Computer Networks 251 (2024) 110611

Contents lists available at ScienceDirect

Computer Networks

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

Survey paper

Understanding the trustworthiness management in the social Internet of Things: A survey

Subhash Sagar [a,*], Adnan Mahmood [a], Quan Z. Sheng [a], Wei Emma Zhang [b], Yang Zhang [c,a], Jitander Kumar Pabani [d]

[a] *School of Computing, Macquarie University, Sydney, NSW 2109, Australia*
[b] *School of Computer Science, The University of Adelaide, Adelaide, SA 5005, Australia*
[c] *School of Information Management, Wuhan University, Wuhan, 430000, China*
[d] *School of Telecommunication Engineering, University of Malaga, Malaga, 29016, Spain*

ARTICLE INFO

Keywords:
Internet of Things
Social Internet of Things
Trustworthiness management
Social relationships
Social objects

ABSTRACT

The next generation of the Internet of Things (IoT) facilitates the integration of the notion of social networking into smart objects, i.e., *things*, to establish a social network of interconnected objects. This integration has led to the evolution of a promising and emerging paradigm of the Social Internet of Things (SIoT), wherein smart objects act as *social objects* and intelligently impersonate social behaviour similar to humans. These social objects are capable of establishing social relationships with the other objects in a network and can utilize these relationships for service discovery. Trust plays an indispensable role in establishing and maintaining such social relationships to achieve the common goal of trustworthy collaboration and cooperation among the objects and guarantee systems' credibility and reliability. In SIoT, an untrustworthy object can disrupt the basic functionality of a service by delivering malicious messages and adversely affecting the quality and reliability of the service. In this survey, we present a holistic review of trustworthiness management in SIoT. The essence of trust in various disciplines and the trust in SIoT have been discussed, followed by a detailed study on trust management components in SIoT. Furthermore, we analyse and compare the trust management schemes by primarily categorizing them into four groups in terms of their strengths, limitations, trust management components (employed in each of the referred trust management schemes), and the performance of these schemes vis-à-vis a number of trust evaluation dimensions. Finally, we discuss the future research directions of the emerging paradigm of SIoT, in particular, in the context of trustworthiness management in SIoT.

1. Introduction

The notion of the Internet of Things (IoT) was prophezied by Kevin Ashton [1] in 1999 as a key paradigm, wherein humans and devices, i.e., objects, would connect and interact over the Internet. Over the last decade or so, this technological viewpoint of IoT became a reality since a network of billions of smart objects (often also referred to as the '*things*') began connecting over the Internet. This evolution of connected smart objects has, therefore, contributed to the considerable number of applications and services having practical implications in our daily lives [2,3]. Some of such applications and services fall in the domains of healthcare, smart cities, smart homes, and smart agriculture. In terms of healthcare, there are numerous applications, e.g., telemedicine to facilitate doctors to monitor the health of patients via wearables embedded with IoT, clinical analytics to study patients together with the site performance, and mhealth to provide two-way communication between the doctors and the patients by employing personal devices [4,5]. Smart cities can benefit from a variety of applications too, e.g., smart grid and smart energy systems can be employed for energy-saving purposes via monitoring of power utilization to optimize energy cost (so as to provide a better consumer service), and fault detection due to environmental hazards; smart transportation system to reduce the travel time and for ensuring efficient traffic management to mitigate the traffic congestion; and smart waste management for facilitating the cities' administration to efficaciously manage and handle massive and ever-increasing volumes of municipal waste via installation of smart bins [6,7]. Smart home applications include smart home automation, smart lighting, smart doors (and smart windows), and smart kitchen appliances [8,9]. Finally, smart agriculture facilitates

[*] Corresponding author.
E-mail addresses: subhash.sagar@mq.edu.au (S. Sagar), adnan.mahmood@mq.edu.au (A. Mahmood), michael.sheng@mq.edu.au (Q.Z. Sheng), wei.e.zhang@adelaide.edu.au (W.E. Zhang), yang.zhang@mq.edu.au (Y. Zhang), jitander.pabani@uma.es (J.K. Pabani).

https://doi.org/10.1016/j.comnet.2024.110611
Received 11 September 2023; Received in revised form 1 May 2024; Accepted 18 June 2024
Available online 26 June 2024

in strengthening traditional farming via precision farming to control and manage livestock and crops more accurately via agriculture drones, livestock monitoring, and smart greenhouses [10].

With the advancement in IoT applications, it is anticipated that there would be approximately 75 billion interconnected devices worldwide by 2025 [11]. As per an estimate of International Data Corporation, the worldwide IoT spending was to the tune of around $742 billion in 2020 and is expected to achieve a growth rate of 11.3% in the following years [12]. Furthermore, IoT is foreseen to have a considerable financial impact of up to $11.1 trillion on the global economy by 2025, wherein factories' operations and equipment optimization would have the highest growth of around $3.7 trillion followed by retail environment, logistics, and navigation, smart cities (i.e., public health and transportation), autonomous vehicles, etc, [13]. Moreover, these billions of IoT devices result in a substantial amount of data exchange, and for which, a state-of-the-art networking infrastructure is highly indispensable to not only reveal the undiscovered operational efficiencies but to devise an end-to-end ecosystem incorporating individuals' needs [2]. In short, IoT is described as a dynamic and global network of infrastructure encompassing both physical and virtual objects with the capability to collect the human and environmental characteristics supporting interoperability using intelligent interfaces and standard communication protocols [3,14,15].

1.1. From IoT to Social Internet of Things (SIoT)

As IoT is of great benefit in various applications, numerous challenges, including but not limited to, heterogeneity, service discovery and composition, and scalability necessitate for designing and developing the IoT infrastructure [16–19]. Heterogeneity is, in fact, one of the considerable concerns since an IoT network comprises of several devices each of varying nature and manufacturer specific operating systems and protocols. This heterogeneous nature impedes the common solution for application development, and thus, the system needs a shared communication paradigm among the devices. Furthermore, information and service discovery is another challenge that needs a novel trusted protocol to ease the exploitation of trust-related services, and with the enormous number of objects, existing solutions to these problems do not really scale up. Therefore, a possible way is to adopt the human sociological behaviour to scale up the current solution. It is pertinent to highlight that humans themselves are heterogeneous, complex, and dynamic in nature, nevertheless, there still exists the notion of social relationship that facilitates in forming the societies among humans based on common interests and needs. Accordingly, information discovery in humans is possible through the principle of small-world phenomena originally suggested by Jon Kleinberg that refers to the short chain of links among the individuals in societies [20,21]. Over the last decade or so, in view of human societies, there has been a lot of research endeavors by scientists in academia and industry, analysing the possibilities of integrating the paradigm of social networking into the IoT ecosystem [22–24]. Moreover, Holmquist et al. [25] introduced the idea of socialization amongst the objects, wherein an easy-to-use technique was devised to establish the relationship between the objects via utilizing the context proximity.

The emerging paradigm of SIoT employs the said integrated concept, wherein each object is not only capable of capturing the surrounding characteristics but also establishes relationships with the other objects in the network. The enhanced capabilities (i.e., socializing with other objects) of these intelligent social objects result in efficient collaboration as they establish their own social network for managing the social relationships and social communities in order to guarantee intelligent decision-making without human intervention [26,27]. For instance, in *smart healthcare*, a smart sensor on the roadside can autonomously alert a smart ambulance of an accident, and thus, an ambulance can look for the required equipment and reach the spot within a minimal time. Similarly, a smart medicine box can interact with sensors on the human body to decide the time and the dosage of medicines. Moreover, in *smart retailing*, the customer's smartphone, without any human intervention, can interact with the customer's refrigerator to create a list of required items that are finished or need replenishment. Accordingly, SIoT can facilitate in addressing numerous research gaps, including but not limited to, the efficient discovery of services and objects, ensuring the scalability similar to that of human social networks, managing social relationships among the intelligent social objects, network navigability with the key idea of smart-world phenomena by utilizing the relationships between the objects, and trustworthiness management among the participating smart objects [28–30]. Moreover, the social characteristics in SIoT have paved the way for the next generation of IoT in a bid to discover the required services via utilizing social relationships with the neighbouring objects. Nevertheless, the risks and uncertainty may diminish the significance of the SIoT paradigm primarily owing to the challenges pertinent to the security, privacy, and trust of these intelligent social objects [30]. For instance, when an object requests a specific service (i.e., referred to as a service requester), then, different service providers may acknowledge the same in order to provide the requisite service and this is where the trustworthiness of these service providers come into play since the one possessing the highest trust would be opted for the requisite service. Besides, security and privacy play an indispensable role in deploying and commercializing the SIoT services. Whilst the traditional solutions, i.e., cryptographic and non-cryptographic ones, have been proposed to address such challenges [14,31], nevertheless, challenges like trust and/or reputation are difficult to address via such solutions. Likewise, there exist malicious objects which can disrupt the basic functionality of a network for malicious purposes by damaging the overall reputation of good (well behavioured) objects or by increasing the trustworthiness of misbehaving objects [32–34]. An efficient trust management system in SIoT is, therefore, imperative for dealing with misbehaving objects (which are capable of jeopardizing the entire network's functionality) by restricting the services of such nodes, and via selecting the reliable and trustworthy objects before relying on the information provided by them.

1.2. Existing surveys on trust management in SIoT

As of date, a plethora of surveys pertinent to trust management in IoT [35–37] have been presented in the research literature. Nevertheless, there are only a few surveys that offer a detailed insight into the trust management systems in the SIoT paradigm. In 2016, Abdelghani et al. [38] published the first survey on trust management in SIoT that briefly discussed the SIoT concept, its trust properties, and compared the presented trust models in terms of varying dimensions, i.e., scalability, adaptability, and resiliency. Nevertheless, this survey lacks a comprehensive discussion of the trust management systems and the trust management components employed in the presented studies. A recently published survey [39] on trust management in SIoT provides a detailed overview of the trust management studies in SIoT and compares the same in terms of different performance metrics, e.g., scalability, adaptability, power efficiency, survivability, and resiliency. However, this survey still lacks reviewing several important aspects of trust, including, but not limited to, trust management components, recent trust-related studies, criteria to analyse the trust management model, and key open research challenges. Furthermore, a survey on trust and friendliness approaches for SIoT is published by Amin et al. [40], wherein the notion of SIoT is reviewed in view of enabling technologies i.e., clouds, multiagent, and Industry 4.0, followed by a comparison of different approaches of trust and friendliness in SIoT. Nevertheless, the survey lacks a discussion of a number of concepts and analysis, i.e., the analysis of trust management schemes, particularly for SIoT, trust management components that are essential for trust management in SIoT.

Table 1
Comparison with recent surveys.

Survey	TM-C	TM-S	TS-A	SIoT-P	TM-R	Description
Abdelghani et al. [38]	~	~	×	×	×	This study presents the comparative analysis of the trust management model for the SIoT environment by taking into account the trust properties and SIoT constraints.
Rashmi et al. [39]	×	~	×	×	×	This study delineates an overview of trust management studies within SIoT and compares the same in terms of different performance metrics and trust-related attacks.
Amin et al. [40]	~	×	×	×	~	This particular survey discusses the trust and friendliness-based approaches in terms of the scalability, adaptability, and the network structure by taking into account the aspects of service composition and social similarity.
Roopa et al. [28]	~	×	×	×	~	This particular study provides a comprehensive overview of current research trends in the context of the SIoT paradigm. Both the service discovery and the composition, relationship management, network navigability, and trustworthiness management are among the discussed trends.
Chahal et al. [41]	✓	~	×	×	~	This survey presents a detailed comparison of protocols, architectures, and trust management for SIoT where the most emphasis is given to the trust management components employed in the literature.
Khan et al. [42]	~	~	×	×	~	This survey discusses a comparative and a comprehensive analysis of SIoT architecture, trust management systems, and open research challenges in SIoT.
This survey	✓	✓	✓	✓	✓	This survey provides an extensive study of the trust management components, a comparison of the trust management schemes, an overview of trust in SIoT-based applications and SIoT platforms, and a summary of future research direction on trust management in SIoT.

Fully Covered: ✓, Not Covered: ×, Partially Covered: ~
TM-C: Trust Management Components, **TM-S**: Trust Management Schemes
TS-A: Trust in SIoT-based Applications, **SIoT-P**: SIoT Platform
TM-R: Trust Management Research Challenges.

A holistic overview of the SIoT paradigm is presented in [28], wherein current research trends in SIoT, i.e., service discovery and composition, relationship management, network navigability, and trustworthiness management are investigated. Yet, this survey lacks a comparison of the latest trust management schemes in the SIoT paradigm as it encompasses the discussion on subjective/objective and dynamic trust management schemes. One of the comprehensive surveys on trust management in SIoT is published by Rajanpreet et al. [41]. The said survey compares and analyzes the trust management systems in multiple domains, i.e., wireless sensor networks and IoT, and subsequently presents a detailed explanation of trust management components employed in the literature. However, the comparison is not solely based on trust management schemes in SIoT but it also includes trust management in IoT, and the clarification of current research challenges for trust computation is also not discussed. The most recent survey on trust management in SIoT is published by Wazir et al. [42] in 2021, wherein the similarities between the IoT and SIoT domains are clarified, SIoT-related architectures are comprehensively discussed, and the trust management system for SIoT are comparatively analysed along with the discussion on future research challenges in SIoT. In view of trust management in SIoT, this study lacks the analysis of trust in SIoT-based applications, discussions on SIoT platforms, and future research challenges, particularly, in terms of trust computation. Table 1 summarizes the researched surveys on trust management in SIoT and also discusses the enhancement in our survey.

1.3. Main contributions of this survey

To address the aforementioned shortcomings in the existing body of literature, this survey targets the topics and approaches which have not yet been covered. Furthermore, the convenience of readers is kept in mind in order to present this survey in a way that is self-sufficient by including the fundamentals of SIoT, the notion of trust, and trust management components in SIoT. After identifying the significance of a trust management system, this survey entails a comprehensive review of trust management schemes in the existing body of literature. The main contributions of our survey are as follows:

(1) We explore the SIoT paradigm and current research directions within SIoT, delve into the fundamentals of *trust* across various disciplines, and examine the trust management components within SIoT;
(2) We categorize the trust management systems into four broad schemes, i.e., recommendation, reputation, prediction, and policy-based trust. In particular, a comparative analysis of these four schemes in terms of strengths and limitations is discussed. Moreover, a detailed analysis of these schemes is also performed on the basis of trust evaluation parameters;
(3) We further review the trust in three SIoT-based applications, i.e., crowdsourcing, smart object recommendation, and the social internet of vehicles, with their respective research challenges, summarize the SIoT platform used in the literature for simulation

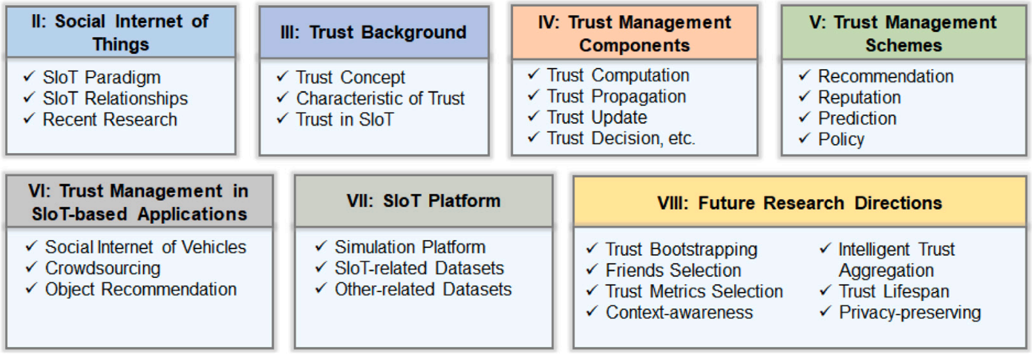


Fig. 1. Taxonomy of this survey.

purposes, and also discuss the datasets currently employed for performance evaluation of trust management solutions;

(4) We present a generalized trustworthiness management framework for SIoT that considers the holistic view of the trust management process employed for SIoT in the studied literature, and;

(5) We identify the future research directions for trustworthiness management in SIoT, particularly, for trust computation purposes.

As a whole, this paper presents a comprehensive review of the recent advancements in trustworthiness management in SIoT and provides a way forward for future research directions. A taxonomy of this survey is depicted in Fig. 1.

1.4. Paper selection

The articles selected in this paper are high-quality papers from reputed transactions (e.g., IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing), journals (e.g., Internet of Things, Computer Networks), and conferences including but not limited to INFOCOM, WWW, and PerCom. At first, the articles' selection process involved the search strings such as "trustworthiness" or "trust" or "trustworthy" + "social internet of things" or "SIoT" or "Social IoT" from resource libraries like IEEE, ACM, Elsevier, Springer, Google Scholar, etc. Successively, the articles are further categorized in terms of top journals and conferences. Moreover, we have included the early access papers from these libraries as well as from arXiv.[1] Finally, the papers are selected based on quality, method novelty, employed social trust metrics, and the proposed techniques that directly influence the scope of this paper (Fig. 2). The remainder of this paper is organized as follows.

Section 2 delineates the SIoT paradigm and current research trends in SIoT. Section 3 deliberates the concept of trust in various disciplines, i.e., sociology, psychology, economics, computer science, and in SIoT. In Section 4, trust management components are discussed in detail. Section 5 presents the comparative analysis of the current state-of-the-art trust management schemes. Section 6 discusses the trust in SIoT-based applications and a number of SIoT-platforms along with SIoT related datasets are briefly discussed in Section 7. Finally, Section 8 provides the future research directions for trustworthiness management in SIoT, whereas, concluding remarks are presented in Section 9.

2. Social Internet of Things (SIoT)

This section provides a fundamental concept of the SIoT paradigm and its significance in terms of various social relationships, and recent research activities and advancements in SIoT.

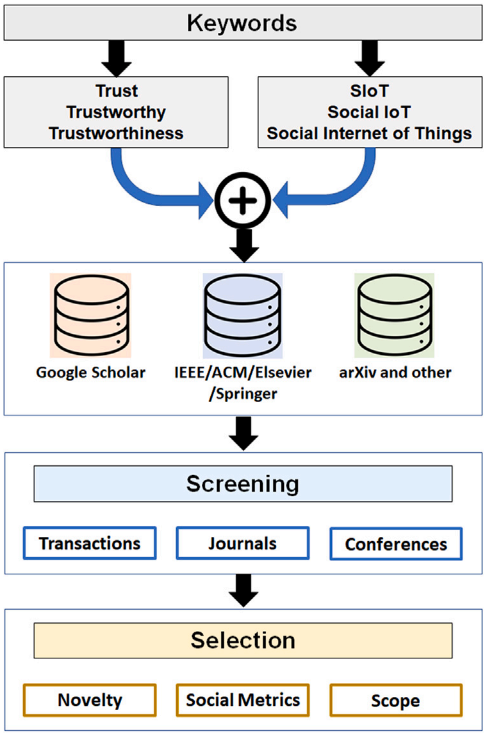


Fig. 2. An overview of paper selection process.

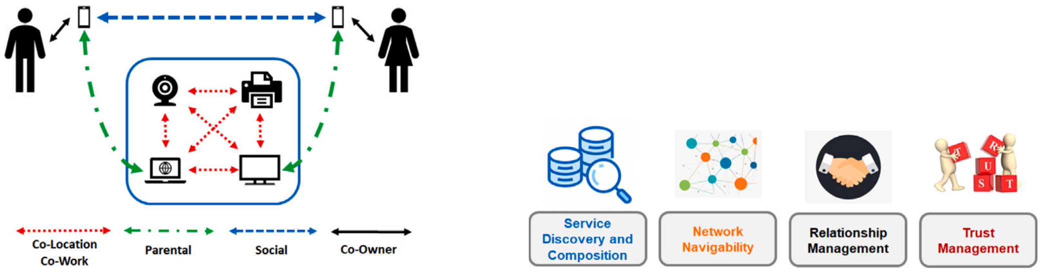
2.1. SIoT paradigm

The idea of the socialization of objects was first conceived in 2001 by P. Mendes [43] wherein the idea of objects participating in the conversation similar to the human social network is presented. Similarly, the authors in [23] explored certain scenarios wherein a person with a smart object can share a particular service with their friend's smart objects through their social circle before the formalization of the SIoT concept by L. Atzori et al. [26]. Subsequently, the concept of the SIoT paradigm has emerged which is intended as, *"the integration of social networking concepts into the IoT domain, wherein each object (referred to as Social Object) is capable of establishing social relationships autonomously with the other objects in the network as per the rules and policies set by their respective owners"*. The SIoT characteristics are highly dependent on social relationships among the objects (Fig. 3(a)) and owners of the objects and some of the frequently occurring relationships are:

2.1.1. Ownership Object Relationships (OOR)

OOR represents the relationships between the objects and their respective owners, i.e., an owner can have multiple devices like

[1] https://arxiv.org/.



(a) Types of relationships in SIoT

(b) Current research areas in SIoT

Fig. 3. SIoT relationships and current research in SIoT.

smartphones, tablets, laptops, etc. This type of relationship results in a high probability of interaction [27].

2.1.2. Social Object Relationships (SOR)

Similar to humans, this type of relationship is established when two or more objects come in contact with each other. For instance, if two individuals are friends and they meet each other regularly then their smartphones may establish a social relationship based on the rules and policies set by their owners [27].

2.1.3. Parental Object Relationships (POR)

POR is correlated with similar objects having the same manufacturer and same production batch within a given period of time. For example, two smartphones of the same model and same manufacturer may establish this type of relationship [27].

2.1.4. Co-location Object Relationships (CLOR)

CLOR represents the relationship among the objects possessing the same location e.g. if two or more objects (e.g., sensors and actuators) provide the services in a home or in an industrial automation environment.

2.1.5. Co-work Object Relationships (CWOR)

In contrast to CLOR, CWOR signifies the relationship involving two or more objects collaborating with each other in a common IoT application in order to accomplish a shared goal. The emphasis in CWOR is on the working relationships between the objects rather than their locations [27].

There are a few unpopular relationships, such as sibling object relationships (SBOR), guest object relationships (GOR), guardian object relationships (GDOR), stranger object relationships (STOR), and service object relationships (SVOR) [28]. SBOR is established among SIoT objects belonging to a family member, and GOR is realized when the SIoT objects are owned by the guests in a social event. Moreover, the GDOR is formed when the SIoT object is dependent on the edge authority or vice versa, and the STOR is established when objects encounter each other in public surroundings. Finally, SVOR exists when objects collaborate with each other in a request/response manner for a particular service.

Furthermore, the SIoT paradigm conveys numerous desirable implications for a future world populated by intelligent objects encompassing the daily life of human beings and aims to support many applications and services by effectively enhancing service discovery and composition. Moreover, applying social networking concepts to the IoT unquestionably prompts favourable circumstances that stretch (i) from the enhanced viability, scalability, and prompt navigability of the network with billions of objects that will populate the IoT in the future (ii) to the arrangement of a degree of trustworthiness that can be built up by utilizing the social relationships among things that are friends and/or having similar interests, and (iii) to the interoperability between the heterogeneous objects. This can be accomplished by exploring the social network and utilizing trustworthy relationships with companion objects.

2.2. Recent research activities in SIoT

In recent years, numerous research articles have been published which provide a detailed insight into the SIoT paradigm and its architectures [44]. The authors in [26,27] introduced the idea of integrating social networking concepts into the IoT in a bid to cope with the issues of service discovery and composition. Besides, the suggested paradigm further facilitates in understanding how an IoT object can establish and manage social relationships with the other objects in a given network. Hence, the resulting paradigm, i.e., SIoT, can support novel applications and services for IoT systems in an efficient and effective manner. Moreover, various SIoT-related challenges are studied in the research literature, and Fig. 3(b) depicts some of these current open key challenges in the SIoT landscape, including but not limited to, (i) service discovery and composition [45,46], (ii) network navigability [47,48], (iii) relationship management [27,49], and (iv) trust management [28,50].

2.2.1. Service discovery and composition

The underlying rationale behind the IoT and SIoT paradigm is to provide services (e.g., healthcare, agriculture monitoring) to the end users. Accordingly, service discovery is of considerable significance and is aimed at discovering the objects and their offered services within real-time environments [51]. As the number of devices are increasing at an unprecedented pace, so as the data exchange between them. It is pertinent to mention that the generated data from these devices is not useful for everyone, and therefore, service discovery is imperative for searching the smart objects providing useful information in a highly dynamic environment. SIoT facilitates at discovering the service, i.e., similar to humans searching for information in their social network by employing different relationships, thereby providing a scalable solution for service discovery. Subsequently, the service composition provides and enables the interaction between the smart objects subsequent to service discovery [52,53].

2.2.2. Network navigability

To make the service discovery process more efficient by utilizing various relationships (e.g., friendship, communities, location) and use these social link to navigate the network, thus reducing the average path length between the participating objects (i.e., service requester and service provider) [47]. In SIoT systems, an object utilizes friends and its friends of friends to search a specific service, nevertheless, it is not feasible for an object to establish a relationship (i.e., to make friendship) with all the objects, and accordingly, a number of researchers have proposed the idea of employing friendship selection methods for choosing minimal friends and to provide the network navigability with reduced path length between the pair of objects using the friendship links [29,48].

2.2.3. Relationship management

Relationship management provides a way of embedding intelligence into smart objects, to make them recognize friends and foes, and to originate, update and terminate the relationship. The authors in [54] introduced the notion of cognitive IoT to integrate intelligence in IoT objects, wherein their goal was to enable the objects to perceive and sense the physical world. However, the SIoT paradigm requires the objects to recognize not only the physical world but also the social world, and this integration demands further exploration [27]. Many research efforts have been made over the years to provide novel ideas for relationship management in terms of friendship selection in the SIoT landscape, wherein different genetic algorithms and appropriate policies have been proposed [49,55,56].

2.2.4. Trustworthiness management

The notion of trust ensures reliable and trustworthy interactions by employing trustworthy social relationships among the objects. A plethora of trustworthiness management systems have been proposed in the literature and have been widely employed in various disciplines (e.g., sociology, psychology, economics, and computer science [57–59]), and numerous applications (e.g., IoT [35,60], Internet of Vehicles (IoV) [61,62], mobile and vehicular ad-hoc networks [63], peer-to-peer networks [64], online social networks [65], e-Commerce [66]). Nevertheless, the SIoT paradigm requires trust management systems that not only deal with the objects but also the social relationships among them. Thus the techniques proposed in the literature cannot be applied directly in the SIoT environment [50]. Recently, numerous studies have been published on trust management in the SIoT environment and a comparative analysis of the same has been summarized in Table 4 by highlighting their respective strengths and limitations. Moreover, Table 5 illustrates the trust management components employed in these studies, whereas Table 6 delineates the evaluation of these studies with various dimensions.

3. Background

The concept of trustworthiness management is evolving rapidly and has been widely employed in various disciplines [57–59,67] and applications (e.g., crowdsourcing, social recommendation) [64,68,69]. It is, therefore, important to distinguish the ideal optimal parameters for any IoT-specific ecosystem.

3.1. Trust as a concept

Trust is a fundamental aspect of human life for building relationships with each other. With the rapid advancements (e.g., in terms of hardware and software) in science, the notion of trust is being integrated and utilized for different disciplines that require human behaviour analysis including but not limited to sociology, psychology, economics, and computer science [70]. The definition of trust varies with disciplines. In its basic form, trust is referred to as the belief of one human (trustor) in another human (trustee) [70], and its notion relies on many facets, e.g., temporal factor, human propensity, and environmental conditions. A brief overview of trust in different domains is illustrated in this section.

3.1.1. Trust in sociology

Sociology studies human social relations, human societies, human–human interactions, and the mechanisms that change and preserve these relations and societies [71]. The primary focus of trust in sociology is to ascertain trustworthy social relationships in a society, where trust is defined as the belief shared by all those involved in a conversation [57]. Furthermore, the authors in [72,73] delineate trust as the means of reducing the complexity in society, and it depends on the belief that humans place on the reactions of his/her counterparts. A different view of trust is provided in Seligman [74], wherein trust is described as reliance and, in usable terms, it is a disposition with respect to the trustor to acknowledge reliance on a trustee.

3.1.2. Trust in psychology

Psychology is a study of a human mind's characteristics, especially, in a specific context [75]. Trust in psychology is referred to as the self-assurance of a human in another human and this assurance varies in a different context, e.g., location, task importance, and time [76]. Likewise, various literature regards trust as a similar characteristic for both social science and psychology, however, the former accounts for trust in terms of societies, whereas, the latter deals with the same at an individual level [57,58]. Furthermore, Josang et al. [77] treats trust as the subjective behaviour via which an individual envisages that its counterpart accomplishes a given activity on which its assistance depends and termed it as *reliability trust*.

3.1.3. Trust in economics

Economics is also a part of social science that deals with the production and distribution of goods and services [78]. Trust in economics is referred to as the reliability in business transactions, wherein one party has the belief in its counterpart's reliability and credibility [59]. In e-commerce, it is possible to mitigate the transaction's risk by incorporating trust dynamics via providing photos of the products, ratings, and reviews when there is no direct interaction between the consumers and the products [79,80]. Likewise, Kazuhiro [81] delineates trust as the character of a business relationship with the end goal that the dependence can be put on the business partners and the deals created with them.

3.1.4. Trust in computer science

In computer science, the main strive is to (a) build a system that is secure, (b) fit for purpose, and (c) in the face of any unexpected vulnerabilities, identify these vulnerabilities easily and recover efficiently [82]. The current computer science systems are about data communication and processing that require secure and trustworthy management [83]. In general, security is all about locks, gates, and fences, however, trust is regarded as when and where we need these enclosures and why they work for a particular environment [84]. Moreover, the early variants of trust look into various aspects of network and data security with one of the earliest by Thompson [85] delineating the trust as a UNIX computer program free from Trojan horses.

3.2. Characteristics of trust

Trust can be evaluated in numerous ways by considering the following characteristics [65]:

Subjective: Subjective trust, in terms of social perspective, is viewed as the evaluation of trust using the centrality of an object, wherein the trust is computed based on the trustor's observation (i.e., direct trust) as well as the opinion (i.e., feedback or indirect trust) of the other objects.

Objective: In contrast to subjective trust, objective trust is evaluated by utilizing the feedback from all the objects in the network, wherein the trust information of each object is distributed and visible to everyone. Moreover, the accessibility of this information is possible via distributed hash tables and this information is maintained by pre-trusted social objects.

Local: It represents the trust based on an object-object relationship, wherein an object evaluates the trustworthiness of another object using local information such as its self-observation and past experience.

Global: In comparison to the local trust, the global trust is considered as the reputation of an object within the network, wherein the trust score of each object is computed by aggregating the local information of each of the other objects in the network.

Context-Specific: Trust of an object towards another object varies with context. A trust relationship between objects is usually dynamic and depends on multiple factors such as temporal factors, location, and energy status.

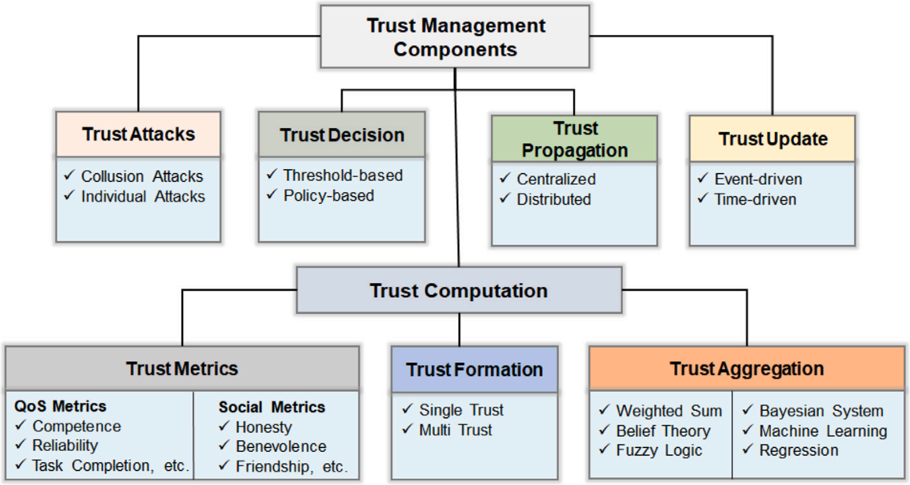


Fig. 4. Components of trustworthiness management in SIoT.

Asymmetric: Trust is an asymmetric property, i.e., if an object A trusts another object B, it does not guarantee that B also trusts A.

3.3. Trust in SIoT

As discussed, trust plays an important role in SIoT to make a trustworthy decision independently without any human intervention. The paradigm of SIoT is more inclined towards social science and a commonly known characteristic of trust in this domain is the "*confidence*" or "*belief* " of an entity towards another entity [40,76]. Thus, in SIoT, trust is widely acknowledged as *the "confidence" of a trustor in a trustee to achieve an objective under a particular setting within a particular timespan* [86,87]. The concept of trust in SIoT is utilized in various applications, including but not limited to social Internet of Vehicles (SIoV) [88], crowdsourcing [89], object recommendation [90], trustworthy service discovery [91], etc.

In the SIoT paradigm, it is imperative to apprehend that a node (either a trustor or a trustee) can be an individual, a device, or an application. Subsequently, trust assessment can be a probability or a value, generally referred to as trust esteem. Furthermore, trust is neither the property of a trustor nor a trustee, in fact, it is the relationship between the two. The foremost objective of trust evaluation is to assess the action of the trustee (or the evaluation of the data it provides) as per the trustor's prospect and trustee's characteristic [40,92]. Thus, it is essential to consider the required parameter for trust quantification as the concept of trust is complex and cannot be measured with a single parameter. Trust of a SIoT object can be seen as the degree of confidence or faith in various characteristics of an object, e.g., the object's ability, integrity, reliability, security, and dependability. Trust in SIoT can be seen as the reputation of an object in the SIoT network based on its direct and indirect understanding and previous transactions [93]. Moreover, it is imperative to discuss and understand the importance of quantifying direct trust as it entirely depends on *feedback*, i.e., the evaluation of the interaction between a trustor and a trustee. It is one of the fundamental characteristics of every trustworthiness model and is tied to how well the information received from the trustee matches the request [94]. In general, the essential components to provide trustworthiness management in SIoT are portrayed in Fig. 4 and are briefly discussed in Section 4.

4. Trust management components

This section presents the essential components that are to be considered for trust management process in SIoT.

4.1. Trust computation

4.1.1. Trust metrics

Trust metrics refer to the features that are chosen and combined for trust purposes. These features can be chosen in terms of a node's social trust metrics and/or quality of service (QoS) trust metrics.

Social Metrics: The social trust metrics represent the social behaviour of nodes in terms of the social relationship between the owners of IoT devices and is measured using integrity, benevolence, honesty, friendship, community-of-interest, and unselfishness [50,113,114].

QoS Metrics: It represents the confidence that a node is able to offer the QoS and is measured in terms of reliability, competence, data delivery ratio, throughput, and task completion [115–117].

4.1.2. Trust formation

Trust formation forms the trust either based on a single aspect, i.e., in terms of positive or negative QoS, or multiple aspects, i.e., trust models that include both QoS and social trust metrics.

Single Trust: Single trust represents the fact that only a single trust metric (e.g. quality of service metric) is used to ascertain the overall trust [118,119].

Multi Trust: It employs the notion of trust as a multi-dimensional concept. For instance, combining a multitude of factors like both social and QoS metrics to form a single trust score [92,113,114].

4.1.3. Trust aggregation

It consists of techniques that aggregate trust observation to obtain a single trust score. Many aggregation techniques have been investigated in the research literature [41], including but not limited to, the one based on weighted sum [113,120], belief theory [100,121], Bayesian system [118,122], fuzzy logic [104,114], regression analysis [110,111], and machine learning [108,123]. Trust aggregation is an important step of any trust computation model, and therefore, it is pertinent to discuss trust aggregation techniques in a comparative manner. Table 2 illustrates each of these aggregation techniques in terms of their strengths and weaknesses.

Weighted Sum: This technique is the simplest and one of the most commonly used aggregation methods. The technique refers to as an average weighted mean of each metric/value, where each metric is assigned a weight to get a single score. Let $M = \{m_1, m_2, m_3, \ldots, m_n\}$ represents the n trust metrics and $W = \{w_1, w_2, w_3, \ldots, w_n\}$ represent the weights of each n trust metrics [113,120], the weighted sum aggregation (WS_A) is computed as:

$$WS_A = \sum_{i=1}^{n} W_i * M_i \tag{1}$$

Table 2
Comparison of trust aggregations techniques.

Techniques	Strengths	Weaknesses
Weighted sum [95–97]	- Low computations cost as it does not require any mathematical function - It is a simple method of aggregating the values.	- An infinite number of possibilities for determining the weights of each value in different environments. - Inability to identify the influence of each value on overall value.
Belief theory [98–100]	- This technique allows to combine data from different independent sources. - Belief theory is appropriate for managing missing data and provides a better method of enumerating vagueness.	- In the presence of malicious objects, the conflicting uncertainty in belief theory may disrupt the opinion of legitimate objects and thus lead to unreliable decision-making.
Bayesian inference [101–103]	- It provides a solid theoretical framework to combine prior information with data. - The inferences in this technique are data dependent and are exact, without dependence on asymptotic estimation	- Bayesian inference requires more expertise to interpret prior distribution beliefs into a mathematically formulated prior distribution to avoid misleading results. - Models with a high number of parameters/metrics often lead to high computational costs.
Fuzzy logic [104–106]	- Fuzzy logic resembles human reasoning that works well even in the presence of ambiguous or vague input. - This nature of fuzzy logic makes this approach suitable for the complex nature of trust evaluation to make decisions efficiently and effectively.	- Fuzzy logic system requires more testing and validation as one problem can have many potential solutions because of no any systemic approach and more human knowledge and expertise dependency.
Machine learning [107–109]	- This technique is more suitable if the number of trust metrics to compute the overall trust score increase when compared with other aggregation techniques.	- It is computationally expensive to utilize a machine learning-driven algorithm and it leads to high latency as the system needs to train the trust model after every transaction.
Regression analysis [110–112]	- Multi-regression analysis has the capability to determine the impact of each trust metric while aggregating the multiple metrics and is able to identify the outlier more efficiently.	- Regression may lead to uncertain results when the dataset used for analysis is insignificant. - Linear regression usually oversimplifies the problem, and thus, it is not recommended for real-world complex problems.

Here the weights can be either *static*, i.e., the weights remain the same for each metric, or *dynamic*, i.e., the weights can change over time.

Belief Theory: It is also referred to as Dempster–Shafer Theory (DST) or evidence theory. Belief theory combines multiple evidence and gives a degree of belief in range {0,1}, where 0 represents no support and 1 represents full support for the evidence. DST provides an uncertainty interval in terms of belief (bel) and plausibility (pla) instead of a traditional probability [100,121]. The belief of a node $\mathcal{N}_j$ in view of node $\mathcal{N}_i$ with respect to an event $\mathfrak{a}$ is computed as:

$$bel(\mathcal{N}_i) = \sum_{a_j \subseteq a} m_{\mathcal{N}_i}(\mathfrak{a}_j) \tag{2}$$

Here $\mathfrak{a}_j$ represents all the basic events of $\mathfrak{a}$, and $m_{\mathcal{N}_i}(\mathfrak{a}_j)$ highlights all the events in view of $\mathcal{N}_i$. Therefore, we can conclude that the belief of a node for an event $\mathfrak{a}$ is computed as:

$$bel(\mathcal{N}_j) = m_{\mathcal{N}_i}(\mathfrak{a}) \tag{3}$$

Subsequently, the plausibility is computed as:

$$pla(\mathcal{N}_i) = 1 - bel(\mathcal{N}_i) \tag{4}$$

Bayesian System: The concept of the Bayesian system is based on Bayes' theorem, i.e., the prior probability, posterior probability about the data/node/interaction, and the likelihood function [118,122]. The trust in the Bayesian system is treated as the random variable and is stated as:

$$p(\mathcal{A}|\mathcal{B}) = \frac{p(\mathcal{B}|\mathcal{A})p(\mathcal{A})}{p(\mathcal{B})} \tag{5}$$

Here $p(\mathcal{A}|\mathcal{B})$ is the posterior probability of $\mathcal{A}$ given $\mathcal{B}$ is true, $p(\mathcal{B}|\mathcal{A})$ is the likelihood of $\mathcal{B}$ given $\mathcal{A}$ is true, $p(\mathcal{B})$ is the probability of $\mathcal{A}$ happening, and $p(\mathcal{A})$ is the prior probability of $\mathcal{A}$.

Fuzzy Logic: In contrast to Boolean logic which takes precise input in the form of 0 or 1, fuzzy logic provides a more realistic understanding similar to human reasoning. Accordingly, fuzzy logic can address the uncertainty and fuzziness in the notion of trust [104,114]. In general, a fuzzy aggregation technique can be divided into the following four phases: (i) *Fuzzy Controller* – to transform the real values into fuzzy sets, (ii) *Fuzzy Logic Rules* – to design the fuzzy logic rules via employing fuzzy intersection, fuzzy union, etc., (iii) *Membership Function (Mapping Function)* – to transform the fuzzy input sets into fuzzy output sets, and (iv) *Defuzzy Controller* – to convert the fuzzy output sets into real values.

Regression Analysis: This statistical process utilizes the slope of the lines to aggregate different independent variables. Regression is divided into two types: (i) *Linear regression*, to make the prediction about one dependent variable based on the information available for one independent variable, and (ii) *multi regression*, to predict the output of a dependent variable based on the information available from many independent variables [110,111]. Mathematically, the linear regression can be seen as: $\mathcal{Y} = m_0 + m_1\mathcal{X}$ and multi regression is computed as:

$$\mathcal{Y} = m_0 + m_1\mathcal{X}_1 + m_2\mathcal{X}_2 + \cdots + m_n\mathcal{X}_n \tag{6}$$

Here m_0 represents the y-intercept of the line, $m_1, m_2, \ldots, m_n$ are the slopes of the lines, $\mathcal{Y}$ is the dependent variable (i.e., aggregated score), and $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n$ are the independent variables (i.e., trust metrics for trust computation).

Machine Learning: Machine learning-based aggregation techniques utilize clustering (i.e., unsupervised algorithms) and classification (i.e.,

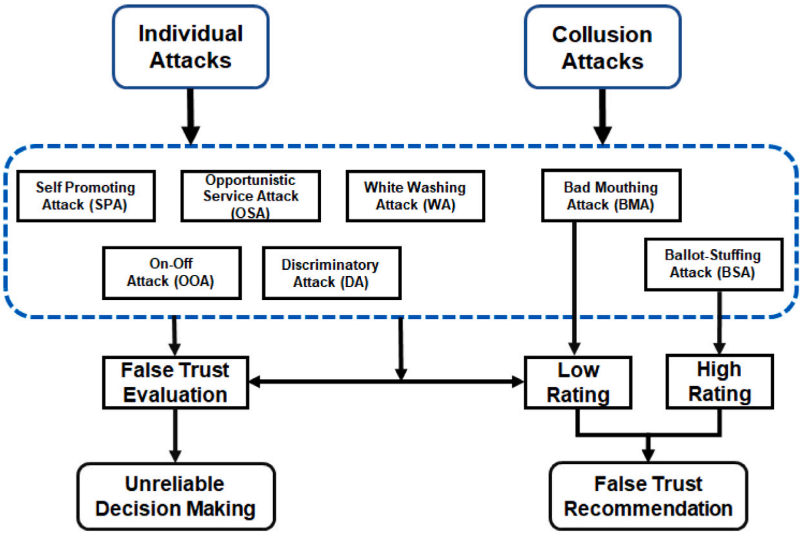

Individual Attacks
Collusion Attacks
Self Promoting Attack (SPA)
Opportunistic Service Attack (OSA)
White Washing Attack (WA)
Bad Mouthing Attack (BMA)
On-Off Attack (OOA)
Discriminatory Attack (DA)
Ballot-Stuffing Attack (BSA)
False Trust Evaluation
Low Rating
High Rating
Unreliable Decision Making
False Trust Recommendation

Fig. 5. Trust related attacks.

supervised algorithms), and are data dependent. If the data is not labelled then aggregation requires two steps: (i) unsupervised algorithms (e.g., k-mean clustering, agglomerative clustering, and spectral clustering) to label the data, and (ii) supervised algorithms (e.g., support vector machine, logistic regression, and random forest) to classify the nodes/objects as either trustworthy or untrustworthy [108,123].

4.2. Trust propagation

Trust propagates facilitates the understanding how the trust propagates in the network and is generally categorized into the following three broad schemes:

Centralized: Centralized schemes rely on a centralized entity that is primarily responsible for (a) gathering trust-related information for the purpose of trust computation and (b) propagating the same in the network [50]. However, centralized controlled frameworks are vulnerable to a single point of failure, wherein the entire network can collapse.

Distributed: In distributed schemes, objects are responsible for both trust computation and propagation within the network without any centralized authority [118,124]. This scheme although provides a solution to the single point of failure, nevertheless, has inherent challenges, i.e., honest trust computation, managing computational capabilities, and unbiased trust propagation in the entire network.

Hybrid: Hybrid schemes are generally used to overcome the challenges posed by both centralized and distributed schemes. Furthermore, hybrid schemes divide the propagation into two common categories, i.e., *locally distributed and globally centralized* and *locally centralized and globally distributed* [50,125].

4.3. Trust update

At the end of a transaction or at any specified time interval, the trust score of a trustee is updated based on it performance. Thus, the update can take place in three ways:

Event-driven: In this approach, trust is updated after each transaction or once an event has occurred [118]. Nevertheless, this type of update increases the traffic overhead in networks with more frequent transactions.

Time-driven: In a time-driven approach, trust is collected and updated periodically after a given interval of time [124,126]. Although this approach overcomes the problem of event-driven approaches, nevertheless, selecting an appropriate time interval remains a challenge.

Hybrid: A number of studies consider both the event-driven and time-driven approaches for trust update where trust is updated periodically and/or in case of an event (after an interaction) [117].

4.4. Trust related attacks

A node can act maliciously with an intent to break the basic functionality of the network and services. There are two types of trust-related attacks as depicted in Fig. 5. These attacks are categorized as individual attacks and collusion-based attacks [28,127].

Individual attacks

Individual attacks refer to the attack launched by an individual object. Some of the common forms of individual attacks are briefly discussed as follows:

Self Promoting Attacks (SPA): In this type of attack, a node can promote its significance by providing a regular good recommendation for itself so as to be selected as a service provider, and once the node is selected as a service provider, it acts maliciously [41].

Whitewashing Attacks (WA): In a whitewashing attack, a node can exit and re-join the network or an application to recover its reputation and wash away its own bad reputation.

Discriminatory Attacks (DA): In DA, a node explicitly attacks other nodes that do not have various common friends by virtue of human intuition or affinity towards friends in SIoT structures. This attack is sometimes referred to as a selective behaviour attack where a node performs well for a particular service/node and ineffectually for some other services/nodes [128].

Opportunistic Service Attacks (OSA): An object can intelligently offer a great service to improve its reputation when its reputation falls in light of offering a bad service. With a high reputation, an object can collude with different objects to perform collusion-based attacks [42].

On-Off attacks (OOA): OOA is similar to OSA, however, in these sorts of attacks, an object provides good and bad services on and off (randomly) to avoid being labelled as a low-reputed node, thereby increasing its chance of being selected as a service provider [41].

Collusion-based attacks

Collusion attacks represent the attack launched by a group of objects to either provide a high rating or low rating to a particular object. Following are some of the collusion attacks:

Bad Mouthing Attacks (BMA): In BMA, a node can deteriorate the reputation of a trustworthy node within the network by providing bad recommendations to diminish its chance of being chosen as a service provider [129].

Ballot Stuffing Attacks (BSA): These attacks are used to boost the reputation of bad nodes within the network by providing good

Table 3
Description of trust management categories.

Category	Description
Recommendation-based trust	- Recommendation-based trust model is based on the idea of soliciting recommendations or feedback from other entities in a network. In the context of SIoT, recommendation-based trust refers to SIoT devices that quantify trust by depending on the experiences or feedback of other devices in the network. - For example, if a device has previously engaged effectively with another device, it may promote that device to other network entities. This approach mimics how social characteristics in human networks work, by employing direct or indirect experiences to measure trustworthiness.
Reputation-based trust	- In reputation-based trust models, an entity's trustworthiness is evaluated based on its reputation, which is often obtained from its previous behaviour and feedback from other entities. In SIoT, a device's reputation may be built on its previous performance, reliability, and the quality of interactions reported by other devices in the network. - This model combines numerous sources of input to provide a holistic perspective of an entity's trustworthiness, reflecting its overall reputation in the network.
Prediction-based trust	- A prediction-based trust model determines an entity's trustworthiness by forecasting its future behaviour using previous data. This method includes analysing an entity's previous behaviour, reliability, and patterns in order to predict its future behaviour. - In SIoT, this might entail applying machine learning algorithms or statistical methodologies to forecast how a device would conduct in future interactions based on its previous history. This methodology is proactive and may alter trust scores when new information becomes available.
Policy-based trust	- Policy-based trust uses specified policies or guidelines to assess the trustworthiness of an entity. In this approach, entities are trusted if they follow particular standards, and regulations established by network or system administrators. In the case of SIoT, this might mean trusting devices based on their adherence to policies, or operating norms. - This strategy guarantees a uniform and standardized approach to trust, focusing on compliance and adherence to established regulations.

recommendations for them so that the bad node can be selected as a service provider [129].

In addition to individual and collusion-based attacks, attackers can launch dynamic attacks with complex and varied attack vectors in various contexts. In these sorts of attacks, attackers may modify their behaviour and execute a mix of attacks (i.e., individual and collusion) to elude the trust management system [129].

4.5. Trust decision

After computing the trust score of a trustee, the main purpose of devising a trust management system is to identify whether a node is trustworthy or untrustworthy by means of using any of the following two techniques:

Threshold-based Decision: In threshold-based decision techniques, a decision is taken on the basis of either a rank-based function or a threshold value [130,131]. Moreover, the threshold values can be adaptive so as to facilitate dynamic environments, whereas static values are specifically employed for a particular application or service.

Context-based Decision: This technique forms the policies that are used to identify and decide whether an object is classified as malicious or not by using the contextual information in terms of location, temporal factor, energy status, etc [130,132].

5. Trust management schemes: Discussion and analysis

As of late, there has been an increased interest in the research community to provide insight into the trustworthiness management systems for SIoT. Therefore, this survey categorizes such systems into four broad categories, i.e., *recommendation-based*, *reputation-based*, *prediction-based*, and the *policy-based schemes*. This section provides a discussion of each of these categories (Table 3) and subsequently, compares the trust management systems that have already been described in the literature by first discussing the pros and cons of these schemes in terms of handling the dynamic behaviour of malicious SIoT objects, suitability of the proposed model for dynamically changing SIoT environments, their computation capabilities, whether or not they are context-aware, and their assumption on initial trust score (i.e., cold start issue). Subsequently, these methods are classified based on the trust metrics employed for trust quantification and the trust-related attacks that they manage.

5.1. Discussion on trust management schemes

This section presents a detailed discussion of the four categorized trust management schemes.

5.1.1. Recommendation-based Trust Scheme (RecTS)

Over the years, a number of recommendation-based trust management systems have been employed, wherein recommendation as a trust metric is exploited in a bid to evaluate the trustworthiness of the nodes in a SIoT network [133]. The trust decision in these approaches is based on both the direct observations as well as the recommendations from the neighbouring nodes to make a more precise decision, i.e., even if

Table 4
SIoT trust computation schemes - A comparative evaluation.

Schemes	Ref.	Attacks	Dynamicity	Computation	Context-aware	Cold start problem
RecTS	Nitti et al. [50]	Static	Yes	Low	No	No
	Khani et al. [91]	Static	No	Low	Yes	No
	Xia et al. [114]	Dynamic	Yes	High	Yes	Yes
	Wei et al. [135]	Dynamic	No	Low	Yes	No
	Chen et al. [113]	Static	Yes	Low	No	No
	Pourmohseni et al. [136]	Static	Yes	High	Yes	No
	Zarandi et al. [140]	Static	Yes	High	No	No
	Zhang et al. [139]	N/A	Yes	High	No	No
	Rehman et al. [141]	Static	Yes	Low	No	No
RepTS	Truong et al. [86]	N/A	No	Low	No	No
	Xiao et al. [117]	N/A	No	Low	No	No
	Azad et al. [142]	Static	Yes	High	No	No
	Truong et al. [143]	N/A	Yes	Low	No	No
	Rajendran et al. [144]	Static	Yes	Low	No	No
	Abdelghani et al. [137]	Dynamic	Yes	Low	No	No
	Lewis et al. [145]	Dynamic	Yes	High	Yes	No
PredTS	Jayasingh et al. [107]	N/A	Yes	High	No	Yes
	Marche et al. [129]	Dynamic	Yes	High	No	No
	Aalibag et al. [146]	Dynamic	Yes	High	No	Yes
	Sagar et al. [147]	N/A	Yes	High	Yes	No
	Abderrahim et al. [148]	Static	Yes	High	No	No
	Magdich et al. [149]	Dynamic	Yes	High	Yes	Yes
	Magdich et al. [150]	N/A	Yes	High	Yes	No
PolTS	Magarino et al. [125]	N/A	Yes	Low	No	No
	Al-Hamadi et al. [131]	Static	Yes	Low	No	No
	Li et al. [132]	Static	No	Low	Yes	No
	Chen et al. [151]	N/A	No	Low	No	No

RecTS: Recommendation-based Trust Schemes, **RepTS**: Recommendation-based Trust Schemes
PredTS: Prediction-based Trust Schemes, **PolTS**: Policy-based Trust Schemes

Attacks	Dynamicity
Static: The attacker's behaviour in this type of attack remains identical, even in different contexts **Dynamic:** The attacker's behaviour in this type of attack changes frequently and adaptive in different contexts	**Yes:** Model can handle dynamically changing environment **No:** Model cannot handle dynamically changing environment

Computation	Context-aware	Cold start problem
High: High computation time **Low:** Low computation time	**Yes:** Integration of context **No:** No context-awareness	**Yes:** No predefined initial trust score **No:** Predefined initial trust score

there are no current direct observations or previous direct observations [134]. As of late, several trust management systems employing recommendation as a trust metric are proposed [50,91,113,114,124,135–139] in the research literature.

Nitti et al. [50] presents the trustworthiness management model for SIoT by employing both the subjective and objective properties of an object. The subjective model is derived by considering the social point of view of an object in terms of its centrality, its own direct experience, and the opinions of neighbouring friends. The objective trustworthiness is employed as a notion of the peer-to-peer network, wherein the information of each object is stored in a distributed hash table and is visible to every object in the network. The computation of objective trustworthiness involves centrality and long and short-term opinions from all the objects in the network. Finally, the static weighted sum aggregation is employed to compute the single trust score. Similarly, the adaptive trust model, suitable for the dynamic changing environment in SIoT is introduced by Chen et al. [113] to isolate the misbehaving nodes performing trust-related attacks. The model considers honesty, cooperativeness, and community-of-interest as the trust metrics, and the recommendation is considered as the direct trust of neighbouring objects. To defend against the good and bad-mouthing from any recommender, a dynamic parameter is considered to control the impact of recommendations for computing the trustworthiness of an object. The performance evaluation of the model is carried out in terms of convergence, accuracy, and resiliency.

Furthermore, Xia et al. [114] delineates a context-aware trustworthiness inference framework by employing two trust metrics, *similarity trust* and *familiarity trust*. The familiarity trust considers the kernel-based nonlinear multivariate grey prediction model to compute the direct trust and recommendations as indirect trust. The similarity trust is computed by employing centrality, and community-interest metrics. To synthesize both trust metrics, a fuzzy logic-based aggregation technique is proposed to get the single trust score. The validity of the model is considered in terms of its resistance to numerous trust-related attacks. Khani et al. [91] presents a mutual context-aware trust evaluation model, wherein three social trust metrics and two QoS metrics are considered to evaluate the trustworthiness of an object. The three social metrics are social similarity in terms of friendship, community-of-interest, and relationships, and QoS metrics are expected and advertised QoS. For context-awareness, the status of a device (energy and computation capability), environment (location), and task type are integrated for trust metrics computation. Finally, the static weighted sum aggregation approach is employed to segregate these independent trust metrics.

Wei et al. [135] proposes a context-aware socio-cognitive-based trust model for service delegation in service-oriented SIoT. The model is dependent on two characteristics, *competence quantification* and *willingness quantification*. The competence is quantified by taking into consideration the degree of importance (DoI) and the degree of social relationships (DoSR), whereas, willingness quantification integrates the degree of contribution (DoC) together with the DoSR. The DoI quantifies service providers' competency in terms of computational power, storage, and communication capabilities, the DoC ensures the willingness of the service providers, and the DoSR is employed as the weighting parameters for both the competence and the willingness. The final trust score is subsequently ascertained by aggregating both trust parameters via the weighted sum technique. Pourmohseni et al. in [136] suggests a new perspective for trustworthiness management by

Table 5
Trust management components employed in SIoT.

Ref.	Trust metrics	Trust aggregation	Trust update	Trust formation	Trust propagation	Trust decision	Trust attacks
Nitti et al. [50]	Social	Weighted sum	Time-driven	Multi-trust	Hybrid	Threshold-based	SPA, WA, OSA, BMA, BSA
Truong et al. [86]	Social	Weighted sum	Event-driven	Multi-trust	Centralized	Threshold-based	NA
Khani et al. [91]	Social and QoS	Weighted sum	Time-driven	Multi-trust	Distributed	Threshold-based	SPA, OOA, BMA, BSA
Jayasinghe et al. [107]	Social	ML-based	Event-driven	Multi-trust	Distributed	Threshold-based	NA
Chen et al. [113]	Social and QoS	Weighted sum	Time-driven	Multi-trust	Distributed	Threshold-based	BMA
Xia et al. [114]	Social	Fuzzy logic	Event-driven	Multi-trust	Distributed	Threshold-based	SPA, OSA, OOA, BMA, BSA
Xiao et al. [117]	Social and QoS	Bayesian system	Hybrid	Single-trust	Distributed	Threshold-based	SPA, BMA, BSA
Chen et al. [124]	Social	Weighted sum	Hybrid	Multi-trust	Distributed	Threshold-based	SPA, BMA, BSA
Magarino et al. [125]	Social	Weighted sum	Event-driven	Multi-trust	Hybrid	Context-based	NA
Marche et al. [129]	Social and QoS	ML-based	Event-driven	Multi-trust	Distributed	Threshold-based	SPA, WA, OSA, OOA, BMA, BSA, DA
Al-Hamadi et al. [131]	Social and QoS	Weighted sum	Event-driven	Multi-trust	Distributed	Context-based	SPA, OSA
Li et al. [132]	Social and QoS	Belief theory	Event-driven	Single-trust	Distributed	Context-based	OOA, BMA, BSA
Wei et al. [135]	Social and QoS	Weighted sum	Event-driven	Multi-trust	Distributed	Threshold-based	OSA, BMA, BSA
Pourmohseni et al. [136]	Social and QoS	Weighted sum	Event-driven	Multi-trust	Distributed	Threshold-based	NA
Zhang et al. [139]	Social and QoS	Weighted sum	Event-driven	Multi-trust	Distributed	Threshold-based	NA
Zarandi et al. [140]	Social	Weighted sum	Event-driven	Multi-trust	Distributed	Threshold-based	NA
Azad et al. [142]	Social and QoS	Weighted sum	Event-driven	Multi-trust	Distributed	Threshold-based	NA
Truong et al. [143]	Social and QoS	Fuzzy logic	Event-driven	Multi-trust	Centralized	Threshold-based	NA
Rajendran et al. [144]	Social and QoS	Weighted sum	Event-driven	Multi-trust	Decentralized	Threshold-based	NA
Abdelghani et al. [137]	Social and QoS	ML-based	Event-driven	Multi-trust	Decentralized	Threshold-based	SPA, WA, OSA, OOA, BMA, BSA, DA
Aalibagi et al. [146]	Social	Filtering	Event-driven	Multi-trust	Distributed	Threshold-based	OSA
Sagar et al. [147]	Social	ML-based	Event-driven	Multi-trust	Centralized	Threshold-based	NA
Abderrahim et al. [148]	Social	ML-based	Event-driven	Multi-trust	Distributed	Threshold-based	NA
Magdich et al. [149]	Social and QoS	ML-based	Event-driven	Multi-trust	Distributed	Context-based	NA
Magdich et al. [150]	Social and QoS and QoS	Ml-based	Event-driven	Multi-trust	Distributed	Context-based	NA
Chen et al. [151]	Social and QoS	Weighted sum	Event-driven	Multi-trust	Distributed	Context-based	NA
Lewis et al. [145]	QoS	Weighted sum	Event-driven	Multi-trust	Distributed	Context-based	Context-attacks
Rehman et al. [141]	QoS	Weighted sum	Event-driven	Multi-trust	Distributed	Threshold-based	OOF, BMA, BSA

Table 6
Evaluation of trust management techniques using various dimensions.

Studies	Scheme	Accuracy	Adaptability	Availability	Integrity	Reliability	Privacy	Scalability	Credibility	Applicability	Response
Nitti et al. [50]	RecTS	H	P	NA	NA	LR	NA	HS	NA	NSA	NEET
Truong et al. [86]	RepTS	NK	F	NA	NA	HR	NA	HS	NA	NSA	NEET
Khani et al. [91]	RecTS	H	P	NA	NA	HR	NA	HS	NC	NSA	NEET
Jayasinghe et al. [107]	PredTS	H	F	L	H	NA	NA	LS	NA	NSA	EET
Chen et al. [113]	RecTS	H	F	L	NA	LR	PP	HS	FC	SA	NEET
Xia et al. [114]	RecTS	H	F	NA	NA	HR	NA	HS	NA	NSA	NEET
Xiao et al. [117]	RepTS	NK	NA	NA	NA	NA	NA	HS	NC	NSA	NEET
Chen et al. [124]	RepTS	H	P	NA	NA	NA	NA	HS	NC	NSA	EET
Magarino et al. [125]	PolTS	NK	F	H	NA	LR	NA	HS	FC	SA	EET
Marche et al. [129]	PredTS	H	F	H	NA	HR	NA	LS	NA	NSA	NEET
Al-Hamadi et al. [131]	PolTS	H	F	H	L	HR	NA	HS	NA	SA	EET
Li et al. [132]	PolTS	H	P	L	NA	LR	NA	LS	NC	SA	NEET
Wei et al. [135]	RecTS	H	F	H	L	HR	NA	HS	NC	NSA	EET
Pourmohseni et al. [136]	RecTS	H	P	H	L	HR	NA	LS	NC	NSA	NEET
Zarandi et al. [140]	RecTS	H	F	H	H	LR	PP	LS	FC	NSA	NEET
Azad et al. [142]	RepTS	H	F	NA	H	HR	PP	LS	NC	SA	EET
Truong et al. [143]	RepTS	NK	P	H	L	LR	NA	HS	NC	SA	NEET
Rajendran [144]	RepTS	H	F	H	L	HR	PP	HS	NC	NSA	EET
Abdelghani [137]	RepTS	H	F	H	H	HR	NA	HS	NC	NSA	NEET
Aalibagi [146]	PredTS	H	F	H	H	HR	NA	HS	NC	NSA	EET
Sagar et al. [147]	PredTS	H	F	NA	H	NA	NA	LS	NA	NSA	EET
Abderrahim et al. [148]	PredTS	H	F	H	NA	HR	NA	HS	FC	NSA	NEET
Magdich [149]	PredTS	H	F	NA	H	HR	NA	LS	NC	NSA	NEET
Magdich [150]	PredTS	H	F	NA	H	HR	NA	LS	NC	NSA	EET
Chen et al. [151]	PolTS	L	P	L	NA	LR	NA	HS	NA	NSA	NEET
Sagar et al. [148]	PredTS	H	F	H	NA	HR	NA	HS	FC	NSA	NEET
Lewis et al. [145]	RepTS	H	F	NA	NA	LR	NA	HS	NA	NSA	NEET
Rehman et al. [141]	RecTS	H	P	NA	H	LR	NA	HS	NA	NSA	NEET

Trust management schemes

RecTS: Recommendation-based Trust Schemes, **RepTS**: Recommendation-based Trust Schemes
PredTS: Prediction-based Trust Schemes, **PolTS**: Policy-based Trust Schemes

Accuracy	Adaptability	Availability	Integrity
H → High L → Low NK → Not Known	F → Full P → Partial NA → Not Addressed	H → High L → Low NA → Not Addressed	H → High L → Low NA → Not Addressed
Reliability	**Privacy**	**Scalability**	**Credibility**
HR → High Reliability LR → Low Reliability NA → Not Addressed	PP → Preserve Privacy NA → Not Addressed	HS → Highly Scalable LS → Less Scalable	FC → Feedback Credibility NC → Node's Credibility NA → Not Addressed
Applicability		**Response**	
SA → Specific Application NSA → No Specified Application		EET → Emphasis on Evaluation Time NEET → No Emphasis on Evaluation Time	

integrating the neutrosophic numbers to model the uncertainty and inconsistency in trustworthiness data before quantifying the trust metrics. Moreover, the QoS trust, social trust metrics (social relationships), and context-trust metrics are employed for quantifying the final trust score. The performance evaluation demonstrates promising results in terms of malicious object detection, however, the limitation of the neutrosophic numbers is not discussed.

Conclusively, the recommendation-based trust model has numerous advantages as shown in Table 4 including, but not limited to, the evaluation of trust when there is no previous communication or the direct observation among the nodes is present, to include the importance and influence of the credible nodes in the network before relying on the information provided by them, etc. Nonetheless, quantifying the credibility of a node in a dynamic environment and the defence mechanism against recommendation-based attacks (e.g., BSA and BMA) is still a major challenge.

5.1.2. Reputation-based Trust Scheme (RepTS)

The concept of reputation has been widely used within the dynamic IoT environment wherein devices/nodes are susceptible to risks owing to incomplete and manipulated information. The reputation of a node can be seen as a behaviour expectation towards other nodes based on experience and the collected referral information [152]. Recently, reputation-based systems have been employed in many fields of computer science, including but not limited to, distributed networks, peer-to-peer networks, and IoT environments where security, privacy, and trust are the critical issues [36]. Many reputation-based trust models [86,117,124,137,142–145,153–155] are employed to enhance the trustworthiness evaluation of a node and to detect the misbehaving nodes in the SIoT network.

Truong et al. [86] presents a trust model, referred to as REK, wherein experience and reputation are employed as an indicator of trust of an object. The computation of experience involves three factors: (1) intensity of interactions, (2) values of interaction in terms of cooperative, uncooperative, and neutral, and (3) the current state of relationships. Subsequently, the trend of experience is analysed via the development of experience (due to cooperative interactions), loss of experience (due to uncooperative interactions), and decay of experience (due to no or neutral interactions). The repudiation perspective of trust involves the concept of *Google PageRank* algorithm wherein both positive and negative reputation are considered to compute the overall reputation of an object. Finally, the model is evaluated in terms of its convergence with minimum iterations. Xiao et al. in [117] proposes an optimal credit and reputation-based trust model for SIoT wherein two parameters credit (referred to as the guarantor) to know whether the object can afford the communication and reputation to evaluate the trustworthiness and to detect the misbehaving node. Moreover, the guarantor is employed to find the object to get the service, and then reputation is employed to evaluate the trustworthiness of the selected object and to detect the misbehaving objects. The performance of the proposed model is carried out by varying the malware probability (i.e., percentage of malicious objects).

Chen et al. in [124] delineates an energy-aware access scheme for service recommendation in SIoT that takes into consideration of the heterogeneous and decentralized environment. The model utilizes reputation from experience, social relationships in terms of friendship and community of interest, and energy status to evaluate the trustworthiness of a node. This energy status consideration allow the balanced distribution of workload among the trustworthy nodes to improve the overall performance. Finally, the effectiveness of the proposed scheme is carried out in terms of rating accuracy, dynamic behaviour, and network stability. The decentralized self-enforcement trust management model is presented by Azad et al. in [142] that utilizes the weighted reputation through feedback generation to compute the trust of an object. The proposed model has three steps: (1) key generation through homomorphic encryption for privacy-preserving and posting a public key to a bulletin board, (2) the generated public key is downloaded by objects, and (3) the reputation of objects is computed through weighted reputation. The self-enforcement is achieved via an automatic trust update through public verifiability by its peers in the network with zero knowledge proof. Finally, the performance of the model is carried out by taking into account the bandwidth required for committing feedback and communication overhead.

A reputation and knowledge-based trust service platform is discussed in [143], wherein the reputation incorporates two trust metrics: recommendation and reputation, and the knowledge assesses an object and its respective owner to compute the knowledge trust metrics of a service. To deal with ambiguous knowledge with vague terms, i.e., “good”, “bad”, “high”, and “low”, a fuzzy logic-based mechanism is introduced for transforming human knowledge into object knowledge. The trust service platform further employs three constituents: *trust agent*, *trust broker*, and *trust management and analysis*. A trust agent is employed for collecting the trust-related data in the SIoT domain and a trust broker is utilized for disseminating the trust-related data to numerous applications and services. Lastly, the trust management and analysis component implements required tasks, including but not limited to, knowledge evaluation mechanisms, information models, reasoning mechanisms, and trust computation algorithms. As of late, Abdelghani et al. [137] proposes a scalable multi-level trustworthiness management model for detecting and mitigating malicious objects capable of performing diverse sorts of attacks. A number of trust metrics are thus employed, including but not limited to, direct experience, rating, the credibility of raters, rating frequency, and social similarity. Extensive experiments are carried out to demonstrate the performance of the proposed model in terms of attack detection rate, precision, recall, etc. The model performs well under all the settings, however, the discussion of trust in terms of context-awareness is missing particularly as the authors claim the multi-dimensionality of trust and context-awareness is one of such dimensions.

Decisively, the reputation-based trust mechanisms have the upper hand while isolating the untrustworthy node for future endeavors but the inclusion of experience has its challenges such as how the old rating influences the current trust evaluation, how to include the forgetting factor for older rating as the characteristic of trust changes rapidly and it is important to include the recent rating, etc. The comparison of a number of schemes relying on a reputation-based trust model is presented in Table 4.

5.1.3. Prediction-based Trust Scheme (PredTS)

The trust management system in the prediction-based model takes into account the current and historical observation to identify and isolate the misbehaving node along with the improved trust computation process to overcome the limitation of trust aggregation techniques in particular the weighted sum approach [156]. The prediction-based systems especially the machine-learning or deep learning approaches have the upper hand when the trust composition step has more trust metrics in comparison with the weighted sum approach. The weighted sum approach fails to obtain the weights of each trust metric to get the single trust score as there can be an infinite number of possibilities of assigning weights to each trust metric in different IoT environments [107]. A number of prediction-based schemes [107,128,129, 146–150,153,157,157] are described as follows and are compared in Table 4. Jafarian et al. [153] delineates a discrimination-aware trust model by taking into consideration of discriminatory behaviour of objects in the SIoT network. An object’s discriminatory behaviours can be attributed due to various reasons including but not limited to the unavailability of computational resources and strong and weak ties of objects in terms of their social relationships. Furthermore, a weighted KNN method is employed to ascertain the trust score by segregating the past and current rating of an object (i.e., service provider). The context-awareness is incorporated as a weight for each rating via a service rating query as rating vector $\langle S, E, SS, f\rangle$ wherein S represents service, E is the energy status, SS is the social similarity and f is the feedback. Finally, the performance is analysed in the presence of numerous trust-related attacks by using the dataset from [158].

A data-centric machine learning-based trust evaluation mode is proposed by Upul et al. in [107] that incorporates the social trust metrics to evaluate the trustworthiness of nodes where the machine learning-based trust aggregation is used to get the single trust score. The machine learning-based aggregation has two steps of clustering (e.g., K-means) and classification (e.g., Support Vector Machine (SVM)) to identify the nodes as trustworthy or untrustworthy. Similarly, Marche et al. [129] introduces a trust-related attack detection model for SIoT, wherein the trust computation process involves two steps: *training phase* and *steady state phase*. In the training phase, trust is computed by employing the three trust metrics: (1) computation capability, a static characteristic of an object to distinguish the powerful devices, (2) relationship factor to consider the relationships between the objects, and (3) external opinion, to obtain the recommendations from neighbouring friends. Furthermore, the training phase is utilized as initial knowledge for the steady state phase. The steady-state step utilizes the initial dynamic knowledge to continuously learn the behaviour of an object. To continuously learn dynamic knowledge, an incremental SVM is employed with goodness, usefulness, and perseverance scores to quantify the trust of an object.

A matrix factorization model is presented in [146] where, at first, SIoT is demonstrated as a bipartite graph in terms of service requester and service provider, then a Hellinger distance is used to build a social network among service requester, and finally, the matrix factorization is used to identify the trustworthy service provider. The model performs well under data sparsity, mitigates cold start problems, and is efficient in identifying malicious objects. Nevertheless, performance evaluation in the presence of many trust-related attacks and the discussion on the suitability of a bipartite graph is not known. A social similarity-based trust computational model is presented in [147] where k-means clustering and random forest classification are used to analyse the trust of the nodes over a period of time. Nevertheless, the proposed solution has no defence mechanism to tackle the trust attacks and is computationally expensive which leads to high latency in dynamic changing environments.

Moreover, a deep learning model is delineated by Masmoudi et al. [128] for segregating malicious nodes performing trust-related attacks. The trust computation process within this model follows a two-step process, i.e., trust composition which includes social and QoS metrics, and deep learning-based trust aggregation. Nevertheless, deep learning aggregation costs higher computational power as well as increases computational latency in dynamic environments. Similarly, Magdich et al. [150] proposes a deep learning-based resilient trust model in an attempt to not only detect the untrustworthy SIoT objects performing a variety of trust-related attacks but also the SIoT objects offering poor services. The model employs knowledge in the context of social similarity, recommendations as an indirect trust, and the reputation of recommenders as trust parameters. Lastly, a deep learning model is trained for classifying untrustworthy objects. One of the most recent works by Sagar et al. [148] presents a framework for trustworthy object classification for SIoT, named *Trust-SIoT*. The framework employs a number of trust parameters, including but not limited to direct and indirect trust in the context of current interaction and feedback, social similarity by considering knowledge graph embedding to embed complex social relationships among the SIoT objects, and the credibility of the objects in terms of their reliability and benevolence. Finally, an artificial neural is employed to classify the nodes as either trustworthy or untrustworthy. The system took into account a number of measures to evaluate the performance of the proposed framework, however, it is equally important to prove the validity of the model in the presence of other key trust attacks. Another recent work suggests a context-aware trust management model for SIoT, known as *CTM-SIoT*. *CTM-SIoT* is a deep learning-based trust model employed to mitigate the malicious objects in the SIoT network. It thus utilizes a number of trust metrics, including but not limited to, owner's trust metrics, reputation, social similarity, and environmental trust (context-trust) metrics. Furthermore, a comparative evaluation of both the weighted and deep-learning-based aggregation is demonstrated in order to suggest the advantages of utilizing the deep-learning-based aggregation. Finally, the proposed model is compared with the state-of-the-art and it can be observed that the proposed model performs well with a slight improvement in F-measure.

In general, the prediction-based scheme has the strength of providing a reliable trust aggregation to segregate the trust metrics and to make the precise trust decision, nonetheless, the computation cost of the prediction model particularly for machine and deep learning needs an optimal and low-cost solution.

5.1.4. Policy-based Trust Scheme (PolTS)

Policy-based trust models depend on pre-defined policies. Policies are the preset rules to evaluate the trustworthiness of nodes to detect malicious behaviour of nodes that have been compromised. These policies rely on network configuration as well as contextual information and can be expressed in mathematical or in language form [159,160]. A number of policy-based trust management schemes on IoT are present in research literature [125,131,132,151,161], however, these schemes are not yet employed in the SIoT. Therefore, we have selected studies that utilize the social behaviour of objects in terms of social trust metrics. We have compared the selected policy-based trust scheme studies as given in Table 4 and a brief description of each main research is described in this section.

Hamid et al. [131] presents an adaptive trust-based decision-making for IoT health systems that rely on different factors including location rating, raters, and witness trust to evaluate the trustworthiness of nodes to eliminate the nodes providing misleading information. The proposed system takes into consideration a number of static trust parameters for trust computation, however, it is important to provide the optimal parameters for different IoT environments. Policy-based security and trustworthy model named $RealAlert$ is proposed by Li et al. [132] to estimate the trustworthiness of a node as well as the data. The model presents the policies based on contextual information to detect the compromising nodes and misleading information by evaluating the model under different trust attacks. Nevertheless, the policies of the proposed model are context-dependent and require human expertise to update the policies for highly dynamic IoT applications.

Moreover, a trust management model is proposed in [151] that combines maximum ratio combining (MRC) and selection combining (SC) to ascertain the trustworthiness of nodes. The trust evaluation process starts with weighting the extracted parameters in the MRC step, subsequently, the output is then transferred to SC to obtain the final single trust score. The performance evaluation shows a promising result, however, the model is evaluated on a limited number of nodes that do not guarantee scalability, and no defence mechanism in the presence of a trust attack is considered. Correspondingly, Magarino et al. [125] presents an enhanced security framework by employing prioritization rules, digital certificates, and trust and reputation policies to perceive a hijacked node providing deceptive information. The trust and reputation policies are direct interaction dependent and reputation is the recommendation of other nodes in the network. The performance evaluation shows that their approach is better at detecting the hijacked nodes than the other compared approaches. However, the evaluation against trust-related attacks is not illustrated. Overall, in general, the policy-based trust models are more suitable for an IoT application that does not have a dynamic nature such as no mobile nodes, a similar context in terms of location and time. Nonetheless, with the dynamic changing environment, it is more challenging to manage and update the policies for different contexts.

5.2. Applicability of trust management schemes in real-world SIoT application

Trust management schemes in SIoT have the potential to be integrated with a number of SIoT applications [162]. This section provides a discussion of a few real-world SIoT applications and their applicability concerning trust management schemes discussed in Section 5.

5.2.1. RecTS

RecTS schemes are intriguing since they rely on feedback or recommendations from other entities in the SIoT ecosystem. These schemes play an important role in a number of SIoT applications, including, but not limited to, smart homes and smart healthcare.

In a *smart home*, smart thermostats, lighting systems, and security cameras communicate with one another. A recommendation-based trust model can be used, in which devices exchange recommendations based on prior encounters. For example, if a smart thermostat communicates successfully with a smart lighting system, it may promote it to other network devices. This creates a trust network, ensuring that home automation runs smoothly and securely.

Furthermore, in *smart healthcare*, devices such as sensors monitoring patients' health, medical devices, and patient management systems require reliable data communication. A recommendation-based trust model can be employed, with devices rating their interactions with one another. For example, a heart rate monitoring sensor that successfully communicates data to a patient management system can boost trust in the system. This assures that only trustworthy devices participate in vital healthcare data sharing, hence improving patient data privacy [163].

5.2.2. RepTS

In RepTS models, both the past behaviour as well as feedback from other entities are integrated to quantify the device's reputation. Here are some instances of real-world SIoT applications where reputation-based trust models can be useful:

In *smart grids*, devices such as smart transformers, smart meters, and other devices must cooperatively communicate with each other. A reputation-based trust model can be used, with each device's reputation evaluated based on its history of event reporting and cooperativeness. For example, a smart meter that routinely gives accurate energy use statistics might have a good reputation and become more trusted throughout the grid. This guarantees stable energy distribution and efficient response management.

Moreover, devices such as traffic sensors, vehicle communication systems, and pedestrian signals in *intelligent transportation systems* must communicate seamlessly. A reputation-based trust model can assist in determining the credibility of these devices. For example, a traffic sensor that consistently gives correct traffic data may be considered more trustworthy, resulting in its data being prioritized for traffic management choices, hence improving road safety.

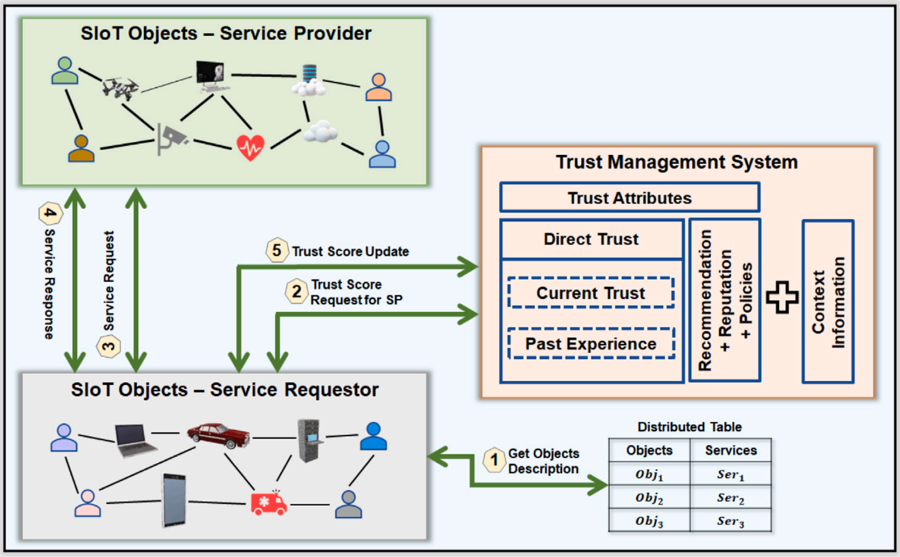


Fig. 6. High-level overview of trustworthiness management system in service-oriented SIoT.

5.2.3. PredTS

PredTS estimates devices' future behaviour based on past interactions. There are a number of real-world SIoT application scenarios where prediction-based trust models could be very useful:

In *Industrial IoT*, devices monitor the functioning of machinery and equipment. A PredTS model can use data from these devices to forecast their future reliability. For example, if sensors in a production line have a track record of correctly predicting equipment breakdowns, their trustworthiness for future maintenance jobs increases. This enables timely maintenance measures and reduced downtimes.

Furthermore, in a *smart home environment*, devices such as lighting, thermostats, and smart appliances can be used to optimize energy consumption. With a prediction-based trust model, the system can utilize devices' previous behaviour to forecast their future energy usage. For example, a smart thermostat that has previously regulated heating or cooling precisely depending on user preferences and weather conditions may be trusted to optimize energy usage in the future.

5.2.4. PolTS

PolTS models are based on preset policies that regulate network interactions and trustworthy decisions. These models are especially effective in contexts where adherence to specified regulations is critical. Some examples of real-world SIoT applications that can successfully use PolTS are smart healthcare and smart cities.

In *smart healthcare*, patient data privacy and security are critical. A policy-based trust architecture can impose stringent data management and access regulations. For example, in a hospital's SIoT network, only devices and systems that follow health data rules would be allowed to access and send patient data. This assures that all transactions inside the network are legal and ethical.

Furthermore, urban policies must be followed while managing *smart city environment* such as traffic systems, public lighting, and waste management. A policy-based trust paradigm guarantees that devices follow local legislation and operating guidelines. For example, a traffic sensor is only trusted to control traffic lights if it adheres to data privacy and real-time responsiveness regulations, therefore contributing to effective urban administration.

5.3. Trust management components: Analysis

Furthermore, Table 5 presents the trust management components (see Fig. 4) vis-à-vis their utilization in the selected schemes. As evident from the table, the research literature has developed some consensus on a number of these trust components (e.g., trust metrics, trust update, trust formation, trust propagation, and trust decision), and accordingly employed similar approaches. Nevertheless, the trust aggregation component is evolving and researchers are exploiting other approaches, including but not limited to machine learning, fuzzy logic, and belief theory, to handle the same. Additionally, trust-related attacks are imperative components of any trust management model, however, most of the studies have not considered providing a discussion of trust-related attacks in terms of experimental evaluation, and only a few have provided the countermeasures for almost all the trust-related attacks [50,129,137]. In general, attacks, such as OOA, BSA, and BMA are some of the attacks that have mostly been investigated in the literature. For OOA attacks, a number of studies considered monitoring the behaviour of nodes in order to identify how the behaviour of SIoT objects changes with interactions. For BSA and BMA attacks, it is considered to employ the weighting factor on the recommendations received from neighbouring nodes in the networks for BSA and to integrate both direct and indirect opinions for BMA.

On a whole, SIoT is foreseen as a network of service providers and consumers (i.e., service-oriented SIoT) with enhanced service discovery and network navigability encompassing different social relationships to employ numerous applications and services, and trust is the indispensable factor in utilizing these services in an unbiased and efficient manner. In light of the comparative analysis and discussion on different trust management schemes, a generalized high-level overview of a trustworthiness management system in SIoT is depicted in Fig. 6. The generalized trustworthiness management follows a total of five steps, wherein *step 1* provides the service requester access to a distributed table to facilitate which object (service provider) provides what service, *step 2* enables the service requester to request the trust score of the objects providing the requisite service from the trust management system, *step 3* lets the object request the service from the service provider possessing the highest trust score, and finally, in *step 4*, once the service response from the service provider is received, the service requester updates the trust score in the trust management system.

5.4. Analysis of trust management schemes

This section evaluates the trust management schemes discussed in Section 5 with a set of dimensions. The selection of these dimensions is considered based on the highly dynamic and distributed nature of the

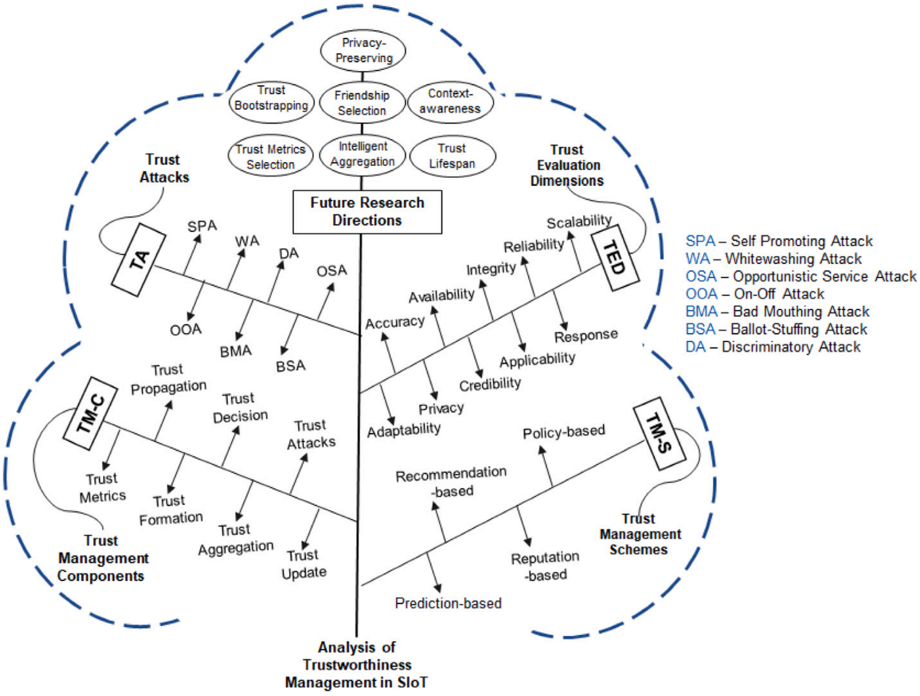


Fig. 7. Summary of trustworthiness management analysis.

SIoT network [164–166]. This section discusses the selected dimensions and the evaluation of the schemes is provided in Table 6:

Accuracy: It refers to the degree of correctness of a trust assessment, which can be ascertained via a percentage of identification of untrustworthy or malicious nodes by employing the appropriate trust evaluation methods that work well under the high percentage of malicious nodes in the network [164].

Adaptability: Owing to the dynamic nature of SIoT, the trust evaluation framework must adapt to the changes in a different context, i.e., environmental conditions, temporal factors, and energy status. Furthermore, adaptability can also be observed in terms of variation in the trust parameters, i.e., which specific trust parameters have to be used in which context and weighting each parameter accordingly in a different context [165].

Availability: The availability signifies that the network services must be available even in the presence of malicious entities. One of the objectives of providing trustworthiness management is to ensure that the malicious entities in the network have a minimum effect on the provision of network services [164].

Integrity: The network integrity implies that the content of a message is protected during the transmission between two objects. An important component of trust computation is to share the feedback and recommendations among the objects so that it could also be employed for trust score computation purposes. Thus, integrity is essential to prevent the data from being modified without consent [166].

Reliability: Reliability is the ability of a system to perform its functions in an uninterrupted manner and error-free without any failure for a particular period of time. In trust management, computation of trust and reputation from past experience can be seen as a reliable system [165].

Privacy: The privacy of an object refers to the private and confidential information disclosure during the interaction with other objects in the trust management system. The private information can be personal or activity information (e.g., the information on with whom the object interacted and the services used by the same) [166].

Scalability: This dimension is important given the dynamic and distributed nature of SIoT, which is significant for a trust management system to be scalable. Moreover, with the increase in the number of objects, accessibility and inquiries to the trust assessment results also increase, thus the trust management must be able to handle the scalable nature of SIoT [164,166].

Credibility: This dimension indicates the quality of information that makes the consumer trust the service provider. In the trust management system, credibility can refer to the object's credibility (i.e., service provider's credibility) or the credibility of the feedback for trustworthy decision-making (in the case of a system utilizing the feedback for trust computation) [164].

Applicability: This dimension signifies the specific applications for which the trust management is designed and the ability of the system to be utilized for various applications and services [164].

Response: Response refers to the response time a trust management system takes to provide the trust assessment result. It is essential for the trust management system to be prompt enough to handle many trust assessment inquiries, update the trustworthiness of an object, and propagate the trust results [164].

The evaluation of the trust management schemes vis-à-vis a set of dimensions is illustrated in Table 6. It can be observed that the recommendation-based schemes are highly accurate and scalable, nonetheless, have average performance in terms of adaptability, reliability, and applicability. Integrity, credibility, and availability remain the major concerns in these schemes. Similarly, reputation-based schemes have higher accuracy, adaptability, and reliability, however, the performance of these schemes deteriorates in terms of integrity, availability, and credibility. The prediction-based schemes are fully adaptable and are highly accurate, nonetheless, they are not reliable, have low credibility, and are less scalable. Finally, it can be observed that the policy-based schemes are highly accurate, however, these schemes demonstrate major concerns in terms of adaptability, availability, reliability, and credibility. In general, the notions of privacy, credibility, integrity, and applicability in most of the schemes have not been addressed. They nonetheless, have laid the emphasis on the response of their proposed model.

The overall discussion (and analysis) pertinent to the existing trust management schemes is illustrated in the form of a "tree" (Fig. 7), i.e., from categorizing the existing studies to future research directions.

6. Trust in SIoT-based applications

The notion of SIoT can be utilized in numerous applications by employing social relationships among participant objects, and some of these applications are discussed in this section.

6.1. Crowdsourcing

Crowdsourcing focuses on the idea of outsourcing a task to a group of people for a business production [167]. Recently, with the advancement in smartphones, and intelligent physical objects, crowdsourcing has emerged as an important platform for service-oriented IoT and is termed as *IoT crowdsourcing* where IoT objects crowdsourced the services to other IoT objects. IoT objects with sensing and communication capabilities can crowdsource a wide range of applications and services including but not limited to *computing resource* [168] where a service provider can provide computing resources to low-powered objects, *ambient sensing* [169] to sense the environment conditions, *energy sharing* to provide wireless charging to the low energy level objects [170]. IoT crowdsourced can be more efficient by exploiting social relationships between service providers and service consumers by means of fast dissemination of information through the social network of objects [171,172].

Recently, SIoT-enabled crowdsourcing on disaster reduction applications is proposed in [173] wherein the Web-based map is designed to recruit the people and their devices (e.g., smartphones, tablets) along with their social profiles to massively transmit the disaster information to provide the disaster task force with enough information for relief support. With the advantage of providing numerous applications, crowdsourcing has its challenges, and providing trustworthy crowdsourcing is one of them wherein the system must guarantee the trustworthiness of crowdsourced services before relying on the information provided by them. Wang et al. in [89] proposes a trustworthy crowdsourcing model in SIoT to cope with the issue of the trustworthiness of objects. The model considers two security aspects by encompassing a socially-aware message forwarding algorithm for social data links in SIoT, and a reputation-based mechanism to detect unreliable participants. Furthermore, a privacy-preserving incentive mechanism for crowdsourcing is proposed by Gian et al. [171] where the social relationships in terms of mutual friendship between computing entities are exploited for efficient utilization of resources and task completion. The inclusion of friendship between the workers in the large-scale SIoT not only benefits in obtaining help from friends but is also suitable for handling collaborative tasks.

In general, consumer-provider relationships enhanced the viability of crowdsourcing, however, many research challenges still need to be addressed, e.g., the trustworthiness of sensed data to prevent the use of polluted data, and the trustworthiness of task computation results to counteract the invalid results from the dishonest participant trying to save their computing resources.

6.2. Smart object recommendation

In a service-oriented SIoT environment, an object can act as the service requester as well as the service provider, and with billions of objects providing numerous services, it is significantly challenging to select the suitable objects providing the desired service, thus, the need for object recommendation and/or service recommendation appeared [174–177]. Similar to the recommendation systems in general, the service/object recommendation aims at suggesting the most relevant service to the requester.

A framework for service recommendation in SIoT is proposed in [174] wherein the social relationships among the participating objects are taken into consideration to provide the appropriate service recommendation. The employed object relationships are *co-location*, *co-work*, *social*, *co-owner*, and *parental*. Furthermore, the boundary-based community detection algorithm is also proposed to detect the social communities among the objects and to enhance the service recommendation approach. Authors in [178] delineated user recommendation schemes for data sharing in SIoT by encompassing the interaction between the SIoT objects and the user. At first, the SIoT object preference is identified in terms of their interaction analysis with users. Subsequently, user interest keywords are extracted from users' social activities. Finally, the schemes recommend the top N users by analysing the user similarity and SIoT object's preference.

A time-aware smart object recommendation model for SIoT is presented in [90] that encompasses the user's preference over a period of time and the social similarity of participating objects. Firstly, a latent probabilistic model is used to learn the user's preference in correspondence with their respective object's use. Secondly, objects' social similarity is estimated by employing their social relationships. A recommendation list is then generated that utilizes the concept of item-based collaborative filtering.

Overall, service/object recommendation will have a substantial impact on service-oriented SIoT systems. However, service/object recommendation has its own challenges including but not limited to the selection of attributes and important relationships from social activity between the objects and among the users, how to include the relationships of highly mobile objects, how to protect the privacy of objects and users, and how to integrates the concept of context while recommending the service/object.

6.3. Social Internet of Vehicles (SIoV)

The Internet of Vehicles (IoV) is the advancement in vehicular ad hoc networks (VANETs) and sensor networking techniques and is conceptualized to solve numerous challenges, including but not limited to the lack of coordination among dissimilar vehicles travelling far from one another, information insufficiency, and scalability [179]. SIoV is the modern trend of IoV [180], wherein social characteristics are integrated with the network of vehicles in a bid to offer new applications, e.g., personalized recommendation and route planning. In SIoV, a vehicle can socialize with other vehicles via sharing common interests, e.g., road situation, traffic information, weather conditions, and media sharing. Moreover, the social aspects of SIoV are not limited to vehicles only. In fact, they can include the socialization of drivers' and passengers' handheld devices, vehicular components, roadside units/infrastructures, etc [181,182]. The implementation of SIoV is still in its infancy, nevertheless, a number of research articles have been published recently in terms of trust management [183–185], computation offloading [186] and other applications of SIoV (i.e., solution for traffic congestion, precise positioning, and vehicles' location protecting) [187–189].

A trust-aware communication architecture for SIoV is proposed (*TACASHI*) in [184] comprising of five elements: (1) the vehicle, (2) vehicles' owners, (3) the passenger via his/her handheld devices, (4) roadside unit and other trust authorities, and (5) the online social network account of both drivers and passengers. Furthermore, the trust quantification process aggregates the inter-vehicular trust, roadside unit trust, location-related trust, and online social network trust. Moreover, the trust score may involve drivers' honesty based on their respective online social network profiles. Similarly, Gai et al. [185] delineates a reputation-based trust management model for SIoV, wherein each vehicle stores its reputation ascertained by other vehicles to avoid the loss of past transactions owing to a highly mobile network. Trust quantification involves multiple trust attributes aggregated together to ascertain a single trust score. The performance evaluation is carried out in terms of success rate and depicts high performance in the presence of malicious vehicles. Nevertheless, the integrity of the model has not been discussed as a malicious vehicle possesses the potential to temper its past reputation to disrupt the functionality of a network.

Furthermore, a friend-matching scheme for SIoV is proposed by Lai et al. [183] in an attempt to forbid sensitive data leakage. The designed scheme is trust-based and ensures privacy preservation and can detect malicious vehicles and efficiently estimate vehicles' credibility to protect their privacy. The scheme encompasses three phases: (1) certificate issuance and update, i.e., a pseudonym is used as a vehicle identifier; (2) trust assessment, i.e., to estimate the credibility of the messages and accordingly, rate the respective vehicle, and (3) friend matching, i.e., by employing the trust scores of neighbouring vehicles having social relationships with each other and their corresponding certificates. The performance analysis is carried out in terms of network overhead and latency. Unfortunately, the performance in terms of malicious vehicles' eviction has not been considered.

In general, the social relationships in SIoV have enhanced the viability of the IoV networks by facilitating the relationships between entities (e.g., vehicles, roadside units, and drivers' and passengers' handheld devices). These relationships are established by taking into consideration the context of the mutual interest of the network entities and can be advantageous in several ways. For instance, the transportation systems in smart cities can be further enriched with SIoV features by collecting data from vehicles based on their social relationships and by taking smart decisions through intelligent analysis. Nevertheless, the nature of SIoV poses numerous research challenges, including but not limited to the highly dynamic nature of SIoV, managing social relationships of highly mobile entities, security, privacy, and trust management, and lack of standard communication architecture.

7. SIoT simulation tools, platforms and SIoT datasets

This section collects the simulation tools utilized for SIoT and the datasets used for the performance evaluation of SIoT-based models.

7.1. SIoT simulation tools

With the extensive research in the emerging paradigm of SIoT, it is significant to identify the appropriate simulation tools that can be used to design the SIoT-specific environment by integrating the social structure of objects. There are many simulation tools (e.g., OMNET++, NS-2, Cooja) that are utilized for the IoT environment [190,191]. However, not all of them are directly used for SIoT to address the complexity of the social structure of objects. This section highlights the simulation tools used for SIoT, especially for the simulation and experimental analysis of trust management systems in SIoT. Some of the frequently used simulation tools used in the literature are discussed as follows:

7.1.1. NetLogo

NetLogo is an open-source and multi-agent programming module, which is suitable for natural, as well as social phenomena [192]. With hundreds and thousands of independent agents, a researcher can give instructions to each one of these agents to explore and analyse the micro-level behaviour of objects/individuals from their interactions. Thus, it is appropriate for complex systems like SIoT. Most recently, this simulator along with the SWIM (*Small World in Motion*) has been used by many studies to evaluate the performance of their proposed trust management systems in SIoT [50,114]. SWIM is introduced as a mobility model for ad-hoc networking to generate synthetic traces of mobility patterns to create a small world. Moreover, SWIM is also able to consider social behaviour similar to humans in real life, and is statistically proven that the synthetic traces from SWIM are similar to that of humans [193]. A few recommendation-based studies [114,135] have utilized the NetLogo simulator for experimental analysis of their work.

7.1.2. Network simulator-3 (NS-3)

NS-3 is a discrete-event open-source simulator and is the successor of NS-2 [194]. It can be employed to create realistic simulation scenarios similar to real-world devices and protocols. Furthermore, NS-3 is documented as the popular tool for network simulation due to its flexibility, utilization in different fields and applications, and adaptability to extend the resources for multiple application domains [195]. Overall, current literature suggests a number of studies on trust management have considered NS-3 simulator to validate their proposed model [113, 131].

7.1.3. Objective modular network testbed in C++ (OMNET++)

OMNET++ is another popular discrete event simulation tool extensively utilized in sensor networks research. Furthermore, OMNET++ is well-established and extensive, thus, it can integrate the external factors for specialized environment needs, e.g., to add the mobility for vehicular network [196], incorporate the social profiles of objects to enhance the application capabilities [197]. In general, due to its flexible nature, this simulation tool can be utilized in various domains and applications.

7.1.4. Others

There are numerous other well-established simulation tools that are considered in the literature for simulating the SIoT paradigm. Some of these tools are MATLAB, Python, and Microsoft Visual Studio. MATLAB is a popular multi-dimensional, multi-paradigm programming, and numerical computing platform utilized by many researchers to create models, develop algorithms, and analyse data. Besides, MATLAB has a dedicated Simulink to design and deploy IoT applications and also offers flexibility and the possibility to integrate and analyse the data from third-party IoT services/platforms (e.g., ThingSpeak [198]). Similarly, research studies in SIoT have also considered Python as a simulation environment, especially for prediction-based studies. As a whole, MATLAB and Python have been the choice for many researchers to validate the performance evaluation of many trust management systems for SIoT [86,91,107,108,146–148]. There are several other least exploited simulation tools (e.g., GlomoSim [199], Cooja [200], Lysis [201], CCNSIM [202]) that are not commonly used by researchers in the literature.

7.2. SIoT platforms

7.2.1. Lysis

It is a cloud-based hybrid platform that requires both the client software and web platform to operate and has the capability to integrate the social properties of the object. Lysis is based on a platform as a service architecture, and it has four major components; real-world layer, virtualization layer, aggregation layer, and application layer. To integrate the social properties, a social enabler component is incorporated by keeping in mind the characteristic of the SIoT paradigm that manages the social behaviour of the object in terms of relationship management, trust management among the objects, searching social virtual objects, and owners' control [201]. In essence, this platform and its architecture have been employed by various studies [203,204].

7.3. SIoT datasets

This section gives insight into the datasets currently present for evaluating the SIoT paradigm, especially, for trustworthiness management systems. Datasets are an important measure to evaluate and validate in an environment similar to real-world scenarios. Moreover, numerous datasets are available for IoT and social networks. However, these datasets cannot be directly applied to the SIoT structure. Some of the datasets utilized in the literature are discussed as follows.

The authors in [205] collect the dataset that can be used to construct the SIoT Network. This dataset is based on real IoT objects employed in Santander City of Spain, which contains a total of 16,216 devices (14,600 for private users and 1616 for the public service provider) with the description of each object in terms of id_device (Device Id), $user\_device$ (Owner Id), $device\_type$ (public or private device), $device\_brand$ (brand mapped in the form of number in range $1\ to\ 12$), and $device\_model$ (models in range $1\ to\ 24$). Furthermore, this dataset also includes the applications and services provided by each object, and the adjacency matrix providing the relationship (OOR, POR, CLOR, and SOR) between each object. In general, this dataset can be used to construct the SIoT network, nevertheless, validating the trust model is not possible as this dataset does not provide the interaction information between the device or any rating or reviews.

The frequently used dataset for evaluating the trust model in SIoT is the SIGCOMM-2009 dataset [206], which can be mapped in the form of a SIoT environment. This dataset contains information on 76 objects in terms of their social profiles (friends and the communities they are involved in) and the interaction (15,776 interactions) between them. The dataset also provides the change in the objects' social profile with respect to time. In addition, researchers have utilized other popular datasets such as Epinions [207] and Yelp[2] in combination with the SIoT dataset [205] to integrate the social structure in order to validate the performance of their trust model. Epinions is an online social network consumer review site and used to decide whether to trust each other or not, and contains more than 75,000 nodes and 500,000+ edges to describe the relationships. Finally, all the trust relationships interact and are combined with review ratings to show the reviews to the user. Similarly, Yelp is a form of social network where users can rate and review many businesses, which contains 1.6 million users, 6 million reviews, and 192,000 businesses. Besides, the Yelp dataset contains user–user relationships. Due to limited real-world datasets for evaluation and validation, most of the researchers formulate their own datasets by taking into consideration the SIoT structure given in [205]. Moreover, a few studies suggest the design of the testbeds to get the required dataset for performance evaluation [208,209].

8. Future research directions

Although the notion of trust management in the context of SIoT has been widely explored and many noteworthy results have been proposed to date, there are still numerous research challenges that need the attention of researchers. This section highlights the future research directions for trustworthiness management in SIoT.

8.1. Trust bootstrapping

Trust bootstrapping is also referred to as the *cold start problem*. It is pertinent to note that the current trust management solutions presume the initial trust score of a newly joined SIoT object to be within the range $\{0, 0.5\}$. However, most of these solutions set the initial trust score of 0.5 and classify the object as *neutral* (i.e., neither *trustworthy* nor *untrustworthy*) [113,210]. This assumption may lead a malicious SIoT object to jeopardize the basic functionality of a SIoT network before it is even identified as an untrustworthy object (or an object may perform a whitewashing attack where it changes its identity and joins the network with a new identity). Thus, it is essential to compute the initial trust of a newly enlisted SIoT object/device instead of using an arbitrary trust value. Recently, the authors in [33] propose a trust framework for crowdsourced IoT services, wherein they utilize the social relationship among the owners of the devices to compute the initial relationship strength, the reputation of the device's manufacturer as the initial reputation of that device, and the reputation of an operating system that the device is using to avoid the limitation of presumed initial trust score. Nonetheless, the proposed solution still needs to assume that the reputation of the device is present and does not take into account the notion of social similarity between a public and a private device. Decisively, the combination of attributes, including but not limited to, social characteristics, long-term history, and reputation could be employed to get the initial trust score of a newly joined SIoT object.

8.2. Friendship selection

Friendship selection is an important factor since the service discovery in the SIoT paradigm is based on the relationship of an object with its friends in a bid to explore the friends of friends providing the specific service. These relationships are established, managed, and updated by a SIoT object and therefore, it is important to identify the right number of friends to prevent the resources (e.g., storage capacity) to be utilized for managing selfish objects. Selfish objects are referred to as objects that intend to preserve their resources (e.g., energy and storage constraints), and utilize their resources for their own purpose or to enhance their reputation in the SIoT network. Furthermore, an imperative aspect of designing a trustworthiness management system for SIoT is to utilize social attributes and these attributes exploit different types of relationships amongst friends. Therefore, an efficient and appropriate friendship selection framework is required that is capable of employing different criteria to establish a number of relationships vis-à-vis different services. Moreover, the proposed framework should include a method to update the trustworthiness of existing as well as new friends to eliminate bad (e.g., selfish) friends. As of now, some possible strategies are suggested by Nitti et al. [49] for friendship selection, wherein a SIoT object sorts all of its friends in a different order by their degrees (i.e., number of friends) to select the new friends in a bid to maximize its cluster and reachability in the whole network. One possible solution could be to maintain the interaction amongst the friends and the friends with maximum interactions within a specified duration should be added to the friendship list.

8.3. SIoT specific trust metrics selection

The key characteristic of SIoT is the integration of IoT and social networks. As of late, a number of research studies consider hybrid SIoT trust metrics [142,151,211]. In fact, the basic building block of a SIoT-based trust management system is the selection of appropriate trust metrics by taking into consideration application/service criteria primarily depending on the dynamic environment (i.e., context information). Recently, a number of trust metrics are employed in some research studies [146,174], including but not limited to, similarity (e.g., friendship, community-of-interest, co-work, and co-location), cooperation between the SIoT objects (e.g., successful and unsuccessful interactions), recommendations, and reputation. However, it is not realistic to consider all the similarities for every application and service, as for a public service provider, it is not possible to ascertain the similarity score between the service consumer and the service provider. Therefore, the selection of trust metrics must follow an application's salient criteria and characteristics before designing an efficient trust management system.

8.4. Context-awareness

Trust is a complex notion and varies with context (e.g., time, location, task, and energy status). In fact, each object trusts another object in a different context [42,70]. Furthermore, owing to the dynamic nature of SIoT in terms of varied applications and services, contextual information is important as the trust management system for a specific application and/or service may not be applicable to other applications and services. A variety of context-aware trust models are proposed in the literature [91,156] suggesting different contexts with the generally considered once being time, location, and objects'

[2] https://www.yelp.com/dataset.

behaviours. However, some of the other contexts are equally important for an efficient trust management system. Therefore, it is important to design a trust model that considers not only the suitable trust metrics but also the context information in terms of where (i.e., location and environmental conditions), what (i.e., objects energy status and task), and when (i.e., temporal information) for the designed application.

8.5. Intelligent trust aggregation

Trust aggregation is an important component of trust management, wherein the selected trust metrics are aggregated to ascertain a single trust score. The conventional aggregation methods suggested in the literature [50,91] employ a linear weighted sum mechanism with randomly assigned weights, which can be either static or dynamic for each of the trust metrics. Nevertheless, the weighted sum approach has some disadvantages, including but not limited to, an infinite number of conceivable outcomes with regard to assessing a weighting factor for each metric and the inability to recognize which trust metric makes the most impact on the overall trust in a specific environment. Consequently, there is a need for an intelligent trust aggregation mechanism to overcome the limitations of conventional aggregation techniques. Lately, the idea of machine learning-based aggregation has been suggested by researchers to obtain the weights of each metric in terms of its importance [108]. However, machine learning-based solutions have their own limitations, e.g., these solutions are computationally expensive and result in increasing computational latency. One possible solution to overcome these limitations is to design an optimized machine learning-based aggregation that aggregates the trust metrics of clusters of objects instead of all the objects in the network to train the models.

8.6. Trust lifespan - decay

It is evident that the trust of a SIoT object towards another object varies with time, however, these variations are subject to decay if there are no or neutral interactions between the objects [63,86]. Owing to the SIoT intrinsic characteristic, SIoT objects during interactions may encounter many other objects, and therefore, it is not viable to store the trust of all the nodes from the past. It is imperative to consider the trust lifespan wherein the trust score of inactive SIoT objects must be subject to decay after a particular duration of time. Truong et al. [86] proposes an experience-reputation model that gives the idea of trust decay over a period of time, wherein the trust of SIoT objects declines based on a strong and weak tie (strong tie represents the strong relationship) with the other SIoT objects. However, the model does not discuss the type of relationships required for ascertaining strong and weak ties. In the SIoT paradigm, different social relationships along with the number of interactions could be utilized to manage the trust lifespan.

8.7. Privacy-preservation

It is pertinent to note that an adversary can eavesdrop on the private social profile of the owners of the objects and find the associated details of the owners using online social networks. Hence, privacy-preserving solutions are essential to address the risks involved and to promote SIoT applications and services. Moreover, there are a few notable studies in the literature pertinent to privacy-preservation for trust management in SIoT [113,142]. Chen et al. [113] utilizes the one-way hash function to encrypt the social information of nodes during the interaction, whereas Azad et al. [142] uses homomorphic encryption to protect the privacy of SIoT objects. Nevertheless, with only a few studies on privacy-preservation in SIoT, a novel and optimal framework of privacy-preserving is considered as an indispensable future research direction for trustworthy SIoT.

8.8. Integration of trust with emerging technology

Over the last decade or so, trust as a security measure has been integrated with several emerging digital technologies, i.e., blockchain and edge computing, in context of the attack detection. There are a number of studies that suggest the idea of employing blockchain for trustworthiness management in IoT/SIoT [212–215]. Most of these studies consider the use of a blockchain-based consensus mechanism in trust management systems [212,215]. However, the use of blockchain is limited to trust-related data storage and retrieval of the final trust score, and not for the quantification of the trust score. Furthermore, some studies consider smart contracts for trust evaluation, nevertheless, the smart contracts are not viable due to their availability on limited platforms [216] and their vulnerability to several attacks, i.e., DoS with block gas limit and interruption of subroutine/functions before the execution of code (reentrancy) [217].

9. Conclusion

Recently, the emerging paradigm of the Social Internet of Things (SIoT) has become a vibrant and a rapidly growing research area. Trust is considered as an impediment for the adoption of the social characteristics amongst the smart objects for establishing trustworthy social relationships and in turn for providing reliable services. In this survey, we have presented a comprehensive discussion on trustworthiness management in SIoT. At first, we classify the trustworthiness techniques into four broad categories, and the strengths and limitations of the referred studies under each of these categories are analysed and compared. We further compare the referred studies in terms of trust management components and a set of key assessment dimensions. Finally, we provide a high-level overview of the generic trust management framework for service-oriented SIoT and put forward future research directions to address various trust-related SIoT research issues.

In essence, the analysis presented in this study suggests the importance and limitations of trust management systems, particularly, for service-oriented SIoT, wherein the recruitment of trustworthy SIoT objects for collaborative activities is imperative. Moreover, ethics and regulations for SIoT in terms of the data collection and distribution, and distinguishing between the social characteristics of public and private information are still in the early stages. Therefore, it is imperative to consider the regulations and a clear understanding of social metrics, particularly, for trust quantification so as to accomplish the idea of socialization of SIoT objects, thereby truly mimicking human behaviour.

CRediT authorship contribution statement

Subhash Sagar: Writing – review & editing, Writing – original draft, Visualization, Validation, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Adnan Mahmood:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Quan Z. Sheng:** Writing – review & editing, Writing – original draft, Validation, Supervision, Resources, Funding acquisition, Conceptualization. **Wei Emma Zhang:** Writing – review & editing, Validation, Supervision, Resources. **Yang Zhang:** Writing – review & editing, Validation. **Jitander Kumar Pabani:** Writing – review & editing, Validation, Methodology.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Subhash Sagar reports was provided by Macquarie University. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] K. Ashton, That 'internet of things' thing, Comput. Commun. 22 (7) (2009) 97–114.

[2] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[3] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

[4] X. Yang, X. Wang, X. Li, D. Gu, C. Liang, K. Li, G. Zhang, J. Zhong, Exploring emerging IoT technologies in smart health research: A knowledge graph analysis, BMC Med. Inform. Decis. Mak. 20 (2020) 260.

[5] Y.A. Qadri, A. Nauman, Y.B. Zikria, A.V. Vasilakos, S.W. Kim, The future of healthcare internet of things: A survey of emerging technologies, IEEE Commun. Surv. Tutor. 22 (2) (2020) 1121–1167.

[6] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, S. Guizani, Internet-of-things-based smart cities: Recent advances and challenges, IEEE Commun. Mag. 55 (9) (2017) 16–24.

[7] Y. Qian, D. Wu, W. Bao, P. Lorenz, The internet of things for smart cities: Technologies and applications, IEEE Netw. 33 (2) (2019) 4–5.

[8] M. Alaa, A. Zaidan, B. Zaidan, M. Talal, M. Kiah, A review of smart home applications based on internet of things, J. Netw. Comput. Appl. 97 (2017) 48–65.

[9] A. Zaidan, B. Zaidan, A review on intelligent process for smart home applications based on IoT: Coherent taxonomy, motivation, open challenges, and recommendations, Artif. Intell. Rev. 53 (1) (2020) 141–165.

[10] P.K.R. Maddikunta, S. Hakak, M. Alazab, S. Bhattacharya, T.R. Gadekallu, W.Z. Khan, Q.V. Pham, Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges, IEEE Sens. J. 21 (16) (2021) 17608–17619.

[11] Statista, Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025, 2020, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. (Accessed 15 April 2020).

[12] M. Torchia, M. Kumar, V. Turner, Worldwide Semiannual Internet of Things Spending Guide, International Data Corporation (IDC), 2017.

[13] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, D. Aharon, The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Global Institute, 2015.

[14] S.A. Hamad, Q.Z. Sheng, W.E. Zhang, S. Nepal, Realizing an internet of secure things: A survey on issues and enabling technologies, IEEE Commun. Surv. Tutor. 22 (2) (2020) 1372–1391.

[15] R. Van Kranenburg, S. Dodson, The Internet of Things: A Critique of Ambient Technology and the All-seeing Network of RFID, in: Network Notebooks, Institute of Network Cultures, 2008.

[16] W.E. Zhang, Q.Z. Sheng, A. Mahmood, D.H. Tran, M. Zaib, S.A. Hamad, A. Aljubairy, A.A.F. Alhazmi, S. Sagar, C. Ma, The 10 research topics in the internet of things, in: IEEE 6th International Conference on Collaboration and Internet Computing, CIC, 2020, pp. 34–43.

[17] S.C. Mukhopadhyay, N.K. Suryadevara, in: S.C. Mukhopadhyay (Ed.), Internet of Things: Challenges and Opportunities, Springer International Publishing, Cham, 2014, pp. 1–17.

[18] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: Challenges, opportunities, and directions, IEEE Trans. Ind. Inform. 14 (11) (2018) 4724–4734.

[19] M. Hosseini Shirvani, M. Masdari, A survey study on trust-based security in internet of things: Challenges and issues, Internet Things 21 (2023) 100640.

[20] J. Kleinberg, Navigation in a small world, Nature 406 (2000) 845.

[21] J. Kleinberg, Small-world phenomena and the dynamics of information, in: Proceedings of the 14th International Conference on Neural Information Processing Systems: Natural and Synthetic, NIPS '01, 2001, pp. 431–438.

[22] M. Kranz, L. Roalter, F. Michahelles, Things that Twitter: Social networks and the internet of things, in: 8th International Conference on Pervasive Computing, PERCOM, 2010.

[23] D. Guinard, M. Fischer, V. Trifa, Sharing using social networks in a composable web of things, in: 8th IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops, 2010, pp. 702–707.

[24] H. Ning, Z. Wang, Future internet of things architecture: Like mankind neural system or social organization framework? IEEE Commun. Lett. 15 (4) (2011) 461–463.

[25] L.E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl5, H.-W. Gellersen, Smart-its friends: A technique for users to easily establish connections between smart artefacts, in: 3rd International Conference on Ubiquitous Computing, Ubicomp, 2001, pp. 116–122.

[26] L. Atzori, A. Iera, G. Morabito, SIoT: Giving a social structure to the internet of things, IEEE Commun. Lett. 15 (2011) 1193–1195.

[27] L. Atzori, A. Iera, G. Morabito, M. Nitti, The social internet of things (SIoT) – when social networks meet the internet of things: Concept, architecture, and network characterization, Comput. Netw. 56 (16) (2012) 3594–3608.

[28] R. M.S., S. Pattar, R. Buyya, V. K.R., S. Iyengar, L. Patnaik, Social internet of things (SIoT): Foundations, thrust areas, systematic review and future directions, Comput. Commun. 139 (2019) 32–57.

[29] M. Nitti, L. Atzori, I. Pletikosa, Network navigability in the social internet of things, in: IEEE World Forum on Internet of Things, WF-IoT, 2014, pp. 405–410.

[30] Z. Cai, Z. He, X. Guan, Y. Li, Collective data-sanitization for preventing sensitive information inference attacks in social networks, IEEE Trans. Dependable Secure Comput. 15 (4) (2018) 577–590.

[31] L. Nie, Y. Wu, X. Wang, L. Guo, G. Wang, X. Gao, S. Li, Intrusion detection for secure social internet of things based on collaborative edge computing: A generative adversarial network-based approach, IEEE Trans. Comput. Soc. Syst. (2021) 1–12.

[32] X. Fan, L. Liu, R. Zhang, Q. Jing, J. bi, Decentralized trust management: Risk analysis and trust aggregation, ACM Comput. Surv. 53 (2020) 1–33.

[33] M.N. Ba-hutair, A. Bouguettaya, A. Ghari Neiat, Multi-perspective trust management framework for crowdsourced IoT services, IEEE Trans. Serv. Comput. (2021) 1.

[34] Z. Li, W. Fang, C. Zhu, Z. Gao, W. Zhang, AI-enabled trust in distributed networks, IEEE Access 11 (2023) 88116–88134.

[35] A.I.A. Ahmed, S.H. Ab Hamid, A. Gani, S. khan, M.K. Khan, Trust and reputation for internet of things: Fundamentals, taxonomy, and open research challenges, J. Netw. Comput. Appl. 145 (2019) 102409.

[36] G. Fortino, L. Fotia, F. Messina, D. Rosaci, G.M.L. Sarné, Trust and reputation in the internet of things: State-of-the-art and research challenges, IEEE Access 8 (2020) 60117–60125.

[37] A. Sharma, E.S. Pilli, A.P. Mazumdar, P. Gera, Towards trustworthy internet of things: A survey on trust management applications and schemes, Comput. Commun. 160 (2020) 475–493.

[38] W. Abdelghani, C.A. Zayani, I. Amous, F. Sèdes, Trust management in social internet of things: A survey, in: 16th International Conference on E-Business, E-Services and E-Society, 2016, pp. 430–441.

[39] M.R. Rashmi, C.V. Raj, A review on trust models of social internet of things, in: Emerging Research in Electronics, Computer Science and Technology, Springer Singapore, 2019, pp. 203–209.

[40] F. Amin, A. Ahmad, G. Sang Choi, Towards trust and friendliness approaches in the social internet of things, Appl. Sci. 9 (1) (2019) 166.

[41] R.K. Chahal, N. Kumar, S. Batra, Trust management in social internet of things: A taxonomy, open issues, and challenges, Comput. Commun. 150 (2020) 13–46.

[42] W.Z. Khan, Q.-u.-A. Arshad, S. Hakak, M.K. Khan, Saeed-Ur-Rehman, Trust management in social internet of things: Architectures, recent advancements, and future challenges, IEEE Internet Things J. 8 (10) (2021) 7768–7788.

[43] P. Mendes, P.P. Mendes, Social-driven internet of connected objects, in: Internet Architecture Board (IAB) Workshop on Interconnecting Smart Objects with the Internet, 2011.

[44] O. Voutyras, P. Bourelos, D. Kyriazis, T. Varvarigou, An architecture supporting knowledge flow in social internet of things systems, in: IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob, 2014, pp. 100–105.

[45] Y. Li, Y. Huang, M. Zhang, L. Rajabion, Service selection mechanisms in the internet of things (IoT): a systematic and comprehensive study, Cluster Comput. 23 (2020) 1–21.

[46] D. Zhang, L.T. Yang, H. Huang, Searching in internet of things: Vision and challenges, in: IEEE 9th International Symposium on Parallel and Distributed Processing with Applications, 2011, pp. 201–206.

[47] R. Abdul, A. Paul, J. Gul M, W.-H. Hong, H. Seo, et al., Exploiting small world problems in a SIoT environment, Energies 11 (8) (2018) 2089.

[48] F. Amin, R. Abbasi, A. Rehman, G.S. Choi, An advanced algorithm for higher network navigation in social internet of things using small-world networks, Sensors 19 (2019) 1–20.

[49] M. Nitti, L. Atzori, I.P. Cvijikj, Friendship selection in the social internet of things: Challenges and possible strategies, IEEE Internet Things J. 2 (3) (2015) 240–247.

[50] M. Nitti, R. Girau, L. Atzori, S. Member, Trustworthiness management in the social internet of things, IEEE Trans. Knowl. Data Eng. 26 (5) (2014) 1253–1266.

[51] S. Pattar, R. Buyya, K.R. Venugopal, S.S. Iyengar, L.M. Patnaik, Searching for the IoT resources: Fundamentals, requirements, comprehensive review, and future directions, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2101–2132.

[52] D. Hussein, S. Han, G.M. Lee, N. Crespi, E. Bertin, Towards a dynamic discovery of smart services in the social internet of things, Comput. Electr. Eng. 58 (2017) 429–443, Elsevier.

[53] A. Khanfor, H. Ghazzai, Y. Yang, M.R. Haider, Y. Massoud, Automated service discovery for social internet-of-things systems, in: IEEE International Symposium on Circuits and Systems, ISCAS, 2020, pp. 1–5.

[54] M. Zhang, H. Zhao, R. Zheng, Q. Wu, W. Wei, Cognitive internet of things: Concepts and application example, Int. J. Comput. Sci. Issues (IJCSI) 9 (6) (2012) 151.

[55] W. Mardini, Y. Khamayseh, M.H. Khatatbeh, Genetic algorithm for friendship selection in social IoT, in: International Conference on Engineering MIS, ICEMIS, 2017, pp. 1–4.

[56] A. Aljubairy, W.E. Zhang, Q.Z. Sheng, A. Alhazmi, SIoTpredict: A framework for predicting relationships in the social internet of things, in: Advanced Information Systems Engineering, 2020, pp. 101–116.

[57] R. Hardin, Trust: A sociological theory, Econ. Philos. 18 (2002) 183–204.

[58] B.R. Schlenker, B. Helm, J.T. Tedeschi, The effects of personality and situational variables on behavioral trust, J. Pers. Soc. Psychol. 25 (3) (1973) 419.

[59] R.M. Morgan, S.D. Hunt, The commitment-trust theory of relationship marketing, J. Market. 58 (3) (1994) 20–38.

[60] S. A., S. Vairavasundaram, K. Kotecha, I. V., L. Ravi, G. Selvachandran, A. Abraham, Blockchain-based trust mechanism for digital twin empowered industrial internet of things, Future Gener. Comput. Syst. 141 (2023) 16–27.

[61] A. Mahmood, S.A. Siddiqui, W.E. Zhang, Q.Z. Sheng, A hybrid trust management model for secure and resource efficient vehicular ad hoc networks, in: IEEE 20th International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT, 2019, pp. 154–159.

[62] J. Bai, Z. Zeng, T. Wang, S. Zhang, N.N. Xiong, A. Liu, TANTO: An effective trust-based unmanned aerial vehicle computing system for the internet of things, IEEE Internet Things J. 10 (7) (2023) 5644–5661.

[63] R. Hussain, J. Lee, S. Zeadally, Trust in VANET: A survey of current solutions and future research opportunities, IEEE Trans. Intell. Transp. Syst. 22 (5) (2021) 2553–2571.

[64] X. Meng, D. Liu, Getrust: A guarantee-based trust model in chord-based P2P networks, IEEE Trans. Dependable Secure Comput. 15 (1) (2018) 54–68.

[65] S.M. Ghafari, A. Beheshti, A. Joshi, C. Paris, A. Mahmood, S. Yakhchi, M.A. Orgun, A survey on trust prediction in online social networks, IEEE Access 8 (2020) 144292–144309.

[66] Y. Cen, J. Zhang, G. Wang, Y. Qian, C. Meng, Z. Dai, H. Yang, J. Tang, Trust relationship prediction in Alibaba E-commerce platform, IEEE Trans. Knowl. Data Eng. 32 (5) (2020) 1024–1035.

[67] A. Mahmood, Q.Z. Sheng, S.A. Siddiqui, S. Sagar, W.E. Zhang, H. Suzuki, W. Ni, When trust meets the internet of vehicles: Opportunities, challenges, and future prospects, in: IEEE 7th International Conference on Collaboration and Internet Computing, CIC, 2021, pp. 1–8.

[68] W. Li, H. Song, ART: An attack-resistant trust management scheme for securing vehicular Ad Hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) (2016) 960–969.

[69] H. Rahimi, H. El Bakkali, A new reputation algorithm for evaluating trustworthiness in E-commerce context, in: Proceeding of National Security Days, JNS3, 2013, pp. 1–6.

[70] W. Sherchan, S. Nepal, C. Paris, A survey of trust in social networks, ACM Comput. Surv. 45 (4) (2013) 1–33.

[71] R. Swedberg, On the use of definitions in sociology, Eur. J. Soc. Theory 23 (3) (2020) 431–445.

[72] M. Deutsch, Cooperation and trust: Some theoretical notes, in: Nebraska Symposium on Motivation, University of Nebraska Press, 1962, pp. 275–319.

[73] J. Jalava, From norms to trust: The luhmannian connections between trust and system, Eur. J. Soc. Theory 6 (2) (2003) 173–190.

[74] A.B. Seligman, The Problem of Trust, Princeton University Press, 2000.

[75] G.R. Henriques, Psychology defined, J. Clin. Psychol. 60 (12) (2004) 1207–1221.

[76] D.M. Rousseau, S.B. Sitkin, R.S. Burt, C. Camerer, Not so different after all: A cross-discipline view of trust, Acad. Manag. Rev. 23 (3) (1998) 393–404.

[77] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2) (2007) 618–644.

[78] R. Backhouse, S. Medema, On the definition of economics, J. Econ. Perspect. 23 (2009) 221–233.

[79] S. Ba, P. Pavlou, Evidence OF the effect of trust building technology in electronic markets: Price premiums and buyer behavior, Manag. Inf. Syst. 26 (2002) 243–268.

[80] J. Riegelsberger, M.A. Sasse, J.D. McCarthy, Shiny happy people building trust? Photos on E-commerce websites and consumer trust, in: Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems, 2003, pp. 121–128.

[81] K. Arai, Trust and trustworthiness in the economy: How they function and how they should be promoted, Hitotsubashi J. Econ. 48 (2007).

[82] D. Artz, Y. Gil, A survey of trust in computer science and the semantic web, J. Web Semant. 5 (2) (2007) 58–71.

[83] R.H.R. Harper, Trust, Computing, and Society, Cambridge University Press, 2014.

[84] W. Harwood, The Logic of Trust (Ph.D. thesis), University of York, 2012.

[85] K. Thompson, Reflections on trusting trust, Commun. ACM 27 (8) (1984) 761–763.

[86] N.B. Truong, T. Um, B. Zhou, G.M. Lee, From personal experience to global reputation for trust evaluation in the social internet of things, in: IEEE Global Communications Conference, GLOBECOM, 2017, pp. 1–7.

[87] N.B. Truong, H. Lee, B. Askwith, G.M. Lee, Toward a trust evaluation mechanism in the social internet of things, Sensors 17 (6) (2017).

[88] R. Iqbal, T.A. Butt, M. Afzaal, K. Salah, Trust management in social internet of vehicles: Factors, challenges, blockchain, and fog solutions, Int. J. Distrib. Sens. Netw. 15 (1) (2019) 1–22.

[89] K. Wang, X. Qi, L. Shu, D. Deng, J.J.P.C. Rodrigues, Toward trustworthy crowdsourcing in the social internet of things, IEEE Wirel. Commun. 23 (5) (2016) 30–36.

[90] Y. Chen, M. Zhou, Z. Zheng, D. Chen, Time-aware smart object recommendation in social internet of things, IEEE Internet Things J. 7 (3) (2020) 2014–2027.

[91] M. Khani, Y. Wang, M.A. Orgun, F. Zhu, Context-aware trustworthy service evaluation in social internet of things, in: International Conference on Service-Oriented Computing, ICSOC, 2018, pp. 129–145.

[92] N. Truong, H. Lee, B. Askwith, G.M. Lee, Toward a trust evaluation mechanism in the social internet of things, Sensors 17 (2017) 1346.

[93] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134.

[94] C. Marche, L. Serreli, M. Nitti, Analysis of feedback evaluation for trust management models in the internet of things, IoT 2 (3) (2021) 498–509, http://dx.doi.org/10.3390/iot2030025.

[95] I.P. Stanimirovic, M.L. Zlatanovic, M.D. Petkovic, On the linear weighted sum method for multi-objective optimization, Facta Acta Univ. 26 (4) (2011) 49–63.

[96] I.Y. Kim, O. De Weck, Adaptive weighted sum method for multi-objective optimization: a new method for Pareto front generation, Struct. Multidiscip. Optim. 31 (2) (2006) 105–116.

[97] R.T. Marler, J.S. Arora, The weighted sum method for multi-objective optimization: New insights, Struct. Multidiscip. Optim. 41 (6) (2010) 853–862.

[98] L. Liu, R.R. Yager, Classic works of the Dempster-Shafer theory of belief functions: An introduction, in: R.R. Yager, L. Liu (Eds.), Classic Works of the Dempster-Shafer Theory of Belief Functions, Springer Berlin Heidelberg, 2008, pp. 1–34.

[99] K. Sentz, S. Ferson, Combination of Evidence in Dempster-Shafer Theory, Sandia National Laboratories, California, 2002.

[100] M. Beynon, B. Curry, P. Morgan, The Dempster–Shafer theory of evidence: An alternative approach to multicriteria decision modelling, Omega 28 (1) (2000) 37–50.

[101] A. Jøsang, R. Ismail, The beta reputation system, in: Proceedings of the 15th Bled Conference on Electronic Commerce, 2002.

[102] K. Weise, W. Woger, A Bayesian theory of measurement uncertainty, Meas. Sci. Technol. 4 (1) (1993) 1.

[103] J.M. Bernardo, A.F. Smith, Bayesian Theory, Vol. 405, John Wiley & Sons, 2009.

[104] P.N. Mahalle, P.A. Thakre, N.R. Prasad, R. Prasad, A fuzzy approach to trust based access control in internet of things, in: International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE, 2013, pp. 1–5.

[105] L.A. Zadeh, Fuzzy sets, in: Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems: Selected Papers by Lotfi a Zadeh, World Scientific, 1996, pp. 394–432.

[106] J. Carbo, J.M. Molina, J. Davila, Trust management through fuzzy reputation, Int. J. Coop. Inf. Syst. 12 (01) (2003) 135–155.

[107] U. Jayasinghe, G.M. Lee, T. Um, Q. Shi, Machine learning based trust computational model for IoT services, IEEE Trans. Sustain. Comput. 4 (1) (2019) 39–52.

[108] S. Sagar, A. Mahmood, Q.Z. Sheng, W.E. Zhang, Trust computational heuristic for social internet of things: A machine learning-based approach, in: Proceeding of IEEE International Conference on Communications, ICC, 2020, pp. 1–6.

[109] S.A. Siddiqui, A. Mahmood, W.E. Zhang, Q.Z. Sheng, Machine learning based trust model for misbehaviour detection in internet-of-vehicles, in: International Conference on Neural Information Processing, ICONIP, 2019, pp. 512–520.

[110] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami, C.-T. Lu, LogitTrust : A logit regression-based trust model for mobile Ad Hoc networks, in: 6th ASE/IEEE International Conference on Privacy, Security, Risk and Trust, 2014.

[111] R. Venkataraman, M. Pushpalatha, T.R. Rao, Regression-based trust model for mobile Ad Hoc networks, IET Inf. Secur. 6 (3) (2012) 131–140.

[112] U. Jayasinghe, H.-W. Lee, G.M. Lee, A computational model to evaluate honesty in social internet of things, in: Proceedings of the Symposium on Applied Computing, 2017, pp. 1830–1835.

[113] I. Chen, F. Bao, J. Guo, Trust-based service management for social internet of things systems, IEEE Trans. Dependable Secure Comput. 13 (6) (2016) 684–696.

[114] H. Xia, F. Xiao, S. Zhang, C. Hu, X. Cheng, Trustworthiness inference framework in the social internet of things: A context-aware approach, in: Proceeding of IEEE Conference on Computer Communications, INFOCOM, 2019, pp. 838–846.

[115] X. Li, G. Zhu, Y. Gong, K. Huang, Wirelessly powered data aggregation for IoT via over-the-air function computation: Beamforming and power control, IEEE Trans. Wireless Commun. 18 (7) (2019) 3437–3452.

[116] X. Sun, N. Ansari, Dynamic resource caching in the IoT application layer for smart cities, IEEE Internet Things J. 5 (2) (2018) 606–613.

[117] H. Xiao, N. Sidhu, B. Christianson, Guarantor and reputation based trust model for social internet of things, in: International Wireless Communications and Mobile Computing Conference, IWCMC, 2015, pp. 600–605.

[118] I. Chen, J. Guo, F. Bao, Trust management for SOA-based IoT and its application to service composition, IEEE Trans. Serv. Comput. 9 (3) (2016) 482–495.

[119] C.V.L. Mendoza, J.H. Kleinschmidt, Mitigating on-off attacks in the internet of things using a distributed trust management scheme, Int. J. Distrib. Sens. Netw. 11 (11) (2015) 1–8.

[120] A.A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A. MacDermott, X. Wang, CTRUST: A dynamic trust model for collaborative applications in the internet of things, IEEE Internet Things J. 6 (3) (2019) 5432–5445.

[121] B. Yu, M.P. Singh, An evidential model of distributed reputation management, in: Proceedings of the ACM 1st International Joint Conference on Autonomous Agents and Multiagent Systems, 2002, pp. 294–301.

[122] F. Bao, I. Chen, J. Guo, Scalable, adaptive and survivable trust management for community of interest based internet of things systems, in: 11th IEEE International Symposium on Autonomous Decentralized Systems, ISADS, 2013, pp. 1–7.

[123] S. Sagar, A. Mahmood, J. Kumar, Q.Z. Sheng, A time-aware similarity-based trust computational model for social internet of things, in: IEEE Global Communications Conference, GlobeCom, 2020, pp. 1–6.

[124] Z. Chen, R. Ling, C.-M. Huang, X. Zhu, A scheme of access service recommendation for the social internet of things, Int. J. Commun. Syst. 29 (4) (2016) 694–706.

[125] I. Garcia-Magarino, S. Sendra, R. Lacuesta, J. Lloret, Security in vehicles with IoT by prioritization rules, vehicle certificates, and trust management, IEEE Internet Things J. 6 (4) (2019) 5927–5934.

[126] S. Namal, H. Gamaarachchi, G. MyoungLee, T. Um, Autonomic trust management in cloud-based and highly dynamic IoT applications, in: ITU Kaleidoscope: Trust in the Information Society, 2015, pp. 1–8.

[127] S.A. Siddiqui, A. Mahmood, Q.Z. Sheng, H. Suzuki, W. Ni, A survey of trust management in the internet of vehicles, Electronics 10 (18) (2021) 2223.

[128] M. Masmoudi, W. Abdelghani, I. Amous, F. Sèdes, Deep learning for trust-related attacks detection in social internet of things, in: Advances in E-Business Engineering for Ubiquitous Computing, Springer International Publishing, 2020, pp. 389–404.

[129] C. Marche, M. Nitti, Trust-related attacks and their detection: A trust management model for the social IoT, IEEE Trans. Netw. Serv. Manag. 18 (3) (2021) 3297–3308.

[130] A. Chakrabarti, Managing trust in the grid, in: Grid Computing Security, Springer Berlin Heidelberg, 2007, pp. 215–246.

[131] H. Al-Hamadi, I.R. Chen, Trust-based decision making for health IoT systems, IEEE Internet Things J. 4 (5) (2017) 1408–1419.

[132] W. Li, H. Song, F. Zeng, Policy-based secure and trustworthy sensing for internet of things in smart cities, IEEE Internet Things J. 5 (2) (2018) 716–723.

[133] V. Mohammadi, A. Rahmani, A. Darwesh, A. Sahafi, Trust-based recommendation systems in internet of things: a systematic literature review, Hum.-Cent. Comput. Inf. Sci. 9 (2019) 1–61.

[134] A.R. Sfar, E. Natalizio, Y. Challal, Z. Chtourou, A roadmap for security challenges in the internet of things, Digit. Commun. Netw. 4 (2) (2018) 118–137.

[135] L. Wei, J. Wu, C. Long, B. Li, On designing context-aware trust model and service delegation for social internet of things, IEEE Internet Things J. 8 (6) (2021) 4775–4787.

[136] S. Pourmohseni, M. Ashtiani, A. Akbari Azirani, A computational trust model for social IoT based on interval neutrosophic numbers, Inform. Sci. 607 (2022) 758–782.

[137] W. Abdelghani, I. Amous, C.A. Zayani, F. Sèdes, G. Roman-Jimenez, Dynamic and scalable multi-level trust management model for social internet of things, J. Supercomput. 78 (6) (2022) 8137–8193.

[138] L. Wei, Y. Yang, J. Wu, C. Long, Y.-B. Lin, A bidirectional trust model for service delegation in social internet of things, Future Internet 14 (2022) 135.

[139] S. Zhang, D. Zhang, Y. Wu, H. Zhong, Service recommendation model based on trust and QoS for social internet of things, IEEE Trans. Serv. Comput. (2023) 1–14.

[140] M. Amiri-Zarandi, R.A. Dara, E. Fraser, LBTM: A lightweight blockchain-based trust management system for social internet of things, J. Supercomput. 78 (6) (2022) 8302–8320.

[141] A. Rehman, K.A. Awan, I. Ud Din, A. Almogren, M. Alabdulkareem, FogTrust: Fog-integrated multi-leveled trust management mechanism for internet of things, Technologies 11 (1) (2023) 27.

[142] M.A. Azad, S. Bag, F. Hao, A. Shalaginov, Decentralized self-enforcing trust management system for social internet of things, IEEE Internet Things J. 7 (4) (2020) 2690–2703.

[143] N. Truong, G.M. Lee, A reputation and knowledge based trust service platform for trustworthy social internet of things, in: 19th International Conference on Innovations in Clouds, Internet and Networks, ICIN, 2016, pp. 1–8.

[144] S. Rajendran, R. Jebakumar, Friendliness based trustworthy relationship management (F-TRM) in social internet of things, Wirel. Pers. Commun. 123 (3) (2022) 2625–2647.

[145] C. Lewis, N. Li, V. Varadharajan, Targeted context-based attacks on trust management systems in IoT, IEEE Internet Things J. 10 (14) (2023) 12186–12203.

[146] S. Aalibagi, H. Mahyar, A. Movaghar, H.E. Stanley, A matrix factorization model for hellinger-based trust management in social internet of things, IEEE Trans. Dependable Secure Comput. (2021) 1.

[147] S. Sagar, A. Mahmood, M. Zaib, Q.Z. Sheng, W.E. Zhang, Towards a machine learning-driven trust evaluation model for social internet of things: A time-aware approach, in: 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous, 2020, pp. 283–290.

[148] S. Sagar, A. Mahmood, K. Wang, Q.Z. Sheng, J.K. Pabani, W.E. Zhang, Trust–SIoT: Toward trustworthy object classification in the social internet of things, IEEE Trans. Netw. Serv. Manag. 20 (2) (2023) 1210–1223.

[149] R. Magdich, H. Jemal, M. Ben Ayed, Context-awareness trust management model for trustworthy communications in the social internet of things, Neural Comput. Appl. 34 (24) (2022) 21961–21986.

[150] R. Magdich, H. Jemal, M.B. Ayed, A resilient trust management framework towards trust related attacks in the social internet of things, Comput. Commun. 191 (2022) 92–107.

[151] J.I.-Z. Chen, Embedding the MRC and SC schemes into trust management algorithm applied to IoT security protection, Wirel. Pers. Commun. 99 (1) (2018) 461–477.

[152] P. De Meo, L. Fotia, F. Messina, D. Rosaci, G.M. Sarne, Providing recommendations in social networks by integrating local and global reputation, Inf. Syst. 78 (2018) 58–67.

[153] B. Jafarian, N. Yazdani, M. Sayad Haghighi, Discrimination-aware trust management for social internet of things, Comput. Netw. 178 (2020) 107254.

[154] U. Jayasinghe, N.B. Truong, G.M. Lee, T.-W. Um, Rpr: A trust computation model for social internet of things, in: IEEE International Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld, 2016, pp. 930–937.

[155] R. Latif, ConTrust: A novel context-dependent trust management model in social internet of things, IEEE Access 10 (2022) 46526–46537.

[156] H. Xia, S. Zhang, Y. Li, Z. Pan, X. Peng, X. Cheng, An attack-resistant trust inference model for securing routing in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 68 (7) (2019) 7108–7120.

[157] Z. Yu, D. Jin, C. Huo, Z. Wang, X. Liu, H. Qi, J. Wu, L. Wu, KGTrust: Evaluating trustworthiness of SIoT via knowledge enhanced graph neural networks, in: Proceedings of the ACM Web Conference, 2023, pp. 727–736.

[158] C. Marche, L. Atzori, M. Nitti, A dataset for performance analysis of the social internet of things, in: IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, 2018, pp. 1–5.

[159] M.B. Monir, M.H. Abdel Aziz, A.A. Abdel Hamid, E.M. EI-Horbaty, Trust management in cloud computing: A survey, in: IEEE 7th International Conference on Intelligent Computing and Information Systems, ICICIS, 2015, pp. 231–242.

[160] Q.H. Cao, M. Giyyarpuram, R. Farahbakhsh, N. Crespi, Policy-based usage control for a trustworthy data sharing platform in smart cities, Future Gener. Comput. Syst. 107 (2020) 998–1010.

[161] L. Gu, J. Wang, B. Sun, Trust management mechanism for internet of things, China Commun. 11 (2) (2014) 148–156.

[162] W.Z. Khan, M.Y. Aalsalem, M.K. Khan, Q. Arshad, When social objects collaborate: Concepts, processing elements, attacks and challenges, Comput. Electr. Eng. 58 (2017) 397–411.

[163] A. Zamanifar, Social IoT healthcare, in: Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications: Emerging Technologies for Connected and Smart Social Objects, Springer International Publishing, Cham, 2020, pp. 1–11.

[164] T.H. Noor, Q.Z. Sheng, S. Zeadally, J. Yu, Trust management of services in cloud environments: Obstacles and solutions, ACM Comput. Surv. 46 (1) (2013) 1–30.

[165] F. Fraile, T. Tagawa, R. Poler, A. Ortiz, Trustworthy industrial IoT gateways for interoperability platforms and ecosystems, IEEE Internet Things J. 5 (6) (2018) 4506–4514.

[166] B. Pourghebleh, K. Wakil, N.J. Navimipour, A comprehensive study on the trust management techniques in the internet of things, IEEE Internet Things J. 6 (6) (2019) 9326–9337.

[167] Howe, Jeff, The rise of crowdsourcing, Wired 14 (2006) 1–4.

[168] K. Habak, M. Ammar, K.A. Harras, E. Zegura, Femto clouds: Leveraging mobile devices to provide cloud service at the edge, in: IEEE 8th International Conference on Cloud Computing, 2015, pp. 9–16.

[169] S.D.T. Kelly, N.K. Suryadevara, S.C. Mukhopadhyay, Towards the implementation of IoT for environmental condition monitoring in homes, IEEE Sens. J. 13 (10) (2013) 3846–3853.

[170] E. Bulut, S. Hernandez, A. Dhungana, B.K. Szymanski, Is crowdcharging possible? in: 27th International Conference on Computer Communication and Networks, ICCCN, 2018, pp. 1–9.

[171] X. Gan, Y. Li, Y. Huang, L. Fu, X. Wang, When crowdsourcing meets social IoT: An efficient privacy-preserving incentive mechanism, IEEE Internet Things J. 6 (2019) 9707–9721.

[172] H. Cui, J. Liao, Z. Yu, Y. Xie, X. Liu, B. Guo, Trust assessment for mobile crowdsensing via device fingerprinting, ISA Trans. (2023).

[173] C.-H. Liu, C.-F. Chiang, Social IoT crowd-sourcing on disaster reduction, in: Encyclopedia of Wireless Networks, Springer Berlin Heidelberg, 2019, pp. 1–6.

[174] A. Khelloufi, H. Ning, S. Dhelim, T. Qiu, J. Ma, R. Huang, L. Atzori, A social-relationships-based service recommendation system for SIoT devices, IEEE Internet Things J. 8 (3) (2021) 1859–1870.

[175] Q.Z. Sheng, J. Yu, W.E. Zhang, S. Wang, X. Li, B. Benatallah, Designing and building context-aware services: The ContextServ project, in: Next-Gen Digital Services. A Retrospective and Roadmap for Service Computing of the Future, Springer International Publishing, 2021, pp. 138–152.

[176] H. Zhang, L. Zhu, T. Dai, L. Zhang, X. Feng, L. Zhang, K. Zhang, Smart object recommendation based on topic learning and joint features in the social internet of things, Digit. Commun. Netw. 9 (1) (2023) 22–32.

[177] A. Khelloufi, H. Ning, A.B. Sada, A. Naouri, S. Dhelim, Context-aware service recommendation system for the social internet of things, 2023, arXiv preprint arXiv:2308.08499.

[178] K. Bok, Y. Kim, D. Choi, J. Yoo, User recommendation for data sharing in social internet of things, Sensors 21 (2) (2021) 462.

[179] A. Mahmood, W. Zhang, Q. Sheng, Software-defined heterogeneous vehicular networking: The architectural design and open challenges, Future Internet 11 (3) (2019) 70.

[180] M. Nitti, R. Girau, A. Floris, L. Atzori, On adding the social dimension to the internet of vehicles: Friendship and middleware, in: IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom, 2014, pp. 134–138.

[181] T.A. Butt, R. Iqbal, S.C. Shah, T. Umar, Social internet of vehicles: Architecture and enabling technologies, Comput. Electr. Eng. 69 (2018) 68–84.

[182] L. Atzori, A. Floris, R. Girau, M. Nitti, G. Pau, Towards the implementation of the social internet of vehicles, Comput. Netw. 147 (2018) 132–145.

[183] L. Chengzhe, D. Yangyang, G. Qili, Z. Dong, A trust-based privacy-preserving friend matching scheme in social internet of vehicles, Peer-to-Peer Netw. Appl. 14 (2021) 2011–2025.

[184] C.A. Kerrache, N. Lagraa, R. Hussain, S.H. Ahmed, A. Benslimane, C.T. Calafate, J.-C. Cano, A.M. Vegni, TACASHI: Trust-aware communication architecture for social internet of vehicles, IEEE Internet Things J. 6 (4) (2019) 5870–5877.

[185] F. Gai, J. Zhang, P. Zhu, X. Jiang, Trust on the ratee: A trust management system for social internet of vehicles, Wirel. Commun. Mob. Comput. 2017 (2017) 1–11.

[186] U. Javaid, B. Sikdar, A secure and scalable framework for blockchain based edge computation offloading in social internet of vehicles, IEEE Trans. Veh. Technol. 70 (5) (2021) 4022–4036.

[187] T. Wang, A. Hussain, L. Zhang, C. Zhao, Collaborative edge computing for social internet of vehicles to alleviate traffic congestion, IEEE Trans. Comput. Soc. Syst. (2021) 1–13.

[188] X. Kong, H. Gao, G. Shen, G. Duan, S.K. Das, FedVCP: A federated-learning-based cooperative positioning scheme for social internet of vehicles, IEEE Trans. Comput. Soc. Syst. (2021) 1–10.

[189] L. Xing, X. Jia, J. Gao, H. Wu, A location privacy protection algorithm based on double K-anonymity in the social internet of vehicles, IEEE Commun. Lett. 25 (10) (2021) 3199–3203.

[190] E. Ojie, E. Pereira, Simulation tools in internet of things: A review, in: Proceedings of the 1st ACM International Conference on Internet of Things and Machine Learning, 2017, pp. 1–7.

[191] M. Chernyshev, Z. Baig, O. Bello, S. Zeadally, Internet of things (IoT): Research, simulators, and testbeds, IEEE Internet Things J. 5 (3) (2018) 1637–1647.

[192] U. Wilensky, NetLogo, 1999, https://ccl.northwestern.edu/netlogo/. Online (Accessed 10 March 2021).

[193] A. Mei, J. Stefa, SWIM: A simple model to generate small mobile worlds, in: IEEE International Conference on Computer Communications, INFOCOM, 2009, pp. 2106–2113.

[194] G.F. Riley, T.R. Henderson, The NS-3 network simulator, in: Modeling and Tools for Network Simulation, Springer, 2010, pp. 15–34.

[195] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, M. Mastroianni, Computer network simulation with NS-3: A systematic literature review, Electronics 9 (2020) 272.

[196] Veins, Veins, 2022, https://veins.car2x.org/. Online (Accessed 10 March 2021).

[197] P. Deshpande, P. Kodeswaran, N. Banerjee, A. Nanavati, D. Chhabra, S. Kapoor, M4M: A model for enabling social network based sharing in the internet of things, in: 7th International Conference on Communication Systems and Networks, COMSNETS, 2015, pp. 1–8.

[198] ThingSpeak, ThingSpeak, internet of things, 2021, https://thingspeak.com/. (Accessed 15 March 2021).

[199] X. Zeng, R. Bagrodia, M. Gerla, GloMoSim: A library for parallel simulation of large-scale wireless networks, ACM SIGSIM Simul. Dig. 28 (1) (1998) 154–161.

[200] A. Dunkels, B. Gronvall, T. Voigt, Contiki - a lightweight and flexible operating system for tiny networked sensors, in: Proceedings of the 29th IEEE International Conference on Local Computer Networks, LCN, 2004, pp. 455–462.

[201] R. Girau, S. Martis, L. Atzori, Lysis: A platform for IoT distributed applications over socially connected objects, IEEE Internet Things J. 4 (1) (2016) 40–51.

[202] S. Mohana, S.S. Prakash, K. Krinkin, CCNSim: An artificial intelligence enabled classification, clustering and navigation simulator for social internet of things, Eng. Appl. Artif. Intell. 119 (2023) 105745.

[203] G. Delnevo, R. Girau, C. Ceccarini, C. Prandi, A deep learning and social iot approach for plants disease prediction toward a sustainable agriculture, IEEE Internet Things J. 9 (10) (2022) 7243–7250.

[204] C. Marche, G.G. Soma, M. Nitti, A cognitive social iot approach for smart energy management in a real environment, IEEE Trans. Netw. Serv. Manag. 20 (4) (2023) 4061–4072.

[205] C. Marche, L. Atzori, V. Pilloni, M. Nitti, How to exploit the social internet of things: Query generation model and device profiles' dataset, Comput. Netw. 174 (2020) 107248.

[206] A.K. Pietilainen, C. Diot, CRAWDAD dataset thlab/sigcomm2009 (version: 2012-07-15), 2012, Downloaded from https://crawdad.org/thlab/sigcomm2009/20120715.

[207] M. Richardson, R. Agrawal, P. Domingos, Trust management for the semantic web, in: International Semantic Web Conference, ISWC, 2003, pp. 351–368.

[208] Z. Lin, L. Dong, Clarifying trust in social internet of things, IEEE Trans. Knowl. Data Eng. 30 (2) (2018) 234–248.

[209] S. Sagar, A. Mahmood, Q.Z. Sheng, S.A. Siddiqui, SCaRT-SIoT: Towards a scalable and robust trust platform for social internet of things: Demo abstract, in: Proceedings of the 18th ACM International Conference on Embedded Networked Sensor Systems, SenSys, 2020, pp. 635–636.

[210] O. Ben Abderrahim, M.H. Elhdhili, L. Saidane, TMCoI-SIOT: A trust management system based on communities of interest for the social internet of things, in: 2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC, 2017, pp. 747–752.

[211] N. Li, V. Varadharajan, S. Nepal, Context-aware trust management system for IoT applications with multiple domains, in: IEEE 39th International Conference on Distributed Computing Systems, ICDCS, 2019, pp. 1138–1148.

[212] L. Xie, Y. Ding, H. Yang, X. Wang, Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs, IEEE Access 7 (2019) 56656–56666, http://dx.doi.org/10.1109/ACCESS.2019.2913682.

[213] R. Latif, B. Yakubu, T. Saba, MarketTrust: blockchain-based trust evaluation model for SIoT-based smart marketplaces, Sci. Rep. 13 (2023).

[214] D.E. Kouicem, Y. Imine, A. Bouabdallah, H. Lakhlef, Decentralized blockchain-based trust management protocol for the internet of things, IEEE Trans. Dependable Secure Comput. 19 (2) (2022) 1292–1306.

[215] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, J. Zhang, A semi-centralized trust management model based on blockchain for data exchange in IoT system, IEEE Trans. Serv. Comput. 16 (2) (2023) 858–871, http://dx.doi.org/10.1109/TSC.2022.3181668.

[216] R. Di Pietro, X. Salleras, M. Signorini, E. Waisbard, A blockchain-based trust system for the internet of things, in: Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, 2018, pp. 77–83.

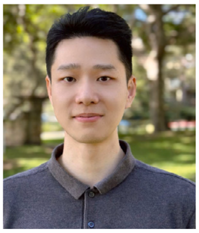
[217] R. Han, Z. Yan, X. Liang, L.T. Yang, How can incentive mechanisms and blockchain benefit with each other? A survey, ACM Comput. Surv. 55 (7) (2022).

Subhash Sagar holds a PhD from Macquarie University, Sydney, Australia. He has shared his expertise as an Associate Research Fellow at Deakin University and as a Lecturer at the Victorian Institute of Technology. Previously, Subhash served as a faculty member at the Department of Computer Science, National University of Computer and Emerging Sciences, Karachi, Pakistan. His research interests encompass the Internet of Things, Social Internet of Things, and Trust Management, evident in his numerous publications in prestigious journals and conferences. With around 20 publications in reputable conferences and journals. Subhash actively contributes to academia. He engages as a reviewer for esteemed publications like IEEE Networking Letters, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Vehicular Technology, and MDPI Sensors, and serves as a Technical Program Committee member and reviewer for notable conferences.

Adnan Mahmood holds a PhD degree in Computer Science and is a Lecturer at the School of Computing, Macquarie University, Sydney, Australia. Before moving to Macquarie University, Adnan has spent a considerable number of years in the academic and research settings of the Republic of Ireland, Malaysia, Pakistan, and the People's Republic of China. His research interests include Software Defined Networking, Internet of Things, Internet of Vehicles, Trust Management, and the Next Generation Heterogeneous Wireless Networks. Adnan besides serves on the Technical Program Committees of a number of reputed International Conferences. He is also a member of the IEEE and the ACM.

Quan Z. (Michael) Sheng is a Distinguished Professor and Head of School of Computing at Macquarie University, Australia. Before moving to Macquarie University, Michael spent 10 years at School of Computer Science, the University of Adelaide, serving in a number of senior leadership roles including interim Head and Deputy Head of School of Computer Science. Michael holds a PhD degree in computer science from the University of New South Wales (UNSW) and did his post-doc as a research scientist at CSIRO ICT Centre. From 1999 to 2001, Michael worked at UNSW as a visiting research fellow. Prior to that, he spent six years as a senior software engineer in industries. Prof. Sheng is ranked by Microsoft Academic as one of the Most Impactful Authors in Services Computing (ranked Top 5 of All Time worldwide) and in the Web of Things (ranked Top 20 All Time). He is the recipient of the AMiner Most Influential Scholar Award on IoT (2007-2017), ARC (Australian Research Council) Future Fellowship (2014), Chris Wallace Award for Outstanding Research Contribution (2012), and Microsoft Research Fellowship (2003). Prof Michael Sheng is the Vice Chair of the Executive Committee of the IEEE Technical Community on Services Computing (IEEE TCSVC) and a member of the ACS (Australian Computing Society) Technical Advisory Board on IoT.

Wei (Emma) Zhang is currently a Lecturer at the School of Computer Science, The University of Adelaide. She obtained her Ph.D. in 2017 from the School of Computer Science, The University of Adelaide. Her research interests include text mining, deep learning, natural language processing, information retrieval, and Internet of Things (IoT) applications. She has close to 100 publications to date as edited books and proceedings, refereed book chapters, and refereed technical papers in journals and conferences including ACM Computing Surveys, TOIT, ACM TIST, WWWJ, Communications of the ACM, ACL, SIGIR, WWW, EDBT, CIKM, ICSOC and CAiSE. Her Ph.D. thesis has been published by Springer as a monograph. She is a member of the IEEE, the ACM and the ACL.



Yang Zhang is currently a postdoc research fellow at the School of Computing, Macquarie University, Sydney, Australia. His research interests include, but are not limited to, natural language processing, citation analysis, knowledge discovery, and informetrics. Yang regularly publishes in various International Conferences and Journals of repute and has also contributed to projects of national significance funded by the National Social Science Foundation of P.R.China and the Australian Research Council.

Jitander Kumar Pabani received his BE degree in Telecommunication Engineering from Mehran University of Engineering and Technology Jamshoro, Sindh Pakistan, and Master of Engineering in Telecommunication Engineering from Hamdard University, Karachi, Pakistan in 2011 and 2014 respectively. He also completed his Post-Graduate Diploma in Statistics in 2017 from the University of Karachi, Pakistan. Currently, he is pursuing his Ph.D. studies at the Department of Communication Engineering, Universidad de Malaga, Spain, funded through the Faculty Development Program by Dawood University of Engineering and Technology, Karachi, and Higher Education Commission of Pakistan. He has been also associated with Dawood University of Engineering and Technology in the capacity of Lecturer since 2016. He has more than 10 years of teaching experience. His area of research includes Underwater Wireless Sensor Networks, Wireless Body Area Networks, Internet of Things, Machine Learning, and Fuzzy Decision Making.