Received September 24, 2020, accepted October 14, 2020, date of publication November 11, 2020,
date of current version November 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3037372

Defining Service-Oriented Trust Assessment for Social Internet of Things

M. JUNAID ASLAM[1], SADIA DIN[2], JOEL J. P. C. RODRIGUES[3,4], (Fellow, IEEE), AWAIS AHMAD[5], AND GYU SANG CHOI[2], (Member, IEEE)

[1]Department of Computer Science, Bahria University, Islamabad 44000, Pakistan
[2]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea
[3]Post-Graduation Program on Electrical Engineering (PPGEE), Federal University of Piauí (UFPI), Teresina 64049-550, Brazil
[4]Instituto de Telecomunicações, 6201-001 Covilhã, Portugal
[5]Department of Computer Science, Air University, Islamabad 44000, Pakistan

Corresponding authors: Sadia Din (saadia.deen@gmail.com) and Gyu Sang Choi (castchoi@yu.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-2019R1A2C1006159, and in part by the Ministry of Science and ICT (MSIT), South Korea, under the Information Technology Research Center (ITRC) support program supervised by the Institute for Information & communications Technology Promotion (IITP) under Grant IITP-2020-2016-0-00313, in part by the FCT/MCTES through national funds and when applicable co-funded EU funds under Project UIDB/50008/2020, and in part by the Brazilian National Council for Scientific and Technological Development—CNPq under Grant 309335/2017-5.

ABSTRACT The rapid advancements in the field of Internet and Social Networks have brought us to the edge of a real-time connected world. As a result, a new paradigm named Social Internet of Things (SIoT) is born. In SIoT, social network merges with the Internet of Things (IoT) to facilitate information and resource sharing among devices in an improved way. Devices seek and provide information among their friends or friends-of-friends. However, the users of this fascinating paradigm meet with issues such as trust and privacy. Hence, trust assessment becomes one of the primary challenges. Existing trust assessment schemes in SIoT are mostly based on the trust of a service provider. The application of such schemes is related to the process of service discovery. However, the ability of a service to act maliciously is overlooked. Literature from related fields shows that services are also capable of acting maliciously. Inspired by that, we aim to define a trustworthiness assessment scheme that is based on trust of service. The application of this scheme is related to the process of service selection. To the best of our knowledge, this is a novel proposition in SIoT. A parameter named Service Trust is proposed. This parameter is mathematically modeled by aggregation of multiple Quality of Service (QoS) parameters. A real-world bike-sharing company dataset is used for evaluation of the proposed scheme. The results attained after analysis are positive. Finally, the conclusion and future work are presented.

INDEX TERMS Social networks, Social Internet of Things (SIoT), service discovery, service selection, trust, trust assessment, service trust, Quality of Service (QoS).

I. INTRODUCTION

In the fast-approaching age of data exchange and communication, billions of devices are envisioned to be exchanging information with each other in real-time. Internet of Things(IoT) is a name given to such a scenario where a huge number of interconnected and heterogeneous devices (often referred to as things) will communicate with each other at any time and any location [1]. These 'things will share resources in the form of ubiquitous services. The traditional Human-to-Object interaction will be extended to Device-to-Device (D2D) Communication [2]. For such a huge number of devices to communicate, different protocols, addressing schemes, and communication standards are envisioned.

For the discovery and provisioning of information and resources in such a scenario, effective searching and selection procedures shall be adopted. However, IoT is considered in its infancy. The information retrieval techniques in IoT are said to be at a similar stage as that of the Web and Internet in the 1990s [3]. Existing approaches use partially or sometimes completely centralized solutions for information

The associate editor coordinating the review of this manuscript and approving it for publication was Sherali Zeadally.

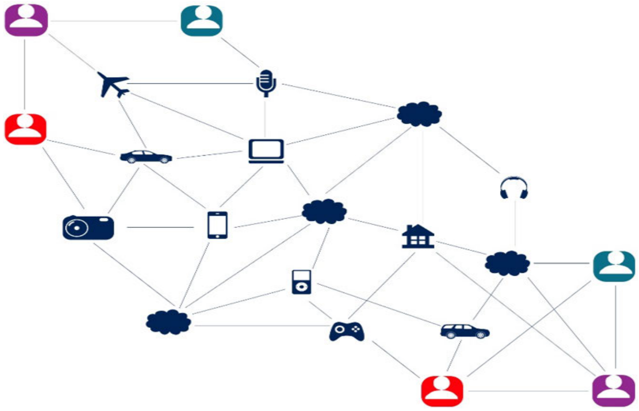


FIGURE 1. Social internet of things.

search and retrieval. Such solutions are not desirable amid the risks of a single point of failure, computational overhead, attacks and issues like scalability and flexibility. The focus of the modern-day Internet of Things (IoT) research is based on decentralized/distributed search and provisioning of information and resources [4]. Nodes requesting and providing services in a distributed manner is a fascinating tale to the minds of researchers, but it entails a plethora of problems.

The integration of Social Networking in IoT is a concept that has been investigated over the years [5]–[8]. The Social Internet of Things (SIoT) is an emerging paradigm in the domain of the Internet of Things (IoT). SIoT is based on the use of Social Network Science (SNS) concepts for improving the network navigability and information discovery in IoT. SIoT allows the objects to create social relationships among themselves based on rules set by their owner. Such a paradigm allows scalability and efficient network navigability. A node having some form of a social relationship with another node is called a friend of that node. The concept of friends and friends-of-friends is taken from social networks. This is evident in the fact that SIoT is reusing the social networking concepts and principles to address problems associated with IoT. The terms nodes, friends, things and objects will be used interchangeably for the remaining of this document. The graphical illustration of Social Internet of Things is provided in Figure 1.

For service discovery and provisioning in SIoT, a node has to search for a particular service between his friends or friends-of-friends [9]. This reduces the time consumption of distributed search in a roughly knitted network to a great extent.

A node has to compute trust in order to discover the desired information/service through its friend(s). For such a discovery to progress, the value of trust is sought and computed from opinion, experience, and recommendation of a friend(s). Trust is also computed by objective parameters such as the computational capacities, degree of a node and response time, etc. Hence, the module of Trustworthiness Management, in the system architecture of SIoT [10], is of vital importance. This module works in line with other modules such as Service Discovery and Service Composition. All of these modules lie at the application layer of SIoT system architecture.

The Trustworthiness Management module is used to deal with the management of information that is required for trust computation. It defines the way trust is sought, computed, and propagated across the network keeping in check the different properties of trust and the IoT network. According to SIoT system architecture, the trustworthiness of nodes must be computed during the process of service discovery and selection. Much of the literature in SIoT focuses on the trustworthiness of the service provider for service discovery, but lacks, to the best of our knowledge, in case of trustworthiness of a service and its use at the time of service selection. We have defined an aggregated Quality of Service (QoS) oriented trustworthiness assessment parameter and proposed its use for service selection in SIoT. The proposed scheme is then evaluated on a real-world dataset.

The paper is organized as follows. In the next section, related work is provided. Section III presents the proposed scheme and methodology. Results and Analyses are provided in section IV. Finally, the document is concluded with a discussion and future work in sections V and VI, respectively.

II. RELATED WORK

This section presents an overview of some notable research work done in trust assessment with respect to the Social Internet of Things and related domains. It is divided into four sections. In the first section, the paradigm of the Social Internet of Things is summarized, and the second section contains a review of trustworthiness assessment techniques proposed in related domains. The next section contains a review of trust assessment approaches in the Social Internet of Things literature. The fourth section summaries the Quality of Service (QoS) oriented trustworthiness.

A. SOCIAL INTERNET OF THINGS

For efficient data exchange and communication in IoT, the use of Social Networking concepts has been proposed in the literature of IoT numerous times [8], [11], [12]. To the best of our knowledge, a definitive architecture and high-level design for socially intelligent interconnected objects have been presented by Antonio I. et. al. [10]. They call it the Social Internet of things (SIoT). Their model will be referred to as 'SIoT' for the remaining of this paper. SIoT exploits the social networking concepts for creating relationships among different objects in the network. The objects create relationships and communicate with each other autonomously based on minimal meditation from their owners. Three major advantages of SIoT include a flexible and scalable network navigability structure which offers effective service and object discovery (a), usage of SNS for addressing the issues of interconnected objects in IoT (b) and the establishment of different levels of trust for the usage of resources and services of other things (referred to as 'friends' in SIoT) (c) [9]. More recently, an extension of SIoT called the Social Internet of Vehicles (SIoV) is proposed [13].

The idea of SIoT network navigability [14] is inspired by the Small World Phenomenon presented by a sociologist Steven Milgram. The principle of this paradigm refers to the fact that there are short chains of associations among different people in societies. Based on this principle a node queries its friends or friends-of-friends for searching and provisioning of a service. Every node in the network; stores information about its relationships, uses search functions, and compute trustworthiness of other nodes.

Five categories of basic relationships among objects in the SIoT architecture include:

- Parental Object Relationship (POR): is established among objects that belong to the same production batch. Such a relationship is usually homogenous in nature.
- Co-location Object Relationship (COOR): is established among objects in the same location (e.g. sensors, objects in a smart home or a bus terminal, etc.). Such objects do not always share resources, but these relationships are essential for creating short links in the network.
- Co-work Object Relationship (CWOR): is created among objects that collaborate with each other to perform a common task. (e.g. Emergency response and telemedicine etc.)
- Ownership Object Relationship (OOR): is established among the objects owned by the same person (e.g. smartphone, smart TV, smart-watch and PlayStation, etc.)
- Social Object Relationship (SOR): is created among objects which come in close proximity to each other periodically or intermittently (e.g. devices and sensors of travel companions, friends and colleagues, etc.) [10].

It is emphasized that such relationships are made autonomously and are different from Social Networks relationships. In a social network, a person chooses to 'follow' or 'add' his friends, himself. In SIoT only the rules for interaction are set by the owner. The resultant relationships are established autonomously among objects.

The SIoT reference architecture is based on three-layers [10]. At the sensing layer (a) the tasks of data acquisition and short-range node collaboration are performed, at the network layer (b) data transmission across different networks is performed and IoT Applications are deployed along with middleware functionalities at the application layer (c). In addition to these layers, there are three basic entities in the SIoT architecture which include: SIoT Server, Gateway and Object.

Figure 2 is the graphical representation of the SIoT Server. SIoT Server incorporates an Application Layer and a Network layer. The application layer is further divided into three sub-layers. The Base sub-layer contains the Semantic Engines, Ontologies of Services, and Databases. Ontologies and semantic engines are used to provide and generate a functional.

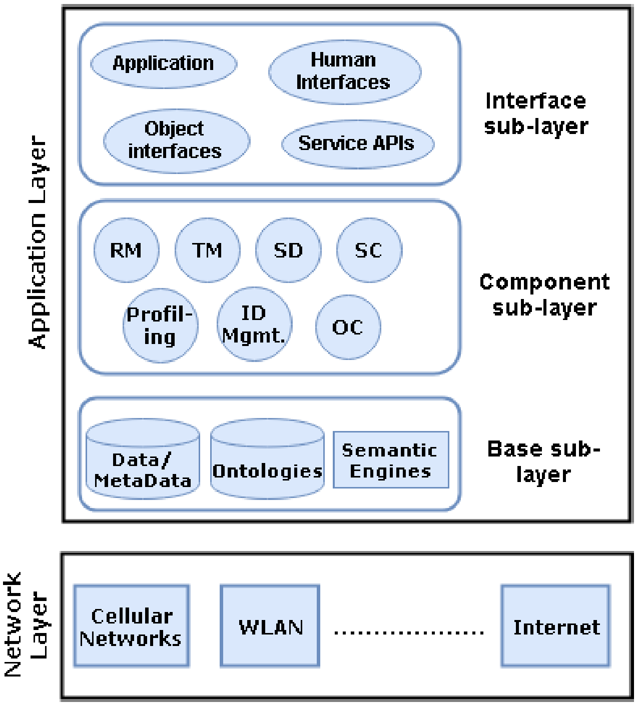


FIGURE 2. SIoT Server in the proposed system architecture of SIoT.

Communication between multiple devices will be carried out using services as interfaces. The database is used to store and manage data of user-profiles, relationships, and data about the activities of an object in the IoT environment. Ontologies and semantic descriptions are stored in a separate database.

The component sub-layer is of prime importance. It contains those modules which are responsible for the implementation of the core functionality of SIoT. These include: Profiling is used for configuration of the information about objects. ID Management is used for assigning unique identification (ID) to all the objects. Owner Control (OC) is assigned the task of the definition of the activities that can be performed, relationships that can be set up and information that can be shared by an object. The relationship Management (RM) module deals with the due meditation of the user in the form of control settings. These control settings are required for an object to update and terminate relationships with other objects. Since objects lack the intelligence of a human, this module is considered a major element of the network. Other components include Trustworthiness Management (TM), Service Discovery (SD) and Service composition (SC). All three of these modules work closely. Our research problem deals specifically with TM which is surmised with SD and SC in one of the following sub-sections.

The interface-sub layer sits above all. As the name suggests, it is where those applications and service APIs are deployed which are used for interacting with the system [10].

The authors have not proposed any explicit implementation for it.

B. TRUST

Trust is a relationship among two entities (trustor and trustee) which are dependent on each other for mutual benefit. This term has multi-dimensional definitions owing to its multi-disciplinary usage. Its value is highly dependent on the context in which it is being used. In Service-Oriented Architectures (SOA) and Web Services (WS) frameworks, trust is considered a key metric for service selection. It is highly likely that a service requestor will select only those service providers who possess a higher value of trustworthiness [15]. Trust in SOA is not mature [16]. The nature of trust in IoT is dynamic, unlike SOA and WS, as the environment of objects changes sporadically [17].

Trust is defined as a subjective probability [18]. It is the expectancy of the user about the performance and functionality of a composite service. Trust is preference-based. It is defined, updated, or self-adjusted from time to time [19]. To involve people in adopting device-to-device communication, incentives and rewards need to be given [2]. The authors have reviewed basic kinds of incentives with an emphasis on sociality and trust. Punishment and reward are given to prevent fraudulent service provisioning and monitoring trust [19]. Some problems and constraints associated with trustworthiness management are provided in [20]. As discussed earlier, in SIoT environment, many devices and entities are involved. These devices are energy scarce and have limited storage and computational resources. In such an environment, devices join and leave networks as they please. Issues that arise from it include, tackling scalability and high-end dynamism. Another issue presented by the authors is criticality and sensitivity of real-world services. Trust needs to be updated and computationally efficient. To achieve it there should be a great deal of focus on improving algorithms and techniques for trust computation and service provisioning.

A trust assessment method based on reputation and knowledge trust metrics is proposed in [21]. Several modules for trust analysis & management and trust models are presented in accordance with a trust-car sharing service. An efficient trust prediction scheme for 'Service-oriented Social Networks' is presented in [22]. The authors have highlighted two existing issues with trust propagation models in the context of social networks. (a) Social networks are mostly large and scalable. The task of trust propagation in such networks is a time-consuming process. (b) Optimization of trust propagation. To tackle these issues, they have proposed the use of hubs for trust propagation. Hubs are few (a) and considered more trustworthy (b). Few hubs minimize the scalability issues while exploiting the correlation between degree distribution and trust distribution of social networks the network can be optimized. In the proposed scheme, Hubs act as referrers between service requestor and provider. The value of the trust of nodes is recorded and updated from time to time on the hub. Given a requestor wants to seek service, to compute the trust of a service provider he will request several hubs which are connected to him and aggregate their referrals of trust values for predicting trust of a service provider.

A contextual trust-based social network model is presented in [23]. Such a network is based on three contextual properties of the social network: Social trust, social role, and social relationship. Social trust is defined as the trust of one node on another regarding a kind of service, or domain of service, in a social network. A social role is defined as the level of activity of a node in a domain of services. Some nodes are experts in their domain and their recommendation holds more value than others. The degree of social intimacy between nodes is defined as social relationships. Nodes that share some form of social relationship are bound to trust each other more than strange nodes. Similarly, the degree of intimacy varies in different forms of social relationships. It is stated that such properties are to be mined from social networks which is a challenging task.

A trust model classification based on four design dimensions is presented in [24]. Trust Composition (a) is a combination of 'Social Trust' and 'QoS Trust'. QoS Trust is a performance-based parameter. It is explained as the trust between a user and its device. It includes factors that affect the completion of a service request and its due response in the form of quality service. It includes cooperativeness, capability, response time and availability, etc. Social Trust is defined as the trust of a person in a social network of IoT device owners. It includes honesty, privacy, centrality, and intimacy, etc. Social Trust is mostly subjective in nature and is based on Sociology.

Trust Propagation (b) refers to the mode of trust dissemination among IoT devices. There can be centralized propagation or distributed propagation. In centralized propagation, the trust of nodes is maintained in a central repository which is accessible to other nodes in the network. A service requestor needs to access this central entity while the discovery and selection of a service. Such solutions are not desirable due to several reasons. While a distributed propagation scheme is based on the exchange of trust values among nodes themselves without a central entity. Nodes that encounter each other share their values of trust and, in some cases, of their friends. Such a scheme offers scalability but brings a lot of computational overhead. The values are sought, compiled, aggregated and updated from time to time, and other trust factors also come into play. For energy scarce IoT devices such a task is extremely energy-consuming.

Trust Aggregation (c) involves aggregating the trust values of opposite natures together and computing a unique value. For example, Throughput and Response Time are two opposite parameters in this situation. Response time needs to be low and throughput needs to be high. Finally, Trust Update (d) is presented by the author. Trust can be updated based on time or event. In time-based updates, trust is updated after some period while in the case of event it can be updated after a transaction is done. The update also involves trust aggregation.

C. TRUST IN SOCIAL INTERNET OF THINGS

For SIoT, trust assessment is a key feature. It is used at every step of service provisioning (i.e. service discovery, service selection, and service composition) and relationship management. Different properties of trust in SIoT have been surmised meticulously in [20]. It is stated that trust in service-oriented environments has the following properties: Direct: based on direct interaction and experience between trustor and trustee, Indirect: based on others opinions, Local: cannot be the same between different couples of nodes e.g. ‘a’ trusts ‘b’ but ‘c’ does not trust ‘b’, Global: every node in the network has its trust value which is known to all of the other nodes in the network, Subjective: a personal opinion, Objective: based on QoS properties of the object, Asymmetric: Trustor and trustee have different levels of trust in each other, Dynamic: it is updated time to time, Context-dependent: varies according to the environment, History-dependent: reliant on previous opinions and experience and Composite: dependent on multiple properties like reliability, competence, intelligence, centrality, reputation, dependability, honesty, and security, etc.

Figure 3 demonstrates an example of SIoT network with ten nodes (each labeled). Node 1 has initiated a decentralized search for a service from its direct friends i.e. D1 and D2. The service is not found on D1 and D2, hence the search has progressed onto friends of its direct friends (FOF). Service is finally found at node 10 which is a FOF node. We can see, there are many paths to reach node 10 but only one of them i.e. (1→ 3 → 6 →10) is chosen. This process is called ‘Network Navigability’ [14]. Here, trust is used to select the nodes for discovering a service.

Three modules in SIoT system architecture which closely work with trust include Service Discovery, which deals with finding a node that possesses a service requested by another node in the network. This module works on the same principle of humans seeking information and friendships (a). Service composition (SC) enables object interaction. Multiple services are combined, and a real-world query is resolved by the means of service composition. After searching for a service, the service is activated using SC (b). Trustworthiness Management understands the process of information extraction and retrieval that is required for service discovery and composition (c) [25].

Trust is perceived as both subjectively and objectively. A subjective trustworthiness management method which is based on solutions proposed for Peer-to-Peer (P2P) networks is presented in [26]. For this purpose, two trust models are presented. Subjective trustworthiness is based on trust semantics taken from the studies of Sociology and Anthropology. As the name suggests, this model is based on the computation of trust based on the personal experience of a user. If two nodes are friends then the one seeking trust, say A, will use the experience of a transaction with the other node, say B, to compute the trust. If nodes A and B are not friends, then this computation is done by querying friends or chains of friends (friends-of-friends) of node A. On the contrary, objective trustworthiness uses Pre-Trusted Objects (PTOs). PTOs manage the trust information of all of the nodes in the network [25]. Any node which is seeking trust queries the PTO. Trust of node A seen by node B is subjective trustworthiness. The information is partly shared between the nodes while the storage is rater based. Trust of node A seen by the entire network is objective trustworthiness. The information is shared globally while the storage is distributed.

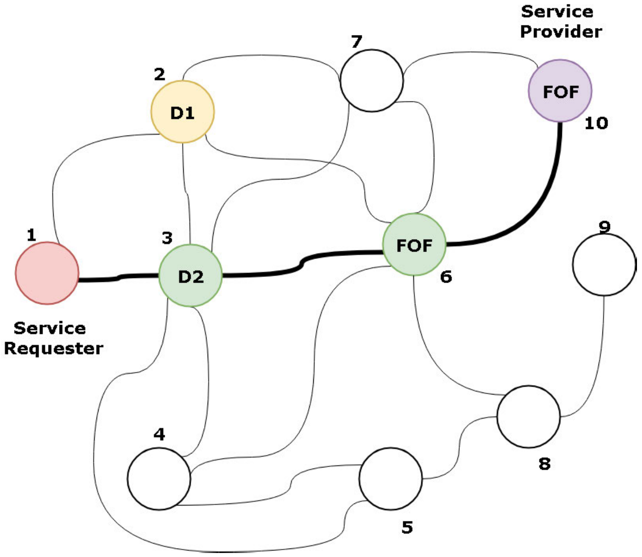


FIGURE 3. Process of service discovery in SIoT.

A lot of literature related to P2P networks has been analyzed in [25] and [26] for the purpose of investigating the malicious behavior of nodes. It is stated that a trustworthy node can also act maliciously under different circumstances. The authors have evaluated their trustworthiness models by applying them in normal circumstances and then under a high concentration of malicious nodes in the network. Their approaches have resulted in the isolation of nearly all malicious nodes in the network.

Trust in SIoT is defined as a perception of trustor about trustee in a particular environment at a particular time, hence called, perceived-trustworthiness [27]. Trust is evaluated by Trustworthiness Attribute (TA) and combinations of TA. A conceptual model of trust is presented by authors. This model indicates that the trustor has propensity, goals, preferences and trust requirements, while the trustee offers features like; integrity, ability, and benevolence. The interaction between trustor and trustee is highly influenced by the environment in which the interaction takes place. Such an environment can influence the interaction by the means of threats and manipulation of the processes, which results in misbehaviors and errors. The perception of trust is also based on the environment. Similarly, a trust assessment method based on bilateral trust evaluation between trustor and trustee is presented in [28]. The model is simulated using data of real social networks like Google+ and Facebook and it is validated on an experimental SIoT network. In another proposition, trustworthiness assessment is modeled on communities of interest [29].

Trust in SIoT is also based on reputation, experience, and knowledge. Considering that, a detailed review of trust in SIoT and a REK Trust Evaluation Model is presented in [2]. These indicators are stated to be based on a social-cognitive process in social science. These trust indicators are then conceptually modeled by using a set of TAs namely, cooperativeness, safety, integrity, reliability, etc. The model is then illustrated by a use-case called 'User Recruitment in Mobile Crowd Sensing'. An interesting aspect of such a trust model is that the trustor can prefer one attribute over the other by assigning weights to the attributes. But the problem is, these attributes are not easily quantifiable. Vagueness in natural language, limitation of data collection, required technology and methodologies, and incorporation of factors as environment and inclination of trustor are some of the reasons which make it an impossible task. So, the authors emphasize on deriving a set of TAs by keeping in mind the conceptual model underlying.

A model termed Quality of Trust (QoT) is then presented for finding multiple social trust paths in a social network. It is defined as the guarantee of a specific level of trust, by taking the contextual properties (social trust, social role, and social relationship) into account, in trust propagation along a certain social trust path. In this model, the user can set the requirements for QoT attributes. Finally, a utility function is used to set the weights of QoT attributes subjectively where one attribute is given more importance than others. Trust propagation is a non-deterministic problem. The authors have proposed an approximation model D-MCBA which is based on an existing model, named the Monte-Carlo method. Trust propagation is done keeping in mind the length of the path as well as satisfying the QoS requirements. In order to select the nodes which, join the path from source to target node, forward and backward search is done. Based on out-degree and in-degree, backward and forward dominating nodes are identified. K-Neighbors finding algorithm is used to select the neighbors to advance the search process. A path is selected, and the value of trust is computed. An optimization process is then performed to select the optimal path based on forwarding and backward search.

In order to conduct the experimental evaluation, no dataset is said to be available that suits the nature of the proposition. Epinions dataset is used for experiments. This dataset contains trust relations between trustor and trustee and has social network properties. Results show that D-MCBA algorithm performs better than the best trust path selection algorithm MONTE_K.

Similarly, several trust assessment metrics and techniques have been used and proposed that satisfy multiple properties of trust in SIoT [30]–[32], [57], and [58].

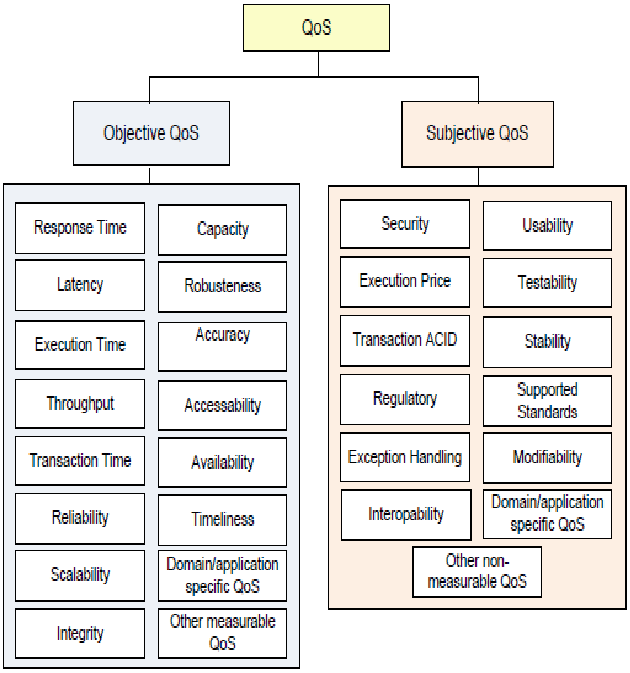


FIGURE 4. QoS metrics classification [37].

D. QUALITY OF SERVICE (QoS) BASED TRUST

Quality of Service (QoS) is considered a quality feature and a non-functional aspect of a service [33]. It is a well-defined, extensively researched upon and discussed metric in literature [34], [35], and [36]. The properties of QoS are used as a Trust Metric (TM). QoS trust metrics are generalized in two classes i.e. Subjective QoS and Objective QoS [37]. Figure 4 represents the classification chart.

The usage of trust in Service-Oriented Architectures (SOA), web services, cloud, and distributed computing is wide-ranging. The use of a QoS metric is dependent on the requirement of a user. Because of the lack of a standard service description and definition framework in SIoT, some of the existing and generalized QoS metrics are being used for the trustworthiness assessment of service in SIoT.

QoS trust is explained as the trust between a user and its device [24]. An improved QoS based trust computation model (which has overcome five faults from the previous model) is presented in [38]. A QoS-based probabilistic approach for learning the trust of a single or composite web service is presented in [39]. Trust assessment approaches in IoT using QoS and social trust metrics are presented in [40] and [41]. A SWARM optimization technique for fault and failure tolerance routing is presented in [42]. This approach satisfies the QoS parameters.

For runtime service discovery, selection, and composition QoS aware approach is presented in [43]. Two non-functional parameters namely, throughput and response time are incorporated with web services and user requests. Such an approach is said to increase customer satisfaction and guarantee a quality experience. It should be noted here that customer satisfaction can also be linked with trust. If a customer has a

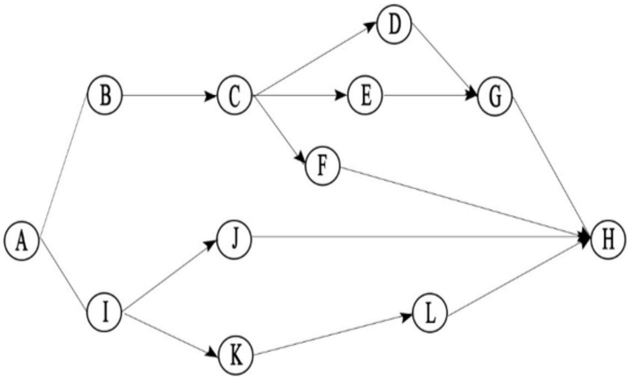


FIGURE 5. Example of a composite service.

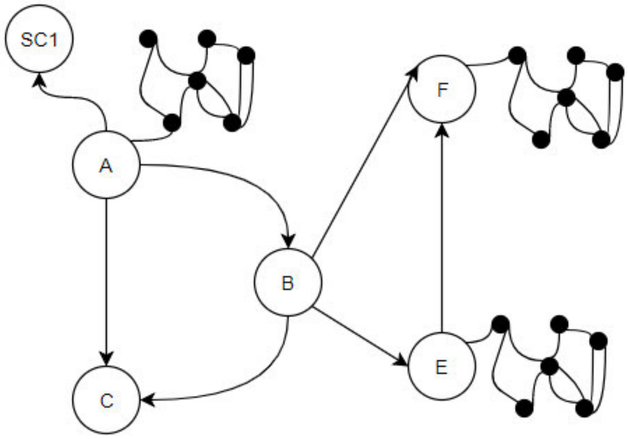


FIGURE 6. Referral links in social networks.

satisfactory experience with a service, such a service has a greater probability of being used again by the customer.

Component services combine to form a composed service Figure 5. Trust computation of component services is done in order to carry an effective service composition [44]. With that, trust is also used for service selection. In the model presented by the proponents of this idea, the selection is based on a parameter called 'Trust degree' and for trust computation two QoS parameters cost and response time are used.

Quality is also linked with Trust. A Quality of Experience (QoE) and Quality of Compliance (QoC) based approach for trust in service composition is presented in [45]. This trust model is based on the concept of 'Direct Trust' and 'Collaborative Rating' in social trust networks. The author argues that the existing web service discovery and composition mechanisms are based on the functional properties of the component services. However, views of services user may differ about its contents. One of the schemes of their model is 'Network Referral' in TrustNet. TrustNet is a representation based on the generation of referral chains in the result of an agents' query. It works based on forming a referral chain from a social trust network of multiple agents Figure 6. For example, an agent 'A' queries its direct link agent 'D' for the reputation of a composite service. D, in turn, asks its links; say Y, E and X. Hence the agents which provide testimony about the service result in the formation of a referral chain. Let's say, [A->D->Y] is a referral chain since E and X did not provide testimony. DS Evidence theory is also used for a similar purpose whereby the degree of satisfaction of service is calculated as a probabilistic function based on evidence degree of satisfaction.

The authors have used an already defined service discovery and selection model based on Semantic Web Services (WSW). They have supplemented the QoS based service selection, used in the previous model, with their own trust computation model based on the user's own subjective experience (QoE) and objective recommendations of other agents (QoC). This way services, of the apparently same functionality, have a different reputation. Both QoE and QoC metrics are then computed and by using a decision matrix right services are selected. Also, the agents are awarded or penalized based on the correctness of their recommendations. A case study is then used to present the results with an emphasis on creating more mechanisms to minimize fraud in such systems. Similarly, a QoS aware and Quality of Experience (QoE) aware traffic information sharing system is provided in [46]. Trust values are computed based on time and context. A directed graph called Trust Graph is used for the representation of trust relations between nodes [47]. An edge from A→B indicates A Trusts B while B→A indicates B trusts A. Also, in this model, trust is considered as an asymmetric entity. Secondly, Trust Level is used to indicate the degree of trust a node possesses. The value of this entity is to be chosen from a set of possible values. The proposed framework follows the traditional SOA model for service matching and selection, with the addition of an entity named QoS Broker. The trust mediator is a part of the QoS broker. It takes services information from services descriptions provided by service providers. Upon the provider's wish to publish services the compatibly of services is verified. The requestor requests the QoS broker, who verifies the request, then fetches a list of services, filters services based on requested QoS properties and finally selects the service with the max level of trust. This framework is then evaluated with the help of a case study. It is concluded that QoS driven requirements and properties of services are essential for finding and selecting the optimal service. Such a framework provides reliability for both services and services provider Figure 7.

With the review of existing literature, the importance of trust in SIoT and related domains becomes evident. It is also gathered that trust assessment is not a very mature area and has enormous potential for research. However, the lack of datasets and experimental platforms remains a hurdle and can only be resolved with time and maturity of this field.

III. SERVICE-ORIENTED TRUST ASSESSMENT FOR SOCIAL INTERNET OF THINGS

As stated earlier, almost all trust assessment and evaluation models in SIoT are based on the trust of the service provider.

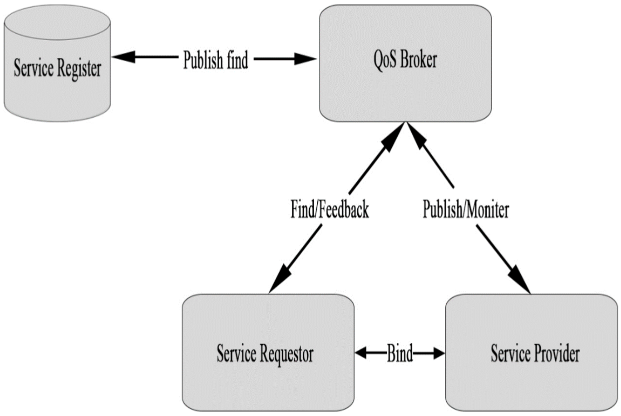


FIGURE 7. **Service selection model using quantitative trust.**

The process of trust assessments is carried out during service discovery. The ability to act maliciously is attributed to the service provider or nodes through which the process of discovery progresses. However, we are inspired by the fact that services can act maliciously as well, and trust computation of service is also important. We believe that existing trust methodologies in SIoT should be primarily used for service discovery but at the stage of service selection, trust assessment of service is required. Much of the literature has been reviewed for the role of trust in SIoT and QoS based trust in the previous section. We now present some literature that best supports our claim of the ability of services to act maliciously and the need for trust assessment for service selection. Due to the infancy of the field of SIoT, literature is presented from the fields of Cloud Computing and SOA.

A model for service selection based on trust of service in SOA is presented in [16]. Trust assessment is used for selecting and delivering a service in the cloud computing environment [48]. Among recent works, an SLA based trust model is proposed for trust assessment of cloud services, upon the basis of which service is selected [49]. Similarly, a model for social sensor cloud services that exploits the social data streams is also presented [50]. It is argued that trust management schemes in Cloud Computing are not fully effective [51]. It is stressed that internal threats to the system are in the form of malicious services. The proposed scheme mitigates the threats from internal services in the form of malware. Such research works are stressing upon the trust of service and its use in service selection in related fields. To the best of our knowledge, a trustworthiness management model which is based on trustworthiness assessment of service has not been proposed yet in the SIoT literature.

Consider the following scenario: In a Smart City SIoT environment, a user searches for a car parking space. A user initiates a distributed search, for the service of 'Car Parking near me' from its direct friends (as per SIoT paradigm, the search can also progress onto friends of its direct friends). The user decides to end the distributed search once four car parking spaces/services are found from its direct friends or no parking is found in a pre-defined time. The user finds four parking spaces nearby. Every parking space has its pros and cons. One of the spaces has less fare and free car parking on weekends. The other has an indoor parking space and there is a social object relationship of the user's car with two of the parked cars in the space. One space does not provide rain and sunlight protection, but it is larger and less crowded than others. The other highly trusted space provides both indoor and outdoor parking services.

All providers have equal or near-equal trust ratings and service specifications. In an ideal case, the user will select one of the 4 car parking service providers upon its trust assessment. But the user also has a secondary trust requirement of 'social relationship with at least two cars and above 4 ratings of the indoor parking service'. Here the user selects one of the providers based on indoor service rating and social relationship factors. The user has the liberty to compromise on service requirements and set thresholds.

We have seen that the user initially discovered the service providers and then, based on secondary requirements, one of the services is selected based on rating. Rating is a subjective QoS trust parameter. User requirements can be 'Indoor space service's availability and operational time'. Availability is also used in the definition of QoS based trust. We are proposing an aggregated parameter named 'Service Trust', which enhances the high-level definitions of QoS parameters in the context of SIoT. It is based on the aggregation of QoS parameters like Availability, Execution Time, Transaction Time and Transaction Factor of service. We propose the application of this parameter at the time of Service Selection in SIoT. In addition to Service Trust, a parameter named 'Social Relationship Factor' is also used for service selection. The parameters, such as; the number of intermediate messages exchanged before service dispatch, round trip time for request and reply, packet transfer time, the bandwidth of the devices involved, network congestion and other routing factors have been ignored because this problem lays at the application layer of SIoT. Figure 8 shows the flow chart of the best-case scenario.

In Figure 9, an example SIoT network of 10 nodes is under observation. Upon discovering the requested service, a user, say j, takes two factors into consideration. The first one is the Service Trust $T_s^{(i)}$, for service i, and the other is Social Relationship factor F between service seeker j and provider k. Node 10 is searching for a service that resides at node 5 and node 4. It is seen that the service is found through node 2 which is a friend of the requestor. Node 2 searches for the desired service in its friend list. It chooses node 1, which searches and finds the desired service at node 5 and node 4. The Service Trust is calculated next and service is selected from the node 5 as it has the highest value of Service Trust and Social Relationship Factor.

A. SERVICE TRUST

Service Trust $T_s^{(i)}$ is defined as an aggregated parameter for every service a node provides. We donate an individual

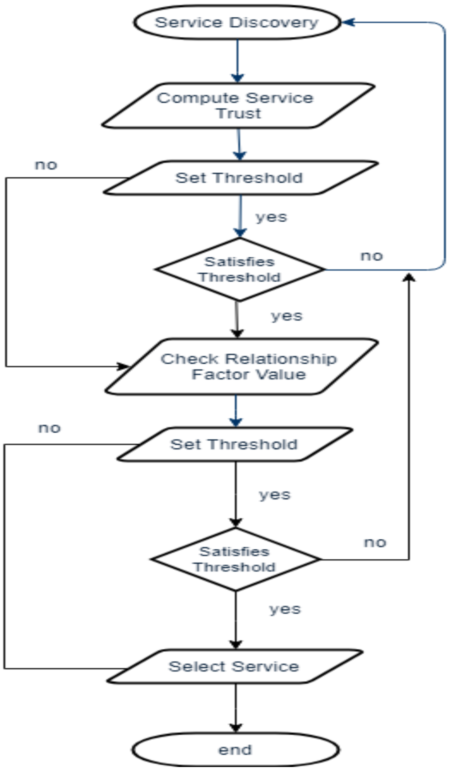


FIGURE 8. **Flow chart of the best-case scenario.**

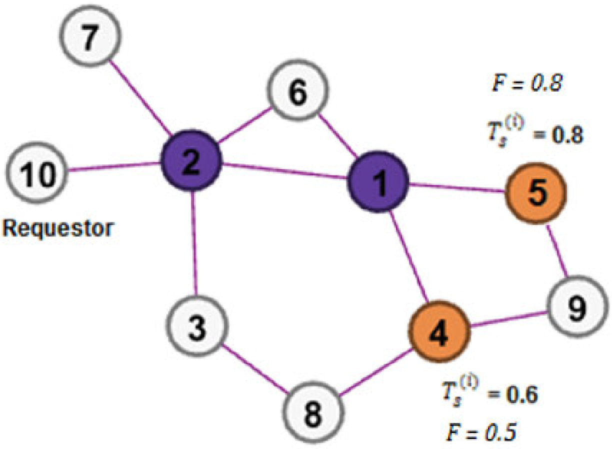


FIGURE 9. **Graphical illustration of the application of Service Trust in service selection.**

service with i. The time at which a service i is requested is denoted by request time $t_{req}^{(i)}$, similarly, the time at which a service dispatch has begun will be called reply time $t_{rep}^{(i)}$. The parameter $t_{rep}^{(i)}$ will have a null value if the node does not dispatch service reply to service request $t_{req}^{(i)}$.

$T_{rep}^{(i)} = \{t_{rep}^{(1)}, t_{rep}^{(2)}, t_{rep}^{(3)}, \ldots, t_{rep}^{(n)}\}$ is a set that contains all the reply times in response to service requests and this set will be made once a service request is received. The dispatch initiation time is taken as reply time because the total time it takes for a service to reach the service requestor depends on network routing factors and not on the ability of the service provider. In the context of our research, a Transaction constitutes one successful service request and a reply that contains service from the provider. Any no. of intermediate messages is ignored. Transaction time t_i of one transaction for service i is then defined as follows:

$$t_i = \begin{cases} 1 - \dfrac{t_{rep}^{(i)} - t_{req}^{(i)}}{t_{maxrep}^{(i)}}, & if\ t_{rep}^{(i)}! = null; \\ 0, & otherwise \end{cases} \tag{1}$$

$t_{maxrep}^{(i)}$ indicates the maximum time for service reply $t_{rep}^{(i)}$. Reply time $t_{rep}^{(i)}$ needs to be less than or equal to $t_{maxrep}^{(i)}$. The value of t_i ranges between 0 and 1. An inclination towards 1 indicates a time-efficient transaction while nearness to 0 indicates vice versa. [52] suggests that it is up to the user to define the QoS requirements for a network routing path selection problem. The path is selected based on a threshold value set for bandwidth. As the Transaction time varies for every service, a similar approach has been adopted by us. Transaction times are also recorded in a set for every transaction. The average of this set is called the Transaction factor T_i.

$$\begin{aligned} ts^{(i)} &= \{t_i^{(1)}, t_i^{(1)}, t_i^{(2)}, t_i^{(3)}, \ldots, t_i^{(n)}\} \\ T_i &= \bar{ts}^{(i)} \end{aligned} \tag{2}$$

Another aggregated metric called Availability Ai is defined. This parameter counts the total no. of transactions successfully done for service. Its value is computed by counting the total no. of non-null (valid) replies from the set of reply times $T_{rep}^{(i)}$. It is computed as follows:

$$\begin{aligned} [P] &= \begin{cases} 1, & if\ P! = null; \\ 0, & otherwise, \end{cases} \\ A_i &= \frac{\sum [P(\forall r_p \in T_{rep}^{(i)})]}{|T_{rep}^{(i)}|} \end{aligned} \tag{3}$$

The above equation uses Iverson Brackett notation for a function P that results in 1 when the condition is true and 0 otherwise. P is applied to every element in the set $T_{rep}^{(i)}$. If the value of an individual reply time is not null, then the summated value is increased by 1. This value is divided by the total no. of elements in the set. The resultant value is a real number ranging between 0 and 1 (both inclusive), with closeness to 1 indicating a strong T_i while nearness to 0 indicates the opposite. Execution time E_i is the total time duration a service takes to execute.

The Service Trust $T_s^{(i)}$ of an individual service is then defined as follows:

$$T_s^{(i)} = \alpha \bar{t_i} + \beta T_i + \varepsilon A_i + \gamma (1 - E_i) \tag{4}$$

Value of $T_s^{(i)}$ is normalized between 0 and 1. α, β, ε, and γ are model parameters.

TABLE 1. **Value of social relationship factor w.r.t SIoT based social relationships.**

Social Relationship Type	Social Relationship Factor
OOR	0.9
CWOR	0.8
CLOR	0.8
SOR	0.6
POR	0.5

B. SOCIAL RELATIONSHIP FACTOR PARAMETER

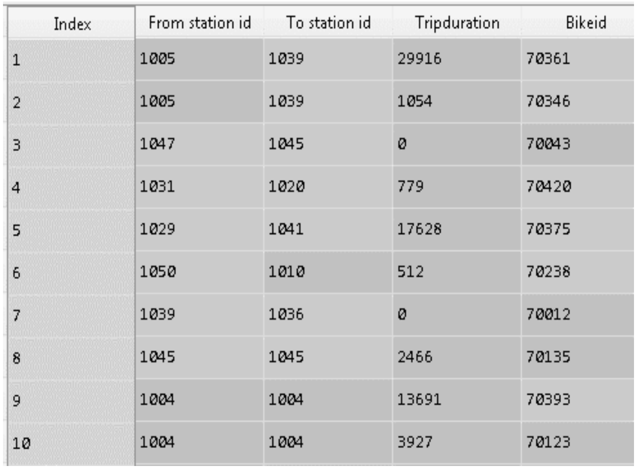
Based on theoretical evidence, [25] has proposed a parameter named Relationship Factor. The values of this parameter are specified with respect to social relationships. The authors have provided theoretical reasoning for the specified values. It is stated that the degree of intimacy in human relations vary person to person hence service trust between service requestor and service provider is also reliant on social relationship. Based on theoretical evidence and common sense, it is obvious that a person relies on his family more than his friends and acquaintances. Similarly, the degree of trusting a close friend, a friend, and a complete stranger is bound to be different [53], [54], and [55].

Based on this approach, we propose the use of a similar parameter called Social Relationship Factor F between two nodes j and k for provisioning of service. Table 1 shows the ratings for F based on different types of Social Relationships. We are adopting similar parametric values as in [25].

C. ANALYSIS OF EXAMPLE SCENARIO w.r.t THE PROPOSED SCHEME

It is seen in Figure 9 that no threshold is set for service selection. Also, the no. of hops for choosing one of the two providers are the same. Furthermore, the service is found at two providers and not one. Such factors are overlooked in the example scenario, but they also come into play when choosing a provider and certainly influence the selection of the service. For example, Service Trust parameter can be used solely for trust assessment if the objects involved have an Object Owner Social Relationship and are part of a smaller network with no malicious services. As stated earlier, the true application and analysis are limited but a lot of research questions and solutions arise from such a simple scenario only.

In energy scarce IoT devices, trust computation at every step of the service discovery is an energy-consuming process and brings excessive computational overhead. The social network under discussion here constitutes of 10 nodes only. While real-world social networks contain millions of nodes. Hence, the tradeoffs between trust parameters become a requirement. For nodes that have a strong degree of social relationship can use fewer trust parameters and save energy. Similarly, Social Relationship Factor can be given priority over Service Trust in some cases.



Index	From station id	To station id	Tripduration	Bikeid
1	1005	1039	29916	70361
2	1005	1039	1054	70346
3	1047	1045	0	70043
4	1031	1020	779	70420
5	1029	1041	17628	70375
6	1050	1010	512	70238
7	1039	1036	0	70012
8	1045	1045	2466	70135
9	1004	1004	13691	70393
10	1004	1004	3927	70123

FIGURE 10. **Data after pre-processing.**

IV. RESULTS

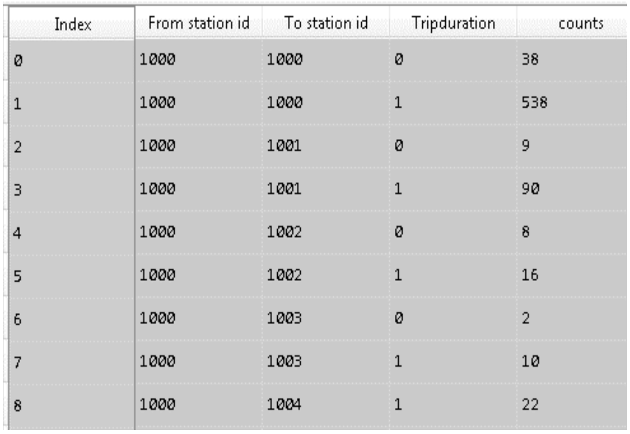
In order to evaluate the proposed mathematical model, a real-world Bike Ride-sharing service dataset is used [56]. This dataset contains data of a public bicycle sharing service called 'Healthy Ride' which is used in Pittsburg, Pennsylvania, US. The dataset includes ten fields (columns), which includes; TripID, BikeID, Trip start station ID, Trip end station ID, and Trip duration, etc. The dataset contains 26973 rows of data. An Intel R Core i3 (2100) @ 3.10 GHz with 4 GB DDR2 RAM is used to analyze the dataset.

A. PRE-PROCESSING AND SYNTHESIS

In order to evaluate the proposed model, some processing is done on the original dataset. The trip data is imported as a Data Frame of Pandas Library in Spyder for Python 3.6. The data values missing for either of 'Trip start station ID' and 'Trip end station ID', are discarded. Upon doing it, the dataset is reduced to 23712 rows. We have proposed to identify valid and invalid trips based on Trip duration. The trip duration is recorded in seconds. If the trip duration value is missing (null) or it is less than 120 seconds and greater than or equal to 12000, the original value is replaced with 0. This results in almost 7% of the data values becoming 0 and this data is deemed as data for invalid rides. The proposed mathematical model has been applied after it.

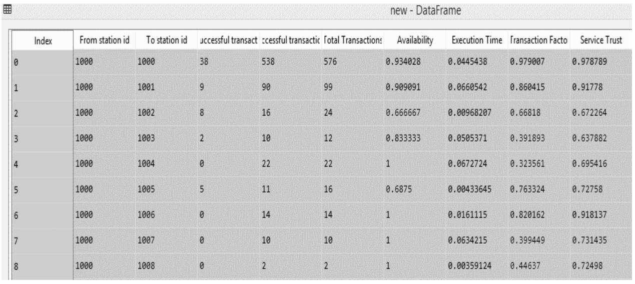
Ride from the source station to the target station has been perceived as a service. Services are grouped based on 'Trip start station ID' and 'Trip end station ID'. This results in the identification of 1673 unique services in the dataset. Data for three modeled parameters; Availability, Execution time and Transaction factor has been computed from the values of Trip duration, Trip start station ID and Trip end station ID for 1673 unique services. Figure 10 shows the data frame after pre-processing.

For computing information of the parameter Availability, the no. of valid and invalid trips for every service has been counted. The formula is then applied, and the values are



Index	From station id	To station id	Tripduration	counts
0	1000	1000	0	38
1	1000	1000	1	538
2	1000	1001	0	9
3	1000	1001	1	90
4	1000	1002	0	8
5	1000	1002	1	16
6	1000	1003	0	2
7	1000	1003	1	10
8	1000	1004	1	22

FIGURE 11. Group of valid and invalid trips.



new - DataFrame

Index	From station id	To station id	uccessful transact	ccessful transactic	Total Transactions	Availability	Execution Time	Transaction Facto	Service Trust
0	1000	1000	38	538	576	0.934028	0.0445438	0.979007	0.978789
1	1000	1001	9	90	99	0.909091	0.0660542	0.860415	0.91778
2	1000	1002	8	16	24	0.666667	0.00968207	0.66818	0.672264
3	1000	1003	2	10	12	0.833333	0.0505371	0.391893	0.637882
4	1000	1004	0	22	22	1	0.0672724	0.323561	0.695416
5	1000	1005	5	11	16	0.6875	0.00433645	0.763324	0.72758
6	1000	1006	0	14	14	1	0.0161115	0.820162	0.918137
7	1000	1007	0	10	10	1	0.0634215	0.399449	0.731435
8	1000	1008	0	2	2	1	0.00359124	0.44637	0.72498

FIGURE 12. Final data of 1672 unique services with three parameters.

stored in another data frame. Figure 11 shows the groups of valid and invalid trips in the form of 1 and 0 counts. Similarly, data for Execution time and Transaction factor is computed. Figure 12 shows the dataset which shows the no. of successful, unsuccessful transactions and total transactions for every service. Also, the three modeled parameters are computed and finally, the values of these parameters are aggregated for the Service Trust parameter. For data normalization, sklearn library is used.

B. EVALUATION

The resulting data is exported to a.xlsx file. The graphs of Service Trust with respective modeled parameters are generated using MS Excel. Figure 13, Figure 14, and Figure 15 show the resulting graphs. The values of Service Trust corresponding to the highest value of Availability shows a near same concentration of values after 0.7. Also, it should be kept in mind that both axes start at 0.3.

It is evident from the graphs that the modeled parameters and Service Trust are positively correlated. Except for Execution time, an increase in the value of QoS modeled parameter results in an increase in Service Trust and the relationship is linear or partially linear in nature. Time and trust are inversely correlated as seen in the graph as well. Hence, the aggregated Service Trust parameter is computed by inverting the values of Execution time i.e. $(1-E_i)$.

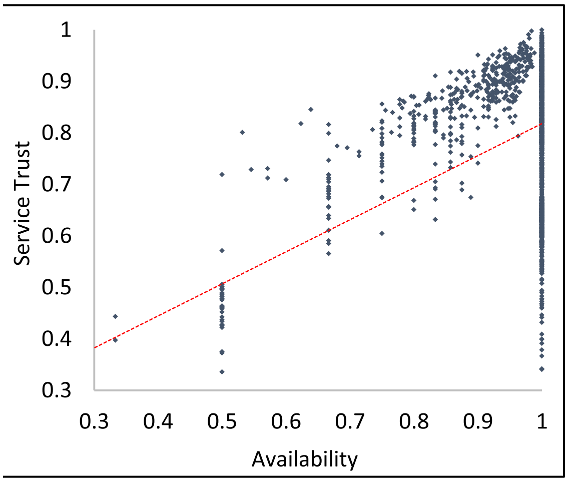


FIGURE 13. Availability vs service trust.

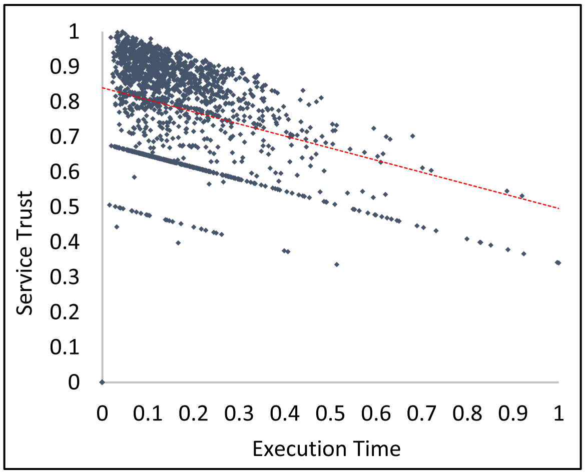


FIGURE 14. Execution time vs service trust.

The subjective trust model [26] is evaluated by analyzing the effects of increasing the concentration of malicious nodes in the network. A similar approach has been adopted here, in terms of invalid rides. In order to induce a higher concentration of invalid rides, the trip duration of services with null values or values less than equal to 600 seconds and greater than equal to 12000 has been changed to 0. This results in more than 29% of the rides deemed invalid. The effects of modeled parameters are then analyzed.

Figure *16*, Figure 17, and Figure 18 are resultant graphs that show that an increase in the concentration of invalid rides has resulted in a similar performance. The data points are more varied and hence stretched across the chart. However, the regression lines show correlation has remained unchanged. There is a slight shift in values of Service Trust with respect to Execution Time. The resulting regression line

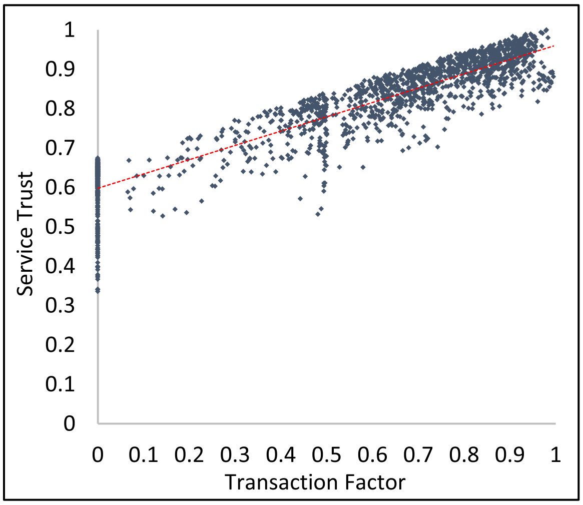


FIGURE 15. Transaction factor vs. service trust.

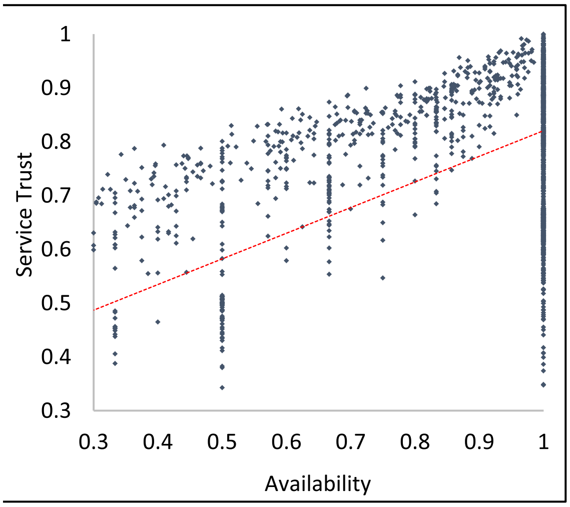


FIGURE 16. Availability vs. service trust after an increase in invalid transactions.

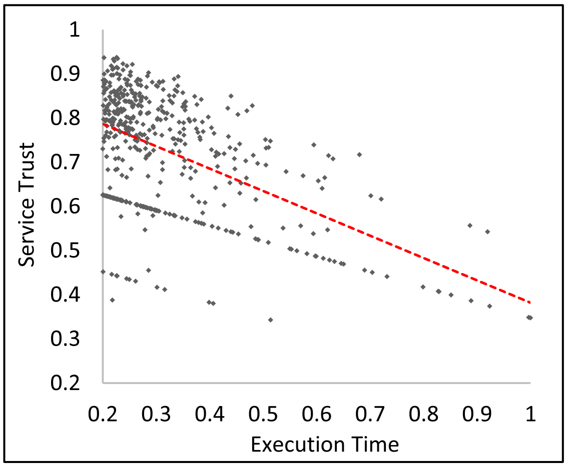


FIGURE 17. Execution Time vs. Service Trust after an increase in invalid transactions.

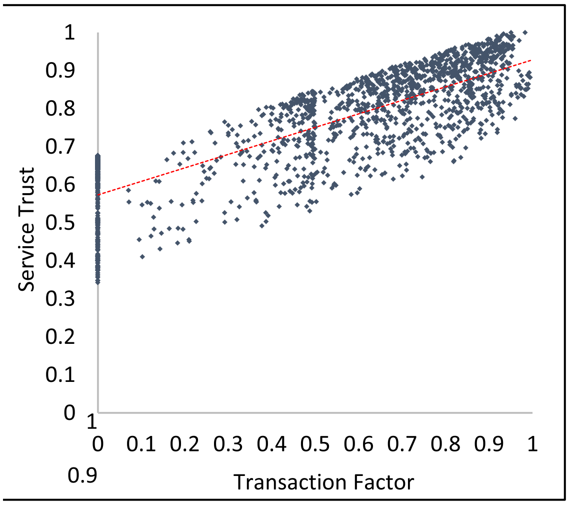


FIGURE 18. Transaction Factor vs. Service Trust after an increase in invalid transactions.

had a positive slope because the filter for increasing malicious services was based on assigning a zero value to service with a duration of less than 600. As a result of that, a major bias was induced in the Execution time parameter since it is entirely reliant on the duration of execution. We have thus presented a graph with a major axis starting from 0.2. As the parameters in the dataset are modeled from the context of this research, such a result is expected.

The existing works have analyzed the effect of their trust models by mapping the proposed parameters with Social network properties, such as clustering coefficients, network diameter and degree distribution of the resulting network, etc. If the proposed scheme works under different circumstances e.g. increased concentration of malicious nodes etc. and the resulting network isolates malicious nodes while following the properties of a social network, the scheme is deemed accurate. Our work is different in that regard.

We are dealing with the trust of a resource whose value is aggregated by calculating Transaction data between different nodes in the network. We cannot analyze this scheme with respect to network properties due to many reasons. In the case of the trust of a service provider, such a node is considered as a target node in social network data. In our case, service is a resource that is held by a node. So, its effect on the entire social network properties and data is out of the scope of this research work. Unavailability of the right kind of datasets is another issue.

V. CONCLUSION

In this paper, a service-oriented trust assessment scheme is proposed for SIoT. Some QoS parameters are analytically modeled and aggregated to propose a parameter named Service Trust. With the analysis of the dataset, a positive correlation between the modeled parameters and Service Trust is seen. Upon increasing the concentration of invalid/malicious services in the network the nature of correlation remained unchanged. Finally, a scenario-based analysis is done in order to present the application of this methodology for Service Selection in SIoT.

This research provides an impetus to conduct further research on trust computation in SIoT. Previous works have focused on Service Provider rather than Service itself. Furthermore, the application/usage of the previous researches remains in the process of discovering a service. The application of our research deals with the employment of trust assessment for selection of a service which (is unprecedented) comes after the process of Service discovery in SIoT. This application further delves into the domain of Service Composition where multiple services are selected and composed to provide a real-world service. So, we can say that trust assessment must be employed for all the stated processes, i.e. service discovery, service selection, and service composition. As concluded in the literature review section of this document, the enormous computational overhead which is entailed with the incorporation of trust assessment processes in every step of service provisioning remains an exhilarating process for energy scarce IoT devices.

VI. FUTURE WORK

Due to the lack of experimental platforms and datasets of this nature, we cannot say yet, about the employment of QoS trust for every Service. Further research can surely prompt direct execution of such methodologies and we can investigate the acknowledgment of the proposed QoS based Service Trust in a better way. Lastly, this research also provides a stimulus to an enormous amount of research that can be garnered by analyzing which trust assessment scheme is to be used under different circumstances.

REFERENCES

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

[2] A. Ometov, A. Orsino, L. Militano, D. Moltchanov, G. Araniti, E. Olshannikova, G. Fodor, S. Andreev, T. Olsson, A. Iera, J. Torsner, Y. Koucheryavy, and T. Mikkonen, "Toward trusted, social-aware D2D connectivity: Bridging across the technology and sociality realms," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 103–111, Aug. 2016.

[3] P. Barnaghi and A. Sheth, "On searching the Internet of Things: Requirements and challenges," *IEEE Intell. Syst.*, vol. 31, no. 6, pp. 71–75, Nov. 2016.

[4] M. Nitti, L. Atzori, and I. P. Cvijikj, "Friendship selection in the social Internet of Things: Challenges and possible strategies," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 240–247, Jun. 2015.

[5] H. Ning and Z. Wang, "Future Internet of Things architecture: Like mankind neural system or social organization framework?" *IEEE Commun. Lett.*, vol. 15, no. 4, pp. 461–463, Apr. 2011.

[6] A. Fast, D. Jensen, and B. N. Levine, "Creating social networks to improve peer-to-peer networking," in *Proc. 11th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2005, p. 568.

[7] Z. Maamar, N. Faci, L. K. Wives, Y. Badr, P. B. Santos, and J. P. M. De Oliveira, "Using social networks for Web services discovery," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 48–55, Jul. 2011.

[8] P. Mendes, "Social-driven Internet of connected objects," in *Proc. IAB Work. Interconnecting Smart Objects Internet*, 2011, pp. 1–3.

[9] 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.

[10] 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.

[11] L. Atzori, D. Carboni, and A. Iera, "Smart things in the social loop: Paradigms, technologies, and potentials," *Ad Hoc Netw.*, vol. 18, pp. 121–132, Jul. 2014.

[12] J. Breslin and S. Decker, "The future of social networks on the Internet: The need for semantics," *IEEE Internet Comput.*, vol. 11, no. 6, pp. 86–90, Dec. 2007.

[13] B. Jain, G. Brar, J. Malhotra, S. Rani, and S. H. Ahmed, "A cross layer protocol for traffic management in social Internet of vehicles," *Future Gener. Comput. Syst.*, vol. 82, pp. 707–714, May 2018.

[14] 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)*, Mar. 2014, pp. 405–410.

[15] E. M. Maximilien and M. P. Singh, "Toward autonomic Web services trust and selection," in *Proc. 2nd Int. Conf. Service Oriented Comput. (ICSOC)*, vol. 4, 2004, p. 212.

[16] Z. M. Aljazzaf, M. A. M. Capretz, and M. Perry, "Trust-based service-oriented architecture," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 28, no. 4, pp. 470–480, 2016.

[17] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.

[18] X. Wu, B. Li, R. Song, C. Liu, and S. Qi, "Trust-based service composition and optimization," in *Proc. 19th Asia–Pacific Softw. Eng. Conf.*, vol. 1, Dec. 2012, pp. 67–72.

[19] Z. M. Aljazzaf, M. Perry, and M. A. M. Capretz, "Towards a unified trust framework for trust establishment and trust based service selection," Dept. Comput. Sci., Univ. Western Ontario, Ontario, ON, Canada Tech. Rep., 2011, pp. 1175–1178.

[20] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sèdes, "Trust management in social Internet of Things: A survey," in *Proc. Conf. E-Bus., E-Services E-Soc.*, vol. 13, 2016, pp. 430–441.

[21] N. B. Truong, T.-W. Um, and G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy," in *Proc. 19th Int. Conf. Innov. Clouds*, 2016, pp. 104–111.

[22] Y. Xu, J. Liu, M. Tang, and X. F. Liu, "An efficient trust propagation scheme for predicting trustworthiness of service providers in service-oriented social networks," in *Proc. IEEE 20th Int. Conf. Web Services*, Jun. 2013, pp. 467–474.

[23] G. Liu, A. Liu, Y. Wang, and L. Li, "An efficient multiple trust paths finding algorithm for trustworthy service provider selection in real-time online social network environments," in *Proc. IEEE Int. Conf. Web Services*, Jun. 2014, pp. 121–128.

[24] J. Guo and I.-R. Chen, "A classification of trust computation models for service-oriented Internet of Things systems," in *Proc. IEEE Int. Conf. Services Comput.*, Jun. 2015, pp. 324–331.

[25] M. Nitti, R. Girau, L. Atzori, and S. Member, "Trustworthiness management in the social Internet of Things first theorital analysis," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1–14, 2013.

[26] 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.

[27] 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, pp. 1–24, 2017.

[28] 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.

[29] 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.

[30] 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.

[31] 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. 2016.

[32] 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.

[33] Z. Zheng, Y. Zhang, and M. R. Lyu, "Investigating QoS of real-world Web services," *IEEE Trans. Services Comput.*, vol. 7, no. 1, pp. 32–39, Jan. 2014.

[34] S. K. Özman and S. Toros, "Damage caused by phytoptus avellanae Nal. and cecidophyopsis vermiformis Nal.(Eriophyoidea: Acarina) in hazelnut," *Acta Hortic.*, vol. 445, no. 3, pp. 537–543, May 1997.

[35] L. Li, S. Li, and S. Zhao, "QoS-Aware scheduling of services-oriented Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1497–1507, May 2014.

[36] Z. Ye, X. Zhou, and A. Bouguettaya, "Genetic algorithm based QoS-aware service compositions in cloud computing," in *Database Systems for Advanced Applications* (Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6588. 2011, pp. 321–334.

[37] Z. M. Aljazzaf and M. Perry, "Trust metrics for services and service providers," in *Proc. Iaria*, 2011, pp. 195–200.

[38] Y. Liu and X. Tang, "A trusted model for service selection in trustworthy service composition," in *Proc. Int. Conf. Comput. Sci. Netw. Technol.*, vol. 2, Dec. 2011, pp. 927–930.

[39] M. Mehdi, N. Bouguila, and J. Bentahar, "A QoS-based trust approach for service selection and composition via Bayesian networks," in *Proc. IEEE 20th Int. Conf. Web Services*, Jun. 2013, pp. 211–218.

[40] F. Bao, I.-R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems," in *Proc. IEEE 11th Int. Symp. Auto. Decentralized Syst. (ISADS)*, Mar. 2013, pp. 1–7.

[41] F. Bao and I.-R. Chen, "Dynamic trust management for Internet of Things applications," in *Proc. Int. Workshop Self-Aware Internet Things*, 2012, p. 1.

[42] M. Z. Hasan and F. Al-Turjman, "SWARM-based data delivery in social Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 821–836, Mar. 2019.

[43] S. Garg, K. Modi, and S. Chaudhary, "A QoS-aware approach for runtime discovery, selection and composition of semantic Web services," *Int. J. Web Inf. Syst.*, vol. 12, no. 2, pp. 177–200, Jun. 2016.

[44] G. Dai and Y. Wang, "Trust-aware component service selection algorithm in service composition," in *Proc. 4th Int. Conf. Frontier Comput. Sci. Technol.*, vol. 2, Dec. 2009, pp. 613–618.

[45] P. Wang, "A trust-based selection approach for QoS-aware service composition provisions," in *Proc. 6th Int. Conf. New Trends Inf. Sci. Service Sci. Data Mining (ISSDM)*, 2012.

[46] L. T. Van, A. I. Abhi, J. Kharel, and S. Y. Shin, "A social Internet of Things (SIoT) based traffic information sharing system," in *Proc. KICS Winter Conf.*, 2018, pp. 322–323.

[47] Y. Kim and K.-G. Doh, "Quantitative trust management to support QoS-aware service selection in service-oriented environments," in *Proc. Int. Conf. Parallel Distrib. Syst.*, Dec. 2013, pp. 504–509.

[48] X. Li, H. Liang, and X. Zhang, "Trust based service selection in cloud computing environment," *Int. J. Smart Home*, vol. 10, no. 11, pp. 39–50, Nov. 2016.

[49] Y. Wang, J. Wen, W. Zhou, and F. Luo, "A novel dynamic cloud service trust evaluation model in cloud computing," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Communications/ 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 10–15.

[50] T. Aamir, H. Dong, and A. Bouguettaya, "Trust in social-sensor cloud service," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jul. 2018, pp. 359–362.

[51] Y. Wang, S. Chandrasekhar, M. Singhal, and J. Ma, "A limited-trust capacity model for mitigating threats of internal malicious services in cloud computing," *Cluster Comput.*, vol. 19, no. 2, pp. 647–662, Jun. 2016.

[52] S. Ahmad and J. Zhang, "Network-state-aware quality of service provisioning for the Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 6, pp. 369–376, 2016.

[53] M. Ruef, "Strong ties, weak ties and islands: Structural and cultural predictors of organizational innovation," *Ind. Corporate Change*, vol. 11, no. 3, pp. 427–449, Jun. 2002.

[54] J. Chirife, M. Sansiñena, M. V. Galmarini, and M. C. Zamora, "Physicochemical changes and sensory characterization of a balsamic vinegar dressing at different Brix," *Food Bioprocess Technol.*, vol. 4, no. 8, pp. 1505–1511, Nov. 2011.

[55] R. Ashri, S. D. Ramchurn, J. Sabater, M. Luck, and N. R. Jennings, "Trust evaluation through relationship analysis," in *Proc. 4th Int. Joint Conf. Auto. Agents Multiagent Syst. (AAMAS)*, 2005, p. 1005.

[56] H. Ride. (2018). *DataHealthy Ride Pittsburgh*. Accessed: Nov. 17, 2018. [Online]. Available: https://healthyridepgh.com/data/

[57] S.-C. Chu, L. Chen, S. Kumar, S. Kumari, J. P. C. J. Rodrigues, and C.-M. Chen, "Decentralized private information sharing protocol on social networks," *Secur. Commun. Netw.*, vol. 2020, pp. 1–12, Jun. 2020, doi: 10.1155/2020/7137480.

[58] S. Garg, K. Kaur, N. Kumar, and J. J. P. C. Rodrigues, "Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 566–578, Mar. 2019, doi: 10.1109/TMM.2019.2893549.

M. JUNAID ASLAM received the master's degree in software engineering from Bahria University, Islamabad, Pakistan, in April 2019. He worked as a Lab Engineer with Bahria University, Islamabad, for over three years. He has over a year of fresh industrial experience in the field of software development. He is currently working as a full-time freelancer and dealing with some chronic health problems. His research interests include trust management and friendship selection in the Social Internet of Things.

SADIA DIN received the master's degree in computer science from Abasyn University, Islamabad, Pakistan, in 2015, and the Ph.D. degree in data science from Kyungpook National University, South Korea, in 2020. During her Ph.D., she was working on various projects, including artificial learning, machine/deep learning, the Internet of Things, and big data analytics. In 2015, she was a Visiting Researcher with the CCMP Laboratory, Kyungpook National University, where she was working on big data and the Internet of Things. She is currently working as an Assistant Professor with the Department of Information and Communication Engineering, Yeungnam University, South Korea. Previously, she was working as a Postdoctoral Researcher with Kyungpook National University, South Korea, from March 2020 to August 2020. Her research areas include big data, 5G, the IoT, and data science. She has published few highly reputed conferences, such as IEEE LCN, ACM SAC, ICC, GLOBECOM, and some SCIE journal at the beginning of her research career. She was also the Chair of the IEEE International Conference on Local Computer Networks (LCN'18). In IEEE LCN 2017, Singapore, she was the chair of couple of sessions. She is serving as a Guest Editor for a journal in Wiley.

JOEL J. P. C. RODRIGUES (Fellow, IEEE) is currently a Professor with the Federal University of Piauí, Brazil, a Senior Researcher with the Instituto de Telecomunicações, Portugal, and a Collaborator of the Post-Graduation Program on Teleinformatics Engineering at the Federal University of Ceará (UFC), Brazil. He is the Leader of the Next Generation Networks and Applications (NetGNA) research group (CNPq), a Distinguished Lecturer of the IEEE, a Representative Member of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the scientific council at ParkUrbis–Covilhã Science and Technology Park. He has authored or coauthored over 900 articles in refereed international journals and conferences and three books, holds two patents, and one ITU-T Recommendation. He is a member of the Internet Society and a Senior Member of ACM. He had been awarded several Outstanding Leadership and Outstanding Service awards by the IEEE Communications Society and several best papers awards. He has been the general chair and TPC Chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE Healthcom, and IEEE LatinCom. He was the Director of the Conference Development—IEEE ComSoc Board of Governors, the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the Past-Chair of the IEEE ComSoc Technical Committee on eHealth, the Past-Chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee Member of the IEEE Life Sciences Technical Community and the Publications Co-Chair. He is the Editor-in-Chief of the *International Journal of E-Health and Medical Communications* and an editorial board member of several high reputed journals.

AWAIS AHMAD received the master's degree in telecommunication and networking from Kyungpook National University, Daegu, South Korea, and the Ph.D. degree in computer science and engineering from Bahria University, Islamabad, Pakistan. In 2014, he was also a Visiting Researcher with INTEL-NTU, National Taiwan University, Taiwan, where he was working on Wukong Project (Smart Home). He is currently working as a Senior Researcher with the Dipartmento di Informatica, Università Degli Studi di Milano, Milan, Italy. Previously, he was working as an Assistant Professor with the Department of Information and Communication Engineering, Yeungnam University, South Korea. He was also serving as a Lab Admin of CCMP Labs, from 2013 to 2017. Since 2013, he has published more than 130 international journals (Cumulative Impact Factor: more than 150)/conferences/book chapters in various reputed IEEE Transactions, *IEEE Magazines*, ACM Transactions, Elsevier, and Springer journals, whereas in leading conferences, i.e., IEEE GLOBECOM, IEEE INFOCOM, IEEE LCN, and IEEE ICC. His research interests include deep learning, machine learning, artificial intelligence, denoising and demosacking, big data analytics, sensor and ad hoc networks, and the Internet of Things. He was a recipient of four prestigious awards, including the IEEE Best Research Paper Award: International Workshop on Ubiquitous Sensor Systems (UWSS 2015), in conjunction with the Smart World Congress (SWC 2015), Beijing, China, the Research Award from the President of Bahria University, Islamabad, Pakistan, in 2011, the Best Paper Nomination Award in WCECS 2011 at UCLA, USA, and the Best Paper Award in 1st Symposium on CS&E, Moju Resort, South Korea, in 2013. He was also awarded the Best Outgoing Researcher of the CCMP Labs. He is also serving as a guest editor in various Elsevier and Springer journals, including *Future Generation Computer Systems* (Elsevier), *Sustainable Cities and Society* (Elsevier), and *Computational Intelligence and Complexity* (Springer), *Multimedia Tools and Applications* (Springer), IEEE Access, and the *Journal of Real-Time Image Processing* (Springer).

GYU SANG CHOI (Member, IEEE) received the Ph.D. degree in computer science and engineering from Pennsylvania State University. He was a Research Staff Member of the Samsung Advanced Institute of Technology (SAIT), Samsung Electronics Company Ltd., from 2006 to 2009. Since 2009, he has been with Yeungnam University, where he is currently a Professor. His research interests include data mining, deep learning, and parallel computing, while his prior research has been mainly focused on improving the performance of clusters. He is a member of ACM.