_R^t(i, j) \quad (7)$$

here, w signifies the weighting factors and in the proposed model, we have identified and compared a combination of weights for the final trust score. In particular, three different weight schemes (Table 2) are utilized in order to ascertain the final trust score. In essence, the weight parameters employ the importance of each trust feature in obtaining the final trust score. The proposed model employs three variants of the weight schemes, Weight Scheme-1 ($WS - 1$) [22], Weight Scheme-2 ($WS - 2$) [38], and equal weights (*Mean*) [39], i.e., mean as the baseline approach of selecting weights.

In summary, Algorithm 1 encapsulates all the steps of trust computation within the proposed framework. The algorithm involves a number of key steps, such as calculating direct trust, considering recommendations from trustworthy entities from the neighbouring nodes, and evaluating social similarity. Finally, these quantified trust metrics are integrated together as the weighted mean of all the trust metrics in order to obtain the final trust score.

The final trust computation needs to consider the following possible scenarios to quantify the trust of an object:

1. All the trust features, $Trust_{DT}^t(i, j)$, $Trust_{SS}^t(i, j)$, and $Trust_R^t(i, j)$ are available.
2. There is no $Trust_{SS}^t(i, j)$ but $Trust_{DT}^t(i, j)$ and $Trust_R^t(i, j)$ are available.
3. There is no $Trust_R^t(i, j)$ but $Trust_{DT}^t(i, j)$ and $Trust_{SS}^t(i, j)$ are available.
4. There is no $Trust_{DT}^t(i, j)$ but $Trust_{SS}^t(i, j)$ and $Trust_R^t(i, j)$ are available.
5. Only $Trust_{DT}^t(i, j)$ is available.
6. Only $Trust_R^t(i, j)$ is available.

Furthermore, each scenario considers a specific combination of trust features, therefore the weights assignments of each scenario are different and can be seen in Table 3.

Algorithm 1 Trust Evaluation with $WS - 1$ Weighted Scheme

```

1: Input:  $\mathcal{P}_{i,j}, \mathcal{N}_{i,j}$ 
2: Output:  $Trust_{FT}^t(i, j)$ 
   Direct Trust Computation ( $Trust_{DT}^t(i, j)$ )
3:  $Trust_{DT}^t(i, j) = \frac{\mathcal{P}^t(i,j)+1}{\mathcal{P}^t(i,j)+\mathcal{N}^t(i,j)+2}$ 
   Recommendations Computation ( $Trust_R^t(i, j)$ )
4: Select neighbouring friends ( $\mathcal{K}$ ) for recommendations
5: if  $\mathcal{K} \neq \{\}$  then
6:    $Trust_R^t(\mathcal{K}, j) = \frac{1}{N} \sum_{N=1}^{|\mathcal{K}|} Trust_{DT}^t(\mathcal{K}_N, j)$  // Local Recommendations from  $\mathcal{K}$  neighbours
7: else
8:    $Trust_R^t(\mathcal{U}, j) = \frac{1}{N} \sum_{N=1}^{|\mathcal{U}|} Trust_{DT}^t(\mathcal{U}_N, j)$  // Global Recommendations from all the
     SIoT objects ( $\mathcal{U}$ ) in the network.
9: end if
10:  $Trust_R^t(k, j) = \frac{1}{N} \sum_{N=1}^m Trust_{DT}^t(k_N, j)$ 
    Social Similarity ( $Trust_{SS}^t(i, j)$ )
11: Input: List of communities ( $\mathcal{C}$ ), list of friends ( $\mathcal{F}$ ), and list of multicast interactions
     ( $\mathcal{M}$ ) of trustors ( $i$ ) and trustees ( $j$ ).
12: Output: Social Similarity ( $Trust_{SS}^t(i, j)$ )
13: Individual Similarity Computation as  $Sim_{CoI}^t(i, j)$ ,  $Sim_{FS}^t(i, j)$ , and  $Sim_{CW}^t(i, j)$ 
14: Community-of-Interest Similarity –  $Sim_{CoI}^t(i, j) = \frac{|C_i \cap C_j|}{|C_i \cup C_j|}$ 
15: Friendship Similarity –  $Sim_{FS}^t(i, j) = \frac{|F_i \cap F_j|}{|F_i \cup F_j|}$ 
16: Co-work Similarity –  $Sim_{CW}^t(i, j) = \frac{|M_i \cap M_j|}{\sqrt{|M_i| \cdot |M_j|}}$ 
    Social Similarity as Trust ( $Trust_{SS}^t(i, j)$ )
17:  $Trust_{SS}^t(i, j) = \frac{1}{n} \sum_{j=1}^n Sim_X^t(i, j)$ 
     // Here 'n' denotes the overall count of similarities under consideration, while 'X' signifies
     each specific similarity.
    Final Trust Classification ( $Trust_{DF}^t(i, j)$ )
18:  $Trust_{FT}^t(i, j) = w_1 * Trust_{DT}^t(i, j) + w_2 * Trust_{SS}^t(i, j) + w_3 * Trust_R^t(i, j)$  //
     The detail of weights ( $w_1$ ,  $w_2$ , and  $w_3$ ) are provided in Table 2.

```

4 Experimental setup and results

The experimental setup and results for evaluating the performance of the proposed trust quantification model are delineated in this section. In general, a number of scenarios are considered to measure the accuracy of the model in observing the behaviour of SIoT objects. The term “node” or “object” in the discussion represents the SIoT objects and is used interchangeably in this section.

4.1 Experimental setup

To conduct the simulations, we have employed Python and utilized the CRAW-DAD dataset [40]. The dataset contains the traces of participants’ devices from the SIGCOMM conference including location proximity, the interaction logs in terms of successful and unsuccessful interactions vis-à-vis participants, list of friends, the interest groups, i.e., social groups, that these participants tend to involve in, and

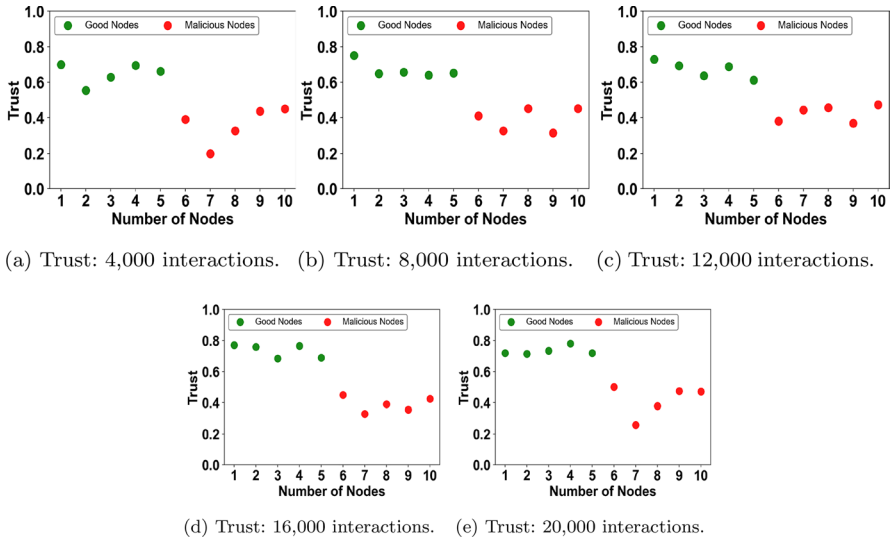


Fig. 3 Trust score of randomly selected good and malicious nodes with varying interactions

other similar message logs. Moreover, it is evident that these traces can be conceptualised in an IoT/SIoT environment [21, 30]. In essence, the dataset encompasses 76 objects each possessing a number of interactions with one another over the span of four days in addition to the social aspects (traces) delineated above. Furthermore, these interactions and social aspects are utilized to quantify the trust features (direct and indirect trust, and social similarity) discussed in Sect. 3.

In addition, we have employed linear interpolation to extend this dataset since linear interpolation preserves the consistency of a dataset [41]. The extended dataset incorporates 150 objects with 20,000 interactions to efficiently realize the proposed model in terms of its experimental evaluation so that the long-term behaviour of the SIoT objects can be observed. In fact, the experimental analysis is carried out by chunking the data vis-à-vis different number of interactions to keep track of trustworthy and untrustworthy objects, and to analyze the behaviour of randomly selected objects.

4.2 Results and analysis

This subsection is further divided into two parts (1) General Analysis where the trust score of randomly selected good (trustworthy) and malicious (untrustworthy) objects is analyzed with varying interaction, and (2) Behaviour Analysis where the trust-based behaviour of randomly selected nodes is discussed.

4.2.1 General analysis

Figure 3 depicts the trust score of randomly selected SIoT nodes analyzed with varying interactions. We have highlighted the behaviour of five good nodes and five

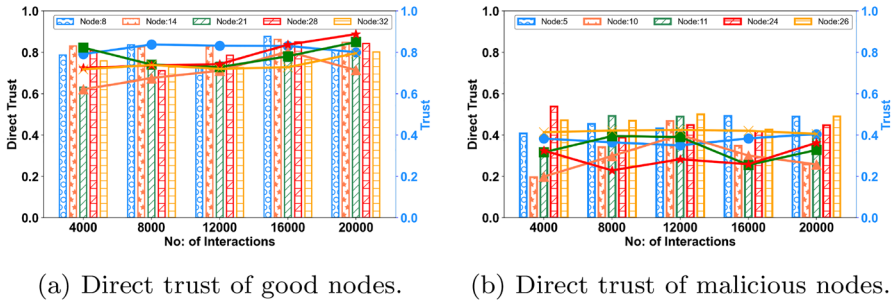


Fig. 4 The effect of direct trust on trust score of randomly selected good and malicious nodes with varying interactions

malicious nodes whose trust score changes significantly with an increase in the number of interactions. It can be seen from the figure that the trust score of good nodes (trustworthy) remains above the threshold θ throughout the interactions, however, the trust score of some of these nodes remains more stable than other nodes due to the presence of malicious nodes in the SIoT network. In general, even in the presence of a number of malicious nodes, the trust score of good nodes remains above the threshold (θ). Similarly, the trust score of malicious nodes remains below the threshold, nevertheless, the trust score of these nodes varies with interactions as the malicious nodes vary their behaviour to improve the trust score. It can be observed from the figures that the proposed model successfully keeps the malicious nodes below the trust threshold θ .

Furthermore, Fig. 4 portrays the reason behind the variation in the trust score of the selected nodes in terms of the trust features with varying interactions. We have only considered the direct trust observation ($Trust_{DT}^t(i, j)$) to analyze the trust score of nodes as this feature is an important aspect of the proposed trust quantification model than the other trust features (i.e., $Trust_{SS}^t(i, j)$, $Trust_R^t(i, j)$). We observe that the trust score of good nodes (Fig. 4a) remains the same from 4000 to 12,000 as the trust features also remain intact. Nonetheless, the trust measure of these nodes increases onward due to an increase in direct trust. Likewise, the trust score of malicious nodes (Fig. 4b) also depends on direct trust more than the other parameters, nevertheless, we perceive that the trust score of these nodes varies with an increase in the number of interaction and the values drop when the interactions count reaches to 20,000. As a whole, it can be observed that the trust score of both the good and malicious nodes is more inclined towards the direct trust score.

The primary objective of the proposed trust model is to efficiently quantify the trust features in order to effectively classify the objects as either trustworthy or untrustworthy. Furthermore, in order to split the object into groups, a threshold (θ) is required, and these threshold values rely on a number of facets (i.e., environmental condition and application requirements). For instance, consider a SIoT application where an object’s credibility is more important than its data, as a result, there can never be a compromise on an object’s credibility in this sort of application. Hence, the threshold must be higher (i.e., $\theta > 0.8$). The threshold value, however,

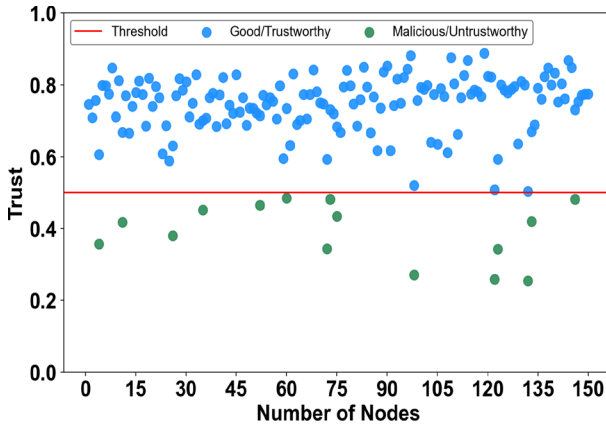


Fig. 5 Trustworthiness of all the nodes in the dataset

might be lower (i.e., $\theta \geq 0.3$) in cases when the data has a higher priority than an object's trust score. The proposed model has used the threshold value of 0.5 (i.e., $\theta = 0.5$) to categorize the objects as either trustworthy or untrustworthy in order to provide the perception that our model classifies them as such. Lastly, Fig. 5 illustrates how the proposed model classifies each node in the dataset as trustworthy or untrustworthy. Nodes with trust values more than θ ($\text{Trust Score} > 0.5$) are designated as trustworthy, and the remaining objects are labeled as untrustworthy. The suggested model with weighted schemes (WS-1) has detected 14 out of 15 objects as being untrustworthy with a detection accuracy of around 94 percent for the given figure, wherein 10% (15 in total) of the objects are malicious or unreliable.

4.2.2 Behaviour analysis

To evaluate the performance of the proposed model with a number of suggested weight schemes, in this subsection, the behaviour of randomly selected nodes in terms of trust-related attacks is analyzed with varying interactions. In particular, we have observed the following dynamic behaviours:

1. *Good Behaviour* In this type of behaviour, a node maintains its trust score throughout the interactions with a trust score above the threshold θ .
2. *Malicious Behaviour* A node acts maliciously in this type of behaviour and thus, its score is always lower than the threshold.
3. *Good to Malicious Behaviour* This type of behaviour represents the change in the reputation of a node with an increase in the number of interactions, in particular, how the reputation of a node decay with interactions.
4. *Malicious to Good Behaviour* In contrast, this behaviour delineates how a malicious node develops its reputation with the increase in the number of interactions.
5. *On-off Behaviour* This type of behaviour is also known as intelligent behaviour wherein the nodes vary their reputation on and off.

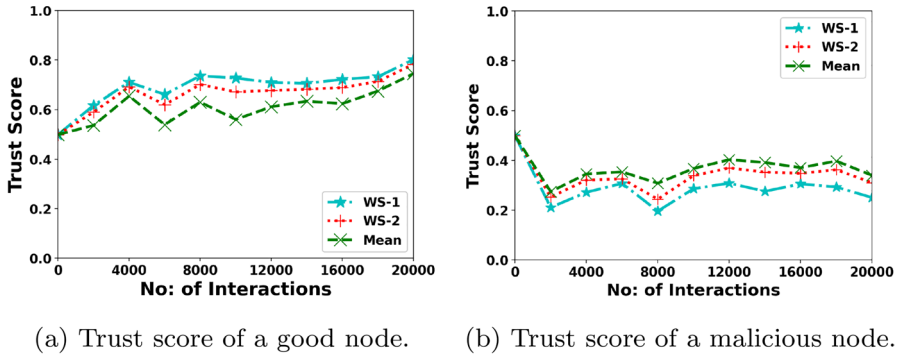


Fig. 6 Trust score of a randomly selected good and malicious node with varying interactions

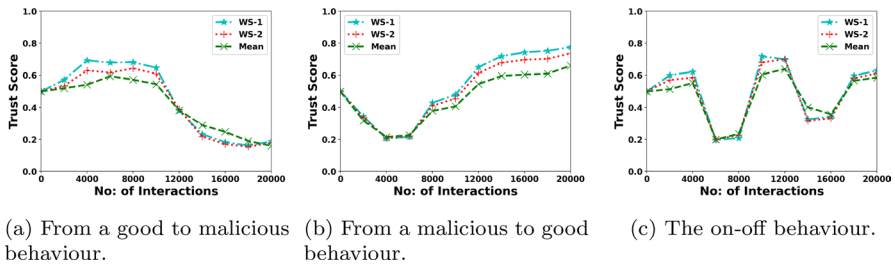


Fig. 7 Trust score of randomly selected nodes with dynamic behaviour

As depicted in Fig. 6a, the proposed trust model successfully quantifies the high trust score for a good node based on its behaviour during the interaction. Similarly, Fig. 6b illustrates the trust score of malicious nodes, and it can be seen the trust score of this node is always low as the nodes are providing malicious services. Moreover, we have compared the trust-based behaviour with three different weight schemes and as illustrated, the WS-1 scheme outperforms the other schemes in providing a higher trust score for a good node and simultaneously providing lower trust for malicious nodes.

Furthermore, the dynamic behaviour of the randomly selected nodes is illustrated in Fig. 7. As can be seen in Fig. 7a how the behaviour (reputation) of a node varies with respect to the interactions and in particular, the reputation of the node decays and our proposed model with different weight schemes has dynamically identified the behaviour based on the interaction of the node within the network. In general, all the weight schemes have identified the behaviour successfully, however, the WS-1 outperforms the other schemes in quantifying the trust score with a higher trust score during the initial interactions and lowest trust score onwards. In contrast to Fig. 7a, the behaviour on how a node can enhance its reputation from malicious to a good node is portrayed in Fig. 7b and it can be observed from the figure that our proposed model can identify the change in

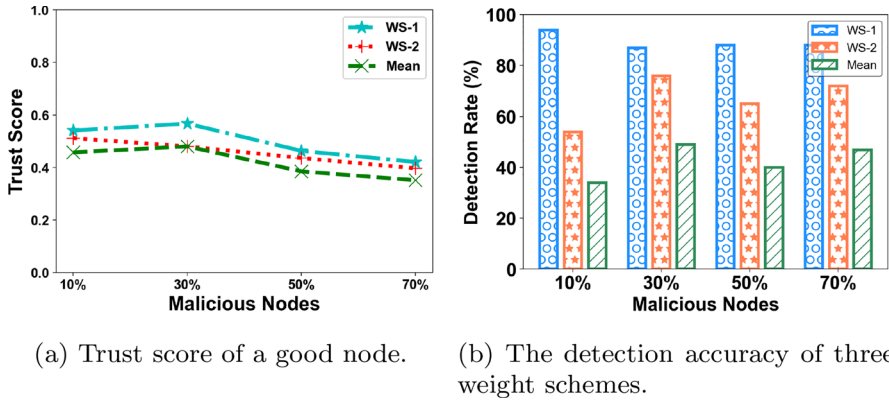


Fig. 8 Trust score of a randomly selected good node and the overall detection accuracy of weight schemes with varying percentages of malicious nodes under different weight schemes

the reputation of a node with WS-1 provides the better quantification. Moreover, Fig. 7 depicts the performance of the model in identifying the on-off behaviour of the objects, and the proposed model can successfully classify the good and malicious behaviour of a node with different trust scores.

Moreover, the aim of any trust model is to identify the untrustworthy nodes in the SIoT network in order to provide reliable services. Therefore, it is imperative to analyze the performance of the model in terms of the detection of untrustworthy nodes with a higher percentage of malicious nodes in the network and to comment on the detection accuracy of the model. Figure 8a presents the analysis of the model in terms of its success rate (trust score) with varying percentages of malicious nodes, and it can be seen that our model can converge with only a few trustworthy/good nodes in the network. Similarly, Fig. 8b portrays the actual detection rate of the model and it can be seen the detection accuracy of our model is higher even in the presence of more than 50% of malicious nodes. In general, the weighting scheme WS – 1 outperforms the other schemes in detecting untrustworthy nodes.

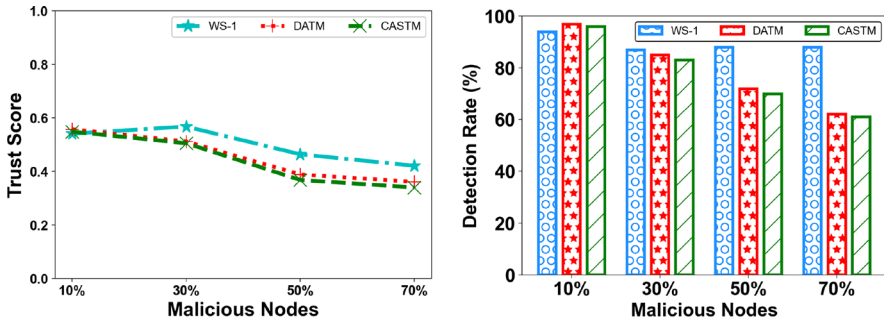
Finally, in order to analyze the validity of the proposed approach, we have compared the same vis-à-vis the following state-of-the-art trust models:

- *CASTM*: A context-aware socio-cognitive-based trust model (*CASTM*) in a bid to facilitate service delegation in service-oriented SIoT has been proposed in [22]. The model combines two characteristics, *competence quantification* and *willingness quantification*. The final trust score is subsequently ascertained by aggregating these two characteristics (trust parameters) via the weighted sum technique.
- *DATM*: Authors in [42] have delineated a discrimination-aware trust model (*DATM*) by taking into consideration the discriminatory behaviour of objects in the SIoT network. The model employs two parameters, i.e., context-based trust encompassing social similarity and feedback, and global reputation features to obtain a single trust score.

Table 4 Detection rate of trust models with varying malicious nodes

% Malicious	WS – 1	DATM	CASTM	% Improvement
10%	94.01	97.02	96.11	-3.10%
30%	87.22	85.10	83.21	4.81%
50%	88.13	72.30	70.34	20.18%
70%	88.09	71.41	69.80	26.20%

Bold values represent the performance improvement of proposed model



(a) Trust score of a good node. (b) The detection accuracy of the proposed trust model.

Fig. 9 Comparison of the proposed trust model vis-à-vis state-of-the-art trust models (*DATM* and *CASTM*) with varying percentages of malicious nodes

Moreover, these trust models employ similar trust characteristics in terms of their distinct trust parameters/features and similar experimental evaluations.

For comparison purposes, we have considered *WS – 1* as our weight scheme for trust evaluation (Algorithm 1) since it achieved higher detection accuracy in contrast to the other two weight schemes (Fig. 8b). Table 4 depicts the effectiveness of the proposed trust model vis-à-vis the state-of-the-art approaches, i.e., *DATM* and *CASTM*. It is quite evident that the proposed model with *WS – 1* outperforms all the other approaches in terms of the detection rate (accuracy) even in the presence of a higher percentage of malicious nodes. In particular, there is an improvement of around 26% with the detection accuracy of around 88% in the presence of 70% malicious nodes in the network. Furthermore, *WS – 1* started with a detection accuracy of 94.01%, the lowest in comparison to the other trust models because of its higher convergence time, however, its performance remains much stable with an increase in the number of malicious nodes.

In addition, we have also compared the performance of the proposed model in terms of the trust score of a randomly selected good node with varying percentages of malicious nodes. It can be thus observed from the Fig. 9a that the proposed model estimated a higher trust score over the varying malicious percentages, and *DATM* and *CASTM* have estimated the trust score of less than 0.5 even when the percentage of malicious nodes is lower. Furthermore, in comparison to *CASTM*, *DATM* performed comparatively better in estimating the trust score of a good node. Finally,

Fig. 9b illustrates the detection accuracy of the trust models with varying malicious nodes and it can be seen that the proposed model ($WS - 1$) outperforms the state-of-the-art trust models in terms of the stable detection rate.

5 Conclusion and future directions

This paper proposes a trust quantification model that amalgamates the notion of trust in aspects of the direct trust of an object towards another object, indirect trust as a recommendation, and social similarities (community-of-interest, friendships, and the degree of co-work relationships). The trust evaluation takes place when an object, i.e., a trustor, interacts with another object, i.e., a trustee. At first, the direct trust of an object is assessed in a subjective manner by utilizing the count of positive and negative interactions. Subsequently, the trustor requests recommendations from trustworthy neighbours, and the degree of social similarity is computed as the trust feature. The final step in the trust quantification is to aggregate all the trust features, i.e., the proposed model employs a weighted sum approach for ascertaining the final trust score. Finally, the experimental evaluations demonstrate how the trust score of randomly selected trustworthy and untrustworthy objects evolve over time and suggest a substantial improvement in the detection accuracy of the proposed trust model vis-à-vis state-of-the-art approaches.

In order to further investigate both the precision and the convergence of the proposed model in a dynamically evolving SIoT context, we intend to propose in the near future a trust model that can integrate context awareness in terms of time and environmental conditions. We further intend to employ knowledge graph embeddings to effectively amalgamate the SIoT relationships in terms of social similarities for a realistic trust assessment.

Acknowledgements Subhash Sagar's research work has been funded via the Macquarie University's Research Excellence Award (Allocation No. 2019050). Adnan Mahmood's research has been supported under the auspices of the Macquarie University's COVID Recovery Research Fellowship Grant 180420387. Quan Z. Sheng's work has been partially supported via the Australian Research Council's Future Fellowship Grant FT140101247 and Discovery Project Grant DP200102298.

Declarations

Conflict of interest The authors confirm that there is no conflict of interest in the submission. All the authors approve the manuscript for publication.

References


1. Ashton K (2009) That 'Internet of Things' thing. *Comput Commun* 22(7):97–114
2. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. *Comput Netw* 54(15):2787–2805
3. Zhang WE, Sheng QZ, Mahmood A, Tran DH, Zaib M, Hamad SA, Aljubairy A, Alhazmi AAF, Sagar S, and Ma C (2020) The 10 research topics in the internet of things. In: *IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, pp 34–43

4. Atzori L, Iera A, Morabito G, Nitti M (2012) The social Internet of Things (SIoT) - when social networks meet the internet of things: concept, architecture, and network characterization. *Comput Netw* 56(16):3594–3608
5. Cai Z, He Z, Guan X, Li Y (2018) Collective data-sanitization for preventing sensitive information inference attacks in social networks. *IEEE Trans Depend Secure Comput* 15(4):577–590
6. Shirvani MH, Masdari M (2023) A survey study on trust-based security in internet of things: challenges and issues. *Internet Things* 21:100640
7. Mahmood A, Sheng QZ, Zhang WE, Wang Y, Sagar S (2023) Toward a distributed trust management system for misbehavior detection in the internet of vehicles. *ACM Trans Cyber-Phys Syst* 7(3):1–25
8. Meng X, Liu D (2018) GeTrust: a guarantee-based trust model in chord-based P2P networks. *IEEE Trans Depend Secure Comput* 15(1):54–68
9. Liu G, Li C and Yang Q (2019) NeuralWalk: trust assessment in online social networks with neural networks. In proceeding of IEEE Conference on Computer Communications (INFOCOM), pp 1999–2007
10. Rahimi Hand El Bakkali H (2013) A new reputation algorithm for evaluating trustworthiness in e-commerce context. In: proceeding of National Security Days (JNS3), pp 1–6
11. Sagar S, Mahmood A, Kumar J, and Sheng QZ (2020) A time-aware similarity-based trust computational model for social internet of things. In: IEEE Global Communications Conference (GLOBECOM), pp 1–60
12. Rousseau DM, Sitkin SB, Burt RS, Camerer C (1998) Not so different after all: a cross-discipline view of trust. *Acad Manag Rev* 23(3):393–404
13. Khan WZ, Arshad Q-A, Hakak S, Khan MK, Saeed-Ur-Rehman (2021) Trust management in social internet of things: architectures, recent advancements, and future challenges. *IEEE Internet Things J* 8(10):7768–7788
14. Sagar S, Mahmood A, Sheng QZ, Pabani JK, and Zhang WE (2022) Understanding the trustworthiness management in the social internet of things: a survey. *arXiv preprint arXiv:2202.03624*
15. Thompson K (1984) Reflections on trusting trust. *Commun ACM* 27(8):761–763
16. Amin F, Ahmad A, Choi GS (2019) Towards trust and friendliness approaches in the social internet of things. *Appl Sci* 9(1):166
17. Truong N, Lee H, Askwith B, Lee GM (2017) Toward a trust evaluation mechanism in the social internet of things. *Sensors* 17:1346
18. Alam S, Zardari S, Noor S, Ahmed S, Mouratidis H (2022) Trust management in social internet of things (SIoT): a survey. *IEEE Access* 10:108924–108954
19. Latif R (2022) ConTrust: a novel context-dependent trust management model in social internet of things. *IEEE Access* 10:46526–46537
20. Rizwanullah M, Singh S, Kumar R, Alrayes FS, Alharbi A, Alnfiat MM, Chaurasia PK, Agrawal A (2023) Development of a model for trust management in the social internet of things. *Electronics* 12(1):41
21. Sagar S, Mahmood A, Wang K, Sheng QZ, Pabani JK, and Zhang WE (2023) Trust-SIoT: towards trustworthy object classification in the social internet of things. *IEEE Transactions on Network and Service Management*, pp 1–1
22. Wei L, Wu J, Long C, Li B (2021) On designing context-aware trust model and service delegation for social internet of things. *IEEE Internet Things J* 8(6):4775–4787
23. Zhang S, Zhang D, Wu Y, and Zhong H (2023) Service recommendation model based on trust and QoS for social internet of things. *IEEE Transactions on Services Computing*, pp 1–14
24. Yu Z, Jin D, Huo C, Wang Z, Liu X, Qi H, Wu J, and Wu L (2023) KGTrust: evaluating trustworthiness of SIoT via knowledge enhanced graph neural networks. In: Proceedings of the ACM Web Conference 2023, pp 727–736
25. Pourmohseni S, Ashtiani M, Azirani AA (2022) A computational trust model for social IoT based on interval neutrosophic numbers. *Inform Sci* 607:758–782
26. Truong NB, Lee GM, Um T, Mackay M (2019) Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the internet of things. *IEEE Trans Inf Foren Secur* 14(10):2705–2719
27. Alnasser A, Sun H, Jiang J (2020) Recommendation-based trust model for vehicle-to-everything (V2X). *IEEE Internet Things J* 7(1):440–450
28. Mohammadi V, Rahmani AM, Darwesh A, Sahafi A (2021) Trust-based friend selection algorithm for navigability in social internet of things. *Knowle-Based Syst* 232:107479
29. Shitharth, Mouratidis H (2023) A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Sci Rep* 13:05

30. Jayasinghe U, Lee GM, Um T, Shi Q (2019) Machine learning based trust computational model for IoT services. *IEEE Trans Sustain Comput* 4(1):39–52
31. Magdich R, Jemal H, Ayed MB (2022) A resilient trust management framework towards trust related attacks in the social internet of things. *Comput Commun* 191:92–107
32. Xia H, Xiao F, Zhang S, Hu C and Cheng X (2019) Trustworthiness inference framework in the social internet of things: a context-aware approach. In: proceeding of IEEE Conference on Computer Communications (INFOCOM), pp 838–846
33. Amiri-Zarandi M, Dara RA, Fraser E (2022) LBTM: a lightweight blockchain-based trust management system for social internet of things. *The J Supercomput* 78(6):8302–8320
34. Kouicem DE, Imine Y, Bouabdallah A, Lakhlef H (2022) Decentralized blockchain-based trust management protocol for the internet of things. *IEEE Trans Depend Secure Comput* 19(2):1292–1306
35. Alam S, Zardari S, Shamsi JA (2022) Blockchain-based trust and reputation management in SIoT. *Electronics* 11(23):3871
36. Selvarajan S, Srivastava G, Khadidos AO, Khadidos AO, Baza M, Alshehri A, and Lin JC-W (2023) An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *J Cloud Comput* 12(1)
37. Ismail R, Jøsang A (2002) The beta reputation system. In: 15th Bled Electronics Commerce Conference, 2502–2511, 2002
38. Nitti M, Girau R, Atzori L, Member S (2014) Trustworthiness management in the social internet of things. *IEEE Trans Knowl Data Eng* 26(5):1253–1266
39. Chen I, Guo J, Bao F (2016) Trust management for SOA-based IoT and its application to service composition. *IEEE Trans Serv Comput* 9(3):482–495
40. Pietilainen AK and Diot C (2009) Crawdad dataset sigcomm2009. <https://crawdad.org/thlab/sigcomm2009/20120715>. 2012-07-15
41. Pownuk A, Kreinovich V (2017) Why linear interpolation? *Mathe Struct Model* 43(3):43–49
42. Jafarian B, Yazdani N, Haghighi MS (2020) Discrimination-aware Trust Management for Social Internet of Things. *Comput Netw* 178:107254

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Authors and Affiliations

Subhash Sagar^{1,3}  · Adnan Mahmood¹ · Quan Z. Sheng¹ · Munazza Zaib¹ · Farhan Sufyan²

✉ Subhash Sagar
subhash.sagar@mq.edu.au

Adnan Mahmood
adnan.mahmood@mq.edu.au

Quan Z. Sheng
michael.sheng@mq.edu.au

Munazza Zaib
munazza-zaib@mq.edu.au

Farhan Sufyan
farhan@galgotiasuniversity.edu.in

¹ School of Computing, Macquarie University, Sydney, NSW 2109, Australia

² School of Computer Application and Technology, Galgotias University, Greater Noida, India

³ Victorian Institute of Technology, Sydney, Australia