Understanding the Trustworthiness Management in the Social Internet of Things: A Survey

Subhash Sagar, Adnan Mahmood, Quan Z. Sheng, Jitander Kumar Pabani, and Wei Emma Zhang

***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) in a bid to establish the 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 the smart objects act as *social objects* and intelligently impersonate the social behaviour similar to that of humans. These social objects are capable of establishing social relationships with the other objects in the network and can utilize these relationships for service discovery. Trust plays a significant role to achieve the common goal of trustworthy collaboration and cooperation among the objects and provide systems' credibility and reliability. In SIoT, an untrustworthy object can disrupt the basic functionality of a service by delivering malicious messages and adversely affect the quality and reliability of the service. In this survey, we present a holistic review of trustworthiness management for SIoT. The essence of trust in various disciplines has been discussed along with the Trust in SIoT followed by a detailed study on trust management components in SIoT. Furthermore, we analyze 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 studies vis-à-vis numerous trust evaluation dimensions. Finally, we discuss the future research directions of the emerging paradigm of SIoT particularly for trustworthiness management in SIoT.**

***Index Terms*—Internet of Things, Social Internet of Things, trustworthiness management, social relationship, social object.**

I. 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][4][5]. 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 several 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 [6][7]. 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 installing of smart bins [8][9]. Smart home applications include smart home automation, smart lighting, smart doors (and windows), and smart kitchen appliances [10][11]. Finally, smart agriculture can strengthen the traditional farming via precision farming to control and manage the livestock and crops more accurately via the agriculture drones, livestock monitoring, and smart greenhouses [12][13].

The development of these applications and services are realized via smart physical objects, e.g., a variety of sensors and actuators, radio-frequency identification devices (RFIDs) [14], smartphones, other data processing devices, possessing the capability to collect, monitor, and analyze the data pertinent to human life and usually interact with one another to accomplish a common goal. This survey interchangeably uses the terminologies of *objects*, *nodes* and *device* to refer to the IoT-enabled things, and trust models are also referred to as trust management systems or trustworthiness management systems.

With the advancement in the IoT applications, it is anticipated that there would be around 75 billion interconnected devices worldwide by 2025 [21] and international data corporation gives the worldwide IoT spending estimation of about $742 billion in 2020, and expects to achieve a growth rate of 11.3% in the period from 2021 to 2024 [22]. Furthermore, IoT is foreseen to have a considerable financial impact of upto $11.1 trillion on the global economy by 2025, wherein factories operations and equipment optimization will 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, [23]. 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 and devise an end-to-end ecosystem incorporating individuals' needs [2]. In

Subhash Sagar, Adnan Mahmood, and Quan Z. Sheng are with the School of Computing, Macquarie University, Sydney, NSW 2109, Australia, e-mail: {subhash.sagar, adnan.mahmood, michael.sheng}@mq.edu.au.

Jitander Kumar is with the School of Telecommunication Engineering, University of Malaga, Malaga, 29016, Spain, e-mail: jitander.pabani@uma.es.

Wei Emma Zhang is with the School of Computer Science, Faculty of Engineering, Computer, and Mathematical Sciences, The University of Adelaide, Adelaide, SA 5005, Australia, e-mail: wei.e.zhang@adelaide.edu.au.

TABLE I: Comparison with recent surveys

Survey	TM-C	TM-S	TS-A	SIoT-P	TM-R	Description
Abdelghani *et al.* **[15]**	∼	∼	×	×	×	- 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.* **[16]**	×	∼	×	×	×	- This study on trust management in SIoT delineates an overview of trust management studies in SIoT and compared the same with different performance metrics and trust-related attacks.
Amin *et al.* **[17]**	∼	×	×	×	∼	- The survey discusses the trust and friendliness-based approaches in terms of scalability, adaptability, and network structure by taking into account the aspects of service composition and social similarity.
Roopa *et al.* **[18]**	∼	×	×	×	∼	- This study provides a comprehensive overview of current research trends in the SIoT paradigm. Service discovery and composition, relationship management, network navigability, and trustworthiness management are among the discussed trends.
Chahal *et al.* **[19]**	✓	∼	×	×	∼	- This survey presents a detailed comparison of protocols, architectures, and trust management for SIoT where the most emphasis is given to trust management components employed in the literature.
Khan *et al.* **[20]**	∼	∼	×	×	∼	- This survey discusses a comparative and comprehensive analysis of SIoT architecture, trust management systems, and open research challenges in SIoT..
This Survey	✓	✓	✓	✓	✓	- This survey provides an extensive study on trust management components, a comparison of trust management schemes, an overview of trust in SIoT-based applications and SIoT platforms, and a summary on 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

short, IoT is described as a dynamic and a global network of infrastructure, emphasising physical and virtual objects with the capability to collect the human and environmental characteristics supporting interoperability using intelligent interfaces and standard communication protocols [3][24][25].

A. 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 [26][27][28][29]. Heterogeneity is of the main concern 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 scale up. Therefore, a possible way is to adopt the human sociological behaviour to scale up the current solution. It is pertinent to mention 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. Subsequently, the 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 [30][31]. 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, analyzing the possibilities of integrating the paradigm of social networking into the IoT ecosystem [32][33][34]. Moreover, Holmquist *et al.* [35] introduced the idea of socialization amongst the objects, wherein an easy-to-use technique was proposed to establish the relationship between the objects via utilizing the context proximity.

The emerging paradigm of SIoT employs the said integrate concept, wherein each object is not only capable of capturing surrounding characteristics but is also able to establish the relationship with the other objects in the network. The enhanced capabilities (i.e., socializing with other objects) of these intelligent social objects results in efficient collaboration as they establish their own social network to manage the social relationships and social communities in order to provide intelligent decision making without human intervention [36][37]. In light of the fact that SIoT can benefit in numerous research gaps including but not limited to the efficient discovery of services and objects, to ensure the scalability like in human social network, managing social relationships among the intelligent social objects, network navigability with the idea of smart-world phenomena whereby utilizing the relationships among the objects, and trustworthiness management among the participating smart objects [18][38].

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 the social relationships with the neighbouring objects. Nevertheless, the risks and uncertainty may diminish the significance of SIoT paradigm primarily owing to the challenges pertinent to security, privacy and trust

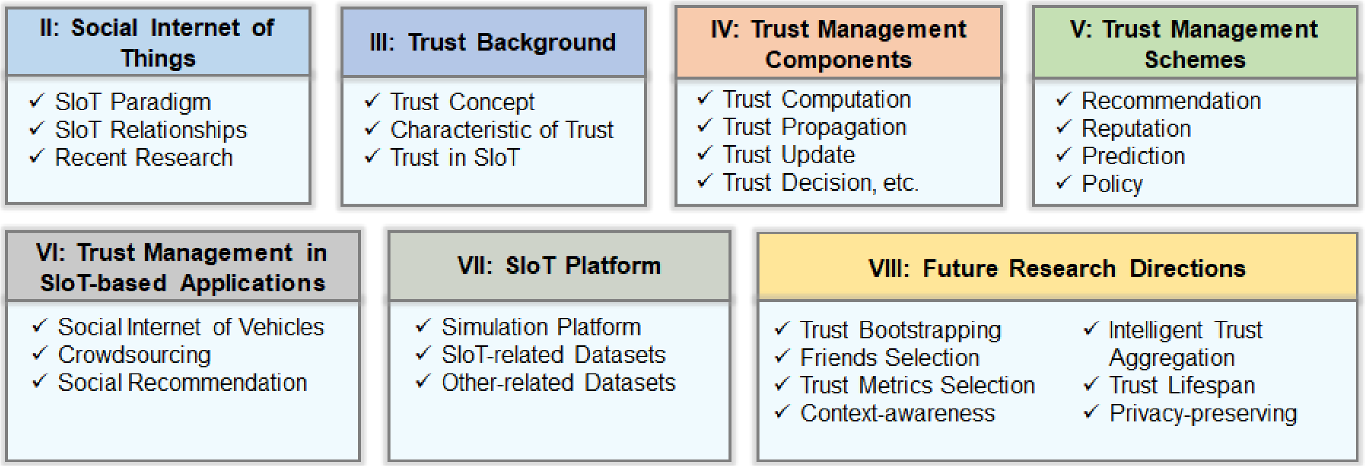


Fig. 1: Taxonomy of this survey

of these intelligent social objects [39]. For instance, when an object request for a specific service (referred to as a service requester), then, different service providers may acknowledge the same in order to to provide the requisite service and this is where the trustworthiness of these service provider come into play since the one possessing the highest trust would be opted for the requisite service. Besides, security and privacy plays an important role for deploying and commercializing of the SIoT services. Although traditional solutions i.e., cryptographic and non-cryptographic ones have been proposed to tackle such challenges [24][40], nevertheless, security challenges like trust and/or reputation are difficult to get addressed via such solutions. Likewise, there exist malicious objects that can disrupt the basic functionality of a network for malicious purposes by damaging the reputation of good (well behavioured) objects or by increasing the trustworthiness of misbehaving objects [41][42]. An efficient trust management system in SIoT is, therefore, imperative for dealing with the misbehaving objects (which are capable of jeopardizing the network functionality) by restricting the services of such nodes and via selecting the reliable and trustworthy objects before relying on the information provided by them.

B. Existing Surveys on Trust Management in SIoT

To date, a plethora of surveys on trust management for IoT [43][44][45] have been presented in the research literature, however, there are only a few surveys that offer a detailed insight on trust management systems for the SIoT paradigm. In 2016, Abdelghani *et al.* [15] 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 on trust management systems and the trust management components employed in the presented studies. A recently published survey [16] on trust management in SIoT provides an overview of trust management studies in SIoT and compared the same in terms of different performance metrics, e.g., scalability, adaptability, power efficiency, survivability, and resiliency. However, this survey still lacks reviewing many important aspects of trust, including but not limited to trust components, recent studies, and open research challenges. Furthermore, Amin *et al.* [17] published a survey on trust and friendliness approaches for SIoT, 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 analysis on trust management schemes, particularly for SIoT, are not discussed.

A holistic view of the SIoT paradigm is explored in [18], wherein the current research trends in SIoT, i.e., service discovery and composition, relationship management, network navigability, and trustworthiness management are investigated. Yet, this survey still lacks the 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 survey on trust management in SIoT is published by Rajanpreet *et al.* [19]. This survey compares and analyzes the trust management system in multiple domains, i.e., wireless sensor networks and IoT, and subsequently presents the detailed explanation of trust management components employed in the literature. Yet, the comparison of 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.* [20] 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 analyzed 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 the future research challenges especially in terms of trust computation. Overall, Table I summarizes the researched surveys on trust management in SIoT and also discusses the enhancement in our survey.

C. 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 to present this survey in a way that is self-sufficient by including 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 deliberate the SIoT paradigm and current research trends in SIoT, the fundamentals of *trust* in various disciplines and the trust management components in SIoT;
2) Subsequently, we distinguish the trust management perspective and categorize the trust management systems into four broad schemes. In particular, a comparative analysis of these 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 review the trust in three SIoT-based applications with their respective research challenges, summarize the SIoT platform used in the literature for simulation 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 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 on 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 Figure 1.

D. 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, etc.), journals (e.g., Internet of Things, Computer Networks, etc.), and conferences including but not limited to INFOCOM, ICDCS, 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.

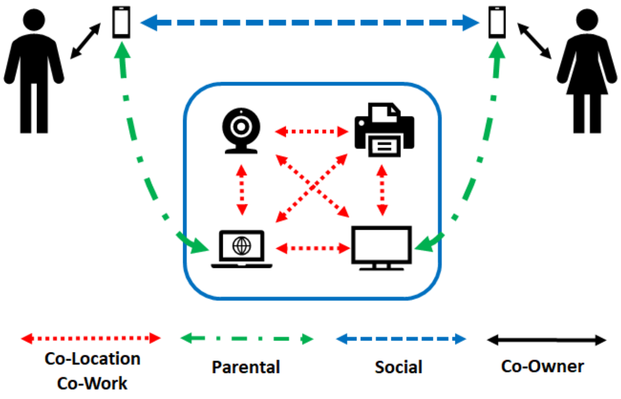


Fig. 2: Types of relationships in SIoT

The remainder of this paper is organized as follows. Section II delineates the SIoT paradigm and current research trends in SIoT. Section III deliberates the concept of trust in various disciplines, i.e., sociology, psychology, economics, computer science and in SIoT. In Section IV, trust management components are discussed in detail. Section V presents the comparative analysis of the current state-of–the-art trust managements schemes. Section VI discusses the trust in SIoT-based applications and a number of SIoT-platforms along with SIoT related datasets are briefly discussed in Section VII. Finally, Section VIII provides the future research directions for trustworthiness management in SIoT, whereas, concluding remarks are presented in Section IX.

II. 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.

A. SIoT Paradigm

The idea of socialization of objects first conceived in 2001 by P. Mendes [46] wherein the idea of objects participating in the conversation similar to the human social network is presented. Similarly, the authors in [33] 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.* [36]. 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 (Figure 2) and owners of the objects and some of the frequently occurred relationships are:

[1] https://arxiv.org/

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 smartphones, tablets, laptops, etc. This type of relationship results in a high probability of interaction [37].

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 [37].

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 [37].

4) Co-location Object Relationships (CLOR): CLOR represent 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 a industrial automation environment.

5) Co-work Object Relationships (CWOR): In contrast to CLOR, CWOR signify the relationship involving two or more objects collaborate 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 [37].

There are a few unpopular relationships, such as sibling object relationships, guest object relationships, guardian object relationships, stranger object relationships, and service object relationships [18].

Furthermore, the SIoT paradigm conveys numerous desirable implications into 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 the service discovery and composition. Moreover, applying social networking concepts to the IoT unquestionably prompts favorable circumstances that stretch (i) from the enhanced viability, scalability, and the 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.

B. 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 [47] [48]. The authors in [36][37] 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 the IoT systems in an efficient and effective manner. Moreover, various SIoT related challenges are studied in the research literature and Figure 3 depicts some of these current open key challenges in the SIoT landscape, including but not limited to, i) service discovery and composition [49][50], ii) network navigability [51][52], iii) relationship management [37][53], and iv) trust management [18][54].

Fig. 3: Current research areas in SIoT

1) Service Discovery and Composition: The underlying rationale behind the IoT and SIoT paradigm is to provide the 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 [55]. 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 the generated data from these devices is not useful for everyone, and therefore, service discovery is imperative for searching the smart objects providing the useful information in a highly dynamic environment. SIoT facilitates at discovering the service, i.e., similar to the humans searching for information in their social network by employing different relationships, hereby providing a scalable solution for service discovery. Subsequently, the service composition provides and enables the interaction between the smart objects subsequent to service discovery [56][57].

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) [51]. 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 [38][52][58].

3) Relationship Management: Relationship management provides the way of embedding the intelligence into smart objects, to make them recognize the friends and foes, and to originate, update and terminate the relationship. The authors in [59] introduced the notion of cognitive IoT to integrate the 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 [37]. Many research efforts have been made over the years to provide the novel ideas for relationship management in terms of friendship selection in the SIoT landscape, wherein different genetic algorithms and appropriate policies have been proposed [53][60][61].

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 [62][63][64]), and numerous applications (e.g., IoT [43], Internet of Vehicles (IoV) [65][66], mobile and vehicular ad-hoc networks [67][68], peer-to-peer networks [69], online social networks [70], e-Commerce [71]). Nevertheless, the SIoT paradigm requires the trust management systems that not only deals 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 [54]. 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 III-VI by highlighting their respective strengths and limitations. Moreover, Table VII illustrates the trust management components employed in these studies, whereas Table VIII delineates the evaluation of these studies with various dimensions.

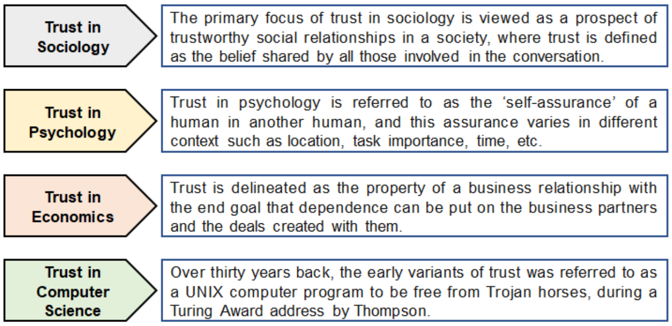
III. Background

The concept of trustworthiness management is evolving rapidly and has been widely employed in various disciplines [62][63][64][72] and applications (e.g., crowdsourcing, social recommendation) [69][73][74]. It is, therefore, important to distinguish the ideal optimal parameters for any IoT specific ecosystem.

A. 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 [75]. The definition of trust varies with disciplines (Figure 4). In its basic form, trust is referred to as the belief of one human (trustor) on another human (trustee) [75], 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.

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 [76]. 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 [62]. Furthermore, the authors in [77][78] delineate trust as the mean of reducing the complexity in society, and it depends on the belief that a human places on the reactions of his/her counterpart. A different view of trust is provided in Seligman [79], wherein trust is described as the reliance and, in usable terms, it is a disposition with respect to the trustor to acknowledge reliance on a trustee.



The primary focus of trust in sociology is viewed as a prospect of trustworthy social relationships in a society, where trust is defined as the belief shared by all those involved in the conversation.

Trust in psychology is referred to as the 'self-assurance' of a human in another human, and this assurance varies in different context such as location, task importance, time, etc.

Trust is delineated as the property of a business relationship with the end goal that dependence can be put on the business partners and the deals created with them.

Over thirty years back, the early variants of trust was referred to as a UNIX computer program to be free from Trojan horses, during a Turing Award address by Thompson.

Fig. 4: Trust definitions vis-à-vis different domains

2) Trust in Psychology: Psychology is a study of a human mind's characteristics, especially, in a specific context [80]. 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 [81]. 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 [62][63]. Furthermore, Josang *et al.* [82] 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) Trust in Economics: Economics is also a part of social science that deals with the production and distribution of goods and services [83]. 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 [64]. In e-Commerce, it is possible to mitigate the transactions risk by incorporating trust dynamics via providing photos of the products, rating, and reviews when there is no direct interaction between the consumers and the products [84][85]. Likewise, Kazuhiro [86] 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.

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 face of any unexpected vulnerabilities, identify these vulnerabilities easily and recover efficiently [87]. The current computer science systems are about data communication and processing that require secure and trustworthy management [88]. 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 [89]. Moreover, the early variants of trust looks into various aspects of network and data security with one of the earliest by Thompson [90] delineating the trust as a UNIX computer program free from Trojan horses.

B. Characteristics of Trust

Trust can be evaluated in numerous ways by considering the following characteristics [70]:

1) 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 trustor's observation (i.e., direct trust) as well as the opinion (i.e., feedback or indirect trust) of the other objects.

2) Objective: In contrast to subjective trust, an 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.

3) 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.

4) 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.

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

6) 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.

C. Trust in SIoT

As discussed, trust plays an important role in SIoT to make 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 [17][81]. 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* [91][92]. The concept of trust in SIoT is utilized in various applications, including but not limited to social Internet of Vehicles (SIoV) [93], crowdsourcing [94], object recommendation [95], trustworthy service discovery [96], 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, the assessment of trust 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 [17][97]. Thus, it is essential to consider the required parameter for trust quantification as the concept of trust is complex and can not be measured with a single parameter. Trust of a SIoT object can be seen as the degree of confidence or faith of various characteristics of an object, e.g., the object's ability, integrity, reliability, security, and dependability. Trust in SIoT can be seen as a reputation of an object in the SIoT network based on its direct and indirect understanding and previous transactions [98]. In general, the essential components to provide trustworthiness management in SIoT are portrayed in Figure 5 and are briefly discussed in Section IV.

IV. Trust Management Components

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

A. Trust Computation

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 [54][117][118].
- *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 [119][120][121].

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 single trust metric (e.g. quality of service metric) is used to ascertain the overall trust [122][123][124].
- *Multi Trust:* It employs the notion of trust as a multi-dimensional concept. For instance, combining multitude of factors like both social and QoS metrics to form a single trust score [97][117][118].

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 [19], including but not limited to, the one based on weighted sum [117][125], belief theory [104][126], Bayesian system [122][127], fuzzy logic [108][118], regression analysis [114][115], and machine learning [112][128]. Trust aggregation is an important step of any trust computation model, and therefore, it is pertinent to discuss the trust aggregation techniques in a comparative manner. Table II illustrates each of these aggregation techniques along with the strengths and weaknesses of the same.

- *Weighted Sum*: This technique is the simplest and one of the commonly used aggregation method. The technique refers to as an average weighted mean of each metric/value, where each metric is assigned with a weight to get the single score. Let $M = \{m_1, m_2, m_3, ..., m_n\}$ represents the n trust metrics and $W = \{w_1, w_2, w_3, ..., w_n\}$

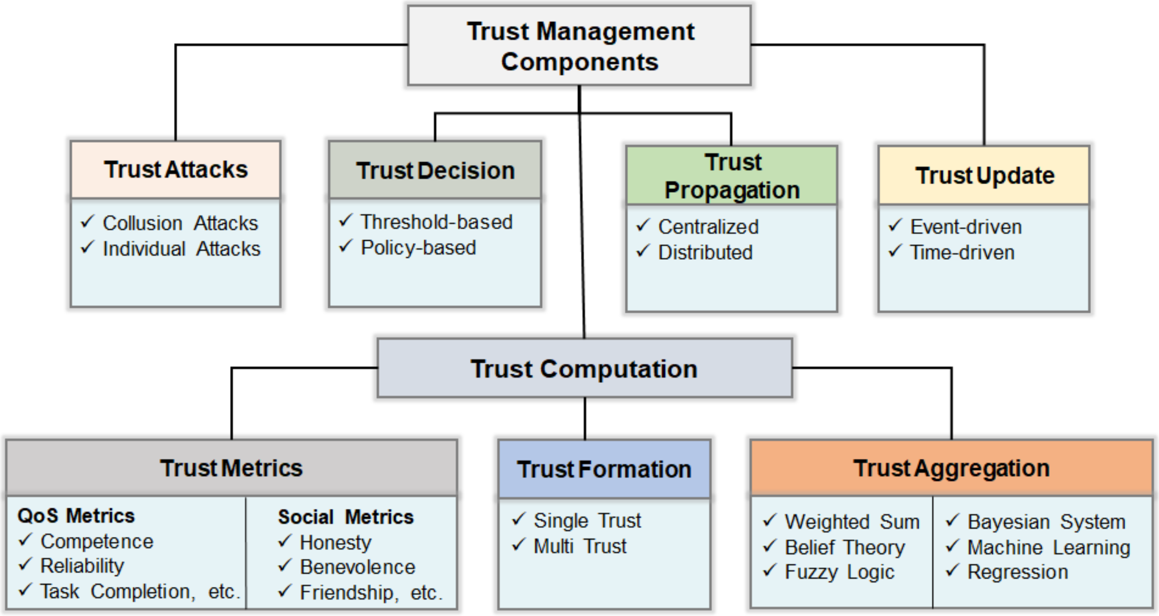


Fig. 5: Components of trustworthiness management in SIoT

represent the weights of each n trust metrics [117][125], the weighted sum aggregation (WS_A) is computed as:

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

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 [104][126]. The belief of a node $\mathcal{N}_|$ in view of node $\mathcal{N}_\rangle$ with respect to an event $\mathfrak{a}$ is computed as:

$$bel(\mathcal{N}_\rangle) = \sum_{a_j \subseteq a} m_{\mathcal{N}_\rangle}(\mathfrak{a}_\mathfrak{j}) \tag{2}$$

Here $\mathfrak{a}_\mathfrak{j}$ represents all the basic events of $\mathfrak{a}$, and $m_{\mathcal{N}_\rangle}(\mathfrak{a}_\mathfrak{j})$ highlights all the events in view of $\mathcal{N}_\rangle$. Therefore, we can conclude that the belief of a node for an event $\mathfrak{a}$ is $bel(\mathcal{N}_|) = m_{\mathcal{N}_\rangle}(\mathfrak{a})$. Subsequently the plausibility is $pla(\mathcal{N}_\rangle) = 1 - bel(\mathcal{N}_\rangle)$.

- *Bayesian System*: The concept of Bayesian system is based on Bayes' theorem, i.e., the prior probability, posterior probability about the data/node/interaction, and the likelihood function. The trust in Bayesian system is treated as the random variable and is stated as follows [122][127]:

$$p(\mathcal{A}|\mathcal{B}) = \frac{p(\mathcal{B}|\mathcal{A})p(\mathcal{A})}{p(\mathcal{B})} \tag{3}$$

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 the 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 uncertainly and fuzziness in notion of trust [108][118]. In general, a fuzzy aggregation technique can be divided into 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 the 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 [114][115]. Mathematically, the linear regression can be seen as

$$\mathcal{Y} = m_0 + m_1\mathcal{X} \tag{4}$$

and multi regression is computed as follows:

$$\mathcal{Y} = m_0 + m_1\mathcal{X}_1 + m_2\mathcal{X}_2 + ... + m_n\mathcal{X}_n \tag{5}$$

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

- *Machine Learning*: Machine learning-based aggregation techniques utilize the clustering (i.e., unsupervised al-

TABLE II: Comparison of trust aggregations techniques

Techniques	Description	Strengths	Weaknesses
Weighted Sum **[99][100][101]**	- This aggregation technique refers to as an average weighted mean of each value, where each metric is assigned with the static or the dynamic weights to get the single score.	- Low computations cost as it does not require any mathematical function. - it is a simple method of aggregating the values.	- Infinite number of possibilities for determining the weights of each value different environments - Inability to identify influence of each value on overall value
Belief Theory **[102][103][104]**	- It is also referred to as Dempster-Shafer theory 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.	- This technique allows to combine data from different independent sources. - Belief theory is appropriate for managing missing data and provides the better method of enumerating vagueness.	- In presence of malicious objects, the conflicting uncertainly in belief theory may disrupt the opinion of legitimate objects, and thus lead to unreliable decision making.
Bayesian Inference **[105][106][107]**	- Bayesian inference is a popular technique for trust computational model where trust is treated as a random variable in the range of [0,1] following a beta distribution to designate the probability distribution of a data/node/interaction. The concept of Bayesian inference is based on Bayes' theorem.	- It provides the 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 the misleading results. - Models with high number of parameters/metric often lead to high computational cost.
Fuzzy Logic **[108][109][110]**	- A fuzzy logic is a many-valued logic processing more than the customary two truth-values of truth and falsehood unlike Boolean logic. This concept of fuzzy logic is realistic for trust aggregation as the node cannot be characteristically labelled as completely trustworthy or completely untrustworthy.	- Fuzzy logic resembles human reasoning that works well even in presence of ambiguous or vague input. - This nature of fuzzy logic makes this approach suitable for complex nature of trust evaluation to make decision 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 **[111][112][113]**	- Machine learning-driven aggregation techniques are normally required two-step process for prediction; i) Unsupervised learning (Clustering) when the training data is not labelled, ii) Multi-class supervised learning (classification) to classify the interactions/nodes into different classes (i.e., trustworthy and/or untrustworthy).	- 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 machine learning-driven algorithm and it leads to high latency as the system needs to train the trust model after every transaction.
Regression Analysis **[114][115][116]**	- It is a statistical process that is used to approximate the relationship between the independent variable. Regression is divided into two categories, i.e., linear and multi-regression. Linear regression in terms of trust is defined as the value of trust depends on one independent variable/metric while in multiple regression, the trust is dependent on more than one independent variable.	- 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 leads to the uncertain results when the dataset used for analysis is insignificant. - Linear regression usually oversimplify the problem, and thus, it is not recommended for real-world complex problem.

gorithms) and classification (i.e., 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 [112][128].

B. *Trust Propagation*

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

- *Centralized:* Centralized schemes rely on a centralized entity which is primarily responsible for (a) gathering trust-related information for the purpose of trust computation and (b) propagating the same in the network [54][124]. 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 [122][129]. 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 the 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 in two common categories, i.e., *locally distributed*

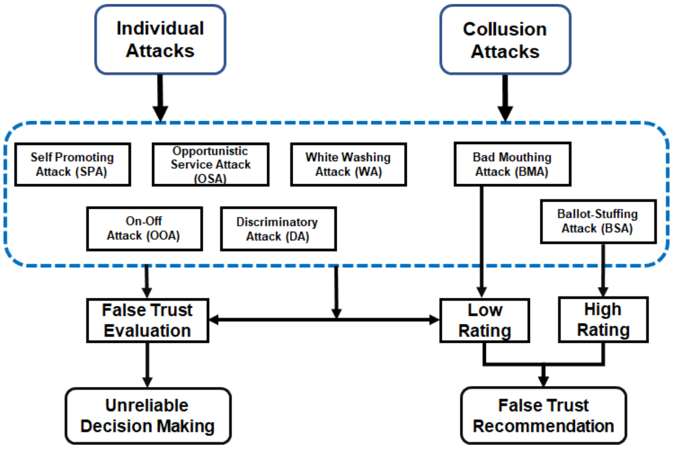

Individual Attacks
Collusion Attacks
Self Promoting Attack (SPA)
Opportunistic Service Attack (OSA)
White Washing Attack (WA)
Bad Mouthing Attack (BMA)
On-Off Attack (OOA)
Discriminatory Attack (DA)
Ballot-Stuffing Attack (BSA)
False Trust Evaluation
Low Rating
High Rating
Unreliable Decision Making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

Fig. 6: Trust related attacks

and globally centralized and *locally centralized and globally distributed* [54][130].

C. Trust Update

At the end of a transaction or at any specified time interval, 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 [122][124]. Nevertheless, this type of update increases the traffic overhead in networks with more frequent transactions.
- *Time-driven:* In time-driven approach, trust is collected and updated periodically after a given interval of time [129][131]. 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 a trust is updated periodically and/or in case of an event (after an interaction) [121].

D. 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 Figure 6. These attacks are categorized as individual attacks and collusion-based attacks [18][132].

- *Individual Attacks:* Individual attacks refer to the attack launched by an individual object. Some of the common form of individual attacks are briefly discussed as follows:
  - *Self Promoting Attacks (SPA):* In this type of attacks, a node can promote its significance by providing 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 [19].
  - *Whitewashing Attacks (WA):* In a white washing attack, a node can exit and re-join the network or an application to recover its reputation and to 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 selective behaviour attack where a node performs well for a particular service/node and ineffectually for some other services/nodes [133].
  - *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 [20].
  - *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 [19].
- *Collusion-based Attacks:* Collusion attacks represent the attack launched by group of objects to either provide the 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 [134].
  - *Ballot Stuffing Attacks (BSA):* These attacks are used for boosting the reputation of bad nodes within the network by providing good recommendations for them so that the bad node can be selected as a service provider [134].

E. 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, decision is taken on the basis of either a rank-based function or a threshold value. [135][136]. 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 [135][137].

V. Trust Management Schemes: Discussion and Analysis

As of late, there has been an increased interest of the research community to provide an insight on trustworthiness management systems for SIoT. Therefore, this survey categorizes these systems into four broad categories, namely *recommendation-based*, *reputation-based*, *prediction-based*, and *policy-based schemes*. This section compares the trust management systems that have already been described in the literature, first discussing the pros and cons of these schemes as well as whether or not they are context-aware. Subsequently, these methods are classified based on the trust metrics employed for trust quantification and the trust-related attacks that they manage.

A. Discussion on Trust Management Schemes

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

1) Recommendation-based Trust Scheme (RecTS): Over the years, a number of recommendation-based trust management systems have been employed, wherein recommendations as a trust metric is exploited in a bid to evaluate the trustworthiness of the nodes in a SIoT network [138]. 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 (even if there is no current direct observations or previous direct observations [139]. As of late, a number of trust management systems employing recommendation as a trust metrics are proposed [54][96][117][118][129][140] in the research literature.

Nitti *et al.* [54] present the trustworthiness management model for SIoT, 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, 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.* [117] 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.* [118] delineate 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 the trust metric, 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.* [96] present 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.

Most recently, Wei *et al.* [140] propose a context-aware socio-cognitive-based trust model for service delegation in service-oriented SIoT. The model is based on two characteristics, *competence quantification* and *willingness quantification*. The competence is quantified by utilizing the degree of importance (DoI) and degree of social relationships (DoSR), and willingness quantification integrates the degree of contribution (DoC) and also 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 provider, and the DoSR is employed as the weighting parameters for both competence and willingness. The final trust score is computed by aggregating both the trust parameters by using the weighted sum technique.

Conclusively, the recommendation-based trust model has numerous advantages as shown in Table III including but not limited to 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.

2) Reputation-based Trust Scheme (RepTS): The concept of reputation has been widely used for the dynamic IoT environment where 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 [146]. Recently, reputation-based systems have been employed in many fields of computer science including but not limited to distributed networks, peer-to-peer networks, IoT environment where security, privacy, and trust are the critical issues [44]. Many reputation-based trust models [91][121][129][141][142][147][148][149] are employed to enhance the trustworthiness evaluation of a node and to detect the misbehaving nodes in the SIoT network.

Truong *et al.* [91] present a trust model, referred to as REK wherein the 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) current state of relationships. Subsequently, the trend of experience is analyzed via development of experience (due to cooperative interaction), loss of experience (due to

TABLE III: Trust computation techniques

Recommendation-based Techniques

Ref.	Trust metrics	Strengths	Limitations	Context-awareness
Nitti *et al.* **[54]**	- Centrality - Credibility - Feedback/opinion	- The envisaged trust model encompasses both the subjective and the objective properties of a node within the network. - Efficient in terms of successfully identifying malicious nodes in the network even in presence of a high percentage of malicious nodes.	- Feedback increases the network traffic overhead due to transmission. - Model responds slowly to dynamic changes in the environment due to predefined trust parameters.	No
Khani *et al.* **[96]**	- QoS metric - Friendship - Community-of-interest - Feedback as recommendations	- This framework considers mutual context-awareness while computing the trust and outperform many existing trust related models. - The model performs well against many trust related attacks, including but not limited to BMA, BSA, SPA, and OOA.	- Fine tuning of trust parameters in lieu of dynamically changing environments has not been taken into consideration.	Yes
Chen *et al.* **[117]**	- Honesty - Cooperativeness - Community-of-interest - Recommendations	- The model is suitable for the dynamically changing environmental conditions. - The proposed model fine tunes the trust parameters primarily depending on dynamically changing environments.	- Defense mechanism against some key attacks e.g., on-off and intelligent behaviour attack, have not been considered. - The selection and fine tuning of some of the important parameters is still an issue in the proposed model.	No
Xia *et al.* **[118]**	- Centrality - Recommendations - Community-of-interest	- The model consider context-awareness and outperform two well known trust models relying on weighted sum approach. - The proposed model performs well in presence of grey-hole attacks and bad-mouthing attacks.	- Integration of context information and discussion on weights for different attributes is missing. - Defense mechanisms against the on-off attacks and intelligent behaviour attacks have not been considered.	Yes
Wei *et al.* **[140]**	- Direct trust - Experience	- A context-aware socio-cognitive based trust model for service delegation is proposed in this paper where the trust quantification process involve two adaptable and dynamic trust characteristic in the form of degree of contribution and degree of importance. - The proposed model has high success rate of tasks in presence of many trust-related attacks such as OSA, BMA and BSA.	- With increase in number of properties included for trust computation, the convergence time of the model also increases rapidly. - The proposed model integrates many trust attributes to compute the trust score, however, the weighted sum aggregation lacks in identifying the appropriate weight for each attribute.	Yes

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 [121] propose 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 by varying the malware probability (i.e., percentage of malicious objects).

Chen *et al.* in [129] delineate an energy-aware access scheme for service recommendation in SIoT that takes into consideration of the heterogeneous and decentralized environment. The model utilizes the 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 allows 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 [141] 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 post 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 model is discussed in [142] wherein the reputation incorporates two trust metrics: recommendation and reputation, and knowledge assess an object and its respective owner to compute knowledge trust met-

TABLE IV: Trust computation techniques

Reputation-based Techniques

Ref.	**Trust metrics**	**Strengths**	**Limitations**	**Context-awareness**
Truong *et al.* **[91]**	- Reputation - Experience	- The proposed model presented two trust metrics, i.e., experience and reputation. The experience is discussed in terms of cooperative, uncooperative and neutral interaction, whereas the reputation involve the positive and negative reputation. - The performance evaluation is analysed via change in the experience over time in term of weak and strong tie and the convergence of the algorithm.	- Analysis of individual trust metrics is present in this paper, however, the combined effect of these metrics to compute the trust of an object is not present. - The performance evaluation in terms of trust computation and trust-related attacks are not present.	No
Xiao *et al.* **[121]**	- Reputation - Credit	- This model is computationally optimal as it only requires two metrics (i.e., credit and reputation) to categorize the nodes as trustworthy or untrustworthy. - All the computations are done by reputation server so the nodes are not responsible for any type of computation.	- All the aspects of trust computation such as trust composition, direct observations, recommendations, etc., are not considered. - Due to centralized computation system, the scalability is the major concern owing to the scalable nature of SIoT.	No
Chen *et al.* **[129]**	- Reputation - Social relationships - Energy status of a device	- Model considers energy-aware technique to balance the workload in the network, and encompasses energy of node, past performance (i.e., reputation) and social relationships to ascertain the trust score. - For dynamic performance enhancement, timeliness of each transaction/interaction is also considered as an evaluation metric.	- Model does not consider any defense mechanism against trust related attacks. - The comparison of energy consumption is analyzed in this model, however, the effect of energy consumption with increase in number of nodes is an important factor that needs to be considered.	No
Azad *et al.* **[141]**	- Reputation - Experience	- A decentralized trust management model is proposed that not only provides the trustworthiness of object in SIoT but also integrates the homomorphic encryption to protect the privacy of the objects. - The model works in self-enforcing manner, thus, there is no need of any trusted third party.	- Performance evaluation of the model has not been carried out in the presence of trust related attacks.	No
Truong *et al.* **[142]**	- Reputation - Knowledge - Experience	- A fuzzy-based trust model is presented by taking into consideration the knowledge, reputation and experience as a trust metrics. - To analyse the applicability of the model, a trust car sharing use case is considered by employing the three metrics, i.e, reliability, pricing and quality.	- The evaluation of model in terms of detecting the misbehaving objects, accuracy of model, and convergence is not present. - Performance in terms of trust-related attacks is also not considered.	No

rics of a service. To deal with the ambiguous knowledge with vague terms, i.e., “good”, “bad”, ‘’high”, and “low”, a fuzzy logic-based mechanism is introduced to transform the human knowledge into object knowledge. Furthermore, a trust service platform is introduced that employs three components: *trust agent*, *trust broker* and *trust management and analysis*. Trust agent is employed to collect the trust-related data in the SIoT domain, and trust broker is utilized to disseminate the trust-related data to numerous applications and services. Finally, the trust management and analysis component implements required task including but not limited to knowledge evaluation mechanisms, information model, reasoning mechanisms, and trust computation algorithm.

Decisively, the reputation-based trust mechanisms have the upper hand while isolating the untrustworthy node for future endeavor 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 IV.

3) Prediction-based Trust Scheme (PredTS): The trust management system in 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 [151]. The prediction-based systems especially the machine-learning or deep learning approaches have upper hand when the trust composition step has more number of 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 their can be infinite number of possibilities of assigning weights to each trust metric in different IoT environments [111]. A number of prediction-based schemes [111][133][134][143][144][145][147][152] are described as follows and are compared in Table V.

Jafarian *et al.* [147] delineate a discrimination-aware trust

TABLE V: Trust computation techniques

Prediction-based Techniques				
Ref.	**Trust metrics**	**Strengths**	**Limitations**	**Context-awareness**
Jayasinghe *et al.* **[111]**	- Community-of-interest - Friendship similarity - Centrality - Cooperativeness	- A data-centric trust evaluation model is proposed which utilizes the machine learning-based trust aggregation to ascertain the single trust metrics instead of a weighted sum aggregation.	- Performance evaluation of the proposed model has not been carried out vis-á-vis various trust-based attacks. - The model suffers with scalability and reliability issue with an increase in the number of nodes.	No
Marche *et al.* **[134]**	- Goodness score - Usefulness score - Preseverance score	- An incremental SVM-based trust-related attack detection model is proposed by employing three score as the indicator of trust: goodness, usefulness, and perseverance score. - All the trust-related attacks are considered to analyse the performance of the model.	- The proposed model performs better in a network with mix of different attacks, nevertheless, performance degrades when individual attacks are considered. - The discussion on various simulation parameters considered for performance evaluation is not known.	No
Aalibagi *et al.* **[143]**	- Similarity - Centrality	- A matrix factorization-based trust model is proposed that utilizes bipartite graph, the hellinger distance and the matrix factorization to identify trustworthy nodes. - The model mitigates the cold start problem and performs well under malicious objects, specifically under OSA.	- The discussion on suitability of bipartite graph over other type of graphs (e.g., hyper graph) is not mentioned. - Evaluation of trust model under various other trust-related attacks is not known.	No
Sagar *et al.* **[144]**	- Community-of-interest - Cooperativeness - Friendship similarity - Co-work similarity	- A machine learning-driven trust evaluation model has been proposed so as to observe the behaviour of nodes over a period of time. - The model has also analyzed the impact of each trust metric on the overall trust score.	- Computationally expensive and results in high latency in highly dynamic environment owing to training the machine learning model more frequently. - Performance evaluation of the proposed model has not been carried out vis-á-vis various trust-based attacks.	No
Abderrahim *et al.* **[145]**	- Sociability - Direct observation - Recommendations	- A scalable and adaptive community-based trust model is proposed to detect trust attacks especially the On-Off attack. - The Kalman filter technique is used to estimate the behaviour of a node.	- The validity of the model is evaluated on the basis of On-Off attack, however, it is important to investigate the behaviour on other trust related attacks.	No

model by taking into consideration of discriminatory behaviour of objects in SIoT network. An object's discriminatory behaviours can be attributed due to various reasons including but not limited to 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 a an object (i.e., or service provider). The context-awareness is incorporated as a weight for each rating via a service rating query as rating vector $< S, E, SS, f >$ wherein S represents service, E is the energy status, SS is the social similarity and f is the feedback. Finally, the performance is analyzed in presence of numerous trust-related attacks by using the dataset from [153].

A data-centric machine learning-based trust evaluation mode is proposed by Jayasinghe *et al.* in [111] 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.* [134] introduce 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, training phase is utilized as an initial knowledge for the steady state phase. The steady-state step utilizes the initial dynamic knowledge to continuously learn the behaviour of object. To continuously learn the dynamic knowledge, an incremental SVM is employed with goodness, usefulness and perseverance score to quantify the trust of an object.

A matrix factorization model is presented in [143] where, at first, SIoT is demonstrated as 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 presence of many trust-related attacks and the discussion on suitability of bipartite graph is not known. A social similarity-based trust computational model is presented in [144] where a k-means clustering and random forest classification is used to analyze 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

TABLE VI: Trust computation techniques

Policy-based Techniques

Ref.	Trust metrics	Strengths	Limitations	Context-awareness
Magarino *et al.* **[130]**	- Direct observation - Reputation	- The framework presents a enhanced security mechanism by exploiting prioritization rules, certificates and trust management policies to detect hijacked nodes in the network. - The performance of the model is improved when compared with the control approach that does not employ the trust and reputation mechanisms to detect the hijacked node.	- Performance evaluation of the model with many trust related attacks such as BMA, BSA, OOA, etc., is not known.	No
Al-Hamadi *et al.* **[136]**	- Location rating - Raters trust - Witness trust	- A trust-based decision making for IoT health system is proposed that considers risks, reliability trust, and health probability for decision making. - The model outperforms the traditional trust computational baseline protocol that filter out only the untrustworthy source without considering the reliability of the source and the relation between the user's health the level of harm.	- Trust computational process of this model relies on static trust parameter, the optimal value for these parameters for dynamic environment is not known.	Yes
Li *et al.* **[137]**	- Data observation - Experience as a history	- A policy-based secure and trustworthy model is proposed to assess the trustworthiness of both the user and the data. - The model can efficiently detect three types of trust attacks (BMA, BSA, and OOA).	- Policies are context dependent, and for highly dynamic IoT applications, system needs to update the policies very frequently or before/after every transaction.	Yes
Chen *et al.* **[150]**	- Energy status - Bandwidth - Quality-of-provider	- The model presents the trust management system exploiting the concept of maximum ratio combining (MRC) and source combining (SC) for IoT security protection. - Performance evaluation of the model is carried out using QoS based trust score with and without MRC based trust. The MRC embedding with trust system performs well under different QoS level.	- The evaluation of the model is carried out on limited number of nodes that does not guarantee the scalability. - Defence mechanism for different type of trust related attacks are is addressed.	No

expensive that leads to high latency in dynamic changing environments.

Moreover, a deep learning model is delineated by Masmoudi *et al.* [133] to segregate malicious nodes performing trust-related attacks, the trust computation process in this model follows a two-step process i.e., trust composition that includes social and QoS metrics, and deep learning-based trust aggregation. Nevertheless, a deep learning aggregation costs more computation power as well as increases the computation latency in dynamic environments. Abderrahim *et al.* [145] present a trust management system employing community-of-interest based trust metrics and Kalman filter to predict the trustworthiness of nodes. The proposed system considers an on-off attack to evaluate the performance, however, it is equally important to prove the validity of the model in presence of other trust attacks. 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.

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 [154] [155]. A number of policy-based trust management schemes on IoT are present in research literature [130][136][137][150][156], however, these schemes are not yet employed in the SIoT. Therefore, we have selected the 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 VI and a brief description of each main research is described in this section.

Al-Hamadi *et al.* [136] present 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 the 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 environment. Policy-based security and trustworthy model named $RealAlert$ is proposed by Li *et al.* [137] to estimate the trustworthiness of a node as well as the data. The model presets the policies based

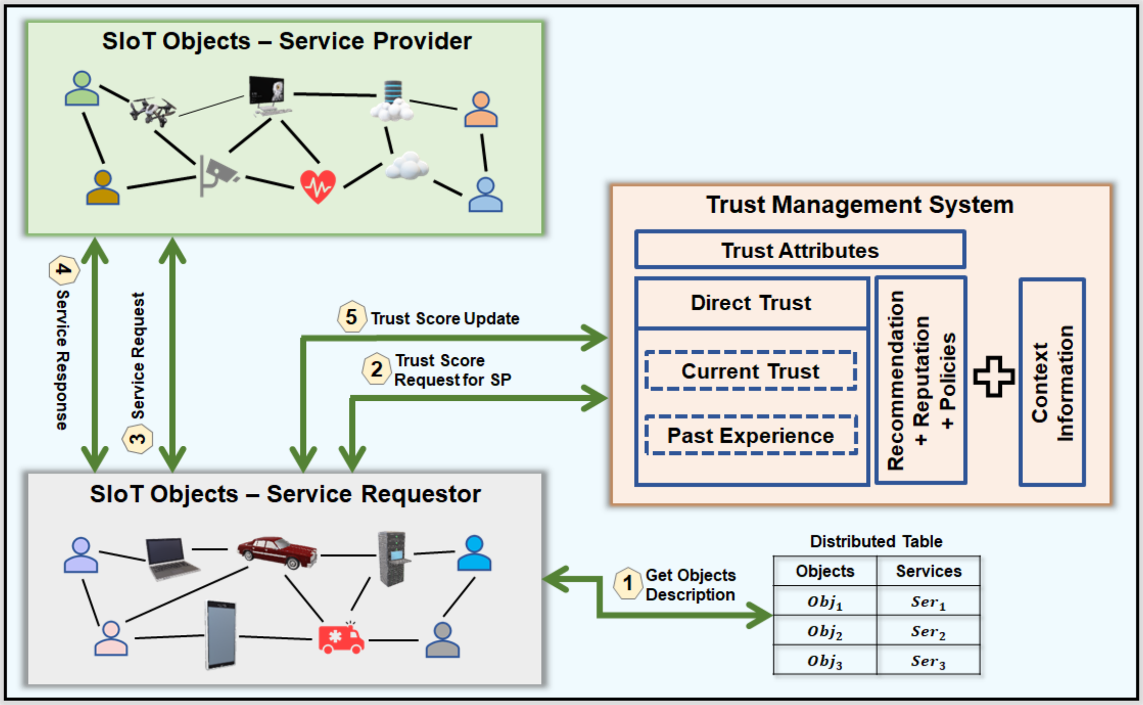
TABLE VII: Trust management components employed in SIoT

Ref.	**Trust Metrics**	**Trust Aggregation**	**Trust Update**	**Trust Formation**	**Trust Propagation**	**Trust Decision**	**Trust Attacks**
Nitti *et al.* **[54]**	Social	Weighted Sum	Time-Driven	Multi-Trust	Distributed and Centralized	Threshold-based	SPA, WA, OSA, BMA, BSA
Truong *et al.* **[91]**	Social	Weighted Sum	Event-Driven	Multi-Trust	Centralized	Threshold-based	NA
Khani *et al.* **[96]**	Social and QoS	Weighted Sum	Time-Driven	Multi-Trust	Distributed	Threshold-based	SPA, OOA, BMA, BSA
Jayasinghe *et al.* **[111]**	Social	Machine Learning-based	Event-Driven	Multi-Trust	Distributed	Threshold-based	NA
Chen *et al.* **[117]**	Social and QoS	Weighted Sum	Time-Driven	Multi-Trust	Distributed	Threshold-based	BMA
Xia *et al.* **[118]**	Social	Fuzzy Logic	Event-Driven	Multi-Trust	Distributed	Threshold-based	SPA, OSA, OOA, BMA, BSA
Xiao *et al.* **[121]**	Social and QoS	Weighted Sum and Bayesian System	Event and Time-Driven	Single-Trust	Distributed	Threshold-based	SPA, BMA, BSA
Chen *et al.* **[129]**	Social	Weighted Sum	Event and Time-Driven	Multi-Trust	Distributed	Threshold-based	SPA, BMA, BSA
Magarino *et al.* **[130]**	Social	Weighted Sum	Event-Driven	Multi-Trust	Centralised and Distributed	Context-based	NA
Marche *et al.* **[134]**	Social and QoS	Machine Learning-based	Event-Driven	Multi-Trust	Distributed	Threshold-based	SPA, WA, OSA, OOA, BMA, BSA, DA
Al-Hamadi *et al.* **[136]**	Social and QoS	Weighted Sum	Event-Driven	Multi-Trust	Distributed	Threshold/Context-based	SPA, OSA
Li *et al.* **[137]**	Social and QoS	Belief Theory	Event-Driven	Single-Trust	Distributed	Context-based	OOA, BMA, BSA
Wei *et al.* **[140]**	Social and QoS	Weighted Sum	Event-Driven	Multi-Trust	Distributed	Threshold-based	OSA, BMA, BSA
Azad *et al.* **[141]**	Social and QoS	Weighted Sum	Event-Driven	Multi-Trust	Distributed	Threshold-based	NA
Truong *et al.* **[142]**	Social and QoS	Fuzzy Logic	Event-Driven	Multi-Trust	Centralized	Threshold-based	NA
Aalibagi *et al.* **[143]**	Social	Filtering	Even-Driven	Multi-Trust	Distributed	Threshold-based	OSA
Sagar *et al.* **[144]**	Social	Machine Learning-based	Event-Driven	Multi-Trust	Centralised	Threshold-based	NA
Abderrahim *et al.* **[145]**	Social	Weighted Sum	Event-Driven	Multi-Trust	Distributed	Threshold-based	OOA
Chen *et al.* **[150]**	Social and QoS	Weighted Sum	Event-Driven	Multi-Trust	Distributed	Context-based	NA

SPA → Self-Promoting Attack, **WA** → Whitewashing Attack, **OSA** → Opportunistic Service Attack, **OOA** → On-Off Attack
BMA → Bad Mouthing Attack, **BSA** → Ballot-Stuffing Attack, **DA (SBA)** → Discriminatory (Selective Behaviour) Attack, **NA** → No Attack

on contextual information to detect the compromising nodes and misleading information by evaluating the model under different trust attacks. Nevertheless, policies of the proposed model are context-dependent that require human expertise to update the policies for highly dynamic IoT applications.

Moreover, a trust management model is proposed in [150] 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 presence of a trust attack is considered. Correspondingly, Magarino *et al.* [130] present 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, the 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.



Objects	Services
Obj_1	Ser_1
Obj_2	Ser_2
Obj_3	Ser_3

Fig. 7: High-level overview of trustworthiness management system in service-oriented SIoT

Furthermore, Table VII presents the trust management components (see Figure 5) 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.

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 to utilize 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 Figure 7. The generalized trustworthiness management follows a total of five steps, wherein *step1* provides the service requester access to a distributed table to facilitates which object (service provider) provides what service, *step2* enables the service requester to request the trust score of the objects providing the requisite service from the trust management system, *step3* 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.

B. Analysis of Trust Management Schemes

This section evaluates the trust management schemes discussed in Section V with a set of dimensions. The selection of these dimensions is considered based on the highly dynamic and distributed nature of the SIoT network [157][158][159]. This section discusses the selected dimensions, and the evaluation of the schemes is provided in Table VIII:

- *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 [157].
- *Adaptability*: Owing to the dynamic nature of SIoT, trust evaluation framework must adapt to the changes in a different context, i.e., environmental conditions, temporal factor, 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 [158].
- *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 [157].
- *Integrity*: The network integrity implies that the content of message is protected during the transmission between two objects. An important component of trust computation is to share the feedback and recommendation among the objects so that it could also be employed for trust

TABLE VIII: Evaluation of trust management techniques using various dimensions

Studies	**Scheme**	**Accuracy**	**Adaptability**	**Availability**	**Integrity**	**Reliability**	**Privacy**	**Scalability**	**Credibility**	**Applicability**	**Response**
Nitti *et al.* **[54]**	RecTS	H	P	NA	NA	LR	NA	HS	NA	NSA	NEET
Truong *et al.* **[91]**	RepTS	NK	F	NA	NA	HR	NA	HS	NA	NSA	NEET
Khani *et al.* **[96]**	RecTS	H	P	NA	NA	HR	NA	HS	NC	NSA	NEET
Jayasinghe *et al.* **[111]**	PredTS	H	F	L	H	NA	NA	LS	NA	NSA	EET
Chen *et al.* **[117]**	RecTS	H	F	L	NA	LR	PP	HS	FC	SA	NEET
Xia *et al.* **[118]**	RecTS	H	F	NA	NA	HR	NA	HS	NA	NSA	NEET
Xiao *et al.* **[121]**	RepTS	NK	NA	NA	NA	NA	NA	HS	NC	NSA	NEET
Chen *et al.* **[129]**	RepTS	H	P	NA	NA	NA	NA	HS	NC	NSA	EET
Magarino *et al.* **[130]**	PolTS	NK	F	H	NA	LR	NA	HS	FC	SA	EET
Marche *et al.* **[134]**	PredTS	H	F	H	NA	HR	NA	LS	NA	NSA	NEET
Al-Hamadi *et al.* **[136]**	PolTS	H	F	H	L	HR	NA	HS	NA	SA	EET
Li *et al.* **[137]**	PolTS	H	P	L	NA	LR	NA	LS	NC	SA	NEET
Wei *et al.* **[140]**	RecTS	H	F	H	L	HR	NA	HS	NC	NSA	EET
Azad *et al.* **[141]**	RepTS	H	F	NA	H	HR	PP	LS	NC	SA	EET
Truong *et al.* **[142]**	RepTS	NK	P	H	L	LR	NA	HS	NC	SA	NEET
Aalibagi **[143]**	PredTS	H	F	H	H	HR	NA	HS	NC	NSA	EET
Sagar *et al.* **[144]**	PredTS	H	F	NA	H	NA	NA	LS	NA	NSA	EET
Abderrahim *et al.* **[145]**	PredTS	NK	F	NA	NA	HR	NA	HS	NA	NSA	EET
Chen *et al.* **[150]**	PolTS	L	P	L	NA	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

score computation purposes. Thus, integrity is essential to prevent the data from being modified without consent [159].

- *Reliability*: Reliability is the ability of a system to perform its functionality 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 [158].
- *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 the activity information (e.g., the information on with whom the object interacted and the services used by the same) [159].
- *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 [157][159].
- *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)[157].

- *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 [157].
- *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 [157].

The evaluation of the trust management schemes vis-à-vis a set of dimensions is illustrated in Table VIII. 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 concern 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 notion 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 a "tree" (Figure 8), i.e., from categorizing the existing studies to the future research directions.

VI. 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.

A. Crowdsourcing

Crowdsourcing focuses on the idea of outsourcing a task to a group of people for a business production [160]. 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* [161] where a service provider can provide computing resources to low powered objects, *ambient sensing* [162] to sense the environment conditions, *energy sharing* to provide wireless charging to the low energy level objects [163]. 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 [164].

Recently, SIoT-enabled crowdsourcing on disaster reduction applications is proposed in [165] wherein the Web-based map is designed to recruit the people and their devices (e.g., smartphones, tablets) along with their social profile 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 [94] propose a trustworthy crowdsourcing model in SIoT to cope with the issue of trustworthiness of objects. The model considers two security aspects by encompassing a socially-aware message forwarding algorithm for social data link 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.* in [164] 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 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 trustworthiness of task computation results to counteract the invalid results from the dishonest participant trying to save their computing resources.

B. 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 [166][167]. 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 [166] 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 [168] 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

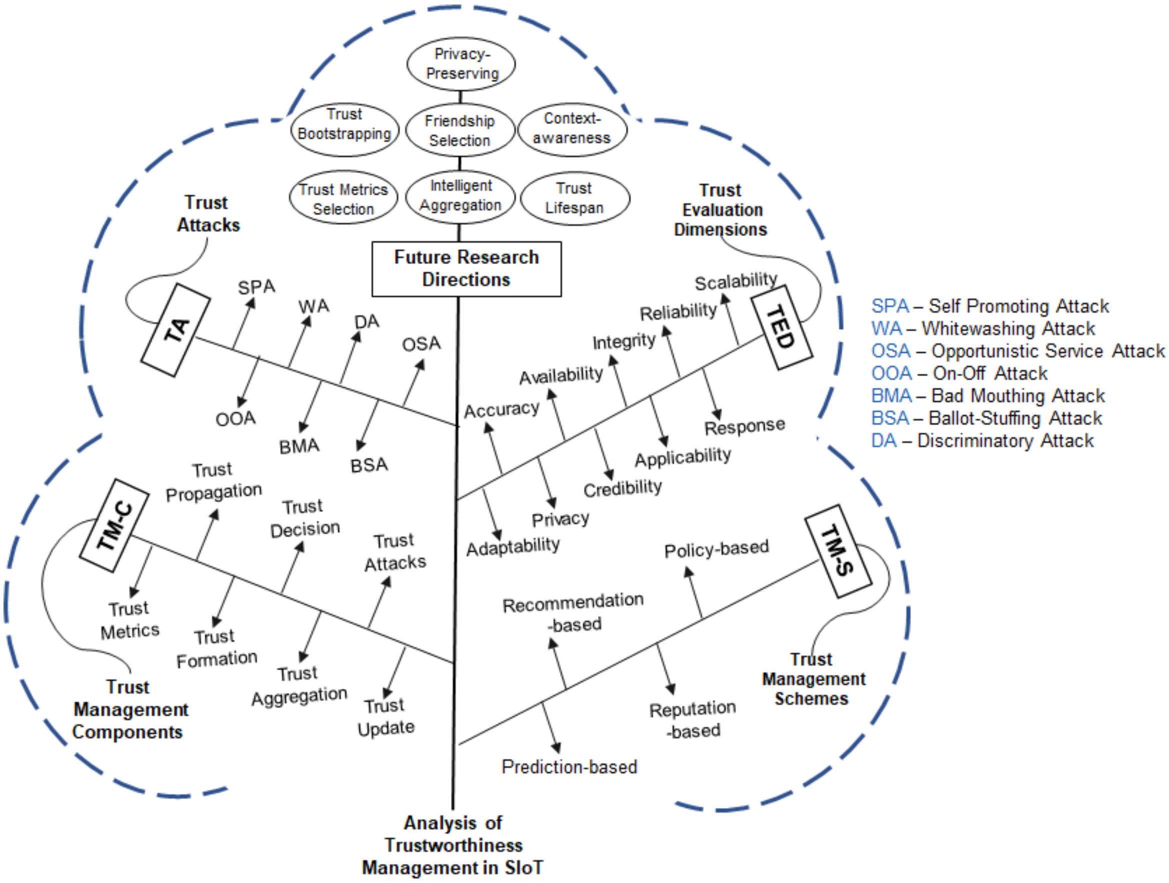


Fig. 8: Summary of trustworthiness management analysis

interest keywords are extracted from users' social activities. Finally, the schemes recommend the top N users by analyzing the user similarity and SIoT object's preference.

A time-aware smart object recommendation model for SIoT is presented in [95] 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, object's social similarity is estimated by employing their social relationships. A recommendation list is then generated that utilizes the concept the 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 selection of attributes and important relationship 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.

C. *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 traveling far from one another, information insufficiency, and scalability [169]. SIoV is the modern trend of IoV [170], 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 in 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 [171][172]. The implementation of SIoV is still in its infancy, nevertheless, a number of research articles have been published recently in terms of trust management [173][174][175], computation offloading [176] and other applications of SIoV (i.e., solution for traffic congestion, precise positioning, and vehicles' location protecting) [177][178][179].

A trust-aware communication architecture for SIoV is proposed (*TACASHI*) in [174] 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 intervehicular 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 profile. Similarly, Gai *et al.* [175]

delineate 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 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 has been proposed by Lai *et al.* [173] in an attempt to forbid the sensitive data leakage. The designed scheme is trust-based and ensure 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 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 the data from vehicles based on their social relationships and via 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.

VII. SIoT Simulation Tools and SIoT Datasets

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

A. 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 [180][181]. 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 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:

1) NetLogo: NetLogo is the open-source and a multi-agent programming module, which is suitable for natural as well as social phenomena [182]. With hundreds and thousands of independent agents, a researcher can give instructions to each one of these agents to explore and analyze 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*) is used by many studies to evaluate the performance of their proposed trust management systems in SIoT [54][118]. SWIM is introduced as a mobility model for ad-hoc networking to generate the 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 [183]. A few recommendation-based studies [118][140] have utilized NetLogo simulator for experimental analysis of their work.

2) Network Simulator-3 (NS-3): NS-3 is a discrete-event open-source simulator and is the successor of NS-2 [184]. 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, adaptability to extend the resources for multiple application domains [185]. Overall, current literature suggests a number of studies on trust management have considered NS-3 simulator to validate their proposed model [117][136].

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 factor for specialized environment needs, e.g., to add the mobility for vehicular network [186], incorporate the social profiles of objects to enhance the application capabilities [187]. In general, due to its flexible nature, this simulation tool can be utilized in various domains and applications.

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, 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 analyze the data. Besides, MATLAB has a dedicated Simulink to design and deploy IoT applications and also offers flexibility and the possibility to integrate and analyze the data from third-party IoT service/platform (e.g., ThingSpeak [188]). 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 managements system for SIoT [91][96][111][112][143][144][145]. There are several other least exploited simulation tools (e.g., GlomoSim [189], Cooja

[190]) that are not commonly used by researchers in the literature.

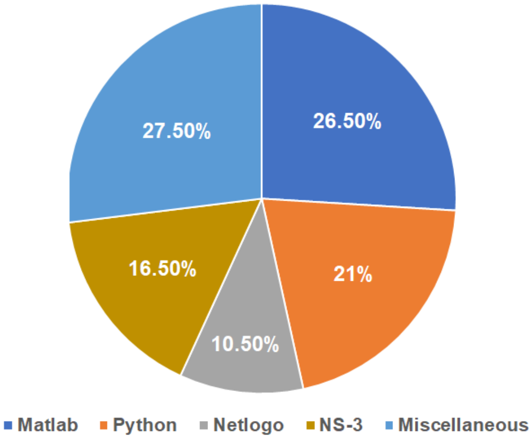


Fig. 9: Percentage of simulation tools used in the selected articles

Figure 9 shows the percentage of each simulation tool utilized for the evaluation of the trust management system in the research works discussed and analyzed in this survey. The miscellaneous part in the figure gives the percentage of articles where the name of simulation tools is not mentioned.

B. 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 can not be directly applied to the SIoT structure. Some of the datasets utilized in the literature are discussed as follows.

The authors in [191] 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 1,616 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 [192], which can be mapped in the form of a SIoT environment. This dataset contains the information of 76 objects in terms of their social profiles (friends and the communities they are involved in), and the interaction (15,776 number of 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 [193] and Yelp[2] in combination with the SIoT dataset [191] to integrate the social structure in order to validate the performance of their trust model. Epinions is the online social network consumer review site and used to decider whether to trust or 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 the 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 [191]. Moreover, a few studies suggest the design of the testbeds to get the required dataset for performance evaluation [194][195].

VIII. 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 attention of researchers. This section highlights the future research directions for trustworthiness management in SIoT.

A. 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*) [145][117]. This assumption may lead a malicious SIoT object to jeopardize the basic functionality of a SIoT network before it is even identified as the untrustworthy object (or an object may perform the 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 [42] 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 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.

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

B. *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 an 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 the 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 the social attributes and these attributes exploit different types of relationships amongst the 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 have been suggested by Nitti *et al.* [53] for friendship selection, wherein an SIoT object sorts all of its friends in 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.

C. *SIoT Specific Trust Metrics Selection*

The key characteristic of SIoT is the integration of IoT and social networks. As of late, a number research studies consider hybrid SIoT trust metrics [141][148][150]. 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 dynamic environment (i.e., context information). Recently, a number of trust metrics are employed in some research studies [143][166], 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 characteristic before designing an efficient trust management system.

D. *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 different context [75][20]. Furthermore, owing to the dynamic nature of SIoT in terms of varied applications and services, the contextual information is important as the trust management system for a specific application and/or service may not be applicable for the other applications and services. A variety of context-aware trust models are proposed in the literature [96][151] suggesting different contexts with the generally considered once being time, location, and objects' 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.

E. *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 [54][96] 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 regards to assessing a weighting factor for each metric and inability to recognize which trust metric makes the most impact on the overall trust in a specific environment. Consequently, there is a need of intelligent trust aggregation mechanism to overcome the limitations of conventional aggregation techniques. Lately, the idea of machine learning-based aggregation has been suggested by the researchers to obtain the weights of each metric in terms of its importance [112]. However, machine learning-based solutions have their own limitations, e.g., these solutions are computationally expensive and results in increasing the 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.

F. *Trust Lifespan - Decay*

It is evident that the trust of an 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 [91][68]. 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 trust score of inactive SIoT objects must be subject to decay after a particular duration of time. Truong *et al.* [91] propose an experience-reputation model that gives the idea of trust decay over a period of time, wherein the trust of SIoT objects decline based on strong and weak tie (strong tie represents the strong relationship) with the other SIoT objects. However, the model does not discuss about 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.

G. 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 detail of the owners using online social networks. Hence, the privacy-preserving solutions are essential to address the risks involved and to promote the SIoT applications and services. Moreover, there are a few notable studies in the literature pertinent to privacy-preservation for trust management in SIoT [117][141]. Chen *et al.* [117] utilize the one-way hash function to encrypt the social information of nodes during the interaction, whereas Azad *et al.* [141] use 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.

IX. Conclusion

Recently, the emerging paradigm of Social Internet of Things (SIoT) has become a vibrant and rapidly growing area of research. Trust is considered as the impediment for the adoption of social characteristics amongst the smart objects for establishing trustworthy social relationships and to provide 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 analyzed and compared. We further compare the referred studies in terms of trust management components and a set of assessment dimensions. Finally, we provide a high-level overview of the generic trust management framework for service-oriented SIoT, and put forward the future research directions to address various trust-related SIoT research issues.

Acknowledgements

Subhash Sagar's research is supported by the Higher Education Commission of the Government of Pakistan and the Macquarie University, Australia (Macquarie University's Research Excellence Award). Adnan Mahmood's research is funded via the Macquarie University's Postdoctoral Research Fellowship. Quan Z. Sheng's research is partially supported by Australian Research Council (ARC) Discovery Project DP20010229 and Linkage Infrastructure, Equipment and Facilities Projects LE180100158 and LE220100078.

References

[1] K. Ashton, "That 'Internet of Things' Thing," *Computer Communications*, vol. 22, no. 7, pp. 97 – 114, 1999.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[4] A. Bouguettaya, Q. Z. Sheng, B. Benatallah, A. G. Neiat, S. Mistry, A. Ghose, S. Nepal, and L. Yao, "An Internet of Things Service Roadmap," *Communication of the ACM*, vol. 64, no. 9, p. 86–95, 2021.

[5] M. Sheng, Y. Qin, L. Yao, and B. Benatallah, Eds., *Managing the Web of Things: Linking the Real World to the Web*. Morgan Kaufmann, 2017.

[6] X. Yang, X. Wang, X. Li, D. Gu, C. Liang, K. Li, G. Zhang, and J. Zhong, "Exploring Emerging IoT Technologies in Smart Health Research: A Knowledge Graph Analysis," *BMC Medical Informatics and Decision Making*, vol. 20, p. 260, 2020.

[7] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The Future of Healthcare Internet of Things: A Survey of Emerging Technologies," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[8] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017.

[9] Y. Qian, D. Wu, W. Bao, and P. Lorenz, "The Internet of Things for Smart Cities: Technologies and Applications," *IEEE Network*, vol. 33, no. 2, pp. 4–5, 2019.

[10] M. Alaa, A. Zaidan, B. Zaidan, M. Talal, and M. Kiah, "A Review of Smart Home Applications Based on Internet of Things," *Journal of Network and Computer Applications*, vol. 97, pp. 48–65, 2017.

[11] A. Zaidan and B. Zaidan, "A Review on Intelligent Process for Smart Home Applications Based on IoT: Coherent Taxonomy, Motivation, Open Challenges, and Recommendations," *Artificial Intelligence Review*, vol. 53, no. 1, pp. 141–165, 2020.

[12] P. K. R. Maddikunta, S. Hakak, M. Alazab, S. Bhattacharya, T. R. Gadekallu, W. Z. Khan, and Q. V. Pham, "Unmanned Aerial Vehicles in Smart Agriculture: Applications, Requirements, and Challenges," *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17 608–17 619, 2021.

[13] M. Pathan, N. Patel, H. Yagnik, and M. Shah, "Artificial Cognition for Applications in Smart Agriculture: A Comprehensive Review," *Artificial Intelligence in Agriculture*, vol. 4, pp. 81–95, 2020.

[14] Q. Z. Sheng, X. Li, and S. Zeadally, "Enabling Next-Generation RFID Applications: Solutions and Challenges," *Computer*, vol. 41, no. 9, pp. 21–28, 2008.

[15] W. Abdelghani, C. A. Zayani, I. Amous, and 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.

[16] M. R. Rashmi and 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.

[17] F. Amin, A. Ahmad, and G. Sang Choi, "Towards Trust and Friendliness Approaches in the Social Internet of Things," *Applied Sciences*, vol. 9, no. 1, p. 166, 2019.

[18] R. M.S., S. Pattar, R. Buyya, V. K.R., S. Iyengar, and L. Patnaik, "Social Internet of Things (SIoT): Foundations, Thrust Areas, Systematic Review and Future Directions," *Computer Communications*, vol. 139, pp. 32 – 57, 2019.

[19] R. K. Chahal, N. Kumar, and S. Batra, "Trust Management in Social Internet of Things: A Taxonomy, Open Issues, and Challenges," *Computer Communications*, vol. 150, pp. 13 – 46, 2020.

[20] W. Z. Khan, Q.-u.-A. Arshad, S. Hakak, M. K. Khan, and Saeed-Ur-Rehman, "Trust Management in Social Internet of Things: Architectures, Recent Advancements, and Future Challenges," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7768–7788, 2021.

[21] "Statista, Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025," https://www.statista.com/statistics/471264/iot -number-of-connected-devices-worldwide/, accessed: 2020-04-15.

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

[23] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "The Internet of Things: Mapping the value beyond the hype." McKinsey Global Institute, 2015.

[24] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1372–1391, 2020.

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

[26] W. E. Zhang, Q. Z. Sheng, A. Mahmood, D. H. Tran, M. Zaib, S. A. Hamad, A. Aljubairy, A. A. F. Alhazmi, S. Sagar, and 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.

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

[28] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[29] A. R. Khan, Q. F. Hassan, and S. Madani, *Internet of Things: Challenges, Advances, and Applications*. Chapman and Hall/CRC, 01 2018.

[30] J. Kleinberg, "Navigation in a Small World," *Nature*, vol. 406, p. 845, 2000.

[31] 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*, ser. NIPS'01, 2001, p. 431–438.

[32] M. Kranz, L. Roalter, and F. Michahelles, "Things That Twitter: Social Networks and the Internet of Things," in *8th International conference on Pervasive Computing (PERCOM)*, 2010.

[33] D. Guinard, M. Fischer, and 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.

[34] H. Ning and Z. Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?" *IEEE Communications Letters*, vol. 15, no. 4, pp. 461–463, 2011.

[35] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl5, and 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.

[36] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a Social Structure to the Internet of Things," *IEEE Communications Letters*, vol. 15, pp. 1193–1195, 2011.

[37] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) – When Social Networks Meet the Internet of Things: Concept, Architecture, and Network Characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594 – 3608, Nov 2012.

[38] M. Nitti, L. Atzori, and I. Pletikosa, "Network Navigability in the Social Internet of Things," in *IEEE World Forum on Internet of Things, WF-IoT*, 2014, pp. 405–410.

[39] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective Data-Sanitization for Preventing Sensitive Information Inference Attacks in Social Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.

[40] L. Nie, Y. Wu, X. Wang, L. Guo, G. Wang, X. Gao, and S. Li, "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," *IEEE Transactions on Computational Social Systems*, pp. 1–12, 2021.

[41] X. Fan, L. Liu, R. Zhang, Q. Jing, and J. bi, "Decentralized Trust Management: Risk Analysis and Trust Aggregation," *ACM Computing Surveys (CSUR)*, vol. 53, pp. 1–33, 02 2020.

[42] M. N. Ba-hutair, A. Bouguettaya, and A. Ghari Neiat, "Multi-Perspective Trust Management Framework for Crowdsourced IoT Services," *IEEE Transactions on Services Computing*, pp. 1–1, 2021.

[43] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, S. khan, and M. K. Khan, "Trust and Reputation for Internet of Things: Fundamentals, Taxonomy, and Open Research Challenges," *Journal of Network and Computer Applications*, vol. 145, p. 102409, 2019.

[44] G. Fortino, L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, "Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges," *IEEE Access*, vol. 8, pp. 60 117–60 125, 2020.

[45] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards Trustworthy Internet of Things: A Survey on Trust Management Applications and Schemes," *Computer Communications*, vol. 160, pp. 475–493, 2020.

[46] P. Mendes and P. P. Mendes, "Social-driven Internet of Connected Objects," in *Internet Architecture Board (IAB) workshop on Interconnecting Smart Objects with the Internet*, 2011.

[47] O. Voutyras, P. Bourelos, D. Kyriazis, and 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.

[48] A. M. Ortiz, D. Hussein, S. Park, S. Han, and N. Crespi, "The Cluster Between Internet of Things and Social Networks: Review and Research Challenges," *IEEE Internet of Things Journal*, vol. 1, pp. 206–215, 06 2014.

[49] Y. Li, Y. Huang, M. Zhang, and L. Rajabion, "Service Selection Mechanisms in the Internet of Things (IoT): a Systematic and Comprehensive Study," *Cluster Computing*, vol. 23, pp. 1–21, 2020.

[50] D. Zhang, L. T. Yang, and 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.

[51] R. Abdul, A. Paul, J. Gul M, W.-H. Hong, H. Seo *et al.*, "Exploiting Small World Problems in a SIoT Environment," *Energies*, vol. 11, no. 8, p. 2089, 2018.

[52] F. Amin, R. Abbasi, A. Rehman, and G. S. Choi, "An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks," *Sensors*, vol. 19, pp. 1–20, 04 2019.

[53] M. Nitti, L. Atzori, and I. P. Cvijikj, "Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies," *IEEE Internet of Things Journal*, vol. 2, no. 3, pp. 240–247, 2015.

[54] M. Nitti, R. Girau, L. Atzori, and S. Member, "Trustworthiness Management in the Social Internet of Things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, 2014.

[55] S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Searching for the IoT Resources: Fundamentals, Requirements, Comprehensive Review, and Future Directions," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, pp. 2101–2132, 2018.

[56] D. Hussein, S. Han, G. M. Lee, N. Crespi, and E. Bertin, "Towards a Dynamic Discovery of Smart Services in the Social Internet of Things," *Computers & Electrical Engineering, Elsevier*, vol. 58, pp. 429–443, 2017.

[57] A. Khanfor, H. Ghazzai, Y. Yang, M. R. Haider, and Y. Massoud, "Automated Service Discovery for Social Internet-of-Things Systems," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2020, pp. 1–5.

[58] V. Mohammadi, A. M. Rahmani, A. Darwesh, and A. Sahafi, "Trust-based Friend Selection Algorithm for navigability in social Internet of Things," *Knowledge-Based Systems*, vol. 232, p. 107479, 2021.

[59] M. Zhang, H. Zhao, R. Zheng, Q. Wu, and W. Wei, "Cognitive Internet of Things: Concepts and Application Example," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 6, p. 151, 2012.

[60] W. Mardini, Y. Khamayseh, and M. H. Khatatbeh, "Genetic Algorithm for Friendship Selection in Social IoT," in *International Conference on Engineering MIS (ICEMIS)*, 2017, pp. 1–4.

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

[62] R. Hardin, "Trust: A Sociological Theory," *Economics and Philosophy*, vol. 18, pp. 183–204, 04 2002.

[63] B. R. Schlenker, B. Helm, and J. T. Tedeschi, "The Effects of Personality and Situational Variables on Behavioral Trust," *Journal of personality and social psychology*, vol. 25, no. 3, p. 419, 1973.

[64] R. M. Morgan and S. D. Hunt, "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing*, vol. 58, no. 3, pp. 20–38, 1994.

[65] A. Mahmood, S. A. Siddiqui, W. E. Zhang, and 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.

[66] A. Mahmood, S. A. Siddiqui, Q. Sheng, W. E. Zhang, H. Suzuki, and W. Ni, "Trust on wheels: Towards secure and resource efficient IoV networks," *Computing*, pp. 1–22, 2022.

[67] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1287–1309, 2016.

[68] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A Survey of Current Solutions and Future Research Opportunities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2553–2571, 2021.

[69] X. Meng and D. Liu, "GeTrust: A Guarantee-Based Trust Model in Chord-Based P2P Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 54–68, 2018.

[70] S. M. Ghafari, A. Beheshti, A. Joshi, C. Paris, A. Mahmood, S. Yakhchi, and M. A. Orgun, “A Survey on Trust Prediction in Online Social Networks,” *IEEE Access*, vol. 8, pp. 144 292–144 309, 2020.

[71] Y. Cen, J. Zhang, G. Wang, Y. Qian, C. Meng, Z. Dai, H. Yang, and J. Tang, “Trust Relationship Prediction in Alibaba E-Commerce Platform,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 5, pp. 1024–1035, 2020.

[72] A. Mahmood, Q. Z. Sheng, S. A. Siddiqui, S. Sagar, W. E. Zhang, H. Suzuki, and 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.

[73] W. Li and H. Song, “ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[74] H. Rahimi and 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.

[75] W. Sherchan, S. Nepal, and C. Paris, “A Survey of Trust in Social Networks,” *ACM Computing Survey*, vol. 45, no. 4, pp. 1–33, 2013.

[76] R. Swedberg, “On the use of definitions in sociology,” *European Journal of Social Theory*, vol. 23, no. 3, pp. 431–445, 2020.

[77] M. Deutsch, “Cooperation and Trust: Some Theoretical Notes,” *Nebraska Symposium on Motivation*, pp. 275–319, 1962.

[78] J. Jalava, “From Norms to Trust: The Luhmannian Connections between Trust and System,” *European Journal of Social Theory*, vol. 6, no. 2, pp. 173–190, 2003.

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

[80] G. R. Henriques, “Psychology Defined,” *Journal of clinical psychology*, vol. 60, no. 12, pp. 1207–1221, 2004.

[81] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, “Not So Different After All: A Cross-Discipline View Of Trust,” *Academy of Management Review*, vol. 23, no. 3, pp. 393–404, 1998.

[82] A. Jøsang, R. Ismail, and C. Boyd, “”A survey of trust and reputation systems for online service provision,” *Decision Support Systems*, vol. 43, no. 2, pp. 618 – 644, 2007.

[83] R. Backhouse and S. Medema, “On the Definition of Economics,” *Journal of Economic Perspectives*, vol. 23, pp. 221–33, 01 2009.

[84] S. Ba and P. Pavlou, “Evidence OF the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior,” *Management Information Systems*, vol. 26, pp. 243–268, 09 2002.

[85] J. Riegelsberger, M. A. Sasse, and 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, p. 121–128.

[86] K. Arai, “Trust and Trustworthiness in the Economy: How They Function and How They Should Be Promoted,” *Hitotsubashi Journal of Economics*, vol. 48, 2007.

[87] D. Artz and Y. Gil, “A Survey of Trust in Computer Science and the Semantic Web,” *Journal of Web Semantics*, vol. 5, no. 2, pp. 58 – 71, 2007.

[88] *Trust, Computing, and Society*. Cambridge University Press, 2014.

[89] W. Harwood, “The Logic of Trust,” Ph.D. dissertation, University of York, 2012.

[90] K. Thompson, “Reflections on Trusting Trust,” *Communications of the ACM*, vol. 27, no. 8, p. 761–763, 1984.

[91] N. B. Truong, T. Um, B. Zhou, and 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.

[92] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, “Toward a Trust Evaluation Mechanism in the Social Internet of Things,” *Sensors*, vol. 17, no. 6, 2017.

[93] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, “Trust Management in Social Internet of Vehicles: Factors, Challenges, Blockchain, and Fog Solutions,” *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, pp. 1–22, 2019.

[94] K. Wang, X. Qi, L. Shu, D. Deng, and J. J. P. C. Rodrigues, “Toward Trustworthy Crowdsourcing in the Social Internet of Things,” *IEEE Wireless Communications*, vol. 23, no. 5, pp. 30–36, 2016.

[95] Y. Chen, M. Zhou, Z. Zheng, and D. Chen, “Time-Aware Smart Object Recommendation in Social Internet of Things,” *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2014–2027, 2020.

[96] M. Khani, Y. Wang, M. A. Orgun, and F. Zhu, “Context-Aware Trustworthy Service Evaluation in Social Internet of Things,” in *International Conference on Service-Oriented Computing (ICSOC)*, 2018, pp. 129–145.

[97] N. Truong, H. Lee, B. Askwith, and G. M. Lee, “Toward a Trust Evaluation Mechanism in the Social Internet of Things,” *Sensors*, vol. 17, p. 1346, 2017.

[98] Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[99] I. P. Stanimirovic, M. L. Zlatanovic, and M. D. Petkovic, “On the Linear Weighted Sum Method for Multi-objective Optimization,” *Facta Acta Universitatis*, vol. 26, no. 4, pp. 49–63, 2011.

[100] I. Y. Kim and O. De Weck, “Adaptive Weighted Sum Method for Multi-objective Optimization: a New Method for Pareto Front Generation,” *Structural and multidisciplinary optimization*, vol. 31, no. 2, pp. 105–116, 2006.

[101] R. T. Marler and J. S. Arora, “The Weighted Sum Method for Multi-objective Optimization: New Insights,” *Structural and multidisciplinary optimization*, vol. 41, no. 6, pp. 853–862, 2010.

[102] L. Liu and R. R. Yager, *Classic Works of the Dempster-Shafer Theory of Belief Functions: An Introduction*. Springer Berlin Heidelberg, 2008, pp. 1–34.

[103] K. Sentz and S. Ferson, *Combination of Evidence in Dempster-Shafer Theory*, 01 2002.

[104] M. Beynon, B. Curry, and P. Morgan, “The Dempster–Shafer Theory of Evidence: An Alternative Approach to Multicriteria Decision Modelling,” *Omega*, vol. 28, no. 1, pp. 37–50, 2000.

[105] A. Jøsang and R. Ismail, “The Beta Reputation System,” *In: Proceedings of the 15th Bled Conference on Electronic Commerce*, 01 2002.

[106] K. Weise and W. Woger, “A Bayesian Theory of Measurement Uncertainty,” *Measurement Science and Technology*, vol. 4, no. 1, p. 1, 1993.

[107] J. M. Bernardo and A. F. Smith, *Bayesian Theory*. John Wiley & Sons, 2009, vol. 405.

[108] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and 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.

[109] 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.

[110] J. Carbo, J. M. Molina, and J. Davila, “Trust Management Through Fuzzy Reputation,” *International Journal of Cooperative Information Systems*, vol. 12, no. 01, pp. 135–155, 2003.

[111] U. Jayasinghe, G. M. Lee, T. Um, and Q. Shi, “Machine Learning based Trust Computational Model for IoT Services,” *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 39–52, 2019.

[112] S. Sagar, A. Mahmood, Q. Z. Sheng, and 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.

[113] S. A. Siddiqui, A. Mahmood, W. E. Zhang, and 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.

[114] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami, and 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.

[115] R. Venkataraman, M. Pushpalatha, and T. R. Rao, “Regression-based Trust Model for Mobile Ad Hoc Networks,” *IET Information Security*, vol. 6, no. 3, pp. 131–140, 2012.

[116] U. Jayasinghe, H.-W. Lee, and 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.

[117] I. Chen, F. Bao, and J. Guo, “Trust-Based Service Management for Social Internet of Things Systems,” *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684–696, 2016.

[118] H. Xia, F. Xiao, S. Zhang, C. Hu, and 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.

[119] X. Li, G. Zhu, Y. Gong, and K. Huang, “Wirelessly Powered Data Aggregation for IoT via Over-the-Air Function Computation: Beamforming and Power Control,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 7, pp. 3437–3452, 2019.

[120] X. Sun and N. Ansari, "Dynamic Resource Caching in the IoT Application Layer for Smart Cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 606–613, 2018.

[121] H. Xiao, N. Sidhu, and 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.

[122] I. Chen, J. Guo, and F. Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2016.

[123] C. V. L. Mendoza and J. H. Kleinschmidt, "Mitigating On-Off Attacks in the Internet of Things Using a Distributed Trust Management Scheme," *International Journal of Distributed Sensor Networks*, vol. 11, no. 11, pp. 1–8, 2015.

[124] Y. B. Saied], A. Olivereau, D. Zeghlache, and M. Laurent, "Trust Management System Design for the Internet of Things: A Context-aware and Multi-service Approach," *Computers & Security*, vol. 39, pp. 351 – 365, 2013.

[125] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A. MacDermott, and X. Wang, "CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5432–5445, 2019.

[126] B. Yu and M. P. Singh, "An Evidential Model of Distributed Reputation Management," in *Proceedings of the 1st ACM International Joint Conference on Autonomous Agents and Multiagent Systems*, ser. AAMAS '02, 2002, p. 294–301.

[127] F. Bao, I. Chen, and 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.

[128] S. Sagar, A. Mahmood, J. Kumar, and 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.

[129] Z. Chen, R. Ling, C.-M. Huang, and X. Zhu, "A Scheme of Access Service Recommendation for the Social Internet of Things," *International Journal of Communication Systems*, vol. 29, no. 4, pp. 694–706, 2016.

[130] I. Garcia-Magarino, S. Sendra, R. Lacuesta, and J. Lloret, "Security in Vehicles with IoT by Prioritization Rules, Vehicle Certificates, and Trust Management," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5927–5934, 2019.

[131] S. Namal, H. Gamaarachchi, G. MyoungLee, and 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.

[132] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "A Survey of Trust Management in the Internet of Vehicles," *Electronics*, vol. 10, no. 18, p. 2223, 2021.

[133] M. Masmoudi, W. Abdelghani, I. Amous, and 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.

[134] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3297–3308, 2021.

[135] A. Chakrabarti, *Managing Trust in the Grid*. Springer Berlin Heidelberg, 2007, pp. 215–246.

[136] H. Al-Hamadi and I. R. Chen, "Trust-Based Decision Making for Health IoT Systems," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1408–1419, 2017.

[137] W. Li, H. Song, and F. Zeng, "Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 716–723, 2018.

[138] V. Mohammadi, A. Rahmani, A. Darwesh, and A. Sahafi, "Trust-based Recommendation Systems in Internet of Things: a Systematic Literature Review," *Human-centric Computing and Information Sciences*, vol. 9, pp. 1–61, 2019.

[139] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A Roadmap for Security Challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[140] L. Wei, J. Wu, C. Long, and B. Li, "On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4775–4787, 2021.

[141] M. A. Azad, S. Bag, F. Hao, and A. Shalaginov, "Decentralized Self-Enforcing Trust Management System for Social Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2690–2703, 2020.

[142] N. Truong and 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.

[143] S. Aalibagi, H. Mahyar, A. Movaghar, and H. E. Stanley, "A Matrix Factorization Model for Hellinger-based Trust Management in Social Internet of Things," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2021.

[144] S. Sagar, A. Mahmood, M. Zaib, Q. Z. Sheng, and 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, p. 283–290.

[145] O. Ben Abderrahim, M. H. Elhdhili, and 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.

[146] P. De Meo, L. Fotia, F. Messina, D. Rosaci, and G. M. Sarne, "Providing Recommendations in Social Networks by Integrating Local and Global Reputation," *Information Systems*, vol. 78, pp. 58–67, 2018.

[147] B. Jafarian, N. Yazdani, and M. Sayad Haghighi, "Discrimination-aware Trust Management for Social Internet of Things," *Computer Networks*, vol. 178, p. 107254, 2020.

[148] N. Li, V. Varadharajan, and S. Nepal, "Context-Aware Trust Management System for IoT Applications with Multiple Domains," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 1138–1148.

[149] U. Jayasinghe, N. B. Truong, G. M. Lee, and 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.

[150] J. I. Chen, "Embedding the MRC and SC Schemes into Trust Management Algorithm Applied to IoT Security Protection," *Wireless Personal Communication*, vol. 99, no. 1, p. 461–477, 2018.

[151] H. Xia, S. Zhang, Y. Li, Z. Pan, X. Peng, and X. Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7108–7120, 2019.

[152] O. Ben Abderrahim, M. H. Elhedhili, and L. Saidane, "CTMS-SIOT: A context-based trust management system for the social Internet of Things," in *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, pp. 1903–1908.

[153] C. Marche, L. Atzori, and M. Nitti, "A Dataset for Performance Analysis of the Social Internet of Things," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2018, pp. 1–5.

[154] M. B. Monir, M. H. Abdel Aziz, A. A. Abdel Hamid, and E. M. EI-Horbaty, "Trust Management in Cloud Computing: A Survey," in *IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, 2015, pp. 231–242.

[155] Q. H. Cao, M. Giyyarpuram, R. Farahbakhsh, and N. Crespi, "Policy-based Usage Control for a Trustworthy Data Sharing Platform in Smart Cities," *Future Generation Computer Systems*, vol. 107, pp. 998–1010, 2020.

[156] L. Gu, J. Wang, and B. Sun, "Trust management mechanism for Internet of Things," *China Communications*, vol. 11, no. 2, pp. 148–156, 2014.

[157] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust Management of Services in Cloud Environments: Obstacles and Solutions," *ACM Computing Survey*, vol. 46, no. 1, pp. 1–30, 2013.

[158] F. Fraile, T. Tagawa, R. Poler, and A. Ortiz, "Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4506–4514, 2018.

[159] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A Comprehensive Study on the Trust Management Techniques in the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9326–9337, 2019.

[160] Howe and Jeff, "The Rise of Crowdsourcing," *Wired*, vol. 14, pp. 1–4, 2006.

[161] K. Habak, M. Ammar, K. A. Harras, and 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.

[162] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the Implementation of IoT for Environmental Condition Monitoring in Homes," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3846–3853, 2013.

[163] E. Bulut, S. Hernandez, A. Dhungana, and B. K. Szymanski, "Is Crowdcharging Possible?" in *27th International Conference on Computer Communication and Networks (ICCCN)*, 2018, pp. 1–9.

[164] X. Gan, Y. Li, Y. Huang, L. Fu, and X. Wang, "When Crowdsourcing Meets Social IoT: An Efficient Privacy-Preserving Incentive Mechanism," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9707–9721, 2019.

[165] C.-H. Liu and C.-F. Chiang, *Social IoT Crowd-Sourcing on Disaster Reduction*. Springer Berlin Heidelberg, 2019, pp. 1–6.

[166] A. Khelloufi, H. Ning, S. Dhelim, T. Qiu, J. Ma, R. Huang, and L. Atzori, "A Social-Relationships-Based Service Recommendation System for SIoT Devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1859–1870, 2021.

[167] Q. Z. Sheng, J. Yu, W. E. Zhang, S. Wang, X. Li, and 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.

[168] K. Bok, Y. Kim, D. Choi, and J. Yoo, "User Recommendation for Data Sharing in Social Internet of Things," *Sensors*, vol. 21, no. 2, p. 462, Jan 2021.

[169] A. Mahmood, W. Zhang, and Q. Sheng, "Software-Defined Heterogeneous Vehicular Networking: The Architectural Design and Open Challenges," *Future Internet*, vol. 11, no. 3, p. 70, 2019.

[170] Nitti, Michele and Girau, Roberto and Floris, Alessandro and Atzori, Luigi, "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.

[171] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social Internet of Vehicles: Architecture and Enabling Technologies," *Computers & Electrical Engineering*, vol. 69, pp. 68–84, 2018.

[172] L. Atzori, A. Floris, R. Girau, M. Nitti, and G. Pau, "Towards the implementation of the Social Internet of Vehicles," *Computer Networks*, vol. 147, pp. 132–145, 2018.

[173] L. Chengzhe, D. Yangyang, G. Qili, and Z. Dong, "A Trust-based Privacy-preserving Friend Matching Scheme in Social Internet of Vehicles," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2011–2025, 2021.

[174] C. A. Kerrache, N. Lagraa, R. Hussain, S. H. Ahmed, A. Benslimane, C. T. Calafate, J.-C. Cano, and A. M. Vegni, "TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5870–5877, 2019.

[175] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the Ratee: A Trust Management System for Social Internet of Vehicles," *Wireless Communications and Mobile Computing*, vol. 2017, pp. 1–11, 2017.

[176] U. Javaid and B. Sikdar, "A Secure and Scalable Framework for Blockchain Based Edge Computation Offloading in Social Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4022–4036, 2021.

[177] T. Wang, A. Hussain, L. Zhang, and C. Zhao, "Collaborative Edge Computing for Social Internet of Vehicles to Alleviate Traffic Congestion," *IEEE Transactions on Computational Social Systems*, pp. 1–13, 2021.

[178] X. Kong, H. Gao, G. Shen, G. Duan, and S. K. Das, "FedVCP: A Federated-Learning-Based Cooperative Positioning Scheme for Social Internet of Vehicles," *IEEE Transactions on Computational Social Systems*, pp. 1–10, 2021.

[179] L. Xing, X. Jia, J. Gao, and H. Wu, "A Location Privacy Protection Algorithm Based on Double K-Anonymity in the Social Internet of Vehicles," *IEEE Communications Letters*, vol. 25, no. 10, pp. 3199–3203, 2021.

[180] E. Ojie and 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.

[181] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally, "Internet of Things (IoT): Research, Simulators, and Testbeds," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1637–1647, 2018.

[182] U. Wilensky, "NetLogo," https://ccl.northwestern.edu/netlogo/, 1999, [Online; Accessed 10-March-2021].

[183] A. Mei and J. Stefa, "SWIM: A Simple Model to Generate Small Mobile Worlds," in *IEEE International Conference on Computer Communications (INFOCOM)*, 2009, pp. 2106–2113.

[184] G. F. Riley and T. R. Henderson, "The NS-3 Network Simulator," in *Modeling and tools for network simulation*. Springer, 2010, pp. 15–34.

[185] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer Network Simulation with NS-3: A Systematic Literature Review," *Electronics*, vol. 9, p. 272, 2020.

[186] "Veins," https://veins.car2x.org/, [Online; Accessed 10-March-2021].

[187] P. Deshpande, P. Kodeswaran, N. Banerjee, A. Nanavati, D. Chhabra, and S. Kapoor, "M4M: A Model for Enabling Social Network Based Sharing in the Internet of Things," *7th International Conference on Communication Systems and Networks (COMSNETS)*, pp. 1–8, 2015.

[188] "ThingSpeak," https://thingspeak.com/, [Online; Accessed 10-March-2021].

[189] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A Library for Parallel Simulation of Large-Scale Wireless Networks," *ACM SIGSIM Simulation Digest*, vol. 28, no. 1, p. 154–161, 1998.

[190] A. Dunkels, B. Gronvall, and 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, p. 455–462.

[191] C. Marche, L. Atzori, V. Pilloni, and M. Nitti, "How to Exploit the Social Internet of Things: Query Generation Model and Device Profiles' Dataset," *Computer Networks*, vol. 174, p. 107248, 2020.

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

[193] M. Richardson, R. Agrawal, and P. Domingos, "Trust Management for the Semantic Web," in *International Semantic Web Conference (ISWC)*, 2003, pp. 351–368.

[194] Z. Lin and L. Dong, "Clarifying Trust in Social Internet of Things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 2, pp. 234–248, 2018.

[195] S. Sagar, A. Mahmood, Q. Z. Sheng, and 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, p. 635–636.

Subhash Sagar received the BS in Electrical (Telecommunication) from the COMSATS Institute of Information Technology, Islamabad, Pakistan and a Master's degree in Computer Science from South Asian University, New Delhi, India in 2012 and 2016 respectively. He is currently pursuing PhD degree at the School of Computing, Macquarie University, Sydney, Australia. Before moving to Macquarie University, Subhash worked as a faculty member at the Department of Computer Science, National University of Computer and Emerging Sciences, Karachi, Pakistan from 2017 to 2019. His current research interests include the Internet of Things, Social Internet of Things, and Trust Management.

Adnan Mahmood holds a PhD degree in Computer Science and is currently a Postdoctoral Research Fellow 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 Republic of Ireland, South Korea, Malaysia, Pakistan, and People's Republic of China. His research interests include Software-Defined Networks, Intelligent Transportation Systems, Internet of Things (primarily the Internet of Vehicles), Trust Management, and the Next Generation Heterogeneous Wireless Networks. Adnan besides serve on the Technical Program Committees of a number of reputed International Conferences. He is a member of the IEEE, IET, and the ACM.

Quan Z. (Michael) Sheng is a full Professor and Head of School of Computing at Macquarie University. Before moving to Macquarie, Michael spent 10 years at School of Computer Science, the University of Adelaide (UoA). 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, Sheng also worked at UNSW as a visiting research fellow. Prior to that, he spent 6 years as a senior software engineer in industries. Prof Sheng's research interests include the Internet of Things, big data analytics, service computing, and Internet technologies. Dr. Michael Sheng is the recipient of the ARC Future Fellowship (2014), Chris Wallace Award for Outstanding Research Contribution (2012), and Microsoft Research Fellowship (2003). He is ranked by Microsoft Academic as one of the Most Impactful Authors in Services Computing (ranked top 5 all time). He is a member of the IEEE and the ACM.

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 PhD 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.

Wei (Emma) Zhang is currently a Lecturer at the School of Computer Science, The University of Adelaide. She obtained her PhD 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 PhD thesis has been published by Springer as a monograph. She is a member of the IEEE, the ACM and the ACL.