IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 16 September 2022, accepted 7 October 2022, date of publication 13 October 2022, date of current version 18 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3213699

SURVEY

Trust Management in Social Internet of Things (SIoT): A Survey

SANA ALAM[1,2], SHEHNILA ZARDARI[3], SHAHEENA NOOR[2], SHAKIL AHMED[2], AND HARALAMBOS MOURATIDIS[4,5]

[1]Department of Computer Science and Information Technology, NEDUET, Karachi 75270, Pakistan
[2]Department of Computer Engineering, Syed University of Engineering and Technology (SSUET), Karachi 75300, Pakistan
[3]Department of Software Engineering, NEDUET, Karachi 75270, Pakistan
[4]Institute for Analytics and Data Science, University of Essex, CO4 3SQ Colchester, U.K.
[5]Department of Computer and Systems Sciences, Stockholm University, SE-164 07 Kista, Stockholm, Sweden

Corresponding author: Sana Alam (sana.email43@gmail.com)

ABSTRACT A survey on trust management in the Social Internet of Things (SIoT) is provided, beginning with a discussion of SIoT architectures and relationships. Using a variety of publication databases, we describe efforts that focus on various trust management aspects of SIoT. Trust management models comprise three themes: trust computation, aggregation, and updates. Our study presents a detailed discussion of all three steps. Trust computation and trust aggregation depend upon Trust Attributes (TAs) for the calculation of local and global trust values. Our paper discusses many strategies for aggregating trust, but ''Weighted Sum'' is the most frequently used in the relevant studies. Our paper addresses trust computation and aggregation scenarios. Our work classifies research by TAs (Social Trust, Quality of Service). We've categorized the research (reputation-based, recommendation-based, knowledge-based) depending on the types of feedback/opinions used to calculate trust values (global feedback/opinion, feedback from a friend, trustor's own opinion considering the trustee's information). Our work classifies studies (policy-based, prediction-based, weighted sum-based/weighted linear combination-based) by trust computation/aggregation approach. Two trust-update schemes are discussed: time-driven and event-driven schemes, while most trust management models utilize an event-driven scheme. Both trust computation and aggregation need propagating trust values in a centralized, decentralized, or semi-centralized way. Our study covers classifying research by trust updates and propagation techniques. Trust models should provide resiliency to SIoT attacks. This analysis classifies SIoT attacks as collaborative or individual. We also discuss scenarios depicted in the relevant studies to incorporate resistance against trust-related attacks in SIoT. Studies suggest context-based or context-free trust management strategies. Our study categorizes studies based on context-based or context-free approaches. To gain the benefits of an immutable, privacy-preserving approach, a future trust management system should utilize Blockchain technology to support non-repudiation and tracking of trust relationships.

INDEX TERMS Social Internet of Things, SIoT, trust, architecture, attacks, future direction, application areas, event-driven, time-driven, context-based, trust attributes.

I. INTRODUCTION

The Internet of Things (IoT) provides a platform to integrate a large number of distributed heterogeneous systems. Ubiquitous computing is the backbone of IoT, indicating a network of uniquely identifiable interconnected smart objects using standard communication protocols [1]. These resource-constrained smart devices communicate and collaborate in various contexts. However, IoT is not just a global network of smart devices, but also encompasses a group of supporting technologies along with the necessary services and set of applications [2]. IoT can be seen as a network whose prime objective is to include devices or nodes which can request or provide services. Moreover, nodes

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

can collaborate to provide a single service [3]. Since the inception of IoT, there has been progress in this paradigm at an unprecedented rate resulting in the innovation of many different visions and contexts such as ''Social IoT'' (SIoT), industrial IoT, and IoT in the healthcare domain.

IoT enables various heterogeneous devices to communicate and collaborate while providing or acquiring different services. However, this collaborative interaction can lead to trust challenges between devices, requiring a decentralized, mobile, cost-effective, low latency, lightweight and scalable trust management framework. The merging of ''social networks'' and the ''internet of things'' leads to the realization of SIoT [4], which has been characterized by the heterogeneity of the software and hardware components and a variety of hardware architectures. In SIoT these heterogeneous devices collaborate and cooperate with each other to achieve a common target [5]. SIoT is a broad term that includes connection solely between people, between ''things'', or between people and things [6]. Geographically dispersed heterogeneous objects can be efficiently discovered through the use of SIoT [7].

SIoT includes both peer-to-peer networks and social relationships amongst multiple autonomous systems, where nodes act as service providers (SPs) or service requesters/ consumers (SRs or SCs). Every object or node on a social network acquires valid responses to their requests as compared to the objects or nodes working individually [8], [9]. The primary goal of SIoT is to decouple things from people and allow them to self-organize – to share computational resources, information, and services. Each object must decide on the type of relationship it has with other objects [9].

User-to-Object Relationships and Object-to-Object Relationships are both possible in a SIoT system, depending on their respective affiliations. Relationship types play a critical role in inter-SIoT communication and the application domain [10]. When ''things'' discover that they have a social nature, they begin to form connections with one another. Based on factors like specifications of entities or nodes, activity patterns, programs installed, services rendered, etc. social links between objects can be constructed [11], [12]. Social relationships in the SIoT can be classified as:

- Parent-object relationship: refers to objects or nodes belonging to the same manufacturer [4], [12] i.e., under the same batch. Mostly the nodes owned by the same manufacturer are homogeneous.
- Co-location relationship: this relationship exists between objects belonging to the same location [4], [12]. Objects can be located in the same city or same workplace depending on their physical location.
- Co-work relationship: objects actually cooperate with each other towards a common application/ goal [4], [12]. The relationship is established between homogenous or heterogenous objects.
- Ownership object relationship: present among objects belonging to the same owner. The objects need not be homogeneous [4].
- Social object relationship: forms when nodes encounter contact, irregularly or consistently, for reasons that are solely connected to relationships among their respective owners [4], [12]. It is normally formed between heterogeneous objects/ nodes.

There is no standard SIoT architecture. However, this section provides a comprehensive study of SIoT architectures presented in the existing literature.

Reference [13] architecture clearly separates server-side and client-side. The base, component, and application layers are server-side. The base layer is a database, and the component layer includes ID management (for storing information related to different aspects of objects ID), object profiling, owner control (for specifying various policies as established by the owners), relationship management, service discovery (based on the discovery of suitable service providers), service composition, and trustworthiness management. The application layer includes service APIs and interfaces to entities. On the client-side (object-side) [13], layers include the first layer: the object layer (consisting of objects and their communication interfaces), the second layer: the object abstraction layer (to facilitate communication among heterogeneous objects), the third layer: social agent (to facilitate communication between objects and SIoT servers) and service management (providing the human-computer interface to administer the behavior of nodes or objects in SIoT).

Reference [4]'s SIoT architecture is based on [13] comprising SIoT server (network and application layers), gateway layer, and object layer. Base, component, and interface sub-layers make up the application layer. Sensing, network, and application layers make up the gateway and object layers.

The architecture [14] has three layers: an ontology layer with a profile handler (for social things and object profiles), a rules handler (which deals with the event-driven actions by users), and a recommendations module (concerned with the database of ontology and real data to deduce recommendations). The control layer contains the system's data model and performance models. The third is the communication layer, which uses RESTful interfaces to communicate with external services.

The study [15] offers the following architecture components: i) actors can publish data and receive control orders to manage it. ii) intelligent system: manages actor interactions. iii) all communications with the system occur through an ''interface'', which allows data and queries to be submitted and produces the needed output, and iv) the ''internet.''

Reference [16] offers a four-component SIoT design. The profiling and Policy Management component assigns unique identifiers to VE (Virtual Entities) and allows for the depiction of a physical entity utilizing the VE's domain ontology. Friends Management (FM) develops and manages a VE friends list. Social Monitoring encompasses tools and tactics for monitoring VEs' social aspects. The Social Analysis component extracts VEs' social features (such as centrality) and their behavior and relationship frameworks and trends.

The paper [17] describes a 4-layer SIoT architecture in the cloud-based platform ''Lysis''. The first layer, called the real world, contains real-world objects called ''things'' that can be physical devices or gateways. It has four modules. i) a hardware abstraction layer to facilitate communication in the associated module at the virtualization level; (ii) a data handler for processing sensor data before forwarding it to the virtualization level; (iii) a device management module that incorporates device functionality; (iv) hardware drivers related to sensors and actuators, called environment interface or protocol adapter. The second layer provides a direct interface to the real world and includes social virtual objects. Using micro engines (MEs), the third layer aggregates data. MEs construct social virtual objects. The application layer deploys apps utilizing one or more MEs.

Reference [18] presents a SIoT service recommendation architecture. Architecture layers include perception, network, and interoperability. The perception layer senses and collects IoT data. This layer can include RFID tags, sensors, etc. The second layer is the network layer. The network layer maps IoT data from the perception layer into communication protocols and sends it to the next layer for processing. The interoperability layer (the third layer) shares data amongst IoT apps due to their varying semantics. The architecture presents a SIoT recommendation system for data from the interoperability and perception layer. This recommendation system uses SIoT data to develop and manage device-device or human-device social relationships.

Reference [19] proposes a three-level social web objects architecture. Object virtualization manages virtual objects (VO). The second level aggregates VOs to create composite VOs (CVOs). The third level, the service level, deploys microservices to handle service requests and execution.

Reference [20] proposes an agent-based technique for integrating edge computing into large-scale SIoT frameworks. The suggested architecture includes three components: i) physical devices (native, foreign, and external devices). ii) in-network edge environment with virtual and social objects, iii) internet services with cloud and social sensors.

The Internet of Vehicle (IoV) paradigm [21] involves data accessibility and interaction made possible by the Internet of Things, considering vehicles as mobile IoT devices that can communicate. By supporting multiple dynamic interactions between vehicles, the IoV paradigm can be extended to the corresponding Social Internet of Vehicles (SIoV) [22]. This allows vehicles to develop and govern social interactions based on owner needs, context, and application. Two vehicles traveling in the same direction can share traffic information despite their distance. A vehicle might also initiate social ties. Even if vehicle owners aren't acquainted, they can create social interactions to share road conditions while commuting to the same area via different routes. Time-tested social ties can be exploited to establish new interactions that enable value-added service. If a driver needs to identify a refueling station with the least amount of waiting time, the car can create new social ties with other vehicles along the route to gather trustworthy information [23]. By utilizing the web of these relationships, SIoV offers a number of novel traffic control applications [24]. This method makes secure and private information sharing between vehicles difficult. MSIoT is a paradigm that incorporates mobility, heterogeneous devices, and the need for standardization through the integration of SIoT, SIoV, and MSN in the same framework [25].

Figure 1 represents a general SIoT architecture, where the first layer involves data sensing, followed by a network layer that connects devices in the sensing layers and the applications that make use of both of these layers. SIoT applications can include service discovery, service management, and components to store and facilitate service provisioning.

SIoT depends on trust between multiple entities. SIoT trust management is more important because unknown devices may be unreliable. Trust management influences how dynamic entities perform specific tasks, the scalability of their interactions, and mobility in a SIoT environment. Unknown and mistrusting SIoT entities that communicate and collaborate highlight the need to secure and trust data during communication and storage on resource-constrained IoT devices.

In a nutshell, our contributions are listed below.

i) Our work includes a list of numerous Trust Attributes (TAs) used in the pertinent studies in addition to providing a full discussion of the different trust properties by classifying them into ''Social Trust Properties'' and ''General Trust Properties''. The two main types of TAs are ''Social Trust'' and ''Quality of Service.'' In addition, the survey categorizes studies based on the types of TAs that were employed.

ii) The survey not only enumerates the methods for trust computation and trust aggregation but also illustrates the scenarios in which these methods are applied in the studies that are of interest.

iii) Our study also classifies the studies (policy-based, prediction-based, weighted sum based/ weighted linear combination based) in accordance with the types of trust computation/ aggregation methods being used.

iv) We've classified the research (reputation-based, recommendation-based, knowledge-based) depending on the types of feedback/opinions used to calculate trust values (global feedback/opinion, feedback from a friend, trustor's own opinion considering the trustee's information).

v) According to the Trust Updates and Trust Propagation Schemes that are being employed, our analysis classifies the studies. In addition to incorporating pertinent research from Google Scholar, IEEE Explore, Science Direct, ACM DL, Springer, ProQuest, and ISI Web of Science, our work also gives publishing trends of pertinent studies in terms of the frequency of publications since 2012.

vi) Our study presents an insight into trust-related attacks in SIoT. The work identifies the attacks as ''Intrin-

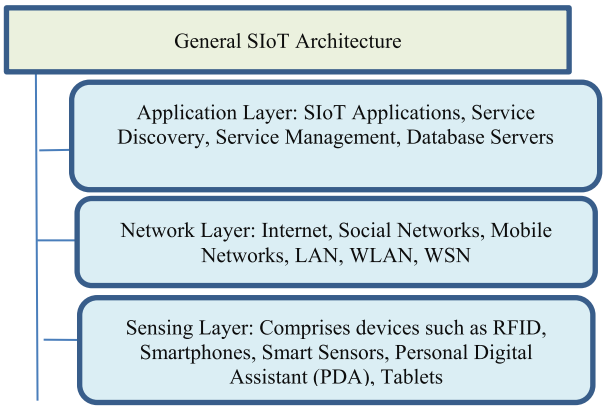


FIGURE 1. General SIoT architecture.

sic'' or ''Extrinsic'' and further elaborates on scenarios that provide resiliency against attacks in the relevant studies.

vii) The survey covers a brief description of the most widely used simulators with respect to trust management in SIoT. Additionally, the study provides a list of simulators/analysis tools utilized in the experiments in the respective studies.

viii) In our survey, we divide research into two camps, those that take a context-based approach to trust management and those that take a context-free approach.

ix) Lastly our work includes Application Areas, Challenges, and Future Direction for trust management in SIoT.

Section I gives a context for our study, followed by related work in Section II. Section III gives the survey methodology, Section IV presents trust management frameworks, and findings in accordance with the pertinent studies, and Section V provides discussion and analysis. Section VI describes SIoT application areas, whereas Section VII discusses challenges and future directions. Section VIII presents the conclusion.

II. RELATED WORK

Trust properties and models are presented in surveys [26], however, the associated trust management systems, simulation tools, and components are not described. These surveys do not include challenges, future directions, and potential trust aggregation schemes.

In [27] a limited number of studies are considered, and analysis is based on various performance metrics. These surveys do not cover trust update schemes, trust properties and trust propagation schemes.

The surveys [28] describe SIoT trust and ''friendliness'' techniques, in which the concept of SIoT is examined for supporting cloud computing, multiagent systems and Industry 4.0. A contrast of various trust and friendliness techniques in SIoT is provided. There is however no discussion of trust management strategies, notably for SIoT.

In [29] a holistic perspective of the SIoT domain is provided, including recent research developments in SIoT, such as the discovery of services and their composition, management of relationships between services, and trust management frameworks. Subjective/ objective and dynamic trust management schemes are described, but a contrast of the most recent trust management frameworks/ models in the SIoT domain is not included.

Another survey [12] contrasts and evaluates trust management approaches in various fields, including Wireless Sensor Networks (WSN) and the Internet of Things (IoT), followed by a description of various trust management aspects. However, the comparison is not limited to SIoT trust management processes; it also incorporates IoT trust management.

The survey [30] presents a comparative evaluation of trust models for SIoT and Online Social Networks (OSN). In [30] the key components and parameters needed to create a realistic trust model specific to MOOC platforms are described, aimed to provide an appealing learning environment for learners. Trust models are compared based on their architecture, the initial value of trust, trust updates, a trust decay factor, context/ risk, resistance to attack, and scalability.

The survey [31] investigates common themes between IoT and SIoT domains; SIoT-related architectures are examined, and SIoT trust management platforms are compared, along with a discussion of future research challenges in SIoT. This work lacks an assessment of trust in SIoT-based applications, SIoT platforms, and potential research challenges in trust assessment for SIoT.

III. METHODOLOGY

This section provides the methodological process, as shown in Figure 2, for conducting the literature review. Figure 3 represents the structure of our survey.

A. SELECTION OF RELEVANT STUDIES

The query used for the selection of papers is *((''SIoT'' OR ''Social internet of things'') AND (''trust'' OR ''TMS'' OR ''DTMS''))*

Where: DTMS – distributed trust management schemes; TMS – Trust Management Schemes.

B. INCLUSION/EXCLUSION OF RESEARCH STUDIES

1) INCLUSION

Only research articles, over the time period 2012-2022, related to trust management in the domain of SIoT are considered. These research articles are published as journal articles, conference papers or book chapters.

2) EXCLUSION

All other studies not related to trust management aspects of SIoT domain are filtered out. The studies which are not in English and research studies for which full text is not available are excluded.

C. FORMATION OF RESEARCH QUESTIONS

The research questions in Table 1 are for analysis purposes, to comprehend the three general steps of the Trust Management Framework (Sec IV).

TABLE 1. Research questions in our research study.

Research Questions	Section Numbers of Analysis
What are the Trust Attributes used for Trust Values Composition / Calculation in research studies?	Section IV (Table 3)
What methods/ techniques are used for Trust Value Calculation/ Aggregation in the relevant research works?	Section IV (Table 3)
What scenarios are used for Trust Value Calculation/ Aggregation in research studies?	Section IV (Table 4)
Which Trust Update Method is being used in research studies?	Section IV (Table 5)
Which Trust Propagation scheme is being used in the studies?	Section IV (Table 6)
Which trust-related attacks are being addressed in the studies?	Section IV (Table 7)
Which simulator/analysis tool is being used for performance evaluation of the proposed trust management schemes in the studies?	Section IV (Table 7)
Classification of studies in accordance with the types of TAs (Social Trust, Quality of Service (QoS) being used.	Section V (Figure 8)
Classification of studies (reputation-based, recommendation-based, knowledge-based) according to the types of opinions/feedback being used (global opinion, feedback from a friend, trustor's own assessment based upon the information provided by the trustee).	Section IV (Figure 9)
Classification of studies (policy-based, prediction-based, weighted sum based/ weighted linear combination based) in accordance with the types of trust computation/ aggregation methods being used.	Section IV (Figure 10)
Classification of studies on the basis of context-based or context-free approach.	Section IV (Figure 11)
What is the publication trend in trust management in SIoT since 2012?	Section V (Figure 7 and Table 8)
What mechanisms are being used for addressing the attacks in the studies?	Section V
Brief Description of each relevant work	Section V

D. ABBREVIATIONS WITH FULL FORM

Table 2 contains a list of the abbreviations which is used frequently in the succeeding sections.

TABLE 2. List of abbreviations with their full forms.

Abbreviations	Meaning
SIoT	Social Internet of Things
BMA	Bad Mouthing Attack
BSA	Ballot Stuffing Attack
GMA	Good Mouthing Attack
SPA	Self-Promoting Attack
WA	Whitewash Attack
DA	Discriminatory Attack
OSA	Opportunistic Service Attack
OOA	On/ Off Attack
NA	Not Available
SP	Service Provider
SC	Service Consumer
SR	Service Requester
TA	Trust Attributes
ML	Machine Learning

IV. TRUST MANAGEMENT FRAMEWORK IN SIoT AND FINDINGS

A. CONCEPT OF TRUST

A deep belief in the dependability, honesty, sincerity, justice, and good confidence of others to carry out a deal, transaction, commitment, agreement, etc. in line with established principles, norms, laws, expectations, and undertakings is referred to as trust [32], [33]. The concept of trustworthiness can be explained in terms of the relationship among entities in trusting exchanges. Trustworthiness, therefore, depends on the attributes of the trustees in the given context [33].

1) TRUST IN VARIOUS FIELDS

The concept of trust isn't restricted to IoT or SIoT; it's also used in psychology, economics, organizational management, sociology, networking, computers, and many other sectors. Trust's definition varies by field [34]. Security has always been a fundamental barrier to technology adoption. SIoT says security and trust are vital for device interaction.

"Sociological trust" refers to an assessor's prior subjective likelihood that a subject (or agent, or group) would conduct particular actions that have an impact on the assessor as defined by Gambetta [35]. The study [36] applied Gambetta's trust concept to the sociological concept of trust by rephrasing it as a continuous variable and quantifying it based on context or risk acceptance.

When people accept risks because of ambiguity or insufficient knowledge, trust is viewed as an expectation in the field of "economics" [37].

Cognitive techniques and orientations have been used to describe "Psychological" trust [38].

In "organizational management," "trust" refers to the degree to which one side is prepared to rely on someone or something with relative security notwithstanding potential consequences [39]. Trust is the willingness to take a chance on someone's competence, integrity, and benevolence, according to a study [40]. They stated that trust isn't always reciprocated.

When it comes to create collaborative settings to maximize system objectives the idea of trust has long been appealing to "communication and network" protocol developers. Trust is defined as "a collection of network-related relationships" [41]. These relationships are based on prior protocol interactions. Because they've been consistent with their protocols, trust has built up between these two entities. Capra [42] suggests human interactions based trust paradigm for MANETs.

In SIoT, trust is a process the trustor employs to assign responsibilities to the trustee and use the trustee's actions that will forward their objectives. The trustor evaluates the trustee's competence and willingness. The trustor acknowledges the risk of being exposed by placing the trustee in a certain environment. Each party evaluates the other's trustworthiness. It's affected by environmental unpredictability, behavioral consequences, and the context of the task [7].

"Trustor" and "Trustee" are the two trusting parties. "Trustor" evaluates "trustee's" trust. Environment,

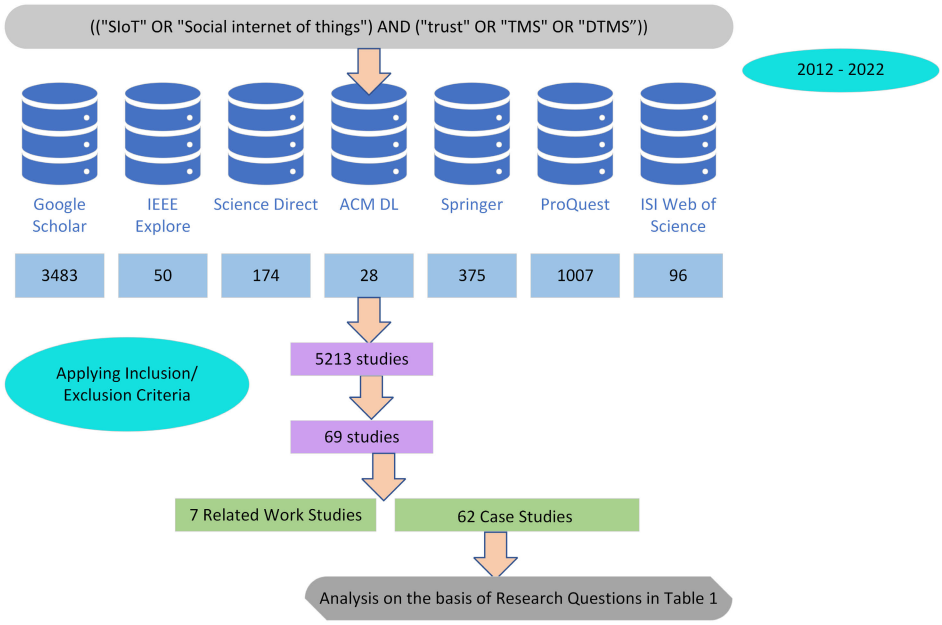


FIGURE 2. Methodological process.

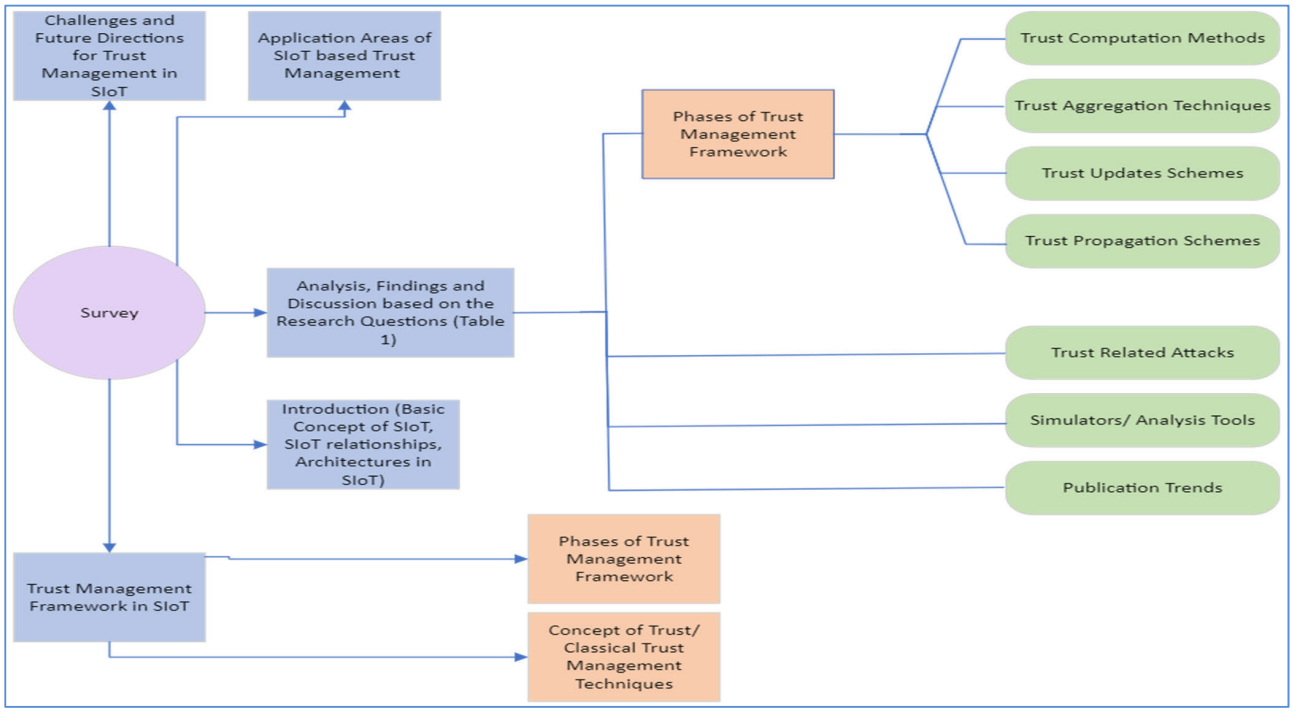


FIGURE 3. Survey structure.

location, time, purpose, etc. affect trust values. In the SIoT context, ''trustors'' and ''trustees'' are ''service consumers/requesters'' and ''service providers''.

2) CLASSICAL TRUST MANAGEMENT FRAMEWORKS AND DEVELOPMENTS

Marsh's 1994 Ph.D. dissertation [43] is considered the first formal, computer-based trust model. His primary problems with trusting were a lack of clarity, a plethora of terminology, and not being formally used in scholarly works and daily life. Marsh proposed a set of subjective variables that might be merged into a single (continuous) trust value [1, 1]. For many, this range means full distrust or trust. Marsh said ultimate trust or distrust is unrealistic. Marsh distinguished three types of trust: fundamental, which exists in all situations, general, which occurs between two individuals in all encounters, and situational, which occurs between two people only when they are in the same setting. Marsh also noted that time

affects trust. Authors who quote Marsh typically simplify his work (e.g., trust is a continuous value, and its composition is unimportant) or don't follow his model because getting values for specific variables required to calculate trust is difficult (e.g., importance, utility, competence, risk).

Centralized or decentralized/distributed trust frameworks are categorized by trust management strategies. To ensure data security, centralized trust-related data management systems typically involve a third party. For IoT objects, a trusted central server delivers robust and effective data administration, maintains data consistency, and makes system deployment easier [44]. One central authority that can compute controls the centralized trust framework [45].

Reference [46] manages a centralized trust management approach. The trust management concept includes a service server and a trust management server. The service server handles node authentication, registration, service discovery, the community of interest proposal, and dynamic similarity computation. The trust management server collects node feedback to calculate contextual trust and reputation to classify and forecast node behavior. The advantage of the centralized trust management approach is that only centralized devices need sufficient hardware for trust management [45]. For a decentralized trust management approach, each decentralized node must maintain trust information about other network nodes for subsequent use, shortening their lifetime [46]. However, these centralized trust management techniques have scalability and single-point-of-failure problems

Next, trust-related frameworks are developed utilizing a decentralized or distributed method to improve scalability and avoid single points of failure. Authentication and cooperation amongst IoT devices facilitate data transmission and sharing in a decentralized trust management system, where trust-related data is stored locally and interactively communicated and shared. As cloud computing, IoT, SIoT, and fog computing gain prominence, trust management remains a concern.

P2P systems play an important role in distributed systems, thus we cover some traditional trust models. Eigen Trust [47] is a popular P2P trust paradigm. Each peer in a P2P file-sharing network has a unique global trust value, reducing the number of inauthentic files downloaded. Pre-trusted peers are a crucial aspect of the Eigen trust model, however, they don't always exist when the community is created, so this feature isn't always beneficial

The CuboidTrust is a global reputation trust management technique that builds four relationships among three trust sources, including resource quality, peer system contribution, and peer trustworthiness (with reporting feedback) [48]. Power iteration calculates each peer's global trust value. This architecture does, however, include the idea of pre-trusted peers, which is not always appropriate. In the CuboidTrust model, direct and indirect trusts receive the same treatment and are not given separate handling

The PeerTrust paradigm uses a transaction-based feedback mechanism to calculate and compare peers' trustworthiness

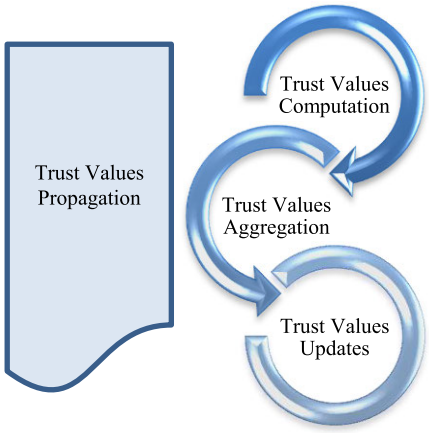


FIGURE 4. General steps in trust management framework in SIoT domain.

[49]. PeerTrust is a reputation-based trust-supporting framework. Five parameters to assess trust includes: feedback from peers, total transactions performed by peers, the legitimacy of the sources of peer feedback, and context factors with respect to transaction and community. It explains a general trust metric to integrate parameters [49]. PeerTrust does not differentiate between task and recommendation trust. It assumes peers with higher trust values always deliver more trustworthy feedback.

AntRep [50], [51] disperses reputation evidence across a P2P network. These authors suggested employing an ant system, which is easily adaptable to P2P networks' dynamic topology, to create trust. AntRep only distributes reputational evidence, not evaluates it

VectorTrust [52] provides P2P trust management. Single value expresses trust level. Along the chains, trust is multiplied. When there are multiple routes between two users, it chooses the most reliable one. Indirect trust is only used when the truster doesn't trust the trustee directly

Distributed approaches are better for scenarios with fewer events and nodes that do not need to execute frequent calculations, as each node in distributed trust management is responsible for maintaining robustness and computing trust degree [45]. Decentralized trust management offers fault tolerance, resiliency, no single point of failure, and increased security.

Further developments lead toward trust management in Multi-Agent Systems (MAS), Wireless Sensor Networks (WSNs), Wireless and Mobile ad hoc networks, Cloud Computing, IoT, and SIoT. However, our study focuses only on the trust management aspects of SIoT. The latest advancements in trust management aspect include the use of blockchain [53], [54], [55], [56] machine learning [57], [58] and deep learning [59], [60] in the trust management frameworks. Blockchain, in particular, provides transparency, immutability, fault tolerance, and enhanced security.

B. GENERAL STEPS IN TRUST MANAGEMENT FRAMEWORK

The general steps in trust management frameworks are depicted in Figure 4. It is to be noted that trust values are

propagated for the computation of global trust / overall trust either in a centralized or decentralized manner.

1) COMPUTATION OF TRUST VALUES

Trust computation steps focus on converting abstract theory and the concept of trust into precise numerical representation (e.g., a fuzzy representation of trust). In short, this step provides a better comprehension of trust by associating understandable and meaningful values with trust. This step is concerned with providing a ''local view'' of trust as experienced by the entity. The computation of trust is based on three basic steps.

- Selection of Trust Attributes based on but not limited to trust properties.
- Computation of Local Trust.
- Computation of Overall Trust / Global Trust.

The properties of Trust Attributes (TAs) are mostly classified as but are not limited to: (i) general trust attributes; and (ii) social trust attributes. General trust attributes reflect the generalized characteristics and are applicable to all domains and contexts. However, trust attributes specifically related to the social context are categorized as social trust attributes. Social networks are crucial for establishing connections of trust between different entities, according to researchers. Golbeck [61], [62] proposes the use of social networks as a bridge to create trust relationships between entities in order to establish the notion of ''Social Trust''.

a: GENERAL TRUST PROPERTIES

- Direct: in this case, trust is based upon direct interactions that take place between the trustor and trustee – generally based on their own experience [26],
  Indirect: in this case, when an entity or trustor has no information regarding the trustee then trust values based upon recommendations are considered. Thus, indirect interactions come into play to determine trust in an entity [26].
- Local: this view of trust solely depends upon the interaction between a trustor and a trustee. To elaborate on this, node a trusts node b, or node f trusts node b but node c does not trust node b. There is a factor of distrust between nodes c and b irrespective of the fact that both a and f individually trust node b. In other words, this trust is computed on the basis of the ''object-object relationship'' [26].
- Global: this value of trust is based upon the cumulative trust value of all nodes (that have interacted with the one being evaluated) towards the node being evaluated. Thus, it can be stated that this trust is computed on the basis of the ''objects-object relationship'' [26].
- Asymmetric: this means a trustor a trusts b, but trustor b does not trust a [26].
- Context-dependent: trust in a given node may vary depending on the context of use [26].
- Subjective: trust is fundamentally a matter of personal opinion based on numerous pieces of information or evidence, some of which may be more important than others [26].
- Objective: this trust value is computed by considering the QoS characteristics of the nodes or devices [26].

b: SOCIAL TRUST PROPERTIES

- Honesty – This trust characteristic states whether a node is honest or not. It is possible that SP provides good services only to those on the friend list and deliberately provides degraded services to other SCs. Nodes that exhibit dishonest attitudes cause extreme damage to trust management in social internet of things networks. Therefore, it is mandatory to draw a line between honest and dishonest nodes. Honesty is assessed by direct and indirect interactions [63].
- Cooperativeness – This feature represents whether a node is cooperative in terms of social aspects or not. In other words, to determine whether the SP and SC are cooperative with each other or not we use cooperativeness. SP can be cooperative with their friends SC and vice versa. Friends tend to cooperate with each other. A node can exhibit cooperativeness only when those are classified as its friends or with those nodes with which it has strong social links [63].
- Community of interest – This feature represents whether the nodes belong to the same community such as co-work, co-location, or not [63].
- Centrality – The centrality defines the importance of nodes with reference to the number of directly connected nodes which is termed *Degree Centrality*. If a node requires only a few intermediaries to contact others, then this indicates that the node is independent in a structural context. This type of centrality is termed *Closeness Centrality*. The third concept of centrality deals with the information flow control in a network. The fourth centrality concept is the quotient of the counts of all shortest paths between nodes in a particular network that consists of the regarded node and the total count of all shortest paths present in that network is termed *Betweenness Centrality* [64].

2) AGGREGATION OF TRUST VALUES

The process of aggregating different trust values based on direct and indirect interactions and experience comes under this step. Various methods are proposed for the aggregation of trust values. This aggregated value provides a broader view of trust.

This section provides a discussion of the methods/ processes involved in the computation of trust. These schemes are further used to calculate the aggregated value which is a vital phenomenon in the overall trust calculation.

Weighted Sum is one of the most commonly used techniques for trust calculation. If P is a set of parameters and W is the set of weights, where each parameter is assigned a weight,

then the weighted sum total value (WSTV) is calculated as:

$$\text{WSTV} = \sum_{i=1}^{n} Wi * Pi$$

where Pi = {p_1, p_2, p_3,...,p_n}; Wi = { w_1,w_2,w_3,...w_n}

Weights can be adjusted dynamically [65], [66] or statically thus providing ease of implementation, with low computational cost.

Bayes' theorem underpins the Bayesian System. Prior probability, posterior probability, and likelihood function are Bayes theory components. When given a prior probability and likelihood function, the goal is to calculate an item's posterior probability [67], [68]. Formula:

$$\rho(x/y) = (\rho(y/x)^* \rho(x))/(\rho(y))$$

where $\rho(x/y)$ = posterior probability of x given that y is true, $\rho(y/x)$= likelihood function of y occurring given that x is true

$\rho(x)$ = prior probability that x would occur

$\rho(y)$ = evidence or probability that y would occur

Inferences depend upon the data.

A machine learning model uses input data to automatically achieve a goal without being explicitly written (i.e., ''hard-coded''). These methods are ''soft-programmed'' to improve with time. Training involves supplying input data samples and desired results. In Machine Learning, unsupervised [69], supervised, and semi-supervised learning is used [70].

Multiplicative Attribute Graphs (MAG) are generative models for node-attribute systems. MAG combines node attributes and affinities to determine connection probability [71]. Positive or negative node affinities can exist. Homophily, heterophily, core-periphery, and Random are four affinities [71], [72]. MAG model reflects interactions between network structure and node's attributes.

Fuzzy logic focuses on uncertainty. It supports approximate values [73]. The fuzzy controller transforms real values into fuzzy logic. Fuzzy logic may easily reflect complex ambiguous problems, unlike Boolean logic, which only takes two values (0 and 1).

Deep learning is the calculation of hierarchical representations of observable data, where higher-level factors are described from lower-level factors [74]. Deep learning can be supervised or unsupervised. Deep learning networks include DNN, CNN, etc. for supervised learning. Deep Boltzmann machines and autoencoders are utilized for unsupervised learning [75]. Deep learning is a multi-layered representation-learning process [76].

The weighted directed graph has weighted vertices and edges. Vertex degree represents edge count. User relationships are represented as edges [77].

Nuclear physics influenced fission computing, which splits the core into subparts while preserving their characteristics. The first stage is to identify an entity that may divide its activities into two or maybe more subordinates, and the second phase is to discover features that can be used to divide resources among its subordinates. The first and second stages might be interchanged depending on the situation. In the third phase, fission computing parameters are set [78].

Table 3 represents the analysis of studies conducted concerning trust computation and trust aggregation schemes. This table includes the TAs used in the corresponding studies and the relevant techniques deployed for trust values computation and trust values aggregation. Table 4 represents the scenarios for trust computation/ aggregation techniques.

3) UPDATES IN TRUST VALUES

With the passage of time, changes occur in an entity's trust due to a number of factors. The entity can: (i) become a target of an attacker(s); (ii) change from being honest to dishonest, etc. The trust values of the entity might vary depending on the scenario and context, so a continuous update process in trust values related to an entity is required. After trust computation and propagation, the previous trust values of nodes can be updated. The two possible schemes for trust updates can be event or time driven as shown in Figure 5.

An event-driven update scheme consumes a much large number of resources as compared to the time-driven. In this scheme, the trust is updated at the end of each interaction or event [12]. The event can be feedback, violation of some privacy rules, environmental changes, etc.

A time-driven update scheme involves a periodic update [12]. The Time-driven scheme is more resource-efficient. It is quite difficult to decide on the granularity level of the time frames which is required for updates. Table 5 presents the categorization of studies by trust update schemes. The update schemes exhibit the dynamic nature of trust, as trust in the entities may change over time. However, many relevant studies have not considered the update mechanism of trust values in their proposed trust management framework/ model. The studies are represented by their reference numbers.

4) TRUST VALUES PROPAGATION SCHEME

Trust propagation schemes fall into 3 categories: Centralized, Decentralized, and Hybrid as represented in Figure 6.

The centralized approach relies on a central authority for trust computation, trust propagation, and trust updating. The positive aspect of this scheme is its ease of understanding and inclusion in a trust management framework. However, the major disadvantage of such structures is the single point of failure [12], [95].

A decentralized approach requires nodes to be responsible for trust calculation, and propagation without the interference of any centralized authority. This approach avoids a single point of failure [12], but it has constraints such as latency, ''honest'' trust calculation, unbiased propagation of trust, and a complicated trust management architecture.

Hybrid or semi-centralized propagation allows part of the trust management framework to be implemented as a centralized structure whereas the other part is implemented as a decentralized or distributed architecture. Thus, it incorporates

TABLE 3. Analysis of studies based on factors involved in computation and aggregation schemes of trust values.

Refs	Trust Attributes/ Trust Composition Metrics	Trust Values Computation and Trust Values Aggregation Techniques
[79]	Direct Trust, Centrality, Cooperativeness, Community of Interest, and Service Value	Weighted Sum and Bayes Model
[63]	Honesty, Experience in the form of recommendations, Cooperativeness, Community of Interest	Weighted Sum
[80]	Reputation, Recommendation, and Knowledge	Fuzzy Logic and Weighted Sum
[81]	Experience, and Reputation	Mathematical Model based on Google PageRank
[82]	Credit, Reputation	The mathematical model or method used is not mentioned
[83]	Satisfaction, Weight assigned in accordance with the cruciality of the service provided, Fading Factor	Weighted Sum
[84]	For Ability Dimension (Availability, Confidentiality, Integrity, Safety, Reliability, Serviceability.) for the Benevolence Dimension (Cooperativeness, Community of Interest), and Integrity Dimension (Similarity and Honesty)	Suggested First Approach (Weighted Sum, Machine Learning, Bayesian Neutron Networks), Suggested Second Approach (Fuzzy Logic). However, in this paper, Weighted Sum along with Fuzzy Logic is used
[46]	Feedback, Social Similarity (Community of Interest, Friendship, Profile of Objects), and Context Weight, Credibility	Probability Density
[85]	Recommendation, Knowledge, and Reputation	Weighted and Directed graph, Weighted Sum
[86]	Direct Trust, Centrality, Cooperativeness, Community Interest, Energy, Service Score, Indirect Trust	Weighted Sum
[87]	Computational Capabilities, Recommendations in the form of External Opinions, Relationship Factor, and Dynamic Knowledge (Goodness, Usefulness, and Perseverance)	Machine Learning and Weighted Sum
[7]	Context, Trustor, Trustee, Analysis of Trustworthiness, Goal, Decision, and Action by the Consequences	Weighted Sum
[88]	Honesty, Cooperativeness, Energy, Centrality, Community of Interest, and Dependability	Weighted Sum
[89]	Reputation and Experience	Weighted Sum
[90]	Context-based Trust, Global Reputation	Weighted-KNN (Machine Learning)
[91]	Similarity (Bayesian, Hellinger, and Connection) and Centrality (Degree and Betweenness-Local Clustering)	Matrix Factorization
[92]	Direct Experience (Preference of any node for a specific interest as compared to other interest, Probability of the node that the interest is satisfied), Indirect Experience	Weighted sum
[93]	NA	The trust calculation technique is not specified. The paper states the use of Deep Chain
[94]	Number of Encounters (interactions) in the real world	NA
[95]	Credibility, Transaction Factor, Relationship Factor, Capabilities regarding Computation, Total Number of Transactions and Feedback, and Centrality	Weighted Sum
[96]	Old trust, Direct and Indirect Trust, number of Interactions (in each interaction 4 properties are calculated namely Intimacy, Sociability, Importance of Transaction, and Feedback of Service)	Weighted Sum
[97]	For User – Trust (Credibility, Reputation\ Direct-Interaction, Frequency of Rating The trend of Rating, Similarity, Strength of a Relationship, Variation represented as Fluctuation), For Device – Trust (requirements related to Security, limitation in accordance to Energy, Capability of the device concerning Constrained), For Service - Trust (Response Time, Availability, Rate of Success, Delay)	Machine Learning and Deep Learning
[98]	Honesty, Cooperativeness, Community of Interest, Competence	Weighted Sum
[99]	Credibility, Transaction Factor, Relationship Factor, Capabilities regarding Computation, Total Number of Transactions, Centrality, and Feedback	Weighted Sum
[100]	Direct Observations, Indirect Experience in the form of recommendations, Sociability	Weighted Sum and Kalman Filter
[101]	NA	Machine Learning
[58]	Direct and Indirect Trust, For Direct Trust (Friendliness, Community of Interest, Reward or Punishment factor, and Cooperativeness)	Machine Learning
[102]	Competence, Willingness, Social Relationship, Experience (through Direct Interaction from nodes that are familiar and from nodes that are not familiar)	Quantification

TABLE 3. *(Continued.)* **Analysis of studies based on factors involved in computation and aggregation schemes of trust values.**

[103]	Expected QoS metric and Advertised QoS metric, Social Similarity in terms of Friendship, Community, and Relations along with Feedback of Trust related to a context	Weighted Sum
[104]	Direct Trust (Community of Interest, Co-work Similarity, and Similarity between Friends), Indirect (Recommendations)	Weighted Sum
[77]	Relative Similarity Value, Implicit Trust Value	Weighted and Directed Graph
[105]	Transaction Time, Transaction Factor, Availability, and Execution Time	Weighted Sum
[106]	Friendship, Social Interest Communities of Objects, Cooperativeness, and Co-work Relationship	Machine Learning
[107]	Recommendation, Global Trust, Local Trust, and Nature of the Trust	Weighted Sum
[108]	Honesty, Truthfulness, Cooperativeness, Rating, Transactions, Community of Interest, Dealing, Observation, Knowledgeable, Reputation, and Personal Opinion.	Soft Set
[109]	Supremacy Factor, Extensive Feedback, Rapid Feedback, Reliability, Personal Trustworthiness, and Impersonal Trustworthiness	Weighted Sum
[110]	Distance (Static Friendship in terms of Distance), Interactions (Dynamic Friendship in terms of Interactions)	Bayesian Inference, Probability Distribution
[111]	Recommendations, Direct Trust, External Similarity Trust (Centrality), and Internal Similarity Trust (Community of Interest)	Multivariate grey prediction model and Fuzzy logic
[78]	Fission Factors (Availability, Size of Crowd, Probability of the existence of a link between any two entities, Cost of Integration, Flow of Users, Rate of Depletion), and Entropy	Fission Computing and Entropy Modelling
[112]	Data Provider Trustworthiness, Quality of Sensed Data, Quality of Data Timeliness	Weighted Sum
[113]	Reputation, Honesty, Quality of Provider, Similarity, Direct-Experience, Rating-Frequency, and Classification Class.	Deep Learning
[71]	Social Relationship between the corresponding devices and the context (Location, Manufacturer, Type of the Device, Technologies for Wireless Connectivity, Operating System, Main Functionality)	Multiplicative Attribute Graph (MAG)

TABLE 3. *(Continued.)* **Analysis of studies based on factors involved in computation and aggregation schemes of trust values.**

[114]	Similarity, Friendship, Community of Interest, Credibility, and Social Contact Index	Weighted Sum
[115]	Direct Trust (Number of Transactions, Relationship Factor), and Opinions of those friends who are common	Weighted Sum
[116]	Recommendation, Honesty, Reputation, Social Similarity, and Knowledge	Weighted Sum
[56]	Reputation, Community Interest, Cooperativeness	Weighted Sum and Information Entropy
[117]	Direct (interaction experience) and Indirect Trust (Recommendation Weight, Social Tie)	Weighted Sum
[118]	Direct Trust (The Ratio of Packet that is Forwarded, The Ratio of Forwarded Flows, The Ratio of Interruptions of Primary User), Indirect Trust	Weighted Sum
[119]	Reliability of Service, the Validity of Feedback	Weighted Sum
[120]	An instance of time, Mutual Friends, Similarity of nodes (Common group based on Interests CIG), Ratio of Packet Delivery	Machine Learning
[121]	The ratio of positive data to the total data	Weighted Sum
[122]	Direct Trust, Centrality of the Node, Energy, Community of Interest, Cooperativeness factor, and Service Score.	Weighted Sum
[123]	Trust is based on Social Relationships, Communication Trust, Operational Trust, and Indirect Trust	Weighted Sum with Exponential Function
[124]	Direct Trust, Indirect Trust, Similarity	Matrix Factorization
[125]	Sociality Factor and Reputation	Weighted Sum
[126]	Direct Interaction Score, Indirect Interaction Score, Direct Relationship and Indirect Relationship	Weighted Sum
[127]	Trustworthiness and Untrustworthiness based on Direct Opinions and Indirect Opinions	Probabilistic Neighbourhood Overlap (P-NO)
[128]	Truth, Indeterminacy, and Falsity	Interval Neutrosophic Numbers (INNs) and Fuzzy Logic
[129]	Honesty, Recommendation Reputation, Knowledge, Social Similarity, Cooperativeness, Community of Interest (CoI) and Inter-Social Object Relationships (I-SoR)	Weighted Sum
[130]	Reputation, Social Relationship, and Energy	Weighted Sum
[131]	NA	NA
[132]	Capability, Commitment, and Satisfaction	Weighted Sum

the advantages of both centralized and decentralized architectures. Table 6 provides the classification based on the propagation schemes deployed for the computed trust values in the relevant studies. These schemes are classified as centralized, decentralized/ distributed, and hybrid/ semi-centralized. The studies are represented by their reference numbers.

C. TRUST RELATED ATTACKS IN THE SIoT DOMAIN

A node or object can use its social connections with other nodes to find the services it needs, but only if there is enough trust between them. The SIoT environment is made up of multiple social objects or devices with different characteristics. Misbehaving objects can take advantage of social interactions for launching attacks on a SIoT system as these malevolent nodes have ulterior motives. These misbehaving nodes or their owners want to get benefits from resources or services, but they do so at the expense of other nodes that can provide such services [133]. Thus, malicious nodes launch attacks on other nodes.

A malevolent node is dishonest and non-cooperative in a social context with the tendency to break the basic functionality of SIoT by executing attacks on various nodes [63]. In this context, trust management is crucial and assists SIoT nodes in overcoming perceptions of ambiguity and the risk of coming into contact with malevolent objects. In order to reduce the impact of malevolent devices, trust management systems for the SIoT encourage objects to collaborate honestly and constructively. These systems also forecast the most trustworthy trustee for a given trustor.

Due to the nature of cyber-physical systems, a successful attack on a SIoT system has the potential to be just as disastrous as the biggest industrial disasters to date [134]. Attacks are broadly categorized into two types: collaborative attacks and individual attacks [12]. These attacks are specifically related to SIoT, hence the attacks listed below are ''Intrinsic Attacks''.

1) COLLABORATIVE ATTACKS

In collaborative attacks entities (SCs) collude to launch an attack on an SP. There are two main types of Collaborative Attacks:

- Bad Mouthing Attack: the SC deliberately provides unsatisfactory feedback after receiving satisfactory service. In this attack, multiple SCs act together and target a particular SP to provide negative feedback. Hence, attackers with bad ratings enhance their reputation by providing negative feedback to nodes having a good reputation. This results in attacking nodes uplifting their reputation scores [12].
- Ballot Stuffing Attack: multiple malevolent nodes collude to increase the reputation of another fraudulent node by constantly providing positive feedback about that node. It thus enhances the opportunities of the adversary being selected as a possible SP. The attackers and the target nodes are often not owned by a single

TABLE 4. Analysis of studies based on scenarios for trust computation/ aggregation techniques.

Trust Computation/ Aggregation Techniques	Scenarios
Weighted Sum	To calculate estimated trust where overall trust is the sum of estimated trust and expected trust [79]. To compute the trust value based on direct observation and past trust values on the basis of TAs [63]. In the aggregation of a Utility Function to compute the overall trust value [80]. The node asks its "Followees" (recommenders/ friends) about their experience with respect to a service provider. However, the node can compute the trustworthiness value of its "Followees" in terms of "mean value". To calculate the "mean value" which is an indication of the Followee's entire observed behavior and reflects the value of expected satisfaction for the next iteration [83], Weighted Sum is used. To compute the final recommendation value of an object on the basis of the transition probability of all the other objects towards that particular object [85]. To determine the trust of one node as perceived by another node based on TAs [86], [87], [98], [99], [115]. In determining trust values between two nodes at a specific time 't' with respect to a specific TA [88], [96]. In the computation of overall reputation or aggregated feedback comprising of the weighted sum of the feedback for a particular node as given by all the other users (nodes) [89]. To infer the trustworthiness of a trustee with respect to the specific task being performed as perceived by the trustor while taking into account the fact that since different features play varying roles in a task, each one must be weighted to represent its importance in the task. [7]. To compute the direct trust value and indirect trust value of a node with respect to another node at a time 't' on the basis of TAs [92], [126]. For subjective trustworthiness: To compute the trust of one node with respect to the other node on the basis of TAs. For objective trustworthiness: To compute the trust of a node as perceived by the whole network based on TAs [95]. To calculate the overall trust of one node as perceived by another node while taking into account the TAs [100], [107], [109], [119], [122], [132]. To accumulate the direct trust values from Context-aware QoS Similarity based Trust (CQoSSTrust) and Context-aware Social Similarity based Trust (CSSTrust) and Contextual Feedback of Trust (CFT) [103].

TABLE 4. *(Continued.)* **Analysis of studies based on scenarios for trust computation/ aggregation techniques.**

	To determine the final trust value of one node as perceived by another node in time 't' based on TAs [104]. To determine the service trust value of a specific service that is being provided by the node on the basis of TAs [105]. To determine the trustworthiness value of the data provider in the edge node after participating task on the basis of the old trustworthiness value of the data provider and the change in the trustworthiness value after this specific task [112]. For the calculation of the global trust value of a node by taking into the evaluation of all the other nodes for that specific node on the basis of TAs [114]. To calculate reputation value based on the direct and indirect experience of one object with reference to the other object in time 't'. Trust value comprises reputation value along with other TAs [56], [125]. To determine the trust of one node as perceived by another node based on TAs at a specific time 't' [117], [118]. To compute an overall trustworthiness value of a sensing node comprising of the latest and previous trustworthiness values [121]. To compute an overall trust value between two nodes for a specific time 't' while taking into account the exponential function. This exponential function represents the exponential decay of the energy content over time [123]. In the trust assessment of a trustor towards a trustee at a specific time 't' while judging a service that is being assessed through the combination of TAs taking into account the weights assigned to these TAs [129]. To calculate the value of trustworthiness between the user and the service by taking into account high timeliness and corresponding to a specific time point 't' [130].
Bayesian System	In the calculation of expected trust values where both expected trust values and estimated trust values comprise the overall trust [79]. To infer the probability for the static trust with reference to distance 'X'. Where 'X' is a continuous random variable to represent the "distance" between two entities linked by any sort of social relationship. [110].
Machine Learning	In assigning scores to the TAs which helps the trust management model to train and adapt itself, thus identifying and reacting to malicious attacks [87]. In assigning weight to the contribution of each of the 'k' previous experiences which are used in the estimation of trustworthiness values [90]. To detect malicious nodes, present in a network [97]. In computing the trust value of the trustee node (where the trustee node is selected from a pool of other nodes on the basis of features assigned according to the context of attack) and in the detection of fraudulent nodes [101].

TABLE 4. *(Continued.)* **Analysis of studies based on scenarios for trust computation/ aggregation techniques.**

	To combine direct and indirect trust values (calculated on the basis of TAs) in order to compute an overall trust value [58]. To combine various trust features (TAs) in order to determine an overall trust value of one node with respect to another node in time 't' [106]. To compute the overall trustworthiness values of nodes on the basis of TAs and to label the nodes as trustworthy or non-trustworthy [120].
Multiplicative Attribute Graph	To compute the trust values that are based on associating suitable attributes to the nodes according to the pre-defined social relationships [71].
Fuzzy Logic	In the representation of ambiguous TAs for the calculation of trust values [80]. To infer new knowledge from a knowledge base and use it in the computation of the overall value of trust by varying weights in accordance with the context [84]. In synthesizing the trust element required for the computation of trustworthiness [111]. Input data of the trust and context criteria assessments are fuzzy values [128].
Multivariate Grey Model	In the prediction of the "direct trust component" of a particular node [111].
Deep Learning	To identify different types of attacks that are generated by malevolent users [97]. To create a model that categorizes nodes (on the basis of interactions between nodes) into various classes in accordance with the type of attacks [113].
Weighted and Directed Graph	In the calculation of Trust Attributes (Relative similarity) between the trustor and the trustee to create an implicit trust framework as a weighted directed graph [77]. To represent relationships amongst different nodes [85].
Fission Computing	In the calculation of trust values on the basis of fission factors [78]. In the edge-crowd incorporation for maintenance of trust and preservation of privacy rules in SIoT [78].
Kalman Filter	To estimate the trust values of the nodes in order to predict the behavior of nodes and provide resiliency against possible attacks [100].
Quantification	Trustworthiness is calculated by combining evaluation results about the quantification of competence and willingness from many sources and integrating them into a single total [102].
Mathematical Model based on Google PageRank	In the calculation of the "reputation trust indicator" which is used as an indicator of trust [81].
Probability Density	To calculate the contextual trust of an object for each context with respect to each service [46].
Probability Distribution	To predict each entity's characteristics and its relationship to its peers [110].
Soft Set	To select the nodes which are considered to be the most trustworthy based on the trustworthiness value [108].
Information Entropy	In the assessment of indirect reputation to reduce the impact of BMA and BSA [56]. To assign the weights of each node used for the computation of the indirect experience factor of trust [56]. In the computation of trust values by using entropy-based fission rules [78].

TABLE 4. *(Continued.)* **Analysis of studies based on scenarios for trust computation/ aggregation techniques.**

Probabilistic Neighborhood Overlap (P-NO)	To restrict the effect of Sybil + SPA, OOA [127]. To prioritize or rank service providers (as trustworthy or not) based on all opinions (direct and indirect) [127].
Matrix Factorization	In extracting latent features of nodes, identifying trustworthy nodes, and mitigating the data sparsity and cold start issues [91]. In computing the trust values based on TAs and in providing resiliency against malevolent attacks in service recommendation [124].
Interval Neutrosophic Numbers (INNs)	This study [128] makes use of INNs due to their versatility and capacity to account for many types of uncertainty in modeling trust relationships and calculating overall trust values [128].
Special Case (First Approach – Weighted Sum, Machine Learning, and Bayesian Neutron Networks)	Trustor propensity and environmental conditions are expressed mathematically by giving weights to individual characteristics (i.e., TAs and TIs) which leads to the calculation of trustworthiness value [84].

owner [12]. Instead, different nodes (attackers) collaborate to enhance the rating of nodes with a low reputation by assigning positive feedback to each other.

2) INDIVIDUAL ATTACKS

These are the attacks that are launched by individual nodes, and comprise:

- Good Mouthing Attack/ Self-Promoting Attack: the entity projects itself as one of the most trustworthy SPs by providing good recommendations about itself [12]. In this instance, the attacker owns multiple SC nodes, all of which provide a good rating to an SP. In other words, the SP and SC are owned by attackers.
- On-Off Attack: a node (SP) tries to maintain a consistent reputation by oscillating between good and bad service provisioning. When the node (SP) judges that its reputation is about to decrease below a threshold, it starts providing good service [12].
- Opportunistic Service Attack: SPs use their high trust value to get selected, but they cooperate with other malicious nodes to launch an attack on the targeted node [12], [31].
- Selective Behavior Attack: an SP provides good service for certain types of services and bad for others, e.g., an SP provides a good service when resource utilization is low, and bad otherwise [12].
- Whitewash Attack: a malicious node leaves the network and then joins after some time to nullify its previously gained trust values [31].
- Discriminatory Attack: nodes render an attack on nodes with whom it does not have strong social relations [31], regardless of the reputation of the other node.

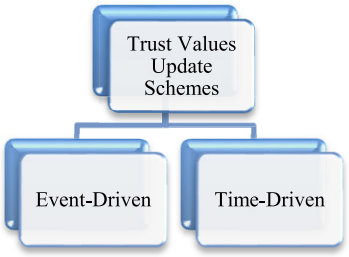


FIGURE 5. Types of trust updates in the SIoT domain.

TABLE 5. Classification of studies on the basis of trust update schemes.

Event-Driven	Time-Driven
[63], [80], [81], [82], [84], [85], [87], [7], [89], [90], [95], [96], [97], [102], [103], [106], [109], [110], [78], [112], [114], [115], [116], [56], [117], [119], [121], [122], [125], [126], [127], [128], [132]	[79], [86], [88], [98], [100], [101], [118]

Attacks are not typically related to SIoT networks, but once launched from outside the network, can cause greater damage to the targeted SIoT networks. These can be categorized as ''Extrinsic Attacks'' such as Denial of Service (DoS) or Distributed DoS, Sybil, Slandering, Message Spoofing, and Storage Attacks.

3) MOST WIDELY USED SIMULATORS/ ANALYSIS TOOLS

A number of simulation environments can be used to realize SIoT systems, these include: Network simulation via ns-3 [135], discrete event network simulation using an object-oriented approach, such as OMNET++, where message passing is used as a medium for the modules to communicate with each other [136]. Other similar types of simulation environments include COOJA, a network simulator for Contiki OS which is a lightweight OS specifically designed for IoT. COOJA enables the simulation of Contiki OS ''motes'' and different levels of granularity [137].

Multi-agent programming to support the modeling of social interaction between agents using NetLogo [138] and support for mobility modeling (by generating synthetic traces of mobility trends) using SWIM (Small World in Motion) [139]. Data analysis environments can be used to combine a number of different algorithms, e.g., Weka (Waikato Environment for Knowledge Analysis) [140]. Other approaches can also be used to develop the behavior of SIoT systems, e.g., using a fuzzy inference system [141]. Fuzzy rules can be derived from interaction with human operators. Apache Jena Framework is another framework to create semantic web and linked data apps [142], supporting various types of inference engines

A simulator specifically for trust and reputation management frameworks [143], targeted for wireless sensor nodes called TRMSim-WSN [144]. It enables a user to define various parameters of the network using XML-based configuration [145].

More general-purpose systems include MATLAB and Octave, to create simulation and data analysis algorithms,

TABLE 6. Classification of studies based on propagation schemes of trust values.

Centralized	Decentralized/ Distributed	Hybrid/ Semi-Centralized
[81], [82], [84], [46], [88], [95], [112], [114], [115], [119]	[79], [63], [85], [86], [87], [7], [89], [90], [91], [92], [93], [94], [95], [96], [98], [99], [100], [101], [58], [102], [103], [104], [77], [105], [106], [107], [108], [109], [110], [111], [78], [113], [114], [116]], [56], [117], [118], [120], [121], [122], [123], [124], [125], [126], [127], [128], [129], [130], [132]	[71], [80], [83], [97]

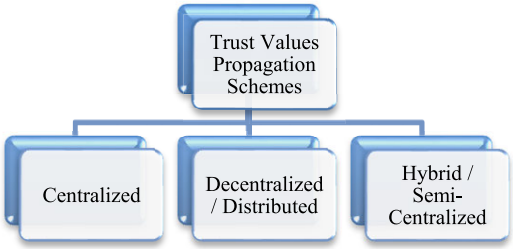


FIGURE 6. Trust propagation schemes.

and create graphical user interfaces [146]. MATLAB includes "Simulink" for designing and deploying IoT-based applications, also enabling integration and analysis of data from third-party platforms.

Table 7 summarizes the simulators/ analysis tool used to evaluate trust in SIoT. This table also shows the type of trust-related attacks considered in the corresponding studies. The term "Extrinsic Attack" is specifically used in Table 7 to differentiate them from "Intrinsic Attacks". All the other attacks where the "Extrinsic Attacks" term is not used are "Intrinsic Attacks".

V. DISCUSSION AND ANALYSIS

A. PUBLICATION TRENDS: SIoT AND TRUST MANAGEMENT

Publication trends related to SIoT and trust management are shown in Figure 7. Details of relevant studies published between 2012 – 2022 are represented in Table 8.

B. BRIEF DESCRIPTION OF THE RELEVANT STUDIES

A brief description of the relevant studies is presented in this section.

Reference [79] presents a trust management framework with respect to the behavior of nodes when BMA is launched. Expected and estimated trust is calculated using a Bayes Model and Weighted Sum, whereas overall trust is the product of the two. To prevent malicious attacks, the trust calculation uses previous and predicted behavior.

TABLE 7. Classification of studies on the basis of simulatops/ analysis tools and trust-related attacks in SIoT.

Ref	Simulator/ Analysis tool	Types of Trust related attacks addressed in the relevant studies
[79]	ns3 and Social Network Visualizer tool SoCNetV1.9	OOA
[63]	ns3 simulator	BMA, BSA, SPA
[80]	Mamdani FIS is used for the calculation of fuzzy logic.	NA
[81]	MATLAB and Python for programming	NA
[82]	Microsoft Visual Studio 2013	Malicious nodes (details not specified regarding types of malicious nodes)
[83]	TRMSim-WSN	Oscillating Behavior attack, Extrinsic Attack (Sybil Attack)
[84]	Apache Jena Framework is used for the analysis based on trust values for the recruitment of users in the MCS scheme	BMA, GMA, BSA
[46]	WEKA, A physical network of 100 objects assigned to 100 different users	Malicious Behavior
[85]	The tool is not named in the article. Evaluation of the trust model is performed by showing effectiveness and performance in comparison to other ranking systems by considering 5 – 100 objects.	NA
[86]	Ns3 and Social network visualizer tool SocNetV 1.9.	OOA
[87]	Comparison between incremental SVM (iSVM) and incremental Machine Learning Algorithm by using Receiver Operating Characteristic (ROC) and Area Under the ROC (AUC) as metrics for performance	DA, OOA, WA, BMA, BSA, OSA, SPA, Extrinsic attack – Sybil Attack
[7]	Practical Setup where each entity is installed with Texas Instruments' Z-Stack (version 2.5.0). The analysis is based on the rate of success, rate of abuse, and unavailable rates of tasks. Facebook, Twitter, and Google+ are used for network connectivity	NA
[88]	SWIM (Small World in Motion) model	Attacks are not addressed explicitly but said that it could protect against Sybil attack (Extrinsic Attack)
[89]	Coding in Java and making use of BouncyCastle cryptographic library	NA
[90]	MATLAB	BMA, SPA, BSA, OSA
[91]	Epinions dataset from Epinions.com (review website) is used for analysis	OSA
[92]	OMNET++	BMA, BSA, WA, DA, SPA
[93]	MATLAB	Malicious nodes are identified

TABLE 7. *(Continued.)* **Classification of studies on the basis of simulatops/ analysis tools and trust-related attacks in SIoT.**

[94]	FB Friend Graph is analyzed in comparison to the real world concerning multiple parameters.	NA
[95]	SWIM (Small World in Motion) model	SPA, BMA, BSA, OSA, OOA
[96]	Simulations are done but the study does not address the simulator being used	BMA, SPA, BSA, OOA, OSA
[97]	The simulator is not disclosed. However, multiple variant set of simulations is conducted.	OOA, OSA, BSA, BMA, DA and SPA
[98]	ns3 and SWIM (Small World in Motion) model	Defense against co-relative service attacks
[99]	SWIM (Small World in Motion) model	NA
[100]	Python Language	OOA
[101]	The simulator is not defined. Data from Facebook, Twitter, and Quora is used.	SPA, BSA, BMA, DA, OSA
[58]	The sigcomm-2009 dataset is used for analysis	NA
[102]	NetLogo Simulator and MATLAB	OSA, BMA, BSA, SPA, WA, DA
[103]	A synthetic data is created with 600 devices (300 SPs and 300 SCs) distributed amongst 200 personals (from a synthetic dataset of Facebook)	SPA, OOA, BMA, BSA
[104]	MATLAB R2020	BSA, GMA, BMA (all based on recommendations)
[77]	FilmTrust (a movie recommender website) dataset is used to analyze the proposed recommender system	NA
[105]	The data set comprises services for bike ridesharing in the real-world scenario is analyzed	NA
[106]	CRAWDAD dataset from SIGCOMM2009 is used for analysis purposes.	NA
[107]	Dataset from the social networking site called Slashdot, Facebook, and Twitter is used for analysis purposes. For visualization, Gephi is used.	NA
[108]	Bitcoin Alpha trust weighted signed network dataset retrieved from Stanford Large Network Dataset Collection is used to perform analysis	NA
[109]	ns3 using C++ platform C++, ns3, and Physical testing were performed on 10 participating entities. 201 sensors were installed in a total of four smart residential areas for the collection of activities.	NA but privacy is provided in the form of a privacy protection paradigm for reliable services based on a Genetic Algorithm Privacy issues are addressed in addition to the secured service delivery
[110]	NetLogo	NA
[111]	NetLogo, SWIM (Swim World in Motion) Model	BMA, Extrinsic attacks (Cheating Attack)
[78]	Numerical Simulations are used over Synthetic Dataset	NA – Only the Extrinsic Attack - Sybil attack is prevented to some extent

TABLE 7. *(Continued.)* **Classification of studies on the basis of simulatops/ analysis tools and trust-related attacks in SIoT.**

[112]	Python 3.6	NA
[113]	Analysis based on real-world data set named Sigcomm. Python is used.	BMA, BSA, DA, SPA, none-attack class attacks (as mentioned in the paper)
[71]	MATLAB, Gephi, SWIM (Swim World in Motion)	NA
[114]	MATLAB	NA
[115]	MATLAB R2018a	SPA, BMA, BSA, OOA, SBA
[116]	COOJA	OOA, OSA, WA
[56]	Private Ethereum based blockchain	BMA, BSA, Extrinsic Attacks (Denial of Service Attack and Storage Attacks)
[117]	Private Ethereum based blockchain	BMA, BSA, Extrinsic Attacks (Denial of Service Attack, Message Spoofing Attack, and Storage Attacks)
[118]	ns2, CRCN	Extrinsic Attacks (Promise-Then-Drop, Trust-Boosting, and Defamation)
[119]	Programming and simulation are in Python and the dataset used is CRAWDAD	GMA, BMA (to some extent through the process of Normalization)
[120]	Google Collab and Python	NA
[121]	NA	Extrinsic Attack (Distributed Denial of Service Attack)
[122]	NA	NA
[123]	The simulator is not mentioned. However, SIoT devices are physically connected to evaluate performance parameters.	Malicious Nodes are identified
[124]	The simulator is not mentioned. However, three datasets FilmTrust, Epinions, and Ciao are used to perform the evaluation	BMA and Malicious Attacks
[125]	MATLAB	NA
[126]	Simulations are done but the study does not address the simulator or blockchain being used	SPA, BMA, BSA, WA
[127]	Simulation is based upon the datasets st-andrewssassy, thlab_sigcomm2009, upb_hyccups, CollegeMsg, and nodobo	BMA/ Extrinsic Attacks (Slandering, Sybil), Sybil + SPA, OOA, BSA, Sybil + Slandering
[128]	The simulator is not mentioned. However, simulations are performed under various scenarios considering a service-oriented environment	SPA, BSA, DA, WA, OSA, BMA Malicious SPs
[129]	COOJA	SPA, BSA, DA, WA, OSA, BMA, OOA
[130]	The authors created a testbed with one workspace, and two smart homes, consisting of 196 objects that are RFID-tagged and equipped with various state-change sensors to track human object usage. To make the data set large enough for experimental studies, two data sets that were published by the MIT AI group were added.	NA

TABLE 7. *(Continued.)* **Classification of studies on the basis of simulatops/ analysis tools and trust-related attacks in SIoT.**

[131]	The experiments are run by using 2 datasets: i) authors' dataset by setting up a test bed including two smart homes and a single workspace. ii) public dataset as a combination of datasets acquired from two data sets of MIT AI group and a CASAS dataset of Washington State University	NA
[132]	Python Libraries	SPA, BSA, DA, WA, OSA, BMA,

Reference [63] provides an adaptive trust management technique to strengthen security against hostile nodes. Dynamically changing node configuration prevents harmful attacks. Trust and network stability are traded off.

Reference [80] outlines a trust paradigm based on reputation and knowledge (based on the object and its ownership). This study examines human-to-human and human-to-object trust. Trust services include agent, broker, management, and analysis. A trust agent collects service-use data, whereas the trust broker distributes it. Trust calculation techniques, reasoning strategies, an information model, and knowledge assessment are described. Human-to-human knowledge is built on cooperation, honesty, experience, and community of interest, whereas human-to-object knowledge is based on services and things. This study employs a car-sharing scenario to demonstrate the important results.

REK is proposed in [81]. TAs include reputation and experience. Interaction intensity, classification of interactions as cooperative, non-cooperative, or neutral, and relationship status are used to calculate experience. Experience is increased, decreased, or decayed based on these factors. The authors conclude it's hard to develop trust, but when the SP is uncooperative, trust decays faster than it grows. Google Page Rank is used for reputation. The trust evaluation methodology uses a human cognitive process.

Reference [82] proposed a credit-and-reputation-based trust model. Credit determines if a node can afford communication, while reputation calculates trustworthiness and identifies malicious nodes. The guarantor finds an appropriate service for SC, and reputation determines the SP's trustworthiness. Once trust is established (>0.5), SP and SC conduct an end-to-end transaction. The reputation server computes the node's reputation once SC rates the SP. This model includes penalties for detecting and isolating malicious nodes.

A hybrid TR design for SIoT (TRM-SIoT) is presented in [83]. In this study, personal encounters define trust, while social interactions define reputation. Fraudulent service provision and recommendation constitute malicious behavior. The model uses fading factor, weight, and satisfaction. SP and SC interactions affect the fading factor. Service ''cruciality'' determines weight. SCs determine satisfaction. If SP and SC interactions for a service surpass a threshold (in this case 5), two trust values are calculated. One reflects long-term satisfaction, and the other is recent trends. The minimum value is chosen.

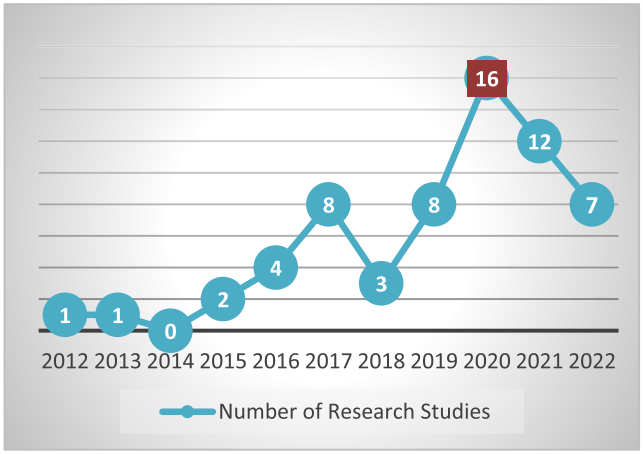


FIGURE 7. **Number of publications over 2012-2022 (max. observed in 2020).**

TABLE 8. **Key research publications over 2012 – 2022.**

Years	Corresponding Research Studies
2012	[99]
2013	[95]
2015	[63], [82]
2016	[80], [83], [85], [121]
2017	[7], [46], [71], [79], [81], [84], [86], [100]
2018	[88], [94], [103]
2019	[78], [96], [108], [111], [113], [122], [123], [131]
2020	[56], [58], [77], [87], [89], [90], [92], [93], [98], [102], [104], [105], [106], [107], [118], [126]
2021	[91], [101], [110], [112], [114], [115], [116], [119], [124], [125], [127], [130]
2022	[97], [109], [117], [120], [128], [129], [132]

Reference [84] suggests a subjective trust-based paradigm. Ability, benevolence, and integrity are key to trust management. ''Ability'' examines SP's (trustee) ability to do a task, ''Benevolence'' measures the trustee's collaboration, and ''Integrity'' measures the trustee's good reputation. The literature proposes a modified, weighted page-rank method to evaluate reputation. Reputation, experience, and knowledge are trust indicators. Mobile Crowd-Sensing is used to evaluate the trust model (MCS).

The architecture presented in [46] includes objects with varied capacities, a server that is responsible for each ''thing's'' authentication and user compatibility, and a trust management system to assess trust values and conduct trust calculations depending on context and feedback. Describes calculating node reputation in multiple contexts and services. Objects' computational capacities divide them into 3 types (high, low, and average). The trust management model has two modules: contextual trust and reputation, and behavioral classification and prediction. Feedback is centralized. This

server saves the node's reputation. Decision trees predict node behavior.

Reference [85] compares the recommendation model to page rank. Weighted and directed graphs show object relationships. Good relationships are measured by an object's outbound links. PR ranks by outgoing connections. This model also filters out suspicious opinions. This model assigns rank values to the most trustworthy objects and zero to others.

Reference [86] computes trust on the basis of TAs. The suggested trust management strategy quickly identifies and segregates unreliable nodes. The technique resists object-oriented attacks.

A trust management model using an ML algorithm is proposed in [87]. This work discovers trust-related attacks and segregates malicious nodes. The proposed mechanism constitutes two stages ''training stage'' and a ''steady-state stage''. To evaluate dynamic knowledge three metrics are described: (i) goodness score which evaluates how benevolent the entity is, (ii) the usefulness score which determines the current behavior of the entity, and (iii) perseverance score evaluates the constancy of the entity.

Reference [7] shows that trust is bilateral, as both SP and SC evaluate each other's trust. The study implies context and services should determine trustworthiness. Success, damage, gain, and cost are used to evaluate trust. The model's unique features are bilateral trust assessment, inferential trust transmission with identical tasks, trust transitivity, trustworthiness updates by delegation outcomes, and trustworthiness modified by a dynamically changing environment.

Reference [88] proposes a paradigm for managing the direct and indirect trust. This work presents a ''DTrustInfer'' technique, where the node with the highest value of centrality is the authenticator. The authenticator forms and issues secret codes to validate node messages.

Reference [89] protects an object's privacy through homomorphic encryption. This paper provides a self-enforcing privacy-preserving technique. The study evaluates the entity's and owner's trustworthiness. Trust assessment protects participant privacy. Different entities' feedback should be confidential and weighted. The bulletin board displays object ratings. Zero-knowledge proofs ensure every entity acts honestly.

Reference [90] introduces a trust management paradigm based on SIoT node behavior discrimination. The study uses DHT to allocate trust providers to the entities. Trust providers store entity trust values for indexes they cover. This study considers similarity and context-based services (using a service rating mechanism). Recent and past ratings are derived using weighted KNN and the decay factor.

Reference [91] uses a bipartite network, matrix factorization, and Hellinger distance to find trustworthy nodes. SIoT is represented as a bipartite graph per SC and SP. The Hellinger distance creates a social structure between SRs and SPs. Reliable SP is found using matrix factorization.

Reference [92] determining trust in SIoT devices based on interest preference, using similarity between the trustor and the entity making the recommendation.

Reference [93] proposes a trust architecture based on a ''Deep Chain'' for SIoT devices using Quora, Facebook, and Twitter. Traditional, conservative, and aggressive trust transitivity calculations evaluate bidirectional trustworthiness between the SP and SC. The suggested method blocks hostile nodes from the network. A context and characteristics based approach can evaluate malicious SIoT behavior. AI algorithms evaluate the trust assessment approach.

To build a mechanism for assessing the strength of links in a SIoT network, [94] assesses the accuracy of using connection statistics from the Facebook Friend graph.

Reference [95] proposes both subjective (distributed) and objective (centralized) trust management models. A distributed hash table is used in the centralized approach by pre-trusted objects, supporting trust queries for service providers. The suggested model isolates malevolent nodes at the cost of increased traffic in the network due to feedback exchange.

Reference [96] suggests basing SP trust on intimacy, sociability, service feedback, and transaction importance. Different service tiers represent SP's quality of service. This study proposes a trust predictability model for OOA based on a node's past behavior.

Reference [97] suggests a trust model comprising of a user, service, and device dimension. The work counters attack using ML and DL. This study classifies users as legitimate, maliciously recommending, and maliciously providing service.

Reference [98] considers direct and indirect interactions for trust computation in a service-oriented environment. The suggested trust management approach considers entity behavior.

Reference [99] proposes a subjective trust management model based on direct and indirect interaction. Indirect engagement considers friends' opinions and experiences. The proposed feedback system combines nodes' credibility and centrality.

Reference [100] presents a ''community of interest'' trust management technique employing a Kalman filter to evaluate and predict trust values. Nodes communicate based on common interests. The proposed technique involves community building, trust value initialization, administrator election, and member updates. After nodes are validated and registered, they elect an ''Admin'' based on trust, sociability, and capability. These admins manage the community of interest.

The model proposed in [101] suggests the use of trust attributes in the context of an attack. In the trust aggregation stage, an artificial neural network algorithm is used whereas a time-driven strategy is used for trust updates.

In [58], a trust aggregation strategy is proposed using K-means clustering, to distinguish between the interactions which are trustworthy and non-trustworthy. To understand

the influence of individual features on the overall trust score, a prediction mechanism for trust is used.

Reference [102] presents a context-aware trust mechanism for SIoT service delegation leveraging competence, social relationship, and willingness. For competence quantification, the Degree of Importance (DoI) and Degree of Social Relationships (DoSR) are considered, whereas willingness quantification also considers the Degree of Contribution (DoC) along with DoSR. DoI measures SPs' storage, communication, and computing capacities. DoC is based upon the willingness of those who are providing services. DoSR weighs competence and willingness.

Reference [103] includes three attributes of social relationship evaluation: friendship, the community of interest, and relationship. To accommodate a context-awareness scenario, the device status, environment, and type of task are included. The presented model selects the most trustworthy services and then proceeds with recommending those services to SCs.

Reference [104] suggests a trust model based on the similarity between nodes in terms of friendship, co-work, and community of interest. The proposed trust model combines two different types: direct trust and indirect trust. Recommendations are taken into account in absence of direct past experience.

Reference [77] proposes a trust recommender system based on implicit trust. To remove the basic problems associated with implicit trusts, the proposed model suggests three key steps: construction of trust networks that are asymmetric, calculating of the trust networks which are latent, and then predicting recommendations based on trust networks.

Reference [105] puts forward a trust management strategy based on trust of service rather than focusing on SP – as the service itself tends to act inappropriately. Service trust is used as a selection criterion, composed of multiple factors such as availability, execution time, response time, and overall transaction time.

Reference [106] proposes a trust strategy based on social similarity where K-means clustering along with random forest classification is used for the analysis of the trust values of nodes.

Reference [107] takes into consideration the trustworthiness of IoT and makes use of Online Social Networks (OSN) to create smart city services. This trust model takes into account the interaction and trust value within an OSN. The trust factor in the proposed trust scheme ensures the integrity of data. The suggested scheme uses publicly available data sets from Slashdot, Facebook, and Twitter.

Reference [108] put forwards a weighted trust scheme using soft set theory.

Reference [109] presents a trust and relationship management mechanism for reliable service provisioning in SIoT called F-TRM on the basis of the friendliness factor. This study advises using a dynamic friendship supervision technique (DFS) with an updated friendship directory (UFD). UFD's encrypted service delivery ensures privacy.

In the research [109], the authors present a Trustworthy Relationship Management (F-TRM) framework based on the principle of friendliness as a means of delivering stable services in the SIoT. For regulating the device's friendliness, a technique called Dynamic Friendship Supervision (DFS) is suggested. The Updated Friendship Directory (UFD) is built using the feedback provided for all the nodes based on their trustworthiness value. On the basis of UFD, a Privacy Protection Paradigm (PPP) is modeled using the Genetic Algorithm based Pseudo Random Sequence Generation (GA- PRSG) technique, and implementation is done through Attribute-based Encryption (ABE) scheme. The proposed strategy also includes a discussion of four models: Dynamic Friendship Supervision (DFS), DFS combined with GA-PRSG (DFS + GA-PRSG), DFS combined with PRSG and ABE (DFS + PRSG + ABE), and DFS combined with GA-PRSG and ABE (DFS + GA-PRSG + ABE).

Reference [110] proposing an algorithm for truthful friend selection using an exhaustive search. Static and dynamic friend relationships are studied. Static friendship metrics include data profiling and distance. Interaction history drives dynamic friendship. Distance and interactions define trust.

Reference [111] calculates SIoT trust with context. Social science and psychology are used to compute node-owner trust. Familiarity and similarity measure trust. Similarity trust uses centrality and community of interest. Direct trust and recommendation determine familiarity trust. Familiarity trust is computed using a kernel-based nonlinear multivariate grey prediction model and fuzzy logic.

Reference [78] proposes a trust and privacy scheme for SIoT based on the concept of ''fission'' computing. The study proposes a scheme that eliminates reliance on centralized servers by building a scalable and distributed approach that leverages end-user devices as mini-edge servers. Edge-crowd integration for trust maintenance and privacy preservation rules.

The trust evaluation scheme in [112] is used to calculate the trustworthiness of data providers with the help of trusted static sensor nodes in edge computing. The study also put forward a service assessment strategy based on trustworthiness, which comprises both local and global assessments of trust.

The trust management scheme presented in [113] includes deep learning for the detection of attacks related to trust and the isolation of malicious nodes.

Reference [71] presents a trust management strategy in SIoT based on a multiplicative attribute graph (MAG). A set of attributes is linked with each node. Trust in this research work is presented as a link probability between two nodes, with the overall between nodes computed using MAG.

Reference [114] suggests a trust management scheme based on cloud-based calculation. Overall, trust is based on direct and indirect trust values.

In [115], a novel methodology for assessing the trustworthiness of nodes and identifying the most reliable SP is proposed. SPs are filtered based on contextual information from

recommendations and QoS in order to reduce trust calculation time and identify the most reliable service provider.

Reference [116] presents an attack detection strategy based on an ML approach to identify and isolate malevolent nodes. Furthermore, in this study, the behavior of the nodes is classified as benign or malicious. This study uses the Weighted Sum technique for trust aggregation.

Reference [56] presents a trust management scheme based on blockchain. For reputation calculation, this study uses Information Entropy. To evaluate trust, this study uses smart contracts.

Reference [117] presents a trust management scheme based on blockchain. A lightweight trust management algorithm is proposed by limiting the interaction overload. Privacy-preserving feature of nodes is addressed. The social tie is computed as similarity-based on ownership, similarity based on owner friendship, and similarity-based on device friendship.

Reference [118] presents energy and trust based opportunistic transmission strategy for CR-SIoT (Cognitive Radio Social Internet of Things). In CR-SIoT, a novel routing parameter uses stopping theory to determine forwarding candidates, and network coding is employed for data transmission between trustworthy nodes. The authors also suggest a game-theoretic approach for allocating the trusted route for CR-SIoT based on estimated network gain.

The study [119] suggests a group-based service-management approach for SIoT. SP is chosen based on trustworthiness and performance analysis. The study examines selfish behavior in SIoT. The study advises punishing selfish behavior in trustworthiness assessments. Reputation assessment is based on the HITS algorithm.

In this research [120], the authors present an intelligent TMS for MOOC (Massive Open Online Course) ecosystems based on ML approaches that can dynamically measure learner trust, allowing not only a categorization but also a forecast of their future conduct.

Reference [121] introduces a trustworthy crowdsourcing scheme in the domain of SIoT by incorporating the concepts of the social cloud and sensing nodes based on a social awareness process. The study put forwards a message-forwarding algorithm to select a winner and determine payment by assessing the reliability of the participants of crowdsourcing. An auction process is incorporated into a crowdsourcing platform that is based on reputation.

The paper [122] provides a dynamic peer recommendation procedure with a trust management method to address MOOC's (Massive Open Online Course) dynamism. This architecture facilitates MOOC participants to select partners, ensures an immersive learning environment, and encourages peer interaction.

This research [123] provides a preference-based trust management approach that considers IoT node operational conditions. The scheme estimates a SIoT member's trustworthiness based on social relationships and residual energy. Co-work, parental object, co-location, and ownership object relationships are studied. On-off time, residual energy, and interference level measure communication trust, whereas manufacturer capabilities and functional and operational support measure operational trust. Recommendations and reputation calculate indirect trust. The technique detects malicious nodes.

Reference [124] puts forward the TIRec model, which incorporates rating along with direct trust, the indirect trust-based relationships, as a trustworthy and lightweight matrix factorization platform based on trust inference. The literature addressed two types of malicious attacks. In order to select trustworthy users, the study proposes a user-weighted centrality metric. The study infers an indirect trust relationship through the use of a path selection algorithm that is lightweight and a trust inference computation algorithm.

This paper [125] offered a multi-tiered architecture for increasing the responsiveness of social entity service provisioning in SIoT contexts. The work uses fog computing to improve the network's navigability, and management of resources along with scalability, and dependability. Based on social characteristics, reputation, and availability of resources, an effective technique for evaluating SP's trust has also been offered.

Reference [126] presents a trust management framework in the SIoT context based on blockchain. The study provides a modifiable and adaptive trust calculation process to increase the reliability of nodes in terms of trustworthiness computation. Blockchain is used for storage and retrieval purposes of the data associated with trust.

This study [127] presents a hybrid trust management system, that combines the intelligence of humans and devices to create HMST (Hybrid Multi-service Social Tie-graph). OSN Social tie-graph of IoT nodes inputs human intelligence into HMST. IoT nodes' direct opinions form the basis for social ties in HMST, including device intelligence. Each social tie's probability is based on its trustworthiness. P-NO (Probabilistic- Neighborhood Overlap) estimates the strength of node ties.

This study [128] presents a computational trust model for decision-making in uncertain SOA-based SIoT contexts. Several specific and general sources of uncertainty were modeled and used in the context with respect to IoT interactions and data analysis. In this model, QoS certainty, recommender honesty, and context circumstances were evaluated independently and combined to generate ultimate trust. INNs were used in the suggested model to consider uncertainty. The proposed model was utilized in a social context.

The study [129] provides an effective, reliable decision-making solution that is applicable to SIoT systems and helps users in a widely dispersed network to prevent malevolent interactions. The study puts forward an attack detection process comprising of three steps: i) actors' identification ii) feature extraction iii) attack classification. The study employs ML techniques to categorize interactions amongst nodes as benign or trustworthy on the basis of social trust and quality of service characteristics.

In the study [130], the authors provide a cutting-edge technique for recommending SIoT services to consumers, particularly those who have little training data. The suggested method uses a latent variable model to first learn user preferences from item or entity usage events. After that, the authors build a knowledge graph by connecting various social links between SIoT devices and user preferences. The suggested approach specifically integrates users, items/ entities, services, and their associated relations into a shared lower-dimensional space. Then, using graph embeddings to break down the SIoT service suggestion into a connected prediction process while taking into account the user's item usage event and the item's social relationships, the authors model SIoT service recommendation as a knowledge graph completion problem.

Object recommendation plays a vital role in trust management. In the study [131], the authors introduced a time-aware SIoT object recommendation model by taking into account the temporal impact on user-object interactions and the social similarity of smart objects. The suggested recommendation mechanism uses events associated with user object usage to develop a latent probabilistic model that tracks user preferences over time. For users who only use a few objects, the model disseminates their preferences on the basis of latent classes that display user and object properties. The suggested technique evaluates the social similarity of smart entities by embedding entities and their social ties in a shared lower-dimensional space. In the last step, the model integrates the user's temporal preference and the entity's social similarity to provide object-based collaborative filtering recommendations.

The study [132] presents a context-dependent trust management strategy (ConTrust) for identifying a trustworthy SP and allocating jobs in SIoT. Integrating trust theory with social networks leads to the generation of a SIoT trust model. Combining capability, commitment, and satisfaction along with feature-property matching enhances trust evaluation and resolves context-dependent problems. This study also provides strategies to incorporate resiliency against trust-related attacks in SIoT.

C. CLASSIFICATION OF STUDIES ACCORDING TO THE TYPES OF TRUST ATTRIBUTES (TAs)

TAs can be broadly categorized into two trust metrics: Social Trust and Quality of Service (QoS) as represented in Figure 8. Examples of Social Trust attributes include: honesty, cooperativeness, centrality, etc. Examples of QoS Trust attributes include capability, response time, number of interactions, throughput, data delivery ratio, energy, etc.

D. CLASSIFICATION OF STUDIES ACCORDING TO THE TYPES OF OPINIONS

Based on the types of assessment (feedback/ opinions) involved in calculating and aggregating trust values, the trust-based decision schemes can be broadly categorized as Reputation-based, Recommendation-based, Knowledge-based, and Hybrid as shown in Figure 9.

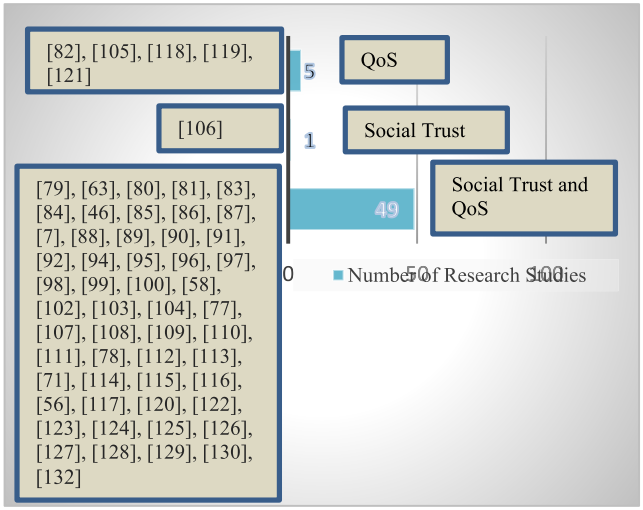


FIGURE 8. Classification of research studies on the basis of types of trust attributes.

- Reputation-based - The reputation of a node includes global opinions in the form of ratings.
- Recommendation-based - Based upon indirect opinions (opinions given by friends or the friends of friends) about a particular node.
- Knowledge-based - using information given by the trustee to analyze its trustworthiness and consists of particular Trust Attributes.
- Hybrid - Consists of more than one of the above-mentioned schemes.

E. CLASSIFICATION OF STUDIES ON THE BASIS OF TYPES OF COMPUTATION/ AGGREGATION METHODS

Based on the type of trust aggregation or trust computation, the trust schemes can be broadly classified as but not limited to Prediction-based, Policy-based, Weighted Sum-based, and Hybrid as depicted in Figure 10.

- Prediction-based - These techniques involve Artificial Intelligence (AI) methods (Such as Machine Learning, Deep Learning algorithms) to predict the trust values.
- Policy-based - These techniques make use of rules or policies such as fuzzy logic by which trust is aggregated or computed.
- Weighted Sum Model / Weighted Linear Combination of Simple Additive Weighting - These techniques' prime focus is to assign weights to different components and then based upon the weights perform trust aggregation or trust computation.
- Hybrid - Consists of more than one above-mentioned scheme.

F. CLASSIFICATION OF STUDIES ON THE BASIS OF CONTEXT-BASED OR CONTEXT-FREE APPROACH

Based upon the inclusion of environment/ context or not during trust computation, trust aggregation, and trust evaluation, the schemes can be broadly classified as Context-based or Context-free as shown in Figure 11.

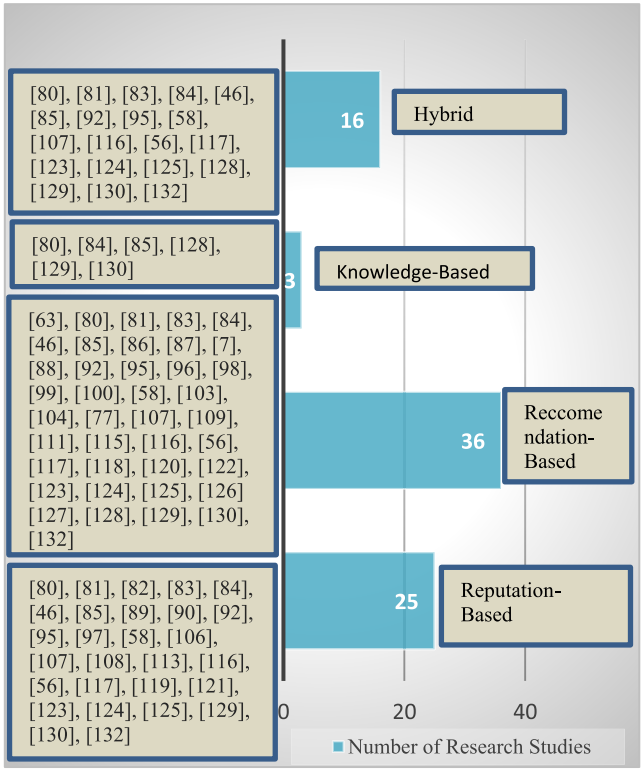


FIGURE 9. Classification of research studies based on types of opinions.

- Context-based - The context is taken into consideration whether it's related to service or device or environment.
- Context-free - The context is not taken into consideration.

G. MECHANISMS TO PROVIDE RESILIENCY AGAINST INTRINSIC AND EXTRINSIC SIoT ATTACKS

This section presents a discussion on the mechanisms proposed in the studies to provide resiliency against Intrinsic and Extrinsic attacks.

In the study [79] A significant criterion for identifying 'on off' selective forwarding attackers is the expected trust. In the implementation, a threshold trust value of 0.4 was set. The object may be the target of an 'on off' attack if the overall trust value is below the threshold value.

In [63], BMA/ BSA is detected by comparing the recommendation with its own trust values, categorizing nodes as honest or dishonest. SPA by node 'j' is detected when it boosts its cooperativeness and/or community-interest trust to increase its chances of being chosen as the service provider but then gives a subpar service. The protocol's honesty-detecting techniques reduce the node 'j's trust.

In the research work [82], the proposed model detects faulty nodes by using 'credit' and 'reputation' as parameters and isolates fraudulent nodes by using penalties for malicious conduct.

In [83], the Platform's algorithm incorporates the random surfer notion to address this issue of the Sybil attack. One log file is preserved per service to combat malicious nodes that change their behavior according to the service they deliver.

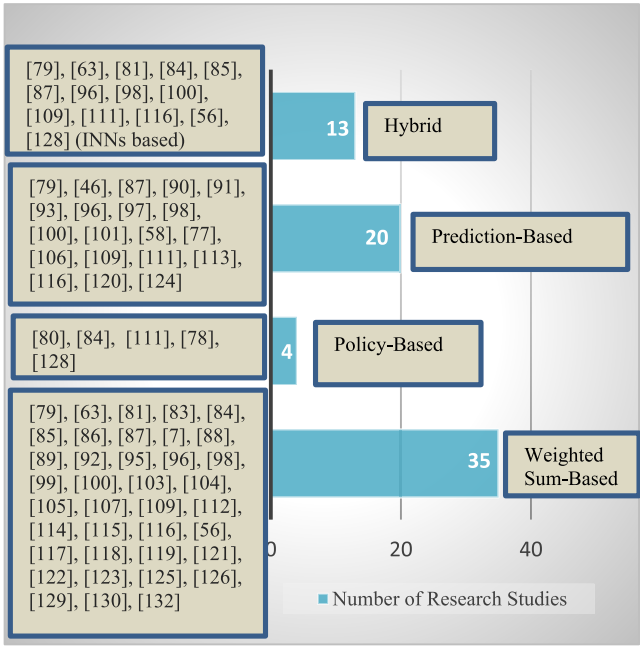


FIGURE 10. Classification of research studies based on types of trust computation/ aggregation methods.

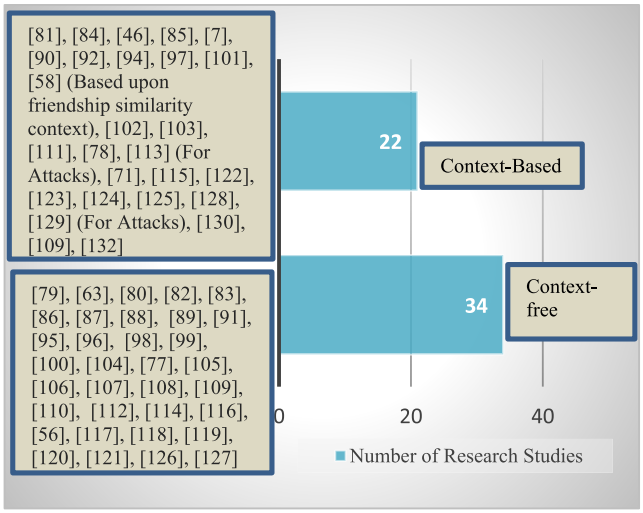


FIGURE 11. Classification of research studies as context-based or context-free approach.

Reference [84], selects four TAs (cooperativeness, community interest, honesty, and similarity) to identify whether a social entity is trustworthy or malevolent, along with the risks associated with SIoT environment, including SPA, BMA, and BSA. These four TAs determine an entity's credibility within a social network.

In [46], the Decision tree is used for the selection of trustworthy SPs. The social similarity which is used as an indicator of credibility (the greater the similarity is, the greater the credibility) is calculated between the selected SP and SR. However, once a malevolent object is detected, it is punished double to prevent fraudulent activity.

Reference [86], takes energy into account to detect 'on off' or selective forwarding attacks as a node performing these attacks will have a relatively higher energy level (because the

node falls into the off state during crucial transactions). The node is isolated from the network when it falls victim to an 'on off' selective forwarding attack because its calculated trust value surpasses the minimum value.

Reference [87] proposes a decentralized trust management approach where each node computes and records data about other nodes to form its own opinion of the network. Hostile attacks like DA that change behavior based on requester are easily detected. Malignant nodes that launch OOA and OSA often change behavior. The proposed approach uses TA 'Dynamic Knowledge' to learn from and adjust to potentially harmful behaviors. The authors use two parameters (Usefulness Score and Perseverance Score) to assess the service provider's behavior. Because the model values direct observations over recommendations, the proposed model also addresses BMA. In BSA, two mutually harmful friends recommend a malicious supplier to the requester node. Such recommendations are only utilized in the startup stage of the model to combat this attack, and as 'Dynamic Knowledge' gains experience, their weight diminishes with the number of transactions. The model automatically avoids SPA and Sybil attacks.

Reference [88] uses DTrustInfer to calculate node trust and Secure codes to secure node communication. Honest nodes mix quickly, but Sybils don't. Using DTrustInfer, cuts the graph between Sybil and honest. This helps find the Sybil region.

In [90] DATM (discriminative-aware trust management), ratings determine trust values. Nodes cannot record their own ratings to prevent SPA. Ratings cannot be given equal weights since BMA/BSA may occur. In this study, attacks are rated based on their owner's reputation and times. The malevolent node that launches OSA causes the trust values to get lower whenever these fraudulent nodes provide subpar services resulting in the detection of OSA.

Reference [91] uses Hellinger distance-based matrix factorization for trust management. Using the proposed method, the trustworthiness of SIoT nodes remains constant during evaluation, except for hostile nodes that conduct OSA. Any drop in trustworthiness detects OSA.

Grouping nodes by CoI (Community of interest) in [92] prevents DA attacks. The proposed system defends against SPA by evaluating trust indirectly and testing recommendations for relevance. The suggested trust scheme counters WA by tracking past trust values. The suggested trust protocol is effective against BMA and BSA because it considers trustor-recommender relationships.

Reference [93] proposes assessing trustworthiness on both sides of the SIoT to protect the trust relationship between the trustor and trustee. SIoT devices accept task delegation based on requests, ensuring resources aren't misused. Only authorized users can use the services, and hostile nodes can't infiltrate the network. This context and characteristics based trustworthiness paradigm can detect malicious SIoT node activity.

In [95] the subjective model states that each node retains and controls the feedback needed to determine local trustworthiness. Malicious nodes that provide misleading references and are connected to unreliable network areas receive negative feedback. The objective approach stores node trustworthiness values in a DHT-structured distributed system on the network. Every node's feedback is weighed to reduce the risk of malevolent nodes providing misleading feedback to undermine the reputation system.

The proposed strategy in [96], tackles SPA by using feedback assessment for a particular service. BMA and BSA are prevented by assessing the trust of a node towards its recommender. The trust predictability approach is used to deal with OSA and OOA.

Reference [97] uses supervised Machine Learning to distinguish malevolent from legitimate nodes. The 'credibility' factor compares the user rating vector with the total rating matrix to determine a node's credibility. If the node's rating differs from most users', it's incredible. It combats BMA, BSA, and SPA. The authors use 'Rating-trend' to determine a user's optimism and network behavior, identifying DA. ''Relationship strength'' measures the strength of the relationship between two nodes to detect colluding attacks.

Reference [98], suggests a trust management approach that uses the 'intended trust' factor to distinguish between the malicious and legitimate nodes.

The study [100] implements a Kalman filter-based prediction model to prevent OOA. When dishonest behavior is discovered, the model recommends punishing the fraudulent nodes twice.

In [101], the model suggests selecting different trust features based on the attack context (SPA, BSA, BMA, DA, OSA). In the machine learning-based trust aggregation phase, the ANN algorithm is used to calculate the trust score. At the output layer of the ANN, a probability determines whether a trustee is malicious or benign, identifying malicious nodes.

In [102], the suggested trust model uses past service records to determine trustworthiness. This prevents SPA. In order to combat OSA, the likelihood of service delegation is decreased if a malicious SP is deemed to be less trustworthy. It can't increase its credibility by quickly offering many services. The malevolent node must break all existing trust relationships with other SRs when joining the network with a new identity, so WA is prevented. To successfully make BMA against an honest SP, a fraudulent node must not only establish a high DoSR factor with SR but also minimize the amount of trust-related information SR gathers from other sources about the honest SP. Certain model conditions prevent BSA. Malicious SPs can't launch DAs without first identifying as many social ties as possible to cause conflict. Dishonest SPs lose trustworthiness if they send DAs to reputable SRs.

In research [103], using feedback variance lowers a dishonest device's trust value when it offers subpar services. According to the model, the honest device's trustworthiness has increased while the dishonest device's has decreased.

Even if previous dishonest devices helped the dishonest node gain trust, it loses it after providing subpar services. Despite bad recommendations destroying the honest device's trustworthiness, following successful service has increased it.

In [104], the model only takes into account the recommendations from the trustor's immediate friends during the merging of recommendations with the direct trust in order to deal with various forms of attacks, such as BSA, BMA, and GMA.

In the research study [109], the proposed mechanism uses the 'Detection Probability' feature which is a measure of a mechanism's capacity to adapt to any network circumstance and sensibly manage incorrect service references during navigation.

Reference [109] ensures service delivery in a secured manner by incorporating the Privacy Protection Paradigm (PPP) constituting of three main phases: (1) Encryption of friend list using Genetic Algorithm based Pseudo Random Sequence Generation (GA- PRSG) technique, (2) Verification of device authentication via inspection of the Updated Friendship Directory (UFD), and (3) Attribute based Encryption (ABE) of the requested data in order to control who has access to it.

Reference [111] Based on Direct Trust and Recommendation Trust computation techniques, the suggested model resists cheating attacks and reduces their impact. The model uses interactive results to confirm the precision of recommendations without being impacted by additional malicious objects. The proposed model combats BMA by removing dishonest recommendations and reducing judgment errors.

In the study [78], the proposed system provides defense against the Sybil attack by not relying on a central reputation system.

Reference [113] proposes an attack-detection system that calls for a thorough examination of node activity. Using deep learning techniques to provide resiliency against BMA, BSA, SPA, and DA.

In the research work [115], the suggested approach penalizes relationship types that value cooperation and honesty less, lowering the likelihood of attacks. The model defends against malicious attacks like SPA, BMA, OOA, and SBA with the help of the optimization strategy utilized to alter the parameter 'weighting factors.' As the percentage of malevolent nodes rises, the value of the weighting parameter also rises, thus strengthening the model's defenses against BSA and BMA.

Reference [116] Using machine learning, the proposed approach extracts and analyses node behavior in fraudulent transactions. Then, it is categorized according to the kind of trust-related attacks that were carried out. These elements are based on the trust system's service quality and social metrics. This paradigm uses reputation and cooperativeness to detect attacks and deal with the attacker node's damaging activities. To cope with OSA, the attacker node is recognized by its low reputation history and positive current reputation value. For WA, the trust mechanism recognizes that the misbehaving node's numerous identities share one IP address. When determining OOA, the model considers its reputation. In OOA attack detection, the model assesses a node's honesty.

In the study [56], feedback is stored on the blockchain, making it transparent and accessible to all nodes thus preventing BMA. Each node in the proposed trust assessment mechanism uses its own and other nodes' expertise. Using entropy to assess reputation indirectly reduces the impact of forged feedback and increases trust assessment reliability. Social connection analysis stops the attack. Trustors also consider cooperativeness and community-interest metrics. Because social connections are granted by trusted owners, this restricts the access of nodes with weak social ties to the trustor. The suggested approach is immune to BSA because it uses direct and indirect experience among system nodes, entropy in reputation analysis, and network social link assessment. Random nodes can't join the system without their owners' permission to prevent a DoS attack. If an authorized node tries to send a fraudulent transaction to the network, its reputation in the trust management system will be ruined, and the system will stop it from sending transactions. The transaction costs reduce the incentive for a malicious node to launch such an attack. The proposed solution uses blockchain technology and unchangeable blockchain data to defend against storage attacks.

In [117], a defense against BMA is provided as there is no way for enemies to influence a node's trust assessment other than by being on its 'counselor list' Each node relies on both its own judgment and the suggestions from its 'counselor list' Nodes regularly edit their list of counselors, removing any nodes whose feedback differs greatly from others. Attack via BSA is addressed by utilizing counselor lists, which shows that the suggested framework is immune to forged positive recommendations. In a Message Spoofing Attack, the blockchain checks the identity of the message sender for each transaction to prevent spoofing authorized users' identities. DoS-launching nodes lose credibility, so the system denies their requests. To prevent DoS, the requester must pay the transaction fee, reducing the attackers' incentive. Only immutable blockchain trust values can be read that provide defense against a Storage Attack

Reference [118] suggests an approach to defend against boost attacks and defamation attacks. In the proposed approach, with the passage of time, the average trust value of victim nodes (Defamation victims or Boost victims) fluctuates until it eventually reaches the average trust value of normal nodes. The suggested method effectively detects malicious nodes in the network by using a novel routing metric to choose candidate forwarders.

In [119], the authors developed a method to punish selfish objects based on their behavior. When a service provider renders an unreliable service in a group, the group manager bans the object from rendering any services. This object cannot request services. False feedback forces an object into the feedback punishment cycle. In this case, group managers disqualify the malicious object from contributing. The mea-

surement criteria are service reliability and feedback validity threshold. A service provider or feedback source is unreliable below a certain point. The model uses cosine similarity to avoid BMA or GMA when assessing feedback honesty.

In the study [121], a reliable crowdsourcing model is put forward to deal with DDoS attacks by crowdsourcing participants. Social awareness is introduced to combat DoS attacks by self-centered nodes in SIoT. To assess the reliability of crowdsourcing participants and identify unreliable participants of crowdsourcing, a reputation method is deployed.

Reference [123], states that the malicious nodes running BMA or SPA display a high volume of activity in a short amount of time. Therefore, numerous operations over a short time period are an indication of potential malevolent behavior. To reduce ownership-based trust violations, edge-based validation and recommendations from the same ownership nodes are used to calculate the value of ownership-based trust. To reduce co-location based trust violation, the edge-based validation and recommendation by the co-location nodes are used to calculate the co-location based trust value.

Reference [124] proposes comparing trust values to identify trustworthy nodes. In a social trust network, a user is trusted if the ratio of trust values acquired or given is greater than distrust values, where the threshold is 0.5. Unreliable users are excluded from trust inference calculations. By emphasizing last-hop users and assessing their dependability, divergent user viewpoints are resolved, and BMA risk is reduced. Neighbor user feedback can identify false recommendations and diminish collusive users' reputations.

Reference [126] prevents the BSA, WA, SPA, and BMA through the use and implementation of complete and accurate service history and information related to trust.

Reference [127] states a slandering attack cannot be repeated in the proposed trust structure because the malicious node 'm' has nothing to gain. The edge {'m'→'y'} would only disappear after the initial impact on node 'y'. Second, (1/b), where b is the number of node 'x' service providers for each service S∗, excluding node 'y', limits the slandering attack's impact. Finally, and most significantly, in order to damage node "y," malicious node "m" must itself be a genuine service provider for some service S∗ to node "x." Value(b) ≫ Value(n) is necessary to reduce the effects of the Sybil + Slandering attack, where b is the total number of trusted service providers of node 'x' and 'n' is the number of instances of malevolent node 'm'. Each instance of the fraudulent node is required to offer trusted services to the targeted node. In a Sybil+Self-Promotional attack and BSA due to the verified provider restriction on the malevolent node instances and a cap on the maximum damage as a consequence of the P-NO computation process, the attacks are self-limiting. In the proposed model, a victim node notifies any untrustworthy behavior by a malevolent node towards the victim node on the SIoT network in order to counteract OOA.

In [128] to tackle the attacks generated by the malicious recommenders, the malevolent recommenders are identified by examining their recommendations and ignoring their opinions over time. Fraudulent SPs are quickly and correctly identified, and users are sent notifications about malevolent SPs.

In [129], Three phases are used to carry out trust-related threat detection. i) actors identification ii) features extraction iii) attacks classification. In the actor's identification phase, for each trust-related attack, three fundamental characteristics (transaction type, malicious node, and targeted node) are noted. In the Feature extraction phase, the tackling of attacks is based on different features (honesty, reputation, and social similarity). To tackle SPA, BSA, and OSA, malevolent nodes' actions can be analyzed and identified on the basis of TAs like reputation, social similarity, and honesty. In order to detect BMA, the study takes into account social similarity and honesty. To identify OOA, the TAs (honesty and reputation) are evaluated. WA is detected by poor reputation and lack of social similarity. Low honesty and reputation values help in identifying the malevolent node launching DA. In the Attacks classification stage, an ML algorithm assesses the values and classifies them in accordance with the conducted attack, if one exists.

In [132] the low reputation value of malevolent SP and penalty mechanism combat OSA. To tackle SPA, misleading feedbacks have less weight (as perceived by SRs), and the trust-related information the fraudulent nodes supply is useless in evaluating the malevolent SP's trustworthiness. Moreover, the framework uses a potential SP's job history to judge its reliability, so preventing the SPA by ensuring that the SR does not accept the prospective malevolent SP's self-recommendation. WA is tackled by identifying weak security issues in addition to the checks related to the identification. To launch DA, an attacker must first find as many social relationships as possible between entities to cause conflict, which is complicated and unrealistic. This leads to the model's adversary being penalized for lack of trust. When a fraudulent node launches DA on a powerful SR, its trust value declines. This leads to unsuccessful DA attempts. For an adversary to launch BMA against a trustworthy SP, it must build a high social connection with SR and restricts the access of SR to trust-related feedback from other entities about the trustworthy SP. Adversaries have a hard time identifying or incorrectly affecting trust-related feedback, thus making BMA hard to launch. To launch BSA, the capability factor should be greater than or equal to the capability threshold and the commitment factor should be greater than or equal to the commitment threshold which is extremely difficult to achieve.

VI. APPLICATION AREAS OF SIoT CONCERNING TRUST MANAGEMENT

A description of application areas of trust management in the SIoT domain as shown in Figure 12 as follows:

A. CROWDSOURCING

Allows people to pool their resources and establish an ad hoc network. The community's resources aid in the resolution of a variety of low-complexity computing tasks.

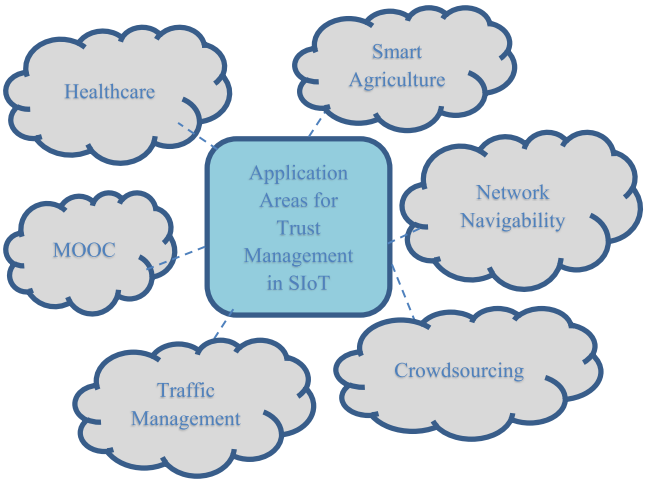


FIGURE 12. Application areas of SIoT with respect to trust management.

Crowdsourcing is considered a huge possibility for IoT to facilitate its nodes' social strength. There are numerous options for crowdsourcing solutions in IoT. Crowdsourcing is a social aspect of IoT that requires trust management [78].

B. MOOC (MASSIVE OPEN ONLINE COURSE)

These intelligent learning ecosystems can enhance learners' access to courses anytime, anywhere. Despite the expansion of MOOCs, disengagement and completion are challenges. Overcrowded MOOCs result in strong interactions, varied communications, and changing behaviors. In quest of a partner who can provide needed service and assistance, trust issues can arise. The lack of trust-based partnerships among learners is a major source of attrition and disinterest [122]. Trust issues may prevent students from communicating with peers. They spend a lot of time looking for a communication and collaboration partner. So, trust evaluation in SIoT can allow learners to find trustworthy peers to collaborate with or minimize uncertainty when they interact. [122].

C. HEALTHCARE SECTORS

IoT health care consists of smart devices that accompany the patient. A third-party company may have deployed these Things/ smart devices for a different purpose [147]. Health care is unknown and risky; therefore, trust is crucial. It's a prerequisite for implementing innovative healthcare services. Patient happiness, adherence, the durability of interaction with healthcare practitioners, and correct and fast diagnosis all influence healthcare quality. Trust represents patients' impressions of healthcare providers and their willingness to recommend one [148]. SIoT improves the healthcare sector's trust evaluation.

D. SMART AGRICULTURE

Smart agriculture integrates IoT, Big Data, GPS, Cloud Computing, and AI into traditional farming. By using a large number of sensors in fields, greenhouses, woodland gardens, and pastures, a smart agricultural IoT platform may collect real-time information on breeding or planting [149]. Malicious sensors for sensing temperature, water level, soil condition, light, etc. affect agricultural decision-making [150]. To effectively cope with SIoT trust-related attacks, several trust-related aspects must be examined depending on the nodes' relationships

E. NETWORK NAVIGABILITY

Short pathways between nodes determine network navigability [151]. To improve the service discovery process by leveraging multiple relationships (e.g., friendship among nodes, communities of interest, and co-location) and exploiting these social links to traverse the network, reducing the average path length [152].

The study [153] highlights friendship selection and node distance during SIoT navigation. According to the report, SIoT nodes route information and service requests, distribute data and assess network member trust. SIoT elements that affect the performance of these operations include the social network's structure, the categories of service/information requests, and the rules for navigating the social network. This study simulates all these elements. Measures of navigability include average path length, network diameter, and component size. This study [153] analyses two types of distances across nodes: geographical distance (computed using objects' most recent coordinates) and object distance (similarity between two objects).

F. TRAFFIC MANAGEMENT

Understanding the Internet of Vehicles (IoV) has led to the Social Internet of Vehicles (SIoV), which evolved from SIoT. In SIoV, vehicles are viewed as smart objects. This capacity to socialize helps these vehicles to handle a range of issues, such as service discovery (SD), which allows heterogeneous vehicles to provide dependable services to SCs. This improves road safety and driver experience. In SIoV, a group of vehicles may have a social aim. SIoV relies on trustworthy services [154].

VII. CHALLENGES AND FUTURE DIRECTION

The following challenges are identified in the trust management framework for SIoT: (i) Lack of context-based simulators/ analysis tools to effectively develop the trust management framework; (ii) Lack of context-based trust management frameworks: many SIoT research studies propose a trust management framework without considering the context for trust computation, aggregation, propagation, and evaluation; (iii) Lack of standard set of Trust Attributes (TAs) which could be evaluated in every trust management framework irrespective of the scenarios being considered; (iv) Lack of resiliency against trust-related attacks: this survey demonstrates that many studies have proposed a trust management framework without incorporating a resiliency mechanism against attacks in SIoT. (v) Lack of using a hybrid trust management approach: this survey shows that there is a lack of using a hybrid approach for trust management which could result in acquiring the benefits of both the centralized and decentralized approaches.

Future research directions associated with trust management in SIoT include: (i) development of standard Trust Attributes to be used in every trust management scheme; (ii) development of context-based simulators for trust management framework; (iii) use of Blockchain for tamper-free storage and calculation of trust values. This would lead to the trustor having enhanced trust in the trustee. The trust ratings provided by SCs after acquiring services should be kept in a tamper-free environment. (iv) more focus on hybrid trust management frameworks to leverage the benefits of both the centralized and decentralized approaches.

VIII. CONCLUSION

Our research study provides a comprehensive analysis in the field of SIoT based on the trust management framework/models. Different SIoT architectures are covered in the introduction section. Social relationships are the pillars of any SIoT architecture in any context. Therefore, this study also covers various social relationships which play an important role in the development of trust management frameworks as part of the introduction section.

Our prime focus is on the analysis of the trust management aspect in SIoT therefore this study covers different aspects of trust in detail. Each trust management framework comprises Trust Attributes (TAs) whose properties are broadly classified as general trust properties and trust properties specifically related to the social aspects in the SIoT domain. Our survey includes the classification of studies on the types of TAs (''Social Trust'' or ''Quality of Service (QoS)'') being used. Any trust management framework is based on three general steps: trust computation, trust aggregation, and trust updates. The three general steps make use of TAs to perform the calculation. The local trust values are accumulated or aggregated to form an overall or global trust by using various trust aggregation schemes. Our research work also covers many distinguished trust computation and trust aggregation techniques in detail. The weighted Sum technique is one of the widely used techniques because of its low cost and ease of use. However, the use of machine learning algorithms is an emerging trend, but these methods are not cost-effective. Our research work also covers the scenarios where various trust computation and trust aggregation schemes are used. When the trust value is computed and aggregated, the next step is to update the already computed or assigned trust values to the nodes present in the network. The analysis of corresponding studies suggests that the most widely used method is event-driven as compared to the time-driven trust update scheme. Trust propagation focuses on three different trust propagation schemes: centralized, distributed/ decentralized and semi-centralized/ hybrid. Based on these studies, the most commonly used trust propagation schemes are decentralized. Although centralized schemes are easier to implement, they lead to a single point of failure. More focus should be given to developing hybrid trust management frameworks so that the benefits of both the centralized and decentralized approaches can be availed.

In the SIoT domain, trust-related attacks fall into two wide categories: collaborative attacks and individual attacks. Hence, our research study presents different attacks addressed in the relevant studies. Our research work also discusses the mechanisms addressed in these studies to provide resiliency against trust-related attacks. Our study also classifies attacks as ''Intrinsic'' and ''Extrinsic'' attacks.

Simulators or analysis tools provide the basis to evaluate trust models in a controlled context, consequently, these have been included in our study. Different trust strategies aim for different use of simulators or analysis tools. ns-3, NetLogo, and MATLAB are some of the most commonly used simulators.

Our research also classifies studies (reputation-based, recommendation-based, knowledge-based) based on opinions (global feedback or opinion, feedback from a friend, trustor's own opinion based on the information provided by the trustee) used in computing and aggregating trust values. We also include the classification of studies (policy-based, prediction-based, weighted sum based/ weighted linear combination based) according to the types of trust computation/ aggregation methods being used in our work.

This survey of trust management frameworks in the SIoT domain suggests that more importance should be given to a context-based approach while developing simulators/ analysis tools for trust management frameworks. A standard set of trust attributes should be developed to be used in every trust management model and scheme irrespective of the context. The analysis also suggests the need to derive a tamper-free technique for storing trust values assuring immutability and transparency. Merging blockchain in the trust management framework is another area that is a domain for future study for supporting trust management in SIoT.

ACKNOWLEDGMENT

The authors are extremely grateful to Dr. Omer Rana (Cardiff University, U.K.) for reviewing and providing his insightful comments on this paper.

REFERENCES

[1] L. Atzori, I. A. Iera, and M. Giacomo, ''The Internet of Things: A survey,'' *Comput. Netw.*, vol. 54, pp. 2787–2805, May 2010.

[2] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, ''Internet of Things: Vision, applications and research challenges,'' *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[3] D. E. Kouicem, Y. Imine, A. Bouabdallah, and H. Lakhlef, ''A decentralized blockchain-based trust management protocol for the Internet of Things,'' *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, pp. 1292–1306, Mar. 2022.

[4] 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,'' *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012.

[5] B. Afzal, M. Umair, G. A. Shah, and E. Ahmed, ''Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges,'' *Future Gener. Comput. Syst.*, vol. 92, pp. 718–731, Mar. 2019.

[6] S. K. Lakshmanaprabu, K. Shankar, A. Khanna, D. Gupta, J. J. P. C. Rodrigues, P. R. Pinheiro, and V. H. C. D. Albuquerque, ''Effective features to classify big data using social Internet of Things,'' *IEEE Access*, vol. 6, pp. 24196–24204, 2018.

[7] Z. Lin and L. Dong, "Clarifying trust in social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 2, pp. 234–248, Feb. 2018.

[8] B. K. Tripathy, D. Dutta, and C. Tazivazvino, "On the research and development of social Internet of Things," in *Internet of Things (IoT) in 5G Mobile Technologies*. Cham, Switzerland: Springer, 2016, pp. 153–173.

[9] M. M. Rad, A. M. Rahmani, A. Sahafi, and N. N. Qader, "Social Internet of Things: Vision, challenges, and trends," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–40, Dec. 2020.

[10] S. Shahab, P. Agarwal, T. Mufti, and A. J. Obaid, "SIoT (social Internet of Things): A review," in *ICT Analysis and Applications* (Lecture Notes in Networks and Systems), vol. 314, S. Fong, N. Dey, and A. Joshi, Eds. Singapore: Springer, 2022, doi: 10.1007/978-981-16-5655-2_28.

[11] L. Atzori, A. Iera, and G. Morabito, "Social Internet of Things: Turning smart objects into social objects to boost the IoT," Newsletter, Nov. 2014. Accessed: Oct. 12, 2022. [Online]. Available: https://iot.ieee.org/newsletter/november-2014/social-internet-of-things-turning-smart-objects-into-social-objects-to-boost-the-iot.html?__hstc=77947915.ab7bf88e972fdd7a7debc8575bac5a80.1457222400146.1457222400147.1457222400148.1&__hssc=77947915.1.1457222400149&__hsfp=3972014050

[12] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social Internet of Things: A taxonomy, open issues, and challenges," *Comput. Commun.*, vol. 150, pp. 13–46, Jan. 2020.

[13] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the Internet of Things," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1193–1195, Nov. 2011.

[14] V. Beltran, A. M. Ortiz, D. Hussein, and N. Crespi, "A semantic service creation platform for social IoT," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 283–286.

[15] A. M. Ortiz, D. Hussein, S. Park, S. N. Han, and N. Crespi, "The cluster between Internet of Things and social networks: Review and research challenges," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 206–215, Jun. 2014.

[16] O. Voutyras, P. Bourelos, D. Kyriazis, and T. Varvarigou, "An architecture supporting knowledge flow in social Internet of Things systems," in *Proc. IEEE 10th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2014, pp. 100–105.

[17] R. Girau, S. Martis, and L. Atzori, "LYSIS: A platform for IoT distributed applications over socially connected objects," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 40–51, Feb. 2017.

[18] Y. Saleem, N. Crespi, M. H. Rehmani, R. Copeland, D. Hussein, and E. Bertin, "Exploitation of social IoT for recommendation services," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 359–364.

[19] S. Ali, M. G. Kibria, M. A. Jarwar, H. K. Lee, and I. Chong, "A model of socially connected web objects for IoT applications," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–20, Sep. 2018.

[20] F. Cicirelli, A. Guerrieri, G. Spezzano, A. Vinci, O. Briante, A. Iera, and G. Ruggeri, "Edge computing and social Internet of Things for large-scale smart environments development," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2557–2571, May 2017.

[21] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, Oct. 2018.

[22] K. M. Alam, M. Saini, and A. El Saddik, "Toward social Internet of Vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.

[23] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social Internet of Vehicles: Review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.

[24] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social Internet of Vehicles: Architecture and enabling technologies," *Comput. Electr. Eng.*, vol. 69, pp. 68–84, Jul. 2018.

[25] A. M. Esfahani, A. M. Rahmani, and A. Khademzadeh, "MSIoT: Mobile social Internet of Things, a new paradigm," in *Proc. 10th Int. Symp. Telecommun. (IST)*, Dec. 2020, pp. 187–193.

[26] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sédes, "Trust management in social Internet of Things: A survey," in *Proc. Conf. e-Bus., e-Services e-Soc.* Cham, Switzerland: Springer, Sep. 2015, pp. 430–441.

[27] 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* (Lecture Notes in Electrical Engineering), vol. 545, V. Sridhar, M. Padma, and K. Rao, Eds. Singapore: Springer, 2019, doi: 10.1007/978-981-13-5802-9_19.

[28] F. Amin, A. Ahmad, and G. S. Choi, "Towards trust and friendliness approaches in the social Internet of Things," *Appl. Sci.*, vol. 9, no. 1, p. 166, 2019.

[29] M. S. Roopa, S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions," *Comput. Commun.*, vol. 139, pp. 32–57, May 2019.

[30] K. Elghomary, D. Bouzidi, and N. Daoudi, "A comparative analysis of OSN and SIoT trust models for a trust model adapted to MOOCs platforms," in *Proc. 2nd Int. Conf. Netw., Inf. Syst. Secur. (NISS)*, May 2019, pp. 1–8.

[31] W. Z. Khan, Q.-U.-A. Arshad, S. Hakak, M. K. Khan, and S.-U.-Rehman, "Trust management in social Internet of Things: Architectures, recent advancements, and future challenges," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7768–7788, May 2021.

[32] S. Slone, "The open group identity management work area," Identity Manag., Sydney, NSW, Australia, White Paper W041, Mar. 2004. [Online]. Available: https://pubs.opengroup.org/onlinepubs/7699959899/toc.pdf

[33] J. K. Adjei, "Explaining the role of trust in cloud computing services," *Info*, vol. 17, no. 1, pp. 54–67, Jan. 2015.

[34] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Comput. Surveys*, vol. 48, no. 2, pp. 1–40, Nov. 2015.

[35] D. Gambetta, "Trust: Making and breaking cooperative relations," 1988. Accessed: Oct. 12, 2022. [Online]. Available: https://philarchive.org/rec/GAMTMA

[36] W. J. Adams and N. J. Davis, "Toward a decentralized trust-based access control system for dynamic collaboration," in *Proc. 6th Annu. IEEE Syst., Man Cybern. (SMC) Inf. Assurance Workshop*, Jun. 2005, pp. 317–324.

[37] H. S. James, Jr., "The trust paradox: A survey of economic inquiries into the nature of trust and trustworthiness," *J. Econ. Behav. Org.*, vol. 47, no. 3, pp. 291–307, Mar. 2002.

[38] R. M. Kramer, "Trust and distrust in organizations: Emerging perspectives, enduring questions," *Annu. Rev. Psychol.*, vol. 50, pp. 569–598, Jun. 1999.

[39] D. H. McKnight and N. L. Chervany, "The meanings of trust," Carlson School Manag., Univ. Minnesota, Minneapolis, MN, USA, 1996. Accessed: Oct. 12, 2022. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=23F60248EC4ED899328E71F48701E6B4?doi=10.1.1.155.1213&rep=rep1&type=pdf

[40] F. D. Schoorman, R. C. Mayer, and J. H. Davis, "An integrative model of organizational trust: Past, present, and future," *Acad. Manag. Rev.*, vol. 32, no. 2, pp. 344–354, Apr. 2007.

[41] J. S. Baras and T. Jiang, "Managing trust in self-organized mobile Ad Hoc networks," in *Proc. 12th Annu. Netw. Distrib. Syst. Secur. Symp. Workshop*, Feb. 2005, pp. 1–2.

[42] L. Capra, "Towards a human trust model for mobile ad-hoc networks," Univ. College London, London, U.K., 2004. Accessed: Oct. 12, 2022. [Online]. Available: https://discovery.ucl.ac.uk/id/eprint/816/1/5.2_ukubinet04.pdf

[43] S. P. Marsh, "Formalising trust as a computational concept," Univ. Stirling, 1994. Accessed: Oct. 12, 2022. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.8227&rep=rep1&type=pdf

[44] L. Wei, Y. Yang, J. Wu, C. Long, and B. Li, "Trust management for Internet of Things: A comprehensive study," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7664–7679, May 2022.

[45] I. U. Din, K. A. Awan, A. Almogren, and B.-S. Kim, "ShareTrust: Centralized trust management mechanism for trustworthy resource sharing in industrial Internet of Things," *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 108013.

[46] O. Ben Abderrahim, M. H. Elhedhili, and L. Saidane, "CTMS-SIOT: A context-based trust management system for the social Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1903–1908.

[47] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P networks," in *Proc. 12th Int. Conf. World Wide Web (WWW)*, 2003, pp. 640–651.

[48] R. Chen, X. Zhao, L. Tang, J. Hu, and Z. Chen, "CuboidTrust: A global reputation-based trust model in peer-to-peer networks," in *Proc. Int. Conf. Autonomic Trusted Comput.* Berlin, Germany: Springer, Jul. 2007, pp. 203–215.

[49] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, Jul. 2004, doi: 10.1109/TKDE.2004.1318566.

[50] M. Dorigo, V. Maniezzo, and A. Colorni, "Ant system: Optimization by a colony of cooperating agents," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 26, no. 1, pp. 29–41, Feb. 1996.

[51] O. C. García, F. H. Triguero, and T. Stützle, "A review on the ant colony optimization metaheuristic: Basis, models and new trends," *Mathware Soft Comput.*, vol. 9, pp. 1–35, May 2002.

[52] H. Zhao and X. Li, "VectorTrust: Trust vector aggregation scheme for trust management in peer-to-peer networks," *J. Supercomput.*, vol. 64, no. 3, pp. 805–829, Jun. 2013.

[53] F. Li, D. Wang, Y. Wang, X. Yu, N. Wu, J. Yu, and H. Zhou, "Wireless communications and mobile computing blockchain-based trust management in distributed Internet of Things," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–12, Dec. 2020.

[54] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. D. Drobintsev, "Trust management in a blockchain based fog computing platform with trustless smart oracles," *Future Gener. Comput. Syst.*, vol. 101, pp. 747–759, Dec. 2019.

[55] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[56] M. Amiri-Zarandi and R. A. Dara, "Blockchain-based trust management in social Internet of Things," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2020, pp. 49–54.

[57] H. Taneja and S. Kaur, "Fake feedback detection to enhance trust in cloud using supervised machine learning techniques," in *Proc. Data Anal. Manag.* Singapor: Springer, 2022, pp. 789–796.

[58] 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 *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[59] S. Wang, Y. Hu, and G. Qi, "Blockchain and deep learning based trust management for Internet of Vehicles," *Simul. Model. Pract. Theory*, vol. 120, Nov. 2022, Art. no. 102627.

[60] M. M. Hassan, M. R. Hassan, S. Huda, and V. H. C. D. Albuquerque, "A robust deep-learning-enabled trust-boundary protection for adversarial industrial IoT environment," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9611–9621, Jun. 2021.

[61] J. Golbeck, "Trust on the world wide web: A survey," *Found. Trends Web Sci.*, vol. 1, no. 2, pp. 131–197, May 2008.

[62] J. Golbeck, "Generating predictive movie recommendations from trust in social networks," in *Proc. Int. Conf. Trust Manag.* Berlin, Germany: Springer, May 2006, pp. 93–104.

[63] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social Internet of Things systems," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 684–696, Nov./Dec. 2016.

[64] A. Landherr, B. Friedl, and J. Heidemann, "A critical review of centrality measures in social networks," *Bus. Inf. Syst. Eng.*, vol. 2, no. 6, pp. 371–385, Dec. 2010.

[65] I. Y. Kim and O. L. de Weck, "Adaptive weighted sum method for multiobjective optimization: A new method for Pareto front generation," *Struct. Multidisciplinary Optim.*, vol. 31, no. 2, pp. 105–116, Feb. 2006.

[66] R. T. Marler and J. S. Arora, "The weighted sum method for multi-objective optimization: New insights," *Struct. Multidisciplinary Optim.*, vol. 41, no. 6, pp. 853–862, Jun. 2010.

[67] A. Gelman, J. B. Carlin, H. S. Stern, and D. B. Rubin, *Bayesian Data Analysis*. London, U.K.: Chapman-Hall, 1995.

[68] J. M. Bernardo and A. F. Smith, *Bayesian Theory*, vol. 405. Hoboken, NJ, USA: Wiley, 2009.

[69] B. Mahesh, "Machine learning algorithms—A review," *Int. J. Sci. Res.*, vol. 9, pp. 381–386, Oct. 2020.

[70] I. El Naqa and M. J. Murphy, "What is machine learning?" in *Machine Learning in Radiation Oncology*. Cham, Switzerland: Springer, 2015, pp. 3–11.

[71] U. S. Premarathne, "MAG-SIoT: A multiplicative attributes graph model based trust computation method for social Internet of Things," in *Proc. IEEE Int. Conf. Ind. Inf. Syst. (ICIIS)*, Dec. 2017, pp. 1–6.

[72] M. Kim and J. Leskovec, "Multiplicative attribute graph model of real-world networks," *Internet Math.*, vol. 8, nos. 1–2, pp. 113–160, Mar. 2012.

[73] L. A. Zadeh, "Fuzzy logic," *Computer*, vol. 21, no. 4, pp. 83–93, Apr. 1988.

[74] L. Deng and D. Yu, "Deep learning: Methods and applications," *Found. Trends Signal Process.*, vol. 7, nos. 3–4, pp. 197–387, 2014.

[75] J. Ahmad, H. Farman, and Z. Jan, "Deep learning methods and applications," in *Deep Learning: Convergence to Big Data Analytics*. Singapore: Springer, 2019, pp. 31–42.

[76] Y. Bengio, I. Goodfellow, and A. Courville, "Deep learning," *Nature*, vol. 521, pp. 436–444, May 2016.

[77] J. Son, W. Choi, and S. M. Choi, "Trust information network in social Internet of Things using trust-aware recommender systems," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 4, 2020, Art. no. 1550147720908773.

[78] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman, "Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 758–776, Mar. 2019.

[79] A. M. Kowshalya and M. L. Valarmathi, "Trust management for reliable decision making among social objects in the social Internet of Things," *IET Netw.*, vol. 6, no. 4, pp. 75–80, 2017.

[80] N. B. Truong, T. W. Um, and G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy social Internet of Things," in *Proc. Innov. Clouds, Internet Netw. (ICIN)*, Paris, France, 2016, pp. 104–111.

[81] N. B. Truong, T.-W. Um, B. Zhou, and G. M. Lee, "From personal experience to global reputation for trust evaluation in the social Internet of Things," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–7.

[82] H. Xiao, N. Sidhu, and B. Christianson, "Guarantor and reputation based trust model for social Internet of Things," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, pp. 600–605.

[83] E. Kokoris-Kogias, O. Voutyras, and T. Varvarigou, "TRM-SIoT: A scalable hybrid trust & reputation model for the social Internet of Things," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2016, pp. 1–9.

[84] 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, p. 1346, 2017.

[85] U. Jayasinghe, N. B. Truong, G. M. Lee, and T.-W. Um, "RPR: A trust computation model for social Internet of Things," in *Proc. IEEE Int. Conf. Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Jul. 2016, pp. 930–937.

[86] A. M. Kowshalya and M. L. Valarmathi, "Trust management in the social Internet of Things," *Wireless Pers. Commun.*, vol. 96, no. 2, pp. 2681–2691, 2017.

[87] C. Marche and M. Nitti, "Trust-related attacks and their detection: A trust management model for the social IoT," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 3, pp. 3297–3308, Sep. 2021.

[88] A. M. Kowshalya and M. L. Valarmathi, "Dynamic trust management for secure communications in social Internet of Things (SIoT)," *Sādhanā*, vol. 43, no. 9, pp. 1–8, Sep. 2018.

[89] M. A. Azad, S. Bag, F. Hao, and A. Shalaginov, "Decentralized self-enforcing trust management system for social Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2690–2703, Apr. 2020.

[90] B. Jafarian, N. Yazdani, and M. S. Haghighi, "Discrimination-aware trust management for social Internet of Things," *Comput. Netw.*, vol. 178, Sep. 2020, Art. no. 107254.

[91] 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 Trans. Dependable Secure Comput.*, vol. 19, no. 4, pp. 2274–2285, Jul. 2022.

[92] S. Talbi and A. Bouabdallah, "Interest-based trust management scheme for social Internet of Things," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 3, pp. 1129–1140, Mar. 2020.

[93] J. S. Kumar, G. Sivasankar, and S. S. Nidhyananthan, "An artificial intelligence approach for enhancing trust between social IoT devices in a network," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*. Cham, Switzerland: Springer, 2020, pp. 183–196.

[94] N. Narang and S. Kar, "Utilizing social networks data for trust management in a social Internet of Things network," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2018, pp. 768–770.

[95] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.

[96] G. Ekbatanifard and O. Yousefi, "A novel trust management model in the social Internet of Things," *J. Adv. Comput. Eng. Technol.*, vol. 5, no. 2, pp. 57–70, 2019.

[97] W. Abdelghani, I. Amous, C. A. Zayani, F. Sèdes, and G. Roman-Jimenez, "Dynamic and scalable multi-level trust management model for social Internet of Things," *J. Supercomput.*, vol. 78, no. 6, pp. 8137–8193, Apr. 2022.

[98] R. Puneetha, M. Vishwas, R. Buyya, M. Venugopal, K. Iyengar, and S. Patnaik, "Trust management for service-oriented SIoT systems," in *Proc. 8th Int. Conf. Inf. Technol., IoT Smart City*, Dec. 2020, pp. 216–222.

[99] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 18–23.

[100] 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 *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 747–752.

[101] P. Hankare, S. Babar, and P. Mahalle, "Trust management approach for detection of malicious devices in SIoT," *Tehnièki Glasnik*, vol. 15, no. 1, pp. 43–50, Mar. 2021.

[102] 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 Things J.*, vol. 8, no. 6, pp. 4775–4787, Mar. 2021.

[103] M. Khani, Y. Wang, M. A. Orgun, and F. Zhu, "Context-aware trustworthy service evaluation in social Internet of Things," in *Proc. Int. Conf. Service-Oriented Comput.* Cham, Switzerland: Springer, Nov. 2018, pp. 129–145.

[104] S. Sagar, A. Mahmood, J. Kumar, and Q. Z. Sheng, "A time-aware similarity-based trust computational model for social Internet of Things," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.

[105] M. J. Aslam, S. Din, J. J. P. C. Rodrigues, A. Ahmad, and G. S. Choi, "Defining service-oriented trust assessment for social Internet of Things," *IEEE Access*, vol. 8, pp. 206459–206473, 2020.

[106] S. Sagar, A. Mahmood, M. Sheng, M. Zaib, and W. Zhang, "Towards a machine learning-driven trust evaluation model for social Internet of Things: A time-aware approach," in *Proc. MobiQuitous, 17th EAI Int. Conf. Mobile Ubiquitous Systems, Comput., Netw. Services*, Dec. 2020, pp. 283–290.

[107] A. U. Rehman, R. A. Naqvi, A. Rehman, A. Paul, M. T. Sadiq, and D. Hussain, "A trustworthy SIoT aware mechanism as an enabler for citizen services in smart cities," *Electronics*, vol. 9, no. 6, p. 918, Jun. 2020.

[108] A. U. Rehman, A. Jiang, A. Rehman, and A. Paul, "Weighted based trustworthiness ranking in social Internet of Things by using soft set theory," in *Proc. IEEE 5th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2019, pp. 1644–1648.

[109] S. Rajendran and R. Jebakumar, "Friendliness based trustworthy relationship management (F-TRM) in social Internet of Things," *Wireless Pers. Commun.*, vol. 123, no. 3, pp. 2625–2647, Apr. 2022.

[110] V. Mohammadi, A. M. Rahmani, A. Darwesh, and A. Sahafi, "Trust-based friend selection algorithm for navigability in social Internet of Things," *Knowl.-Based Syst.*, vol. 232, May 2021, Art. no. 107479.

[111] H. Xia, F. Xiao, S.-S. Zhang, C.-Q. Hu, and X.-Z. Cheng, "Trustworthiness inference framework in the social Internet of Things: A context-aware approach," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2019, pp. 838–846.

[112] T. Li, G. Huang, S. Zhang, and Z. Zeng, "NTSC: A novel trust-based service computing scheme in social Internet of Things," *Peer, Peer Netw. Appl.*, vol. 14, no. 6, pp. 3431–3451, 2021.

[113] M. Masmoudi, W. Abdelghani, I. Amous, and F. Sèdes, "Deep learning for trust-related attacks detection in social Internet of Things," in *Proc. Int. Conf. e-Bus. Eng.* Cham, Switzerland: Springer, Oct. 2019, pp. 389–404.

[114] A. M. T. Ali-Eldin, "A cloud-based trust computing model for the social Internet of Things," in *Proc. Int. Mobile, Intell., Ubiquitous Comput. Conf. (MIUCC)*, May 2021, pp. 161–165.

[115] R. Abidi and N. B. Azzouna, "Self-adaptive trust management model for social IoT services," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2021, pp. 1–7.

[116] R. Magdich, H. Jemal, C. Nakti, and M. Ben Ayed, "An efficient trust related attack detection model based on machine learning for social Internet of Things," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2021, pp. 1465–1470.

[117] M. Amiri-Zarandi, R. A. Dara, and E. Fraser, "LBTM: A lightweight blockchain-based trust management system for social Internet of Things," *J. Supercomput.*, vol. 78, no. 6, pp. 8302–8320, Apr. 2022.

[118] X. Wang, X. Zhong, L. Li, S. Zhang, R. Lu, and T. Yang, "TOT: Trust aware opportunistic transmission in cognitive radio social Internet of Things," *Comput. Commun.*, vol. 162, pp. 1–11, Oct. 2020.

[119] B. Farahbakhsh, A. Fanian, and M. H. Manshaei, "TGSM: Towards trustworthy group-based service management for social IoT," *Internet Things*, vol. 13, Mar. 2021, Art. no. 100312.

[120] K. Elghomary, D. Bouzidi, and N. Daoudi, "Design of a smart MOOC trust model: Towards a dynamic peer recommendation to foster collaboration and Learner's engagement," *Int. J. Emerg. Technol. Learn.*, vol. 17, no. 5, pp. 36–56, Mar. 2022.

[121] K. Wang, X. Qi, L. Shu, D.-J. Deng, and J. J. P. C. Rodrigues, "Toward trustworthy crowdsourcing in the social Internet of Things," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 30–36, Oct. 2016.

[122] K. Elghomary and D. Bouzidi, "Dynamic peer recommendation system based on trust model for sustainable social tutoring in MOOCs," in *Proc. 1st Int. Conf. Smart Syst. Data Sci. (ICSSD)*, Oct. 2019, pp. 1–9.

[123] U. S. Premarathne, "Residual energy aware trust computation method for social Internet of Things," in *Proc. 14th Conf. Ind. Inf. Syst. (ICIIS)*, Dec. 2019, pp. 470–475.

[124] B. Cai, X. Li, W. Kong, J. Yuan, and S. Yu, "A reliable and lightweight trust inference model for service recommendation in SIoT," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10988–11003, Jul. 2022.

[125] G. Sciddurlo, I. Huso, D. Striccoli, G. Piro, and G. Boggia, "A multi-tiered social IoT architecture for scalable and trusted service provisioning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

[126] L. Wei, J. Wu, and C. Long, "Enhancing trust management via blockchain in social Internet of Things," in *Proc. Chin. Autom. Congr. (CAC)*, Nov. 2020, pp. 159–164.

[127] N. Narang and S. Kar, "A hybrid trust management framework for a multi-service social IoT network," *Comput. Commun.*, vol. 171, pp. 61–79, Apr. 2021.

[128] S. Pourmohseni, M. Ashtiani, and A. A. Azirani, "A computational trust model for social IoT based on interval neutrosophic numbers," *Inf. Sci.*, vol. 607, pp. 758–782, Aug. 2022.

[129] R. Magdich, H. Jemal, and M. B. Ayed, "A resilient trust management framework towards trust related attacks in the social Internet of Things," *Comput. Commun.*, vol. 191, pp. 92–107, Jul. 2022.

[130] Y. Chen, Y. Tao, Z. Zheng, and D. Chen, "Graph-based service recommendation in social Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 17, no. 4, 2021, Art. no. 15501477211009047.

[131] Y. Chen, M. Zhou, Z. Zheng, and D. Chen, "Time-aware smart object recommendation in social Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2014–2027, Mar. 2020.

[132] R. Latif, "ConTrust: A novel context-dependent trust management model in social Internet of Things," *IEEE Access*, vol. 10, pp. 46526–46537, 2022.

[133] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "When social objects collaborate: Concepts, processing elements, attacks and challenges," *Comput. Electr. Eng.*, vol. 58, pp. 397–411, Feb. 2017.

[134] A. A. Mawgoud, M. H. N. Taha, and N. E. M. Khalifa, "Security threats of social Internet of Things in the higher education environment," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*. Cham, Switzerland: Springer, 2020, pp. 151–171.

[135] T. R. Henderson, M. Lacage, G. F. Riley, C. Dowell, and J. Kopena, "Network simulations with the ns-3 simulator," *SIGCOMM Demonstration*, vol. 14, no. 14, p. 527, 2008.

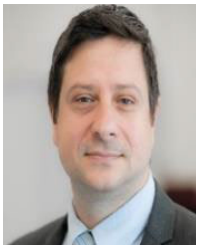
[136] A. Varga, "OMNeT++," in *Modeling and Tools for Network Simulation*. Berlin, Germany: Springer, 2010, pp. 35–59.
[137] A. Velinov and A. Mileva, "Running and testing applications for Contiki OS using Cooja simulator," in *Proc. Inf. Technol. Educ. Develop. (ITRO)*, 2016, pp. 1–10.
[138] S. Tisue and U. Wilensky, "NetLogo: A simple environment for modeling complexity," in *Proc. Int. Conf. Complex Syst.*, vol. 21, 2004, pp. 16–21.
[139] A. Mei and J. Stefa, "SWIM: A simple model to generate small mobile worlds," in *Proc. IEEE 28th Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 2106–2113.
[140] S. Singhal and M. Jena, "A study on WEKA tool for data preprocessing, classification and clustering," *Int. J. Innov. Technol. Exploring Eng.*, vol. 2, no. 6, pp. 250–253, 2013.
[141] S. Chaudhari, M. Patil, and J. Bambhori, "Study and review of fuzzy inference systems for decision making and control," *Amer. Int. J. Res. Sci., Technol., Eng. Math.*, vol. 14, no. 147, pp. 88–92, 2014.
[142] S. Siemer, "Exploring the apache Jena framework," Tech. Rep., 2019.
[143] F. G. Marmol and G. M. Perez, "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.* Germany: IEEE, 2009, pp. 1–5, doi: 10.1109/ICC.2009.5199545.
[144] R. K. Kodali and S. Soratkal, "Trust model for WSN," in *Proc. Int. Conf. Appl. Theor. Comput. Commun. Technol. (iCATccT)*, Oct. 2015, pp. 903–906.
[145] B. Musznicki and P. Zwierzykowski, "Survey of simulators for wireless sensor networks," *Int. J. Grid Distrib. Comput.*, vol. 5, no. 3, pp. 23–50, Sep. 2012.
[146] A. Knight, *Basics of MATLAB and Beyond*. London, U.K.: Chapman-Hall, 2019.
[147] G. Ruggeri and O. Briante, "A framework for IoT and E-health systems integration based on the social Internet of Things paradigm," in *Proc. Int. Symp. Wireless Commun. Syst. (ISWCS)*, Aug. 2017, pp. 426–431.
[148] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues," *IEEE Access*, vol. 6, pp. 17246–17263, 2018.
[149] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and IoT based food traceability for smart agriculture," in *Proc. 3rd Int. Conf. Crowd Sci. Eng. (ICCSE)*, 2018, pp. 1–6.
[150] K. A. Awan, I. U. Din, A. Almogren, and H. Almajed, "AgriTrust—A trust management approach for smart agriculture in cloud-based internet of agriculture things," *Sensors*, vol. 20, no. 21, p. 6174, Oct. 2020.
[151] M. Nitti, L. Atzori, and I. P. Cvijikj, "Network navigability in the social Internet of Things," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Apr. 2014, pp. 405–410.
[152] R. Abdul, A. Paul, J. M. Gul, W.-H. Hong, and H. Seo, "Exploiting small world problems in a SIoT environment," *Energies*, vol. 11, no. 8, p. 2089, Aug. 2018.
[153] C. Marche, L. Atzori, A. Iera, L. Militano, and M. Nitti, "Navigability in social networks of objects: The importance of friendship type and nodes' distance," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2017, pp. 1–6.
[154] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social Internet of Vehicles: Factors, challenges, blockchain, and fog solutions," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, 2019, Art. no. 1550147719825820.

SANA ALAM is currently pursuing the Ph.D. degree with the NED University of Science and Technology. She is also working as a Senior Lecturer with the Department of Computer Engineering, Sir Syed University of Engineering and Technology, Pakistan. She has multiple publications in reputed journals. Her research interests include software engineering, the IoT, the SIoT, big data, and blockchain.

SHEHNILA ZARDARI is an Academic and a Researcher. She is currently working as a Professor at the NED University of Engineering and Technology, Karachi. She is also the Chairperson with the Department of Software Engineering, NED University of Engineering and Technology. She has a number of publications in reputed journals and conferences. Her research interests include software engineering, big data, artificial intelligence, the IoT, and blockchain. She has been awarded the Academic Excellence Award by the Sindh Higher Education Commission, in 2022. She is a reviewer of several journals and is on the program committee of several distinguished conferences. She has been a keynote speaker at various conferences for promoting research in the field of software engineering.

SHAHEENA NOOR received the master's degree in computer systems from the NED University of Engineering and Technology and the Ph.D. degree in computer engineering with a specialization in computer vision and image processing from Hamdard University, Karachi, Pakistan. She has been working as an Assistant Professor with the Department of Computer Engineering, Sir Syed University of Engineering and Technology (SSUET), since January 2007. She has an experience in the areas of research and academics. She has written more than ten research papers in different journals, conferences, and a book chapter. Her research interests include object recognition and activity recognition. She is a member of the IEEE Computer Society (Karachi Section). She worked voluntarily as the Chairperson of the IEEE SSUET Computer Society from March 2016 to February 2017. She is serving as an Advisor for the IEEE SSUET Computer Society, since February 2018. She is also serving as a reviewer for local and well-reputed international journals.

SHAKIL AHMED received the master's degree from the NED University of Engineering and Technology, Karachi, Pakistan, in 2006, and the Ph.D. degree from the University of Putra Malaysia, in 2014. He is currently the Chairperson of the Department of Computer Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan. He has around 20 national and international publications in journals and conferences. His research interests include information security, data mining, and information theory.



HARALAMBOS (HARIS) MOURATIDIS is currently a Professor and the Director of the Institute for Analytics and Data Science (IADS), University of Essex. He has published more than 185 articles (H-index 38) and he has led and/or participated in projects of overall value of c.€30M, funded by the U.K. and the EU. His research interests include secure software systems engineering, requirements engineering, and information systems development. He is interested in developing methodologies, modeling languages, ontologies, tools and platforms to support the analysis, design, monitoring of security, privacy, risk, and trust for large-scale complex software systems. He is a fellow of the U.K. Higher Education Academy and Standards-Maker of the British Standards Institution for the "Privacy-By-Design" and "Software and Systems Engineering" National Committees. He is elected as the Vice-Chair of the IFIP WG on Secure Engineering, an Expert Fellow of the U.K. Digital Economy Network Plus, on the register of ENISA's experts and a member of its WG on European Cybersecurity Skills Framework, and a member of working groups at ERCIM, IFIP, and the BCS.