A Survey of Trust Management Schemes for Social Internet of Things

Simon Wewoliamo Kuseh[1], Henry Nunoo-Mensah[2], Griffith Selorm Klogo[3], and Eric Tutu Tchao[4]

[1,2,3,4]Department of Computer Engineering, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
[1]kusehsw@gmail.com
[2]hnunoo-mensah@knust.edu.gh (*)
[3,4][gsklogo.coe, ettchao.coe]@knust.edu.gh

Received: 2021-11-19; Accepted: 2022-01-15; Published: 2022-01-23

Abstract— Social Internet of Things (SIoT) involves integrating social networking concepts in the Internet of Things (IoT) to enhance social interactions among IoT objects and users. SIoT is envisaged to provide adequate service selection and discovery. Trust is an essential factor whenever social concepts are discussed in communication networks. Trust usually leads to a mutual relationship between two parties (i.e., the trustor and trustee) where they both enjoy mutual benefits. For secure social relationships, Trust management (TM) is a crucial feature of SIoT. The primary aim of this work is to provide a comprehensive review of trust management proposals/schemes available for SIoT. Four main trust calculation algorithms for trust management were selected for this review, and they were examined in detail. The IEEE Xplore, Scopus, ResearchGate, and Google Scholar databases were searched for articles containing the terms "Trust aggregation approaches in IoT", and "Trust computation in SIoT" with a particular emphasis on works published between 2018 and 2021. The paper also discussed the pros and cons of each TM technique, trust metrics/features, contributions, and limitations of the state-of-the-art SIoT TM proposals in the literature. The paper further provides open issues and possible research directions for entry-level researchers in the domain of SIoT.

Keywords— Internet of Things, IoT, Social Internet of Things, SIoT, Trust.

I. Introduction

The proliferation of the Internet of Things (IoT) is worth mentioning. This phenomenon is due to the vast application areas and accessibility to technology for such IoT services. There has been a paradigm shift towards People's Internet, i.e., "Everything", instead of the earlier IoT focus of connecting computers [1]. The shift has contributed immensely to the swell in using IoTs for monitoring, enhancing productivity, and aiding decision-making processes. Areas that have seen a tremendous application of IoT are intelligent society, air quality monitoring, healthcare, and the supply chain industry [1]. A study [2] showed that in 2020, the manufacturing industry topped the list of top ten sectors that have received high traction for IoT platform usage. The transportation/mobility, energy, and healthcare, to mention a few, followed manufacturing in their respective order. Figure 1 shows the number of connected devices in billions for the past years and projections into 2025. It is projected that about 75.44 billion devices are expected to be connected by 2025 [3].

Despite advancements in IoT and the upsurge in the popularity of intelligent objects for aggregating data, many concerns persist. Some of which are individual identification and privacy in the IoT environment. Data owners are concerned about the potential misuse of their aggregated sensitive data and the desire not to disclose private information without compromising control [4]. A report by [5] found that privacy and security issues posed the highest levels of threat to the IoT. The reported threat levels were 62% and 54% for privacy and security, respectively.

These trust-related concerns were estimated to be twice as high as concerns such as physical safety and a high mean time to repair (MTTR) failed objects. The recorded threat levels were 27% and 24% for physical security and MTTR, respectively [5]. The presented figures for privacy and security show that securing and proposing privacy-preserving schemes for the network is paramount and worth investigating by IoT researchers.

A new paradigm, the Social Internet of Things (SIoT), is emerging in the quest to ensure privacy and enhance trust within the IoT. The IoT has been modeled as a social network with collaborative and communal characteristics [6]. SIoT is described as intelligent objects forming social bonds with one another. These social bonds inform their social networks and enable people and devices to interact, aiding information sharing [7]. SIoT reuses ideas and values of human social networking in addressing IoT-related issues. As a result, models used in human social networks can also address IoT-related problems [7], [8]. SIoT comprises friends and friends-of-friends nodes. The node that maintains a social relationship with another node is a friend. The friends-of-friends concept is based on human social networks. It refers to the friends of a friend node that are not directly connected to a node of interest or within its social network. Integrating social network concepts into IoT improves network navigability and service discovery. Other benefits of this integration include effortless scalability of the network and a high degree of trust among friends, but how will these social nodes access the trustworthiness of a node they wish to interact with? Which trust features should be considered in computing the

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

trustworthiness of a node? These are research questions that need to be addressed.

Trust is essential when it comes to situations that involve a high degree of doubt [9]. These situations span numerous application areas, and IoT is no exception. For example, in IoTs, intelligent objects are constantly at risk of being compromised by malicious entities, thus introducing doubt into the network. Concerning IoTs, TM is predominantly applied to but not limited to the following areas: secure data aggregation, malicious node identification, and secure routing. The whole idea of trust can generally be categorized based on the use as being subjective or objective [9]. Also, trust can be classified as either a QoS or social trust, depending on its properties. Social trust considers the following: intimacy, honesty, centrality, connectivity, and privacy. Trust can also be characterized as either behavioral or computational, considering the setting within which it is applied. Finally, behavioral trust defines trust between humans and organizations, while computational trust is between devices or networks.

TM models ensure the fair assessment of the reputation and trustworthiness of communicating nodes and enhance the network's performance by monitoring network activities to reduce risk to sensor nodes on the network [10]. The trust assessment involves two individuals, a trustee, and a trustor. Trust is defined mainly as a measure of uncertainty [11]. Trust is seen as a critical requirement for service discovery, according to [12]. The service requestor will likely choose only service providers with a greater level of trustworthiness [13]. For secure social relationships, trust management becomes a critical issue in SIoT that needs to be addressed. Risk mitigation, authentication, security, and data transfer guarantee that IoT devices are approved. The concept of trust is identified as an immediate solution to help SIoT services to resolve the sense of uncertainty and reduce risks when making decisions [14]. Trust helps one measure trustworthiness, truthfulness, security, and reliability [8].

In literature, many techniques are used for trust computation, but the common technique is Weighted-Sum. Weighted-Sum is linear and does not properly model trust, which is non-linear. Trust features are also assigned weights manually. Current techniques do not also consider indirect trust features in trust computations. Therefore, trust management is an essential part of SIoT. Following the works of [15], [16], [17], [18], much research is needed on non-linear trust management techniques in SIoT as thousands of devices are being connected to the internet and establishing social tiers.

The primary goal of this paper is to discuss state-of-the-art techniques for trust management in SIoT. The paper undertakes this by sourcing articles introducing state-of-the-art trust-based SIoT proposals made from 2018 to 2021.

The modes of operations, contributions, trust evaluation metrics, strengths and limitations of the candidate trust and reputation management proposal papers are discussed and presented. To the best of our knowledge, no survey paper has discussed the state-of-the-art proposals from 2018 to 2021, thus necessitating this paper. The rest of the paper is presented as follows. Section II discusses the concepts of trust, SIoT, and trust-related attacks. Section III discusses related works or techniques for trust management in SIoT. Open issues and future research directions trust-based SIoT research are presented in section IV. Conclusions are presented in Section V.

II. Systematic Literature Review

IoT technology is evolving, and new ways of connecting and interacting between these devices are emerging. According to a survey, privacy and security concerns were the most serious threats to the Internet of Things. According to the data, the stated threat levels for privacy and security were 62 percent and 54 percent, respectively, according to the data [5].

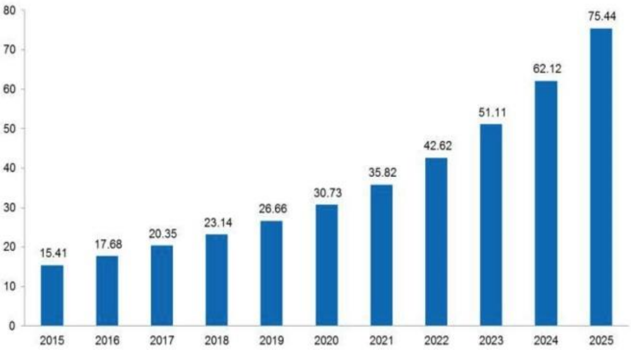


Figure 1. Connected network devices in billions.

This section presents the concept of SIoT, Trust management, and trust-related attacks in SIoT.

A. *Social Internet of Things (SIoT)*

Social networking has become ubiquitous and has made significant strides in other domains. In the domain of IoT, SIoT is the integration of social constructs that enhances social interactions among IoT objects and users. The integration ensures effective information discovery and promotes scalability [19]. In SIoT, devices can smartly interact with each other or even openly share data with humans and related devices [20]. SIoT is a modern concept that has emerged as a subfield in IoT. SIoT enables smart devices and users to interact, enabling services to be provided among devices and users. Based on minimal guidance from their owners, the devices form relationships and interact with one another on their own. SIoT can enhance numerous real-life applications with a complete SIoT platform [21]. Other variants of SIoT include Social Internet of Vehicles (SIoV), Artificial Social Internet of Things (ASIoT). Figure 2 shows a typical SIoT.
Based on how devices relate; emulating social relationships exhibited by human beings, there are five basic categories of relationships among devices in SIoT [22], [23] include:

1) Parental object relationship (POR): This relationship describes devices manufactured by the same manufacturer during the same period. This relationship is easily applied during item production; it does not alter over time and only changes by system disruption/obsolescence events.

2) Co-location object relationship (C-LOR): is defined between objects in the same location (for example, sensors, and objects in a smart home or a bus terminal, etc.). These devices often do not share resources, but these connections are essential for establishing short links in the network.

3) Co-work object relationship (C-WOR): established between nodes that work together to complete a shared purpose (For example, emergency response and telemedicine)

4) Ownership object relationship (OOR): Establish among devices owned by the same individual/user. The logical inference of this principle into a richer interface profile is the ownership entity relationship.

5) Social object relationship (SOR): The final relationship is formed when devices interact, either occasionally or constantly, for reasons related to their owners' relationships. Similar to how people exchange contact information, the devices exchange their social profiles autonomously if properly configured. The guiding concept is that devices with similar traits and profiles share best practices to solve problems that "parents" have already encountered.

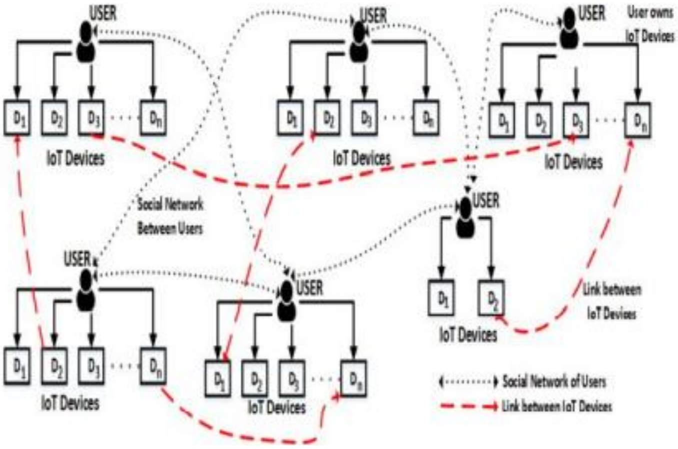


Figure 2. Typical SIoT

B. SIoT Reference Architecture

The reference architecture for SIoT comprises three layers viz., the Application, Network, and Sensing layers. The responsibility of the sensing layer is to perform data collection and node cooperation in short-range and local networks. The network layer is responsible for data transmission through various networks. The application layer is responsible for the deployment of IoT applications as well as middleware functionality. The basic components of the architecture and the layers include; SIoT server, gateway, and object. Figure 3 gives a representation of the reference architecture.

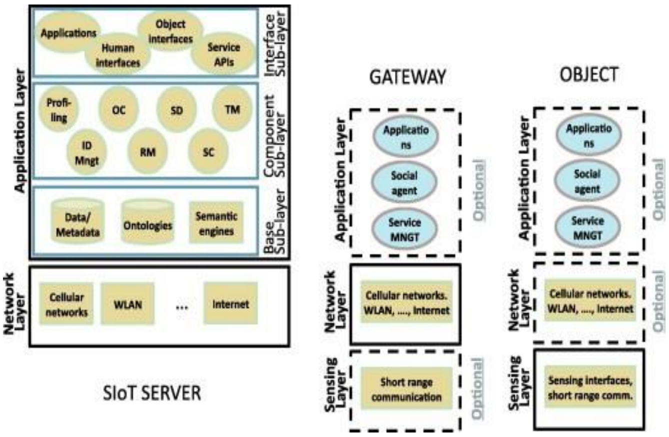


Figure 3. The SIoT reference.

The SIoT server does not include the Sensing layer; however, it encompasses the Application Layer and a Network layer. The application layer comprises three sub-layers. The base sub-layer holds the database for data storage and processing and the related identifiers. These keep track of social entity profiles and relationships and the behaviors of objects in the natural and virtual worlds. Human data (both object owners and visitors) are also handled.

The value of the component sub-layer cannot be overstated. It includes the modules that are in charge of implementing SIoT core features. The objective of the ID management module is to create an ID that uniquely recognizes all possible kinds of devices in the SIoT system. Profiling tends to configure information about a device manually and automatically. The owner control (OC) defines the activities that an object can perform, such as the information that can be exchanged and how relationships are set up.

The Relationship Management (RM) module discusses the user's due diligence in control settings to update and terminate relationships with other objects. Since objects lack the intellect of humans, this module is regarded as a critical component of the network. The service discovery (SD) element is a crucial piece that aims to find which objects can provide the necessary service in the same way humans pursue friendships and knowledge in social networking services.

The service composition (SC) component allows objects to communicate. The majority of the time, the contact is linked to an entity wanting to retrieve—information about the natural world or to locate a particular service offered by another object. The trustworthiness management (TM) part is concerned with determining how the information provided by any of the parties will be handled. Reliability is based on the actions of the electronic device and is inextricably mainly linked to the relationship management module. Trustworthiness can be quantified using well-known concepts from literature, such as centrality and reputation, which are essential in analyzing social networks.

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

The last sub-layer sits on top of the interface sub-layer. This layer interfaces and interacts with objects and humans by deploying the relevant applications and service APIs. In [22] a specific implementation is not provided.

C. Trust in SIoT

Trust is a deep conviction in something's reliability, fact, or capacity. Trust usually leads to a mutual relationship between two parties (trustor and trustee) where they both enjoy mutual benefits. Due to its integrative application, this word, trust, has multi-dimensional meanings. Trust plays a significant role in SIoT by enabling objects to perform the functions of service provisioning and relationship management [24]. A significant amount of data is exchanged among service users in today's world through devices such as apps, computers, sensors, cameras, etc. If data is exchanged with untrusted users, it may be used maliciously.

Trust management has emerged as a critical problem in SIoT, and there are various mechanism and computational trust models in literature for improving trustworthiness among social objects [25]. Figure 2.2.1 illustrates a trust mechanism made of the following: trust establishment (trust composition and trust aggregation), trust propagation and storage, and trust update [26]. The trust composition stage considers the various features used in computing trust values. The trust aggregation stage involves various techniques (weighted sum, machine learning, blockchain, fuzzy logic) that combine trust features to calculate a final trust value.

Regardless of the technique adopted for trust aggregation, some important trust properties need to be considered in social objects interactions [27]. These properties include the subjective and transitive nature of trust [9]. The subjective nature of trust indicates that a device D1 that trusts device D2 does not directly translate to D2 also trusts D1. Trust being transitive implies that if device D1 trusts D2, D2 trusts D3. D1 can deduce some level of trust on D3 depending on the value of trust in D2 and D2's trust in D3. Due to this property, trust information can be passed from one device to the next in SIoT, thus resulting in trust chains. Other trust properties include trust being dynamic, composite, and asymmetric [28].

D. Trust Related Attacks

In SIoT, malicious devices usually perform various trust attacks to disrupt the proper functioning of the social network. Some of these attacks are as follows:

1) Self-promoting attack (SPA): a device enhances its importance by flaunting its ability so that it would be selected as a service point.

2) White-washing attacks (WA): a misbehaving node will exit and re-enter the application to wipe away its bad reputation.

3) Bad-mouthing attack (BMA): it ruins the reputation of good devices being selected as service points by offering a low trust rating against them.

4) Ballot stuffing attack (BSA): improves the credibility of bad nodes (by making good recommendations for them) to increase the likelihood of bad nodes being chosen as service providers.

5) Opportunistic service attacks (OSA): a device can promote itself by deliberately cooperating with other devices to increase its credibility on the network. This is mainly done if the device believes its reputation is deteriorating due to poor service. It will readily collaborate with other malicious nodes to execute bad-mouthing and ballot-stuffing attacks if it has a good reputation.

6) Malicious devices perform discriminatory attacks (DA) by discriminating and targeting: nonfriends or nodes without strong social links.

7) Random attacks (RA): with On-and-off attacks, misbehaving devices switch between good and bad conduct, earning a good reputation when launching attacks.

III. Research Methodology

This section gives a brief overview of the various techniques (Weighted Sum, Machine Learning, Blockchain, and Fuzzy Logic) adopted as mechanisms for computing trust in SIoT. The methodology used for selecting research works in trust computation is also detailed.

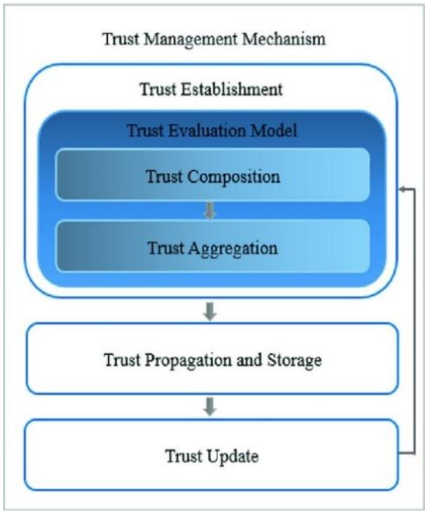


Figure 4. Trust management mechanism

A. Trust Aggregation Approaches

1) Weighted Sum: The Weighted Sum method is a simple method that is commonly employed in single-dimensional situations [29]. The weighted sum method is prominent for aggregating trust scores, and many reputation systems use it [26]. With the weighted sum technique, each trust metric is assigned a value ranging from 0 to 0.9 depending on the impact of the metric in computing the final trust score. The weighted sum is one of the typical trust aggregation methods, especially when measuring trust in vehicular networks. The disadvantage of the weighted sum approach is the manual assignment of trust metrics. The process makes it unable to identify which trust

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

metric has the most significant impact on trust in a particular environment [30].

2) Machine Learning: In recent years, there has been much interest in machine learning (ML). Many domains are developing with ML, and it is also being used for IoT security. ML appears to be a potential answer for protecting IoT devices from cyber assaults. It takes a different approach to defend against attacks than other standard methods.

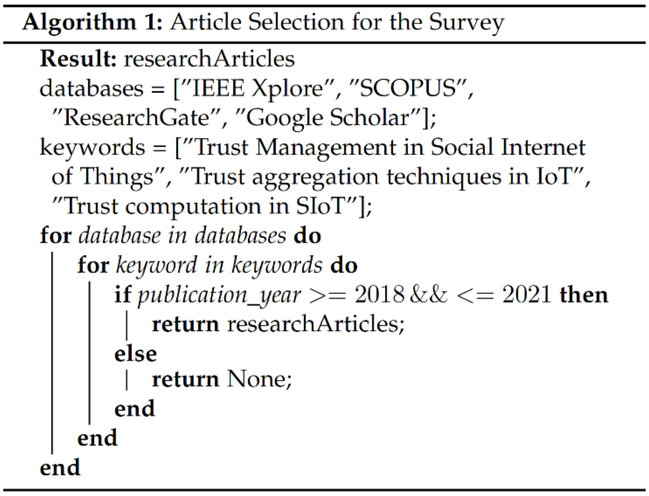
3) Blockchain: The emergence of Blockchain in securing shared information among distinct objects cannot be overemphasised. Generally, the Blockchain plays a pivotal role in ensuring privacy within SIoT. The authentication and authorisation of accessing data in SIoT can be accomplished quickly, in a trusted, secure, and decentralised manner. While on the road, the sharing and storage of vehicular data in SIoV can be selective and restricted by smart contracts to only certain vehicles [31].

4) Fuzzy Logic: Fuzzy logic is a type of many-valued logic that deals with approximate reasoning rather than fixed and accurate reasoning. Compared to typical binary sets, fuzzy logic variables may have truth values ranging from 0 to 1. Fuzzy logic has been expanded to include the concept of partial truth, in which the truth value might range from totally true to completely false. Furthermore, particular membership functions may be used to manage these degrees when linguistic variables are involved.

A trust value in the range (1.25, 1.25) implies extremely low trust, a trust value in the range (0, 2.5) low trust, a trust value in the range (1.25, 3.75) medium trust, a trust value in the range (2.5, 5) high trust, a trust value in the range (3.75, 6.25) high trust, etc. As a result, a node with a trust value of 0.25 has 75% extremely low trust (a membership function) and 25% low trust (another membership function). Fuzzy logic is a set of principles for reasoning with fuzzy measurements. Many reputation systems use weighted sums to aggregate ratings or comments. Raters with a better reputation or transaction relevance have a higher weight.

B. *Methodology for Selecting State-of-the-art Trust Computational Models*

A search was conducted in several databases to determine the frequency with which research in the field of trust management in the Internet of Things has been conducted (IEEE Xplore, Scopus, ResearchGate, and Google Scholar). "Trust Management in Social Internet of Things", "Trust aggregation techniques in IoT" and "Trust computation in SIoT" were the keywords used to search for related research works in trust management in SIoT with a year range from 2018 to 2021. The procedure for selecting existing trust management schemes for SIoT for this study is presented in Algorithm 1.



Algorithm 1: Article Selection for the Survey

```
Result: researchArticles
databases = ["IEEE Xplore", "SCOPUS",
  "ResearchGate", "Google Scholar"];
keywords = ["Trust Management in Social Internet
  of Things", "Trust aggregation techniques in IoT",
  "Trust computation in SIoT"];
for database in databases do
    for keyword in keywords do
        if publication_year >= 2018 && <= 2021 then
            return researchArticles;
        else
            return None;
        end
    end
end
```

C. *Existing State-of-the-art Trust Computation Models*

Table 1 presents the most up-to-date Trust Computation Models available today. Jayasinghe et al. [32] proposed a machine learning-based trust assessment model that combines several direct trust features to produce a final trust score for decision making. Knowledge, experience, and reputation were the primary trust attributes used in the proposed model. An unsupervised technique, K-means, is used to label the data. Then, SVM was used to train the model to identify the non-linear boundaries of trustworthy and untrustworthy interactions between nodes. The authors also claim that the algorithms proposed in their study could be clustered so that end devices could perform a fraction of the analysis to attain the same performance enhancement. That feat is beneficial due to the scalability and collaborative nature of IoTs. However, the direct trust attributes used in their study were inadequate for deciding a node's trustworthiness.

Sagar et al. [14] proposed a computational trust model that extracted vital features viz., direct trust metrics and indirect trust metrics to compute trust in SIoT. The overall single trust score was computed for each node in the SIoT environment using a machine learning-based approach to classify a node as either trustworthy or otherwise. Experimental results from their studies indicated that the Community-of-Interest (CoI) and Reward/Punishment significantly impacted the overall score. Their model reported low accuracy when direct and indirect trust were employed. However, higher accuracy is observed when the direct trust was used singly.

Sagar et al. [30] suggested a time-aware trust computational framework for SIoT environments. They combined social information and object-object interactions as the significant attributes used to compute a node's trustworthiness. They used Random Forest to aggregate these trust metrics to compute a final score representing the overall trustworthiness. Their work presented a single point of failure as social profiles of objects were stored in a local authority.

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

Khanfor et al. [33] developed a framework for recruiting trustworthy devices/ workers in Spatial Mobile crowdsourcing (SMCS). A filtering process was used to filter workers based on object selection and object relation criteria as defined by the requirements of the service requestor. The authors used the Louvain algorithm for community detection using predefined relations. That procedure helped to reduce the search space. Finally, an integer linear program (ILP) was used to recruit trustworthy workers based on their skill sets, trustworthiness, and recruitment cost. Simulation results showed better performance of the CD-ILP algorithm over the benchmark stochastic approach. A central server was used for recruiting workers, which presented a single point of failure to their work.

Rehman et al. [34] proposed a weight-based technique for selecting a trustworthy node for interaction by another node based on parameters defined by the node. The authors employed soft set theory using the parameters defined by the user node to select the most trusted network node. Each node would look for different parameters in selecting a trustworthy node. Predefined weights values were assigned to trust attributes that do not represent an attribute's actual weights for different interactions.

Babar et al. [35] proposed Trust Management using a Machine Learning Algorithm (TM-MLA) to find trustee devices and detect if a device was malicious or benign. The proposed technique consisted of trust composition, aggregation, and trust update phases. Different trust features were chosen depending on the attack during the composition phase. The authors used Artificial Neural Network (ANN) to compute a trustee's trust score. Their proposed model was potent against bad-mouthing, ballot stuffing, and self-promoting attacks. The proposed technique outperformed traditional weighted sum techniques. However, trustworthy devices may be declined due to less interaction between trustor and trustee.

Oualhaj et al. [36] proposed a novel decentralized trust management model that utilized Blockchain technology based on the Markov chain. The trust value was calculated by neighboring nodes called miners based on the honesty and cooperation rate. Their proposed algorithm also detected malicious nodes and coalitions that provided extreme trust values. Simulation results showed that the node's trust value depended on the number of malicious messages sent. The number of miners recruited to form a coalition also depended on the number of trusted nodes in the network. The computation of their trust value did not consider the indirect behavior of a node.

Masmoudi et al. [37] suggested a trust evaluation mechanism that was based on deep learning. Their technique focused on the trust establishment phase of the trust management mechanism. Employing various trust features, the authors used a deep learning model for their trust aggregation technique. That was built to detect malicious nodes and classify them into four types of trust attacks: Bad-Mouthing, Ballot-Stuffing Attack, Self-Promoting Attack, Discriminatory Attack, and none-attack. Results showed that their proposed method exhibited better precision, recall, and F1 score than traditional ML techniques. However, a holistic view of trust management was not considered.

He et al. [38] developed a trust-up mechanism for underwater acoustic sensor networks (UASNs). An environmental model designed considering the impact of the underwater environment, such as mobility of water flow and the instability nature of acoustic communication, was considered for trust update. An essential degree trust update technique was also explicitly proposed for crucial nodes to mitigate priority attacks. Reinforcement learning is utilized for trust updates in three phases. An efficient trust update mechanism is proposed for UASNs, but other sections of the trust management mechanism were not considered.

Truong et al. [39] proposed a novel trust computation model for creating and maintaining trust between mobile device users in Mobile Crowdsensing (MCS) Called Experience-Reputation (ER). The weighted sum technique was used for aggregating reputation and experience trust indicators for computing the final trust value for mobile device users. The proposed trust-based technique was deployed for recruiting mobile device users for sensing in MCS tasks relying on Quality of Data (QLD) and provides a better way of detecting malicious users. The model only relied on centralized indirect trust indicators for computing trust values.

Adewuyi et al. [40] designed a trust management model for collaborative applications tailored towards collaborative downloading applications. The trust parameter was determined by a node either objectively or subjectively depending on the needs of the node. A trust aggregation function based on the weighted sum method was used to calculate trust values. The concept of trust maturity was introduced to address the issue of trust update. A novel trust management method that addressed trust aggregation, trust storage, propagation, and trust updates was developed. However, much resource was needed for trust computation.

Sagar et al. [41] designed another time-aware trust computational model that employed direct and indirect trust metrics for calculating the trust values of nodes. A weighted sum technique was used to aggregate similarity-based direct trust features; Community-of-Interest Similarity, Friendship Similarity, Co-work Similarity, and recommendations from neighboring to calculate a node's final trust score. The technique was computationally effective but did not have an effective trust value update mechanism.

Sharma et al. [42] proposed a novel trust management scheme for computing trust, considering the sociological perspective of human behavior in Social Networking Services (SNS). A deterministic expression based on Boolean logic enforces trust at the circuit level using current/historic trust values and severity and inventive metrics. The proposed model is lightweight and can be implemented at the hardware level—no Trust updates mechanism.

Premarathne et al. [43] developed a novel trust management technique by considering trust as a multi-dimensional requirement considering the social relationships

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

among devices. A weighted average method was used to calculate trust values based on predefined existing relationships and residual energy content of SIoT devices. The method was reliable in identifying known trust-related attacks, provided their social relationship trust was violated.

Mahmood et al. [44] proposed a hybrid trust management model in Vehicular Ad hoc Networks (VANETs) for detecting misbehaving vehicles and preventing them from becoming cluster heads. Their method used a weight-based mechanism. The suggested framework implemented a composite metric for clustering that considers both trust values and available resources in selecting a cluster head. A weight-based mechanism used these metrics for real-time detection and elimination of malicious nodes inside a cluster before they become cluster heads. Resource utilization was improved by randomly selecting cluster heads. The proposed scheme scaled very well with increasing cluster size.

Wei et al. [45] proposed a computational trust model for service delegation in SIoT. Their model was context-dependent by combining the task type and the specific environment to provide a service. A service requester (SR) announced the availability of a task. At the same time, a service provider (SR) responds to the request by considering if it can complete the said task. The SR used competence, willingness, and social relationship in computing the SP's trustworthiness and delegated a task based on the computed trust value. The SP executed the task and returned the results to the SR. The SR then evaluated the results and performed the necessary update. The proposed model was capable of addressing most trust-related attacks.

The discriminative-aware trust management system (DATM) proposed by Jafarian et al. [46] computes trust in SIoT objects by considering some nodes' discriminative nature and social relations in providing services. A service requester calculates the service provider's trust value using two primary metrics: context-based trust and global reputation. A parameter was introduced to weigh the importance of context-based trust against global reputation. The trust computation model presented a credibility update mechanism for raters to overcome recommendation-related attacks. Simulation results demonstrated that the model could effectively detect discriminative devices and deal with bad-mouthers compared to the other four baseline methods. Scalability and objects' resource limitation were not taken into consideration.

Xia et al. [47] proposed a context-aware framework for managing trust in SIoT capable of dealing with some trust-related attacks. Their proposed framework was based on sociological and psychological concepts of human trust generation, distinguishing trust into two categories. These categories were familiarity trust (FT) and similarity trust (ST). Direct trust (DT) and recommendation trust (RT) were used to measure FT. However, external similarity trust (EST) and internal similarity trust (IST) were used to estimate ST. A kernel-based computation model was designed to compute the direct trust of an object. A fuzzy logic mechanism was then used to synthesize the trust elements finally. The model could effectively defend against bad-mouthing attacks with an increasing number of malicious objects. The model, however, was not resilient under dynamically changing environments.

Rehman et al. [48] took advantage of online social networks (OSN) and trustworthiness in the IoT to develop new services for smart cities. This trust model considered everyone in an OSN's interaction relationships and trust value. The system of trustworthy communities was built by taking local and global trusted factors into account. Trust factors were used to reduce the mixing of false data by untrustworthy third parties. Their proposed model used public datasets from Twitter, Facebook, and Slashdot. Filtration techniques are used to filter trusted nodes in OSN. Their results showed that Twitter was more sustainable than the other OSN, with 90.03% trusted nodes after filtration.

A novel hybrid trust management technique for trust management in industrial automotive plants was proposed by Boudagdigue et al. [49]. New sets of industrial relationships were defined for objects relationships called industrial communities. Every community had a community leader (CL). CL managed the trust of community nodes by computing trust using three metrics viz. cooperation, direct and indirect honesty, and the results sent to a central server. The proposed architecture was energy efficient and capable of dealing with trust-related attacks. Their proposed model had a single point of failure as trust values were computed only by community leaders and stored in a central server.

Awan et al. in [50] designed a lightweight, event-driven trust computation mechanism called AgriTrust for managing trust and detecting malicious nodes in smart agriculture. Three different trust management models: sensors to the base station, base station to cloud, and cloud to the base station, were involved in the trust computation process. Each module used its trust features. A central authority was used to compute trust using a statistical model. The mechanism effectively detected whitewashing and on-off attacks whiles using reduced energy resources.

Khani et al. [51] proposed a mutual context-aware trust model which considers the trust evaluation from both the service provider and the service consumer perspective. Three different contexts: the status of the device, the environment, and the task type, were considered for trust evaluation. A weighted-based technique was adapted using both dependent and independent trust metrics to evaluate the trust of a device based on the three contexts. The proposed model showed better performance in detecting BMA, BSA, SPA, and OOA attacks.

Abdelghani et al. [52] designed a machine learning technique for trust evaluation by classifying nodes into malicious and benign classes. Different ML algorithms, Naive Bayes, Multi-Layer Perceptron, and Random Tree implemented in the WEKA tool were considered for training the proposed model. Multi-Layer Perceptron showed better performance in the classification task. The proposed model was not able to determine a particular type of attack.

A Blockchain-based framework for enforcing trust among collaborative devices from different vendors in a decentralized

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

nature called IoT-passport was proposed by Tang et al. [53]. Their proposal was aimed at enabling cross-platform collaboration. The framework consists of three main components for enforcing trust, trust-based collaboration, hierarchical trust synchronization, and collaborative IoT services. Trust-based collaborations were achieved on the blockchain by using hierarchical smart contracts. Hierarchical trust synchronization was enforced in their proposal by using local and global trust domains.

Kowshalya and Valarmathi [54] proposed a dynamic trust management technique, DTrustInfer, for secure communication in SIoT by computing trust among nodes using direct and indirect trust metrics. Trust features such as honesty, energy, the community of interest, and cooperativeness are used for computing trust. An authenticator with the highest trust values among neighboring nodes was chosen to distribute secret codes padded with messages when a node wanted to communicate with another node. The authenticator also verified user credentials. The proposed framework outperformed the subjective-objective and adaptive trust models when Brigtkite and Epinions datasets were used.

TABLE I
STATE-OF-THE-ART TRUST COMPUTATION MODELS

Authors	Technique	Trust Metrics	Contribution	Limitation
Sagar et al. [14]	Machine Learning	Direct and Indirect metrics	A novel model using direct/indirect trust metrics	Low accuracy when direct and indirect trust metrics are employed
Jayasinghe al. [32]	Machine Learning	Knowledge, Experience, and reputation	A novel direct trust model for computing trust	Direct trust attributes used are inadequate for deciding the trustworthiness of a node
Sagar et al. [30]	Machine Learning	Social information and object-object interactions	Time-aware trust computational framework	Single point of failure as social profiles of objects is stored in a local authority
Khanfor et al. [33]	Machine Learning	Social information and object-object interactions	Framework for recruiting trustworthy devices/workers in SMCS	A central server is used to recruit workers with a single point of failure.
Hankare et al. [35]	Machine Learning	Trust attack features and varying dynamic situation	Using trustworthiness to detect malicious devices	Trustworthy devices may be declined due to less interaction between trustor and trustee.
Jafarian et al. [46]	Machine Learning	social Similarity, the importance of the service, and the provider's remaining energy	Designed a discriminative-aware trust management system	Scalability and objects' resource limitation were not taken into consideration
Abdelghani et al. [52]	Machine Learning		A model for classifying nodes into malicious and benign classes	The proposed model is not able to determine a particular type of attack.
Rehman et al. [48]	Machine Learning	Local and global trusted factors	Used trustworthiness in SIoT to provide new services for smart cities	Predefined weights values are assigned to trust parameters
Masmoudi et al. [37]	Deep Learning	Trust attack features and behaviors of malicious nodes	Technique for detecting and classifying malicious nodes into four types of trust attacks	A holistic view of trust management was not considered.
He et al. [38]	Deep Learning	Multi-dimensional trust metrics	Trust update technique to mitigate against priority attacks in UASNs	other sections of the trust management mechanism are not considered
Oualhaj et al. [36]	Blockchain	Honesty and Cooperation	Novel decentralized trust management model	The indirect behavior of a node is not considered in computing trust score
Tang et al. [53]	Blockchain	Access Evaluation Rules and Post-access Rules	Framework for enforcing trust among collaborative devices called IoT-passport	The proposed model is computationally intensive
Rehman et al. [34]	Weighted Sum	Metrics are defined by user node	Weight-based technique for selecting a trustworthy node for interaction by another node	Predefined weights values are assigned to trust parameters
Truong et al. [39]	Weighted Sum	Reputation and Experience	Trust computation model for creating and maintaining trust between mobile device users	Calculate trust scores, indirect trust indicators are centralized.
Premarathne et al. [43]	Weighted Sum	Predefined existing relationships as well as the residual energy content of SIoT devices	The method is reliable for identifying known trust-related attacks if social relationship trust is violated	Not verified under numerous trust attacks scenarios
Adewuyi et al. [40]	Weighted Sum	A trust parameter is determined by a node either objectively or subjectively depending on the needs of the node	Trust update technique using trust maturity	Much resource is needed for trust computation

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

Authors	Technique	Trust Metrics	Contribution	Limitation
Sagar et al. [41]	Weighted Sum	Direct and indirect trust metrics	Designed a time-aware trust, the computational model	It does not have a reliable way of updating the trust value.
Wei et al. [45]	Weighted Sum	Competence, willingness, and social relationship	Designed a computational trust model for service delegation in SIoT	BMA has negative effects on the proposed model, and the convergence time increases with an increase in the number of properties
Boudagdigue et al. [49]	Weighted Sum	Cooperation, direct and indirect honesty	A novel hybrid trust management technique for trust management in industrial, automotive plants	The proposed model has a single point of failure as trust values a computed only by community leaders and stored in a central server
Awan et al. [50]	Weighted Sum	Each module uses their own trust features	Designed a lightweight, event-driven trust computation mechanism, AgriTrust	A central authority is used to compute trust
Khani et al. [51]	Weighted Sum	Dependent and independent trust metrics	A mutual context-aware trust model is proposed	SPA is possible at the initial stages with fewer number transactions
Kowshalya et al. [54]	Weighted Sum	Honesty, energy, a community of interest, and cooperativeness	Proposed a TM technique, DTrustInfer, for secure communication in SIoT.	The proposed model cannot mitigate some common trust attacks
Aslam et al. [12]	Weighted Sum	Objective and Subjective QoS	Designed a service-oriented trust management method	Predefined weights were assigned to trust metrics based on social relationship factors only

IV. Result and Discussion

In this section of the paper, open issues and research challenges identified during the survey are discussed, and future research directions are outlined. A summary of the problems identified is centered on scalability, computational complexity on resource-constrained infrastructure, single point of failure of proposed schemes, over-generalization of proposed schemes, etc.

Scalability is one major issue that has not been addressed adequately in the reviewed literature. As the social networks of devices keep increasing, the trust computation mechanisms need to adapt to this increasing number of social devices. A device needs to store and compute the trust values of trustees as it continuously socializes with more devices each day. Most trust mechanisms have failed to factor in scalability when designing trust management mechanisms.

TM techniques with higher computational costs hurt the efficiency of resource constraint devices in SIoT systems for on-time service delivery. The most recent proposed methods do not adequately address resource utilization in trust computation. It needs to be considered in future TMM proposals. Also, trust update and storage are worth mentioning as current literature on the topic lacks comprehensive trust score update/storage and propagation. These are considered a very integral part of any TM.

Trust management mechanisms do not mainly address specific applications needs in SIoT. Most techniques are more general and may degrade performance when applied in some applications. The unavailability of datasets for designing and testing TM also poses another challenge in trust computation in SIoT environments. Future research in TM can focus on building application-specific TM rather than general ones. Due to the variations in requirements and specifications for mitigating attacks in different application scenarios. Another line of research is developing lightweight and comprehensive TMs that address every aspect of trust computation and consider SIoT devices' dynamicity.

The social relationship of objects and the concept of apology and trust regain in SIoT is another direction of research that needs to be pursued. Also, TMs resilient towards trust-related attacks need further investigation as the current state-of-the-art still has not adequately addressed this issue.

V. Conclusion

The paper gives a comprehensive review of the various techniques that are used for managing trust in the domain of SIoT. The paper introduces SIoT as a new area in IoT and outlines some of its benefits. The paper further went on to enumerate some of the challenges facing SIoT, and, notably, among them is trust. The concept of trust and some trust-related attacks are introduced. Four main techniques: Weighted Sum, Machine Learning, Blockchain, and Fuzzy Logic are utilized for trust computation in SIoT environment. A detailed examination of the state-of-the-art trust computation approaches is also provided and discusses their significant contributions and limitations. Open issues, challenges, and future research directions of trust management in SIoT are presented finally.

References

[1] S. G. H. Soumyalatha, "Study of iot: Understanding iot architecture, applications, issues and challenges," InternationalJournal of Advanced Networking and Applications (IJANA), 201.

[2] K. L Lueth Top 10 IoT applications in 2020: Access on :20 May,2021 Available: https://iot-analytics.com/top-10-iot-applications-in-2020/ July 8, 2020 2020.

[3] A. Rehman, A. Paul, M. A. Yaqub, and M. M. U. Rathore, "Trustworthy intelligent industrial monitoring architecture for early event detection by

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

exploiting social iot," in Proceedings of the 35th Annual ACM Symposium on Applied Computing, pp. 2163–2169, 2020.

[4] J. Y. Kinza Sarwar, Sira Yongchareon, "A brief survey on iot privacy: Taxonomy, issues and future trends," Springer Nature Switzerland AG 2019, p. 208–219, 2019.

[5] J. Lima. (2016). Could consumer distrust kill IoT? Why calls for security, privacy and transparency should not be ignored. Available: https://www.cbronline.com/internet-of-things/could-consumer-distrust-kill-iot-why-calls-for-security-privacy-and-transparency-should-not-be-ignored-4859978/.

[6] L. Atzori, A. Iera, G. Morabito, and M. J. C. n. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," vol. 56, no. 16, pp. 3594–3608, 2012.

[7] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: Present and future challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483–2495, 2018.

[8] M. Rashmi and C. V. Raj, A review on trust models of social Internet of Things, pp. 203–209. Springer, 2019.

[9] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, "The adoption of socio-and bio-inspired algorithms for trust models in wireless sensor networks: A survey," International Journal of Communication Systems, vol. 31, no. 7, p. e3444, 2018.

[10] V. U. Rani and K. S. Sundaram, "Review of trust models in wireless sensor networks," Int. J. Comput. Inf. Syst. Control Eng, vol. 8, pp. 371–377, 2014.

[11] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, "Pstrm: Privacy-aware sociopsychological trust and reputation model for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 13, no. 5, pp. 1505–1525, 2020.

[12] M. J. Aslam, S. Din, J. J. Rodrigues, A. Ahmad, and G. S. J. I. A. Choi, "Defining service-oriented trust assessment for social internet of things," vol. 8, pp. 206459–206473, 2020.

[13] E. M. Maximilien and M. P. Singh, "Toward autonomic web services trust and selection," in Proceedings of the 2nd international conference on Service oriented computing, pp. 212–221.

[14] 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 ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1–6, IEEE.

[15] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sedes, "Trust` management in social internet of things: a survey," in Conference on e-Business, e-Services and e-Society, pp. 430–441, Springer, 2016.

[16] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social internet of things: A taxonomy, open issues, and challenges," Computer Communications, vol. 150, pp. 13–46, 2020.

[17] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions," International Journal of Distributed Sensor Networks, vol. 15, no. 1, p. 1550147719825820, 2019.

[18] W. Z. Khan, S. Hakak, M. K. Khan, et al., "Trust management in social internet of things: Architectures, recent advancements, and future challenges," IEEE Internet of Things Journal, vol. 8, no. 10, pp. 7768–7788, 2020.

[19] S. Ali, M. G. Kibria, M. A. Jarwar, H. K. Lee, I. J. W. C. Chong, and M. Computing, "A model of socially connected web objects for iot applications," vol. 2018, 2018.

[20] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. J. I. I. o. t. J. Xiang, "Privacypreserving and lightweight key agreement protocol for v2g in the social internet of things," vol. 5, no. 4, pp. 2526–2536, 2017.

[21] J. S. Kumar, G. Sivasankar, and S. S. Nidhyananthan, An artificial intelligence approach for enhancing trust between social IoT devices in a network, pp. 183–196. Springer, 2020.

[22] L. Atzori, A. Iera, G. Morabito, and M. J. C. n. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," vol. 56, no. 16, pp. 3594–3608, 2012.

[23] L. Atzori, A. Iera, and G. J. I. c. l. Morabito, "Siot: Giving a social structure to the internet of things," vol. 15, no. 11, pp. 1193–1195, 2011.

[24] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "When social objects collaborate: Concepts, processing elements, attacks and challenges," Computers & Electrical Engineering, vol. 58, pp. 397–411, 2017.

[25] A. Jøsang, C. Keser, and T. Dimitrakos, "Can we manage trust?", in International Conference on Trust Management, pp. 93–107, Springer, 2005.

[26] J. Guo and R. Chen, "A classification of trust computation models for service-oriented internet of things systems," in 2015 IEEE International Conference on Services Computing, pp. 324–331, IEEE, 2015.

[27] A. Rezvanian, B. Moradabadi, M. Ghavipour, M. M. D. Khomami, and M. R. Meybodi, "Social trust management," in Learning Automata Approach for Social Networks, pp. 241–279, Springer, 2019.

[28] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sedes, "Trust` management in social internet of things: a survey," in Conference on e-Business, e-Services and e-Society, pp. 430–441, Springer, 2016.

[29] J. R. S. C. Mateo, "Weighted sum method and weighted product method," in Multi criteria analysis in the renewable energy industry, pp. 19–22, Springer, 2012.

[30] S. Sagar, A. Mahmood, Q. Z. Sheng, M. Zaib, and W. E. Zhang, "Towards a machine learning-driven trust evaluation model for social internet of things: A time-aware approach," arXiv preprint arXiv:2102.10998, 2021.

[31] 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.

[32] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine learning based trust computational model for iot services," IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 39–52, 2018.

[33] A. Khanfor, A. Hamrouni, H. Ghazzai, Y. Yang, and Y. Massoud, "A trustworthy recruitment process for spatial mobile crowdsourcing in large-scale social iot," in 2020 IEEE Technology & Engineering Management Conference (TEMSCON), pp. 1–6, IEEE, 2020.

[34] 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 2019 IEEE 5th International Conference on Computer and Communications (ICCC), pp. 1644–1648, IEEE, 2019.

[35] S. Babar, P. Mahalle, et al., "Trust management approach for detection of malicious devices in siot," Tehnicˇki glasnik, vol. 15, no. 1, pp. 43–50, 2021.

[36] O. A. Oualhaj, A. Mohamed, M. Guizani, and A. Erbad, "Blockchain based decentralized trust management framework," in 2020 International Wireless Communications and Mobile Computing (IWCMC), pp. 2210–2215, IEEE, 2020.

[37] M. Masmoudi, W. Abdelghani, I. Amous, and F. Sedes, "Deep` learning for trust-related attacks detection in social internet of things," in International Conference on e-Business Engineering, pp. 389–404, Springer, 2019.

[38] Y. He, G. Han, J. Jiang, H. Wang, and M. Martinez-Garcia, "A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks," IEEE Transactions on Mobile Computing, 2020.

[39] N. B. Truong, G. M. Lee, T.-W. Um, and M. Mackay, "Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the internet of things," IEEE Transactions on Information Forensics and Security, vol. 14, no. 10, pp. 2705–2719, 2019.

[40] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A. MacDermott, and' X. Wang, "Ctrust: A dynamic trust model for collaborative applications in the internet of things," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5432–5445, 2019.

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

[42] C. Sharma, M. A. Alam, and A. Khalique, "A novel trust establishment model in siot network based on sociological aspects of users in social networking services," Indian Journal of Science and Technology, vol. 12, p. 17, 2019.

[43] U. S. Premarathne, "Residual energy aware trust computation method for social internet of things," in 2019 14th Conference on Industrial and Information Systems (ICIIS), pp. 470–475, IEEE, 2020.

[44] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A hybrid trust management heuristic for vanets," in

DOI : http://dx.doi.org/10.25139/inform.v7i1.4284

2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 748–752, IEEE, 2019.

[45] L. Wei, J. Wu, C. Long, and B. Li, "On designing context-aware trust model and service delegation for social internet of things," IEEE Internet of Things Journal, 2020.

[46] B. Jafarian, N. Yazdani, and M. S. Haghighi, "Discriminationaware trust management for social internet of things," Computer Networks, vol. 178, p. 107254, 2020.

[47] 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 IEEE INFOCOM 2019-IEEE Conference on Computer Communications, pp. 838–846, IEEE, 2019.

[48] 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, 2020.

[49] C. Boudagdigue, A. Benslimane, A. Kobbane, and J. Liu, "Trust management in industrial internet of things," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3667–3682, 2020.

[50] K. A. Awan, I. Ud. 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, 2020.

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

[52] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sedes, "Trust` evaluation model for attack detection in social internet of things," in International Conference on Risks and Security of Internet and Systems, pp. 48–64, Springer, 2018.

[53] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "Iot passport: A blockchain-based trust framework for collaborative internet-ofthings," in Proceedings of the 24th ACM symposium on access control models and technologies, pp. 83–92, 2019.

[54] A. M. Kowshalya and M. Valarmathi, "Dynamic trust management for secure communications in social internet of things (siot)," Sa¯dhana¯, vol. 43, no. 9, pp. 1–8, 2018.