



Review

# Towards Trust and Friendliness Approaches in the Social Internet of Things

Farhan Amin <sup>1</sup>, Awais Ahmad <sup>2</sup> and Gyu Sang Choi <sup>1,\*</sup>

<sup>1</sup> Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 280, Korea; farhan@ynu.ac.kr

<sup>2</sup> Department of Computer Science, Bahria University, Islamabad 44000, Pakistan; aahmad.marwat@gmail.com

\* Correspondence: castchoi@ynu.ac.kr

Received: 27 November 2018; Accepted: 21 December 2018; Published: 4 January 2019



**Abstract:** The Internet of Things (IoT) is an interconnected network of heterogeneous entities, such as sensors and embedded devices. During the current era, a new field of research has emerged, referred to as the social IoT, which mainly includes social networking features. The social IoT refers to devices that are capable of creating interactions with each other to independently achieve a common goal. Based on the structure, the support of numerous applications, and networking services, the social IoT is preferred over the traditional IoT. However, aspects like the roles of users and network navigability are major challenges that provoke users' fears of data disclosure and privacy violations. Thus, it is important to provide reliable data analyses by using trust- and friendliness-based properties. This study was designed because of the limited availability of information in this area. It is a classified catalog of trust- and friendliness-based approaches in the social IoT with important highlights of important constraints, such as scalability, adaptability, and suitable network structures (for instance, human-to-human and human-to-object). In addition, typical concerns like communities of interest and social contacts are discussed in detail, with particular emphasis on friendliness- and trust-based properties, such as service composition, social similarity, and integrated cloud services.

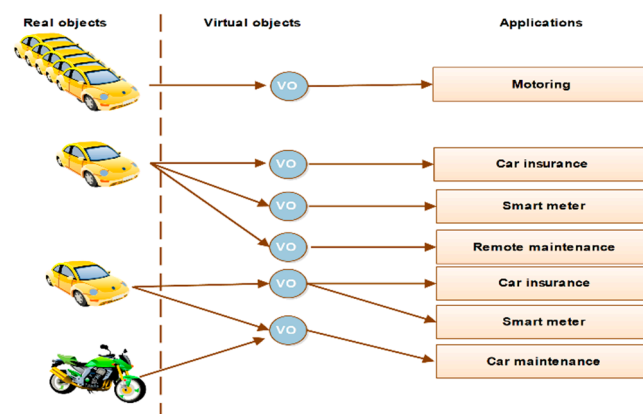
**Keywords:** Internet of Things; trust; social Internet of Things; trust management

## 1. Introduction

One of the most important areas of the future Internet is the Internet of Things (IoT). Generally, physical objects are connected to the Internet using sensors and actuators because they effectively expedite technology advancements in the IoT by providing a number of services [1]. In the IoT, linking various objects is referred to as object–object interconnection. More recently, virtual objects (VOs) stand in for real-world entities as their digital counterparts [2]. They are extensively used in the IoT as a bridge to connect the physical world by providing a digital depiction of data, and they have interesting features that shape real-world objects, including the interactions of users with systems in the IoT [2]. Projects like SENSEI [3], Future Internet (FIWARE) [4], the Collaborative Open Market to Place Objects at your Service (COMPOSE) [5], and Internet of Things-Architecture (IoT-A) [6] are typical examples.

In Figure 1, cars represent an automobile manufacturing company. Real objects are represented by cars and bikes, and the term virtual object, represents a relationship. Each virtual object is associated with a single car or a number of cars [4]. When a customer needs to buy a car, the virtual object could be used to register the car with an insurance company or to obtain remote maintenance from an automobile manufacturing database. Here, we can perceive a virtual object as being created with more than one association. In addition, if a customer is registered with a single virtual object that can handle

different types of services offered by an automobile manufacturing company, such as car insurance and smart meters, the concept of the many-to-many association appears.



**Figure 1.** Virtual objects interacting in the Internet of Things (IoT).

In the IoT, data collection and scalability are major concerns [5]. First of all, data collection by using VOs is a fairly challenging task. In the real world, the IoT-based infrastructure has hundreds of millions of devices that can connect to each other over the Internet, which makes things quite complicated. To encompass humans in this context is a reasonable means to overcoming the complexity, because data collection and monitoring via the IoT is identical to a human's social life. Once data collection is completed after processing, analysis, and mining, the acquired data can provide diverse intelligent services. However, from the perspective of scalability, it has been observed that IoT search engines are not scalable with respect to the number of devices [7], and hence, cannot handle a huge number of received queries. In the IoT, there exists the possibility of fake objects, such as people who cannot get the right services, and objects may work as malware, hacking data from other objects. The attacker nodes in that network include smart dust and fake particles that can steal secure information concerning military situations (e.g., at the border of a country) [7]. In order to avoid such problems, the social Internet of Things proposes the integration of social networking and the IoT.

In the social IoT, objects can make any number of friends (other objects) as factual objects to get the right services. This advantage makes the social IoT superior to the IoT. The relationship between friends and friends of friends is established using a relationship query. Here, relations among diverse people are developed that are truly based on their social interests, real-life relations, similarity of background, etc. Finally, as explained by Militano [8], the social IoT offers efficient and scalable discovery of objects and services by using human social network principles. Additionally, the social IoT not only provides a facility towards better network navigation, but it is also useful in a finding various tasks. Thus, an object can correctly discover various services, and can effectively perform a number of tasks, the same as a human can [9]. These tasks are performed based on the specific trust level between people, or sometimes, friends. Hence, the trust level among the devices can be increased exponentially when friends (IoT devices) interact with each other. This phenomenon was discussed by Rabadiya, Makwana [7] and Atzori, Iera [10], among others, in earlier studies.

The purpose of this study is to address the above-stated problems by classifying friendliness- and trust-based approaches in the social IoT. Trust among peers in the IoT and friendliness using service discovery have been widely investigated in the past. However, this is a recent trend for researchers in the social IoT. Therefore, we present the following contributions to the research community for the social IoT.

- In this study, the social IoT, its notations, definitions, the necessity for the social IoT, the basic concept of trust, the properties of trust, and its models (including constraints, such as scalability and adaptability) are explained.

- A classified catalog of friendliness and trust is described, based on survey studies over the past six years.
- Each study regarding friendliness and trust in the social IoT is described, with suitable examples.
- Critical problems and challenges, such as integrated cloud services with trust, social contacts, and friendliness-based service composition in designing better solutions for the social IoT, are investigated.

Overall, this study is organized as follows. In Section 2, social network definitions and concepts, the social cloud, its structural models, and crowdsourcing are explained in detail. In Section 3, the definition of trust and friendliness, their basic properties, and the state of the art in peer-to-peer (P2P) and client/server-based networks in the social IoT are described in detail. In Section 4, the catalog of trust- and friendliness-based approaches in the social IoT is explained. Open discussion, future work, and further research directions are discussed in Section 5. Finally, Section 6 is the conclusion to our research.

## 2. The Social IoT Paradigm

### 2.1. Social Network Definition and Concepts

The social IoT is defined as an IoT where things are autonomously capable of establishing relationships with other objects related to humans [11]. Generally, the social IoT signifies an ecosystem that allows people and smart objects to interact within a social structure based on relationships [8]. The social ecosystem is illustrated in Figure 2. In this figure, a social network adjoining an individual or organization favors acquiring diverse information. Afterward, the collected information (big data) becomes an intelligent service through the process of sophisticated interference [8].

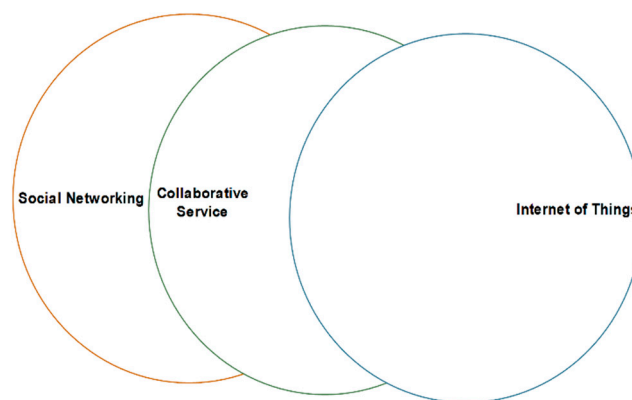
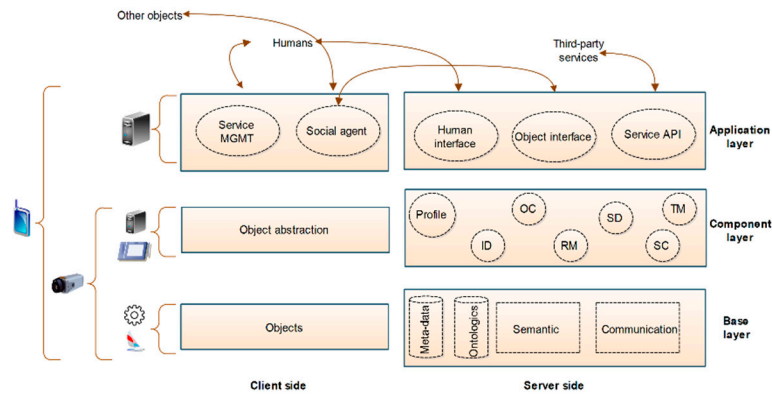


Figure 2. The social IoT paradigm.

Currently, there exists a driving motivation for researchers to study the social IoT, because it has the potential to discover different features, including service composition and object discovery [12]. Additionally, it can be used to distribute the environment in order to access services from the real world using sensor [1,13].

We refer readers to a recent social IoT-based model suggested by Nitti, Atzori [14]. In this model, the authors proposed a possible approach to solving various issues, like service discovery and composition. They introduced a novel paradigm comprised of three main layers: the base layer, the component layer, and the application layer, as described in Figure 3 Nitti, Atzori [14]. The base layer includes services for databases, semantic engines, and communication. The component layer is used as a host tool for satellite component implementation, and the application layer acts as an interface between objects and humans. This layer is used to provide connection services. On the left-hand side, the client is divided into a further three layers: objects, object abstractions, and social agents. The objects layer is comprised of physical objects. The object abstractions layer acts as an

interface between the attached devices. This interface is controlled by common languages. The third layer is comprised of a number of agents, and its function is to make connections between attached objects and social IoT-based servers. Service management provides two services: one is an interface and the second monitors and controls the behavior of objects. This architecture provides a basic building block for the entire social IoT domain.

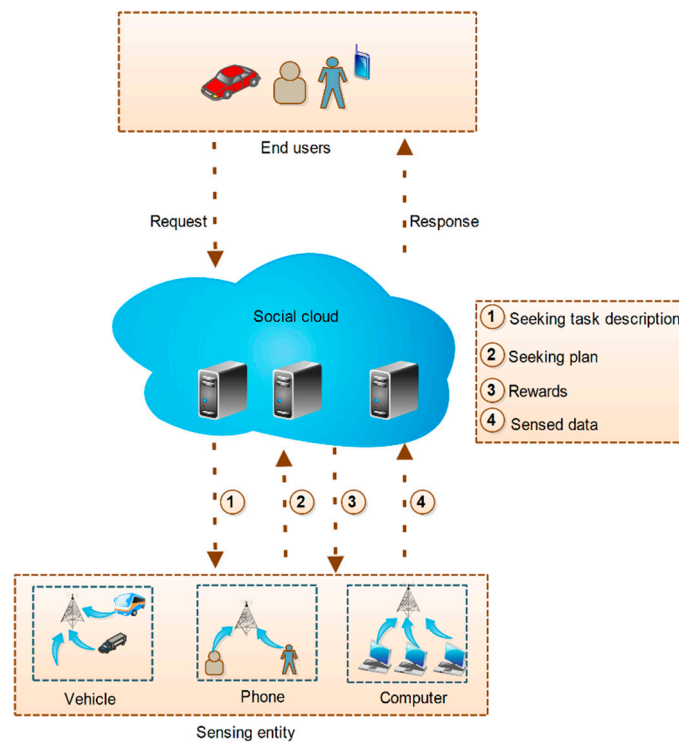


**Figure 3.** The basic architecture for the social Internet of Things (SIoT).

## 2.2. The Social IoT and the Cloud

The evolution of the IoT is transforming our lives into cyber-physical-social-hyperspace layers [15]. The social cloud is closely related to the social IoT, and possibly improves resource sharing in social networks. The social cloud plays a pivotal role in various areas, including software crowdsourcing, where it serves as a shared infrastructure. Another example is a social cloud-supported approach that helps to reduce communication breakdowns due to asymmetries in media and the time preferences among family members of different age groups [15]. Crowdsourcing is the act of taking a job that is traditionally performed by a designated agent (usually an employee) and outsourcing it. Generally, it describes a large group of people in the form of an open call.

Figure 4 explains the general scenario of crowdsourcing used in the social IoT. It comprises three entities: the social cloud, end users, and sensing [16]. Here, the sensing entity holds various types of data, e.g., vehicles, phone users, and computer data. The social cloud is used to process the data complying to its type. When the end user requests a specific type of data, the steps in providing the requested service are as follows. First of all, the request is processed in a social cloud according to a specific sequence of instructions. Afterward, the request is sent to the sensing entity, which forwards this request to the social cloud. Finally, it will be sent again as feedback to the end user. This scenario describes the structure of a social IoT-based network.



**Figure 4.** Model of crowdsourcing in the social IoT.

### 2.3. The Social IoT and Multiagents

The concept of the multiagent system (MAS) is not a new one in the IoT. It has been investigated in the literature for a few years. According to one study [17], it is a group of systems that are connected to each other by using agents. There are so many systems that are already using a P2P file-sharing system, crowdsourcing (as described in Section 2), and e-commerce platforms. These can be modeled as an open, dynamic MAS [18]. This research has been conducted by numerous researchers, and hence, they concluded that MASs are always boosted by using artificial intelligence (AI) and its relevance to emerging technologies [17]. In association with social networks, it is a high-level abstraction for capturing the social relationships among the different agents. These agents can be represented as a human being or as software entities [18]. These networks are called open because they can come from any background, and in addition, they have heterogeneous abilities for organizational affiliations and credentials, etc. [18]. These agents are sometimes deemed to have dynamic behavior because their decision-making processes are independent of each other and they can leave or join the system at will. Usually, the agents face QoS issues due to their limited capabilities. They may need to rely on resources from other agents in order to accomplish their goals. If the agents cannot offer the required QoS or resources, their decisions may not be trustworthy, and may involve a certain level of risk. In this case, the IoT agent needs to rely on another agent, called a trustor agent. Those agents who can received the resources from the trustor agent are called trustee agents [18].

### 2.4. The Social IoT and Cluster-Based IoT Nodes

IoT-based applications usually rely on machine-to-machine (M2M) communications [19], such as a smart grid or smart meter. In these applications, objects usually use point-to-point connections for communications, and a unique, embedded hardware module is also required to connect tiny devices. The advantage of M2M communications is to provide good connectivity among a large number of low-cost devices with the least amount of human intervention, or no intervention [19]. According to recent survey statistics, more than 100 billion IoT devices are connected worldwide. By 2025, that number will increase (i.e., an addition of more than US\$11 trillion [20]). Due to the huge number of

connected devices, energy efficiency and wireless access congestion issues arise [19]. In order to solve these problems in parallel, and improve energy efficiency, numerous joint clustering schemes have been proposed. These methods are mainly based on resource management and the interconnection of devices [20], according to a recent study [19]. Numerous M2M methods have been proposed in the past and are based on different criteria, such as M2M-achievable signal-to-interference-plus-noise ratio. There are few studies in which a scheme is handled by using priority [19]. Data priority and the proposing of energy-efficient congestion-based methods are mitigated by using various clustering algorithms. These algorithms introduce various ways to enhance energy conservation issues [19].

Data priority is the flow of data from specific M2M devices. The transmitted and collected data have a higher priority. The joint consideration of clustering formation and power demonstrates better results. Tsiropoulou et al. [19] discussed an energy, interest, and physical aware-based framework for coalition formation and resource distribution among wireless IoT applications [19]. In their proposed framework they assigned a holistic utility-based function to various IoT devices. This framework is divided into two stages. In the first stage, a coalition head will be determined for each coalition in a time-based slot. In the second stage, QoS prerequisites of M2M devices are formulated via holistic utility functions. The authors simulated numerical results and found the framework to be an energy-efficient approach that can be used for the coordination of various devices. Similar work was investigated by Tsiropoulou and Eirini et al. in [20]. In this study, a number of M2M devices are initialized from different clusters based on a low-complexity Chinese restaurant process (CRP). Afterwards, a cluster head is elected from among the members of each cluster. The contribution of this study is to select a cluster head. The selected cluster head can harvest and store energy in a stable manner. The authors used RF signals by adopting the wireless powered communication (WPC) paradigm. Finally, it is good to prolong the operation of the network [20]. Lin et al. [21] demonstrated an adaptive self-organizing multihop cluster-based approach for mobile wireless networks. The radio network relies on a code-division multiple access (CDMA)-based scheme and has a multimedia support. The nodes are organized into a number of nonoverlapping clusters. The clusters are formed independently so they can be controlled and reconfigured dynamically (nodes can even move easily) [20]. Gerla et al. [22] proposed a heuristic routing strategy by using a fading channel for cluster-based multihop mobile wireless networks. Usually, frequent change of a cluster head will affect the performance of various scheduling allocation protocols. So in order to tackle this problem, the authors designed the least cluster change (LCC) algorithm. This framework has two conditions. In the first, two cluster heads come within range of each other; the second might be only when the nodes become disconnected from any other cluster. The advantage of this algorithm is to provide faster delivery of packets, and it uses cluster head token scheduling. In token-based scheduling, gateway-node scheduling speeds up packet delivery along multihop paths [21]. Table 1 describes the abbreviations that we have used throughout the paper. In Table 2, we compare various cluster-based classification frameworks. These are based on various parameters, such as energy-efficiency, privacy throughput, and security. In these frameworks, we observed that the authors try to provide highly energy-efficient algorithms, and hence, the throughput of the network is definitely increased. We observed after reviewing the research, that most authors have not discussed security and privacy paradigms. Hence, none of the above-discussed cluster head selection algorithms are secure. In Table 3, we offer a brief comparative evaluation by using some recent studies.



**Table 1.** List of abbreviations.

Abbreviation	Expansion
COI	Community of interest
C-LOR	Co-location object relationship
C-WOR	Co-work object relationship
DDL	Device Description Language
F	Flooding
DHT	Distributed hash table
IoT	Internet of Things
IoT-A	Internet of Things-Architecture
MANET	Mobile ad hoc network
M2M	Machine-to-machine communications
OOR	Object ownership relationship
P2P	Peer-to-peer
PD	Probability distribution
PTO	Pretrusted object
POR	Parental object relationship
QoS	Quality of service
RM	Relationship management
SNS	Social networking service
SDP	Service discovery protocol
SoC	Social cloud
SOR	Social object relationship
TM	Trustworthiness management
TFA	Trustworthiness-based flooding
VO	Virtual object
WSN	Wireless sensor network

**Table 2.** Cluster-based frameworks classification.

Paper	Advantages	Disadvantages
Tsiropoulou, Paruchuri [19]	<ul style="list-style-type: none"> <li>This framework is effective and energy-efficient for a group of M2M devices, because this method will allocate the resources in an energy-efficient manner; hence, it will be helpful in prolonging of battery life of M2M devices. Finally, the throughput is increased.</li> </ul>	<ul style="list-style-type: none"> <li>There is no security or privacy-based criteria proposed in this framework.</li> </ul>
Tsiropoulou, Mitsis [20]	<ul style="list-style-type: none"> <li>Due to the use of Nash equilibrium, the optimal charging transmission power of a cluster head is derived.</li> <li>This method is energy-efficient for cluster heads; hence, it will be a good framework that is used to increase overall network throughput.</li> </ul>	<ul style="list-style-type: none"> <li>There is no real test bed used in this framework.</li> <li>There is no discussion related to a security paradigm.</li> </ul>
Lin and Gerla [21]	<ul style="list-style-type: none"> <li>This network architecture proposes three advantages, the first is to provide spatial reuse of the bandwidth due to high node clustering.</li> <li>The bandwidth can be shared or reserved in a controlled fashion in each cluster.</li> <li>The cluster algorithm is robust in the face of topological changes caused by node motion, node failure, and node insertion or removal.</li> <li>Throughput is increased.</li> </ul>	<ul style="list-style-type: none"> <li>In this network architecture, there is no security or privacy paradigm discussed.</li> </ul>
Gerla [22]	<ul style="list-style-type: none"> <li>Throughput and energy efficiency is achieved by using radio channel access, code scheduling, and channel variation.</li> <li>The runtime is reduced by using the design of a parallel simulator.</li> </ul>	<ul style="list-style-type: none"> <li>There is no real test bed used for the evaluation of this framework.</li> <li>There is no security or privacy criteria proposed in this framework.</li> </ul>

**Table 3.** Indicative and comparative evaluation of current studies.

<b>Friendliness- and Trust-Based Approaches for SIoT</b>	<b>Description</b>	<b>Features</b>	<b>Issues/Lacking</b>
A Survey of Trust Computation Models for Service Management in Internet of Things System [23]	<ul style="list-style-type: none"> <li>Classification is performed based on earlier trust models such as trust propagation, trust aggregation, trust update, and trust formation.</li> </ul>	<ul style="list-style-type: none"> <li>This study highlights the services providing paradigm in IoT.</li> <li>It identifies various research gaps that are helpful for IoT system designers.</li> </ul>	<ul style="list-style-type: none"> <li>No information is available regarding to friendliness-based Trust properties, such as service search, service model, etc.</li> </ul>
Trust-Based Service Management for Social Internet of Things Systems [24]	<ul style="list-style-type: none"> <li>A unique trust model is proposed based on fuzzy logic.</li> </ul>	<ul style="list-style-type: none"> <li>This study ensure QoS and delivery ratio.</li> <li>Consumed energy between sensors (which allowed people to compute the trust level among social networks) is calculated.</li> </ul>	<ul style="list-style-type: none"> <li>Friendliness based properties such as centralized and distributed service search are still missing.</li> </ul>
Trustworthiness Management in the Social Internet of Things [1]	<ul style="list-style-type: none"> <li>The purpose of this study is to address the uncertainty and to suggest various strategies in order to establish trustworthiness among nodes.</li> </ul>	<ul style="list-style-type: none"> <li>This strategy is effective for any malicious nodes in a network.</li> </ul>	<ul style="list-style-type: none"> <li>The only difficulty is with a static or fixed topology. Hence, trust cannot dynamically adapt to the change in topology.</li> </ul>

### 2.5. The Social IoT and Industry 4.0

Industry 4.0 is a technological revolution in logistics and manufacturing systems [25], referred to as the automation of industries. The concept of the IoT is largely being discussed in the past, and it acts as a major approach towards industry 4.0. We already know that a large amount of data is generated by social networks. So, the integration of social media and the IoT is witnessed in various areas, such as traffic routing and product design. [25]. However, the potential of industry 4.0 has rarely been explored [25]. Industry 4.0 is a great revolution because it enables people to prepare and implement smart production for logistics in the IoT. Logistics plays an important role in manufacturing, such as providing various services for the manufacturing supply chain and service. Seven rules for logistics are widely used: the right product, in the right quantity, at the right quality, in the right place, at the right time, and at the right cost for the right customers [26]. The available traditional solutions for logistics use exponential technologies [26], and hence, they cannot prepare smart products. Additionally, the complexity of the supply chain process related to hyperconnected global supply requires up-to-date methods and convenient parameters for the operation of processes. Researchers are still working on it, and are trying to find a near optimal solution (i.e., industry 4.0). Juhasz and Bányaí [26] identified a few challenges from current studies on the consequences of supply in the automotive industry from the aspect of industry 4.0. In addition, they derived four models that are identified in the current literature. These four models are used in optimization and only in the sequences of the supply chain between two tiers related to cost. However, these proposed models use direct and indirect supply and sequencing, with or without horizontal cooperation. Li and Parlikad [25] discussed a sensible solution for the improvement of system-level performance in industrial production plants by integrating the social IoT (SIoT). They proposed an industrial-system performance management infrastructure model that is used for the cooperation of assets (by the sharing of status data), and operation management is done by sharing machine data [26]. Banyaie et al. [27] discussed a smart scheduling solution by using supply chain management for industry 4.0. This research model proposed an integrated supply model for Federation of Malaysian Manufacturers (FMM) delivery [27]. Moreover, this methodological model is used for real-time smart scheduling of assignments for first-mile and last-mile delivery tasks used by delivery companies. They solved a smart scheduling problem by proposing a newly developed



metaheuristic algorithm [27]. Table 4 compares some studies related to industry 4.0 and the IoT. In this table, we have identified some industry 4.0 technological objectives: supply chain coordination, embedded systems, and automation. The framework implementation is performed by using a testbed, a simulation, or a case study. The enterprise type demonstrates the organization size feasible for either small-scale or large-scale organizations. Finally, the area of optimization is based on assets (the term used in the industrial Internet of Things (IIoT) or production (the term used in industry 4.0).

**Table 4.** Comparison of studies related to industry 4.0 and the IoT.

Study	Industry 4.0 and the IoT			
	Technological objective	Implementation	Enterprise type	Area of optimization
Social Internet of Industrial Things for Industrial and Manufacturing Assets [25]	Supply chain applications	Case study	Good for small-scale	Assets
What Industry 4.0 Means for Just-In-Sequence Supply in the Automotive Industry [26]	Supply chain applications	Case study	Ideal for small-scale and medium-sized enterprises	Production
Smart Scheduling: An Integrated First-Mile and Last-Mile Supply Approach [27]	Supply chain applications	Benchmark and numerical simulation	Good for large-scale	Production

### 3. Trust and Friendliness in the Social IoT

The concept of trust is not new: it has frequently been studied in numerous disciplines, including psychology and the computer sciences [28]. It remains very hard to keep to a precise discussion regarding the concept of trust. This is due to its extensive use in different dimensions and disciplines. Before building trust, the trustor and trustee agree with each other on matters like time, location, activity, etc. There are some key properties of trust, in general, including transitivity, comparability, personalization, and asymmetry. A general example of using trust is explained in Figure 5. If a person named Alice trusts her friend Bob, and Bob trusts his friend Carol, then it means Alice can trust Carol. Transitivity or transitivity relations have remained the most significant and controversial phenomenon in the past. This is the ability to trust someone who is not directly known [1]. In real life, we can say that trust is not always transitive, and it mainly depends on the particular service that was requested earlier [29]. Computability is a reference point for trust components, and is the ability to compose trust for different people [30]. In conclusion, trust composability is the power to make a decision for people. Keeping this fact in mind, when we assign different values to different friends, there exists a need for a composition function that provides a service. The benefit of the composition function is to increase the accuracy of the results that are populated during the computation. People in a social IoT environment always remain careful, but doubtful, because they are always worried about their privacy and the disclosure of confidential data [31].

Figure 6 demonstrates an ideal conceptual trust-based model for social networks. In this model, trust will be attained by making a connection between trustors (who behave in a particular way under the environmental conditions) and trustees. This procedure is called harmonization [32]. Usually, harmonization is achieved by accumulation, and an observation is made by trustors about trustees. The environmental conditions between two parties (for either the trustee or the trustor) are considered risks that are taken during each interaction and observation. The trustor's authority is not limited to handling the requirements of the trustor's preference and to the trust of the trustee [32]. In this case, environmental conditions, such as threats and risks, remain topmost concerns. Friendliness is another property, and it is used to find neighbor objects by making social relationships among them. The social IoT model explained in Nitti, Atzori [14], states that every node in a network is an object, and it is capable of establishing a social relationship with other objects according to rules set by the owners [33]. There are several types of relationship, given as follows.

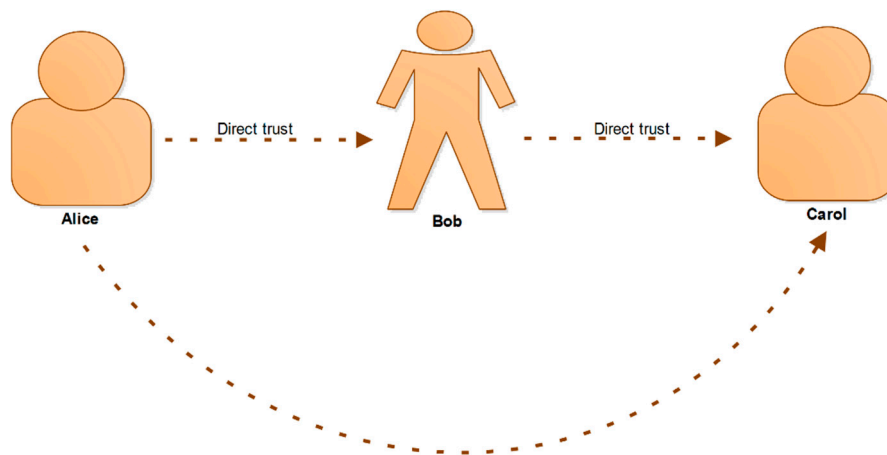


Figure 5. Basic trust mechanism.

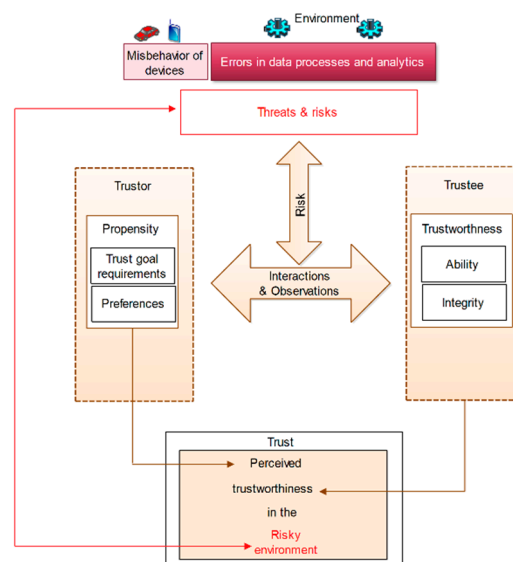


Figure 6. Conceptual trust model in the social IoT.

**Object ownership relationship (OOR):** this kind of relationship is created among objects that belong to the same owner (for example, it occurs between smart devices of the same user, such as a smartphone and a laptop).

**Co-location object relationship (C-LOR):** the relationship exists when fixed devices are located in the same place, and moreover, is established among both heterogeneous and homogeneous objects (for example, sensors and actuators, like smart devices, have short links because they are unlikely to cooperate towards a common goal).

**Parental object relationship (POR):** these objects are created by the same owner or producer, and this relationship is mostly established among homogeneous objects (i.e., the same-generation devices made by the same manufacturer).

**Co-work object relationship (C-WOR):** this is established between single or multiple devices where functionality is combined to accomplish a common goal.

**Social object relationship (SOR):** this is a created consequence of frequent meetings between objects, and usually, the objects come into contact due to owner relations (smart objects belonging to a friend's coworker and to classmates could establish this type of relationship). The relationships between objects in a social network and a complex network are established by using network navigability.

Based on the above discussion, one can observe that trust and friendliness in the social IoT are very important. The difficulty is only one of ensuring reliable data analysis and qualified services

that can be used to enhance user services [31]. Moreover, current user demands to make a fear-free platform using trust and friendliness promote user acceptance of future IoT services and solutions.

### 3.1. Current State of the ART in Peer-To-Peer and Client/Server Networks

The underlying ideas of friendliness are trust and using local information about an object, finding another object for a specific service in a distributed way [14]. There are only a few studies about trust in the IoT and the social IoT. A recent study [34] addressed the link selection method in the social IoT. In this method, objects make friendliness-based connections to other objects by using links. The first step in this study was to analyze network navigation by using a simulation. They tried to find service discovery among objects, aiming to find the number of connections on the basis of the available number of hubs in the network. A similar effort was made in an attempt to find a way towards an exchange of information between members with feasibility based on trust [1]. Those authors proposed subjective and objective approaches to address the problem. Both of these approaches provide a future for both P2P and social networks. In objective-based trustworthiness, information regarding the network is centric. The trustworthiness value is stored in a special type of table called a distributed hash table (DHT). The network information is managed by a distinctive type of object, referred to as a pretrusted object (PTO). Subjective trustworthiness is local because it is accessed and updated on its own or by friends [1]. The difficulty in this study is choosing a static or a fixed topology. This means that trust cannot dynamically adapt to change [34]. A similar type of study suggested a trust-based model based mainly on fuzzy logic that is only suitable for IoT-based systems [24]. Here, quality of service was considered, including delivery ratio, measurement of packet ratio (forward and delivery), and consumed energy between sensors, which allowed people to compute the trust level among social networks and boost the level of social relationships among owners and devices [24]. Saied et al. [35] suggested a scheme that is fully based on security. This scheme works as a shield against attacks. They provided context-aware and multiservice-based features for the IoT. However, their method was based on only centralized servers. These servers are used for gathering and dissemination of trust data [34] among peers. This type of feature is not available in the IoT environment. The integration of QoS and social trust was described by Bao and Chen [36]. In their study, two recommendation systems including direct and indirect trust were proposed. Both of these are used to update the trust value. The trust evaluation and response in the case of dynamically changing conditions was a real challenge in this investigation. Moreover, dealing with misbehaving nodes in a dynamic network and increasing the performance of trust-based applications were not addressed.

### 3.2. Current State-Of-The-Art in the Social IoT

Zhou and Chao [37] explained an interesting media-based traffic security system for the IoT. They designed a system based on multimedia classification, and finally proposed a traffic security architecture. The aim of this study was to obtain various features, including flexibility and efficiency. During a review of this study, it was noticed that a direct recommendation for observation was considered with no information on an indirect recommendation.

Based on this safety and security discussion, Chen and Helal [38] anticipated a new security-based system for the IoT. In their investigation, a device description language (DDL)-based system was designed. The DDL language was employed because one can easily specify safety constraints and related knowledge. However, this scheme is more suitable for actuators and sensors that are used in the IoT. The authors did not consider the social relationships among devices and owners.

Liu, Wang [39] suggested a taxonomy for online social networks that is divided into three generations, classifying a separate method for trust-based relations in each generation. In the first generation, weak sociality features exist whereby people in that generation cannot make new friends or make new friends from friends of a friend, referring to an “implicit generation problem”. The second generation is based on the medium of sociality and the binary numbers (0, 1), which indicate if someone is your friend or not. In this type of relationship, participants are allowed to increase their relationships

by choosing from a list, or by adding friends or friends of friends. One can do that if one stays in the same social network. Lastly, the third generation is quite diverse, compared to the others, whereby different types of relationship exist amongst the nodes. People easily create a relationship through different social networks. Furthermore, this generation allows a user to make a new relationship based on trust [40].

In Table 5, a summary of research work over the past six years is presented. Table 6 compares several current studies by considering the relationships between humans and objects. Abdelghani, Zayani [28] reported a survey based on the importance of trust. During this survey, a few basic concepts and trust-based properties are explained, including different trust notations and related concepts. Trust-related attacks with citations, including some unresolved issues, are also mentioned during the survey. However, a complete classification of surveys based on the various trust properties, such as distributed and centralized search, is not explained. Suryani et al. [41] conducted a brief study on trust-based methods. They grouped different studies based on dynamics and periodic and hierarchical features. Their objective was to discover the latest trust assessment methods in the IoT. According to investigators, this study provides a better method of trust assessment in the IoT domain; however, they did not consider service search metrics (centralized, distributed, etc.). These two different types of search metrics will be discussed in detail later.

Yan, Zhang [42] investigated the properties of trust (centralized and distributed). In the investigation, various trust properties that affect the relationships between objects were explored. The relationships were classified into five categories, and the authors suggested a real model in order to achieve trust in the IoT. This module is comprised of several layers, including interlayers and cross-layers. The novel contribution from this study is establishing trust-based relationships. It can be used in a practical way by providing intelligent services. Guo et al. [23] classified trust-based models, especially for providing services in the IoT. This classification is mainly based on earlier trust models, like trust propagation, trust aggregation, trust updates, and trust formation. They summarized current studies based on insight into trust computation for the IoT. They clearly summarized the pros and cons of each study by highlighting the effectiveness of any attacks. Finally, different research gaps were identified by using trust composition, trust propagation, and trust aggregation. These research gaps are helpful to IoT system designers, especially in designing support for future applications.

Table 7 portrays the social IoT constraints in terms of scalability, adaptability, power efficiency, and survivability. In this table, a comparison of different studies (in descending order) is presented with an aim to identifying the most scalable network covered by various authors. Based on the comparison, Yan et al. [42] discussed power efficiency, but they did not discuss the rest of the constraints, such as scalability and adaptability, etc.

**Table 5.** Summary of current studies. (✓: Check mark symbol).

Table 1: Comparison of Trust Aggregation Methods												
Studies	Year	Friendliness						Trust				
		Service Composition		Service Search		Service Model		Trust Aggregation			Trust Update	
		Direct	Indirect	Centralized	Distributed	Subjective	Objective	Bayesian Systems	Belief Theory	Dynamic Weighted Sum	Event-Driven	Time-Driven
Our study	2018	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Guo, Chen [23]	2017	✓	✓	-	-	-	-	✓	✓	✓	✓	✓
Chen, Bao [24]	2016	✓	✓	-	-			-	-	-	-	-
Abdelghani, Zayani [28]	2016	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Nitti, Atzori [14]	2015	✓	✓	-	-			-	-	-	-	-
Nitti, Girau [1]	2014	✓	-	✓	✓	✓	✓	-	✓	✓	-	-
Yan, Zhang [42]	2014	✓	-	-	-			-	-	-	-	-

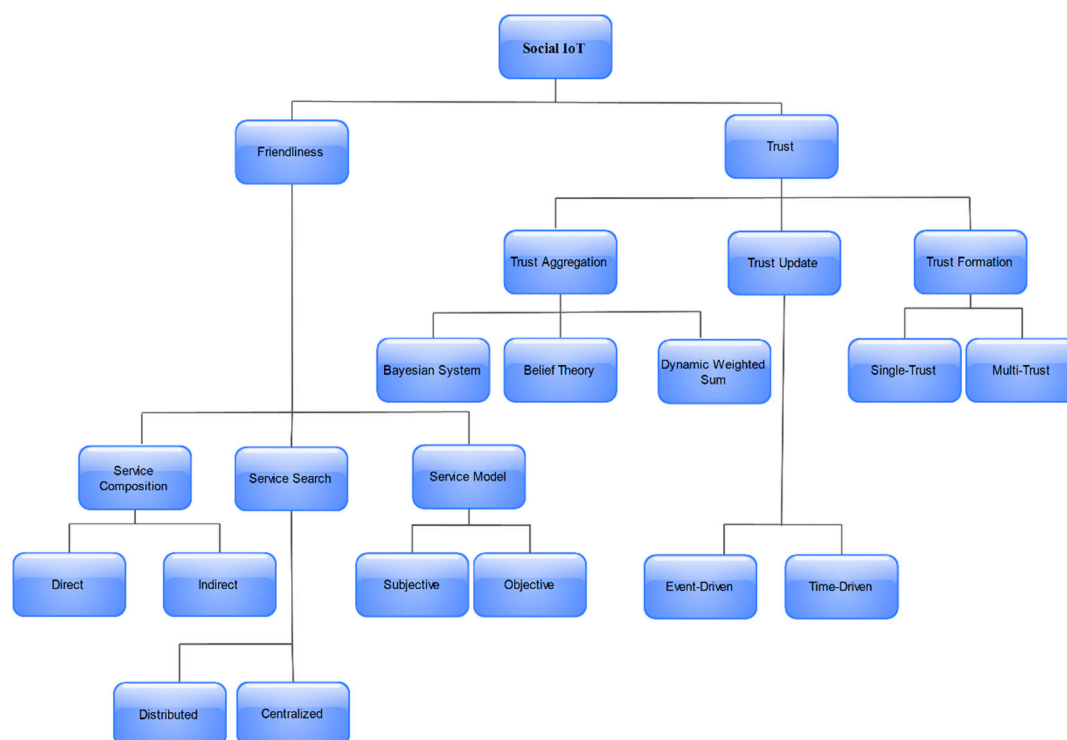
**Table 6.** Network structure-based classification. (X: NO).

Research Work	Relations between Humans	Relations between Objects
Chen, Bao [24]	X	✓
Nitti, Atzori [14]	X	✓
Ben Saied, OLIVEREAU [35]	X	✓
Chen, Chang [34]	X	✓

**Table 7.** Basic social IoT constraints. (✓: Check mark symbol).

Research Work	Year	Scalability	Adaptability	Power Efficiency	Survivability	Resiliency
Chen, Bao [24]	2016	✓	-	-	-	-
Nitti, Girau [1]	2014	✓	-	-	✓	-
Yan, Zhang [42]	2014	-	-	✓	-	-

Figure 7 describes the classified catalog of trust- and friendliness-based approaches in the social IoT.

**Figure 7.** Friendliness- and trust-based network classification in the social IoT.

In Table 5, a summary of research work over the past six years is presented. Chen et al. [24] discussed some friendliness-based properties, such as service composition; however, trust-based properties such as trust aggregation and trust updates, etc., were not highlighted. Similarly, Guo, Chen [23] populated various trust properties, yet no information is available regarding friendliness-based properties. To the best of our knowledge, and as depicted in Table 5, no other surveys considered various trust- and friendliness-based properties together.



#### 4. Classification of Trust- and Friendliness-Based Approaches in the Social IoT

The classified catalogs of friendliness and trust are described in Figure 7. Friendliness is further classified into service composition, service search, and the service model. Service composition class is divided into direct and indirect services. The service search class is divided into distributed and centralized searches. Finally, the service model class is split into subjective- and objective-level groups. Trust is classified into trust aggregation, trust update, and trust formation. Trust aggregation has three groups: Bayesian systems, belief theory, and dynamically-weighted sum. Trust update is classified into event-based and time-driven approaches. Finally, trust formation is classified into single trust and multi-trust.

##### 4.1. Service Composition

To find a service in a network, a service discovery protocol (SDP) is usually used. Service composition is learned through interaction itself or other friend-experienced self-observations. The service composition class is then further divided into direct and indirect services.

##### Direct and Indirect Service Composition

Direct service composition is a collection of honesty, community-interest, and cooperativeness values, which are assigned by node  $i$  to node  $j$ , mainly based on direct observation and interaction between the two nodes [28]. This is generally referred to as direct composition. Indirect service composition is collected through feedback from friends or someone's recommendations. If the two nodes have never interacted in the past, node  $i$  will consider indirect trust, which is based on the observations and past experiences of other connected nodes. Chen et al. [43] used a similar definition in their study by developing a filter scheme for trust management. Their designed scheme is used to combine direct and indirect trust. Moreover, a weighted sum function was designed. This function is used to aggregate trust. In their model, the trustor and trustee do not have any past experiences. Moreover, trust is entirely based on a friend's opinion and can be transitive.

In Abderrahim, Elhdhili [44], the authors proposed a system mainly based on communication interests. The novelty of their work is based on three aspects. First is a set of nodes known as a community of interest (COI). Each set of nodes shares the same type of interest, controlled by the administrator. The second aspect prevents ON/OFF attacks, and the last aspect covers predictions. These aspects are handled by a Kalman filter. The system integrates both direct and indirect trust; however, it is not capable of handling a number of attacks.

##### 4.2. Service Search

As mentioned earlier, thousands of objects in the IoT are connected to each other, and hence, each object looks among its friends for a service provided by another object. This is called a service search.

According to Nitti et al. [14], a service search in the IoT is a challenging task. The motivation of the social IoT is to boost object discovery and the composition of services by objects that have access to the real world [14]. To conduct a service search for objects, a network must be navigable [14]. Kleinberg [45] is one of the famous scientists who have developed, and devoted significant effort to, this topic [14]. He defined it as a feature that is linked to the number of short paths that exist among pairs of nodes in a network [45]. Many studies discussed different formal definitions [46,47], and all of them agree on the fact that, for a network to be navigable, all or most of the paths must be connected. This may happen only if a giant component exists in the network, and there also exists a shortest path between each pair of nodes. These features are necessary for global network navigability; for example, a network selection of paths between node  $i$  and node  $j$  is done by a central node that has information about the entire network structure. In local network navigability, node  $i$  selects next-hop  $k$  on the basis of local information, which is typically related to its adjacent nodes. After that, node  $k$  proceeds with its local information using its own direct contacts, and elects the next-hop node that it considers closest

to node  $j$ . This procedure is known as decentralized search. We will discuss it in the next sections in detail by using various studies and comprehensive examples. According to Kleinberg [45], a network is navigable when it contains a complete connection among all edges, or a network is considered navigable when a giant component exists. The service search class is further divided into distributed search and centralized search.

#### 4.2.1. Distributed Search

The network is navigable when each node has global information about the network Nitti, Atzori [14].

Nitti, Girau [1] discussed a service search problem in the IoT by proposing a distributed system. A possible solution for centralized network navigation was presented during their investigation by proposing five heuristics. These heuristics are completely based on local network properties and are expected to influence the overall network.

Chen, Ling [48] proposed a trust-based approach that contains a number of parameters and factors that may affect security. A timeline property during each cycle was considered, which is used to increase the performance of the system. In order to measure the performance of a system, they conducted a number of simulations, mainly based on rating accuracy, stability in the network, and finally, response rate.

#### 4.2.2. Centralized Search

In this case, nodes post local information about their network. The best example is Facebook: we only know our friends or friends of our friends [14]. A centralized search is based on a central entity, and this might be a virtual trust service designed by an IoT device or in the cloud.

Nitti, Girau [1] introduced a very interesting model using trust. The aim of their work was to provide a service-based model. The investigators individually defined subjective and objective models. In the objective model, trust is implemented by using a DHT. This is a centralized entity that stores the node's trust, feedback, and queries about trust. Moreover, each node in the network can use the same information. While reviewing their work, we noted that the objective model needs pretrusted nodes and a hash table to store values. Therefore, to consider pretrusted nodes in the IoT environment is a question that needs to be addressed appropriately. Saied et al. [35] suggested a trust manager-based model. This model is centralized and has the facility to keep and store trust-based information using IoT devices. Additionally, it has a feature to answer service requests as required.

### 4.3. The Service Model

In a P2P overlay network, two types of model normally exist, including subjective- and objective-based trust models [49]. The P2P systems discussed by Sawamura, Aikebaier [49] are comprised of peer processes. Moreover, during communications, each peer can by itself obtain information regarding objects. The service model class is further divided into subjective- and objective-based models.

#### 4.3.1. Subjective-Based Model

Subjective-based trust is achieved by using direct connections among peers Sawamura, Aikebaier [49]. The focus of the study by Sawamura et al. was to explain the confidence of each peer that can be measured in the duration of communications, their frequency, and their differences. Nitti, Girau [13] explained safe ways to use information amongst users. In their proposed framework, each node is responsible for computing the trust value for friends based on its own information or as recommended by other common friends [13]. A feedback system is provided that is based on credibility and centrality. This concept is used to evaluate the trust value.

#### 4.3.2. Objective-Based Model

The objective-based trust model is a network-centric model Nitti, Girau [1]. The trust value of a node is stored in a DHT. To keep and store the file data, a secure hash algorithm (SHA) is usually used. The structure of the DHT is based on the key space. Each node has a set of keys in order to access the stored data from the DHT.

Sawamura, Barolli [50] proposed a similar model for P2P systems by evaluating several types of protocols, like flooding (F), trustworthiness-based flooding (TFA), etc.

The trust-based approaches in the social IoT are classified into two subcategories based on trust aggregation and trust update.

#### 4.4. Trust Aggregation

To collect valuable trust-based material through experiment is called trust aggregation Abdelghani, Zayani [28]. Moreover, it is based on feedback or self-observation. The trust aggregation model was investigated simultaneously with Bayesian systems, dynamically-weighted sums, and belief theory [2,12]. The details of these diverse models are given below.

##### 4.4.1. Bayesian Systems

According to the probability definition, a random value is considered a trust value that is followed by a probability distribution (PD) Abdelghani, Zayani [28]. Whenever an event happens, its parameter is updated accordingly. As Bayesian systems are fully based on statistical data, they are very popular in computer science and other fields Abdelghani, Zayani [28].

Jøsang [51], introduces a scheme which is based on a random value and calculates a trust range between (0, 1). A beta distribution method was followed, in which the number of all outcomes (including a positive and negative experiment in a single trial) was mapped to parameters (0, 1). The objective of this study was to compute the average trust value. A similar type of study was presented by Ganeriwal, Balzano [52], which used an applied Bayesian system to represent a reputation model. This model was used in a wireless sensor network (WSN) environment. Their objective was to compute the sensor node score by taking binary values, such as (0, 1), including positive/negative input. Their method is applicable to two kinds of attack: ballot stuffing and bad mounting Ganeriwal, Balzano [52].

##### 4.4.2. Belief Theory

The belief theory class is a very popular method for collecting evidence Abdelghani, Zayani [28]. This method is used to measure reasoning and uncertainty in probability theory.

Jøsang [51] proposed a model for subjective logic. This is an opinion-based model. Yu and Singh [53] developed an autonomous system for agents based on the Dempster–Shafer theory [Beynon, Curry [54]]. The main idea in this study was to make a perfect model based on belief, disbelief, and uncertainty. The opinion about specific node  $a$  is denoted with  $(b, d, u, a)$ .

Another study carried out by Suryani, Selo [41] discussed various variables, such as  $b$ ,  $d$ , and  $u$ , representing belief, disbelief, and uncertainty, respectively. The weight,  $b + d + u = 1$ , and assigned weights are sometimes called the base rate. The base rate is calculated based on evidence. In this case, average trust is known as the expected probability, and is calculated by using a mathematical formula, such as  $b + au$ . Finally, subjective parameters can be used separately to combine options, such as discount and consensus value.

##### 4.4.3. Dynamically-Weighted Sums

To calculate aggregate evidence by using weighted sums is now a popular trend [28]. There are many reputation-based systems that aggregate ratings/feedback using weighted sums. On the other hand, raters with a better reputation (i.e., transaction relevance) have a higher weight. There are

numerous methods available that can be used directly to take aggregate feedback by using dynamic weighted sums. In such cases, those with a better reputation have higher weights assigned. Nitti, Girau [1] provided a feedback solution to calculate indirect trust aggregation by assigning reliability as a weight. Chen, Guo [43] used similarity as a weight for indirect trust aggregation. Additionally, direct and indirect trust properties were employed. The assigned weights can dynamically adjust themselves during the early design phase.

#### 4.5. Trust Update

If the trust value is updated, it will be affected. There are two classes: event-driven and time-driven.

##### 4.5.1. Event-Driven Approaches

In this method, after an event has occurred, the trusted data for a node are updated accordingly. This phenomenon was described by Abdelghani, Zayani [28]. Whenever a service is requested, feedback regarding the service quality is sent to the trust manager in the cloud. This kind of environment is called the encounter-based environment because the recommendations can be sent upon receiving the request.

Ben Saied, OLIVEREAU [35] suggested a trust manager for centralized environments. This trust manager is capable of keeping a record of trust-based information for IoT devices. Their system is intelligent because it automatically selects an IoT device to answer a service request. Xiao, Sidhu [55] discussed a model mainly based on reputation. Reputation is a measure of trust in an object. The reputation parameter is considered a guarantor for the social IoT. In the first instance, a request is made by one object to other objects in the network. Their objective is to find a guarantor. The role of the guarantor is to provide a number of services Xiao, Sidhu [55]. Later, it uses reputation to measure trust. The researchers Chen and Guo [56,57] simulated a model in a real environment and concluded that their trust model can be used in different social IoT environments. Their model is used to detect malicious nodes, and afterwards will impose some penalties as well.

##### 4.5.2. Time-Driven Approaches

Evidence is collected periodically on the basis of recommendations provided by friends and on self-observation. Trust is updated by using a trust aggregation method. During this interval, if no evidence is collected, then trust decay is applied over time. The reason is that anyone can trust the present information Abdelghani, Zayani [28]. An exponential-based decay function was proposed. This function can adjust the rate of trust by itself over a specific time interval [14]. This function was developed by keeping in mind specific application requirements.

Chen and Guo [56] introduced a hierarchical trust community for mobile ad hoc networks (MANETs). A dynamic model was presented that can be used to learn from past experience. This method can adapt to changes in environmental conditions, and thus, ensures performance maximization. Their proposal is realistic in case of node failure, and it is unable to capture events in cases of disconnection. It was proven that it is helpful to maximize application performance by reducing the false positive and false negative ratios in mobile nodes. Finally, it was claimed that QoS is improved by using this system.

#### 4.6. Trust Formation

The concept of trust formation is simple: it is a property of kindness, which is transferred to a person called a trustee. Usually, the trustee holds and controls (or simply is) the owner of this property. Sometimes, trust formation is used for mutual benefits, or sometimes it is used for charity. In the literature, we classify trust formation into single trust or multi-trust.

#### 4.6.1. Single Trust

Single trust is considered by fact that only one trust property is considered in a trust protocol. In this scenario, service quality is believed to be the most important metric in service-based IoT systems [30]. In the social IoT, QoS is usually affected, and hence, trust is the relationship between the service requester and the service provider. In this scenario, we can easily guess that trust in a social IoT-based system is actually always acting pairwise.

#### 4.6.2. Multi-Trust

Multi-trust always implements trust in a multidimensional way. It means there are multiple trust properties considered for the formation of trust. For example, Guo and Chen [30] considered various trust properties together, including honesty, intimacy, and unselfishness. These properties are used for MANETs. Moreover, there are multiple ways to enact trust formation. Some of them are described below.

- First is where one person can easily use trust properties without combining them. He/she has a minimum threshold value for each trust property, which is based on application-based requirements [23].
- One can use a trust scale by using a confidence technique for trust establishment. This idea is used to scale the most important properties with less important properties, which represents confidence. As previously stated, that confidence value is used to establish trust among multiple persons.
- One can use the weighted sum. This is the aggregate of individual trust values. Moreover, assigned weight can reflect the application-based requirements [57].

### 5. Open Discussion, Challenges In, and Future Research Directions for Trust- and Friendliness-Based Approaches in the Social IoT

In the previous section, we reviewed current methods for trust- and friendliness-based approaches in the social IoT. These are based on our classifications. We summarized main areas that have not been well investigated by using current studies. In this section, we will discuss main open issues, challenges, and their possible remedies, with a focus on several aspects.

Based on the discussion of the above survey, we can find a number of issues in the area of trustworthiness and friendliness in the SIoT. First, trust evaluation lacks concern with context awareness and the user's (trustor's) subjective properties. Evaluation of trust-computed results is not personalized. Thus, it is hard to provide IoT services. So, our finding is that "only me, only now, and only here" kinds of services are still an unachieved target.

The second finding is that there is still a lack of literature and trusty frameworks that can provide all proposed trust objectives. Previous concerns, such as the subjective and objective models proposed in some research [24] are still in the evaluation phase, and hence, cannot be completely used for practice in trusty social networks.

The third aspect is the trusted computing platforms used for the social IoT and cloud platforms [15] that have been proposed. They could be too complicated or heavy for tiny sensors to adopt. There is a need to introduce a lightweight solution for sensors (because they have limited computation and memory capabilities).

The fourth aspect is regarding industry 4.0 and the SIoT. We identified several studies related to the IoT and industry 4.0. But little attempt was made with respect to social networks. There is a need to explore the relation between the SIoT and industry 4.0 in detail. We already know that a lot of data are generated by social networks. Hence, the integration of social media and the IoT has been witnessed in various areas, such as traffic routing, product design, etc. [25]. It could be helpful, in the future, to use trusty social networks in the automation of industries.

Fifth is the relationship between objects using OOR or POR [14,33], which are helpful in finding human object location. Researchers are working on the findings of real-time GPS tracking systems.

The concept of OOR would be helpful in this regard. We carefully investigated the literature but found a limited attempt at it. Additionally, if trust is incorporated into POR, it will be better.

Sixth is the service search. Link selection and service search are the backbone of social networks. Numerous researchers presented their work [49], and people are still working on this idea to make more greedy methods for the selection of links. There are many heuristic-based algorithms that have already been proposed [14]. But these methods are not effective. They have not been tested using real-time datasets. There is a need to use new algorithms by using real data sets.

Except for the above open issues in the current literature, we still face a number of challenges related to trust management in moving towards the final success of the SIoT. These challenges are given below.

### 5.1. Trust Aggregation

Trust aggregation is the first untouched research area. In this method, the reviewed methods mostly depend on belief theory. We have already discussed in detail various studies regarding this area in the above section.

#### Challenges

Regression analysis is one of the popular statistical modeling terms, and is applicable to the IoT. It occurs especially when nodes can access a centralized trust manager [28]. Usually, IoT devices are limited in power and resources, and hence, analysis is conducted using the cloud. IoT feedback is comprised of service-based features such as energy. The provision of QoS-based feedback and traffic congestion in the network by using the cloud is quite a difficult task, because statistical analysis has a quite a high impact on the service quality paradigm with respect to the cloud.

Finally, based on detailed discussions, providing accuracy by using an estimation of trust is still questionable.

### 5.2. Innovative Social Trust Metrics

This future research direction helps to find more and more innovative and novel ideas for friendliness- and trust-based approaches.

#### Challenges

Social similarity is an emerging way to rate a trustee/recommender. However, the COI, social contacts, service composition, and social similarity still remain problems. Aside from this property, the rest of the properties (like honesty, centrality, cooperativeness, and selfishness) need to be explored further.

### 5.3. Scalability

Scalability has been partially ensured, while power efficiency has practically been ignored. It is a very hot issue in the IoT.

#### Challenges

The service search space for the IoT and push-based periodic trust are not scalable. In this case, there is a need to add more devices to make it scalable. To solve this issue, encounter-based propagation was proposed by Chen and Guo [58]. The traffic rate is reduced by the sharing of information among IoT devices. We already know that most IoT devices are tinyGuo, Chen [23]. So, it is impractical for each IoT device to store a trust value for all the rest of the devices in order to make a decision. Therefore, based on this argument, a more scalable storage method is required that follows a heuristic design-based principle. There are some possible solutions in this case (for instance, to select those



nodes that post the highest trust value and that were recently interacted with) [Bao, Chen [59]]. Finally, a new and scalable service search method is required for the future.

#### 5.4. Integrated Cloud Service with a Trust Service

In cloud computing, trust is a perfect service when provided to members by considering a group. It is the service facility provided to an IoT group member, mainly based on trust. This is called a high-quality service.

##### Challenges

Our key finding while reviewing the related studies was that they simply applied to the trust-based models used in traditional social networks. Most of them were effective in preventing attacks, but they did not consider friendliness parameters, such as subjective- and objective-level trust. Another key finding was that the majority of the studied models did not involve human-to-object or object-to-human social relationships, even though both of these are required. We can conclude that it is only the start of the friendliness and trust research journey, and more models that have been designed especially for social IoT-based systems are needed.

#### 5.5. Network Navigability and Types of Relationship

Network navigation in the social IoT is still an unexplored area and still has several challenges. We need new tools and methods to evaluate when the network structure is navigable in a specific social IoT-based scenario, and to evaluate how we can shape the network structure. So far, network navigability has been assessed and measured by only a few properties derived from network theory, such as average path length and average degree.

##### Challenges

From our knowledge to date, there are no studies that are able to confirm the importance of relationships like OOR and POR for network navigability. It could happen: a subset of these relations is enough to efficiently navigate through the network and the navigability could be improved by creating new types of relationships. Some of them may be old, and they are now representing the minimal set to efficiently move from one object to any other. Furthermore, even if the existing set of relations is good enough, we are still missing information regarding their roles in the network and the relative importance of each of them.

#### 5.6. Adaptive Trust Management Models

Researchers have proposed various adaptive-based models [24] for trust management in the SIoT. These models are used to develop trust-based values for members of the entire network. The successful connection is based on computed trust values.

##### Challenges

Our finding, after careful investigation, is that the subjective model is better than the objective model. Even though both models have numerous pros and cons, in the subjective model, each node is used to store and manage feedback locally and to calculate trust values. This mechanism is intended to avoid a single point of failure, and is also an infringement of the values of trustworthiness. On the other hand, the objective model is based on the DHT of a single node, and is responsible for maintaining a global table. Hence, it is based on a single point of failure. In contrast, the subjective approach has a slower transitory response, which is particularly evident when dealing with nodes with dynamic behavior. In contrast, the objective approach suffers from this kind of behavior, since a node's trustworthiness is global for the entire network. Researchers usually adopt both approaches in

their work. After careful investigation, we observed that there is a need to develop a new method by merging both of these approaches in the future.

## 6. Conclusions

Trust has recently emerged with friendliness as an efficient means of navigating the social Internet of Things. In this paper, we highlighted the significance of trust and friendliness in the social IoT. Moreover, we explained the basic architecture of the social IoT using various definitions and notations. These explanations are from several perspectives, such as the relationship between the cloud and the social IoT, the role of multiagents in the social IoT, the relations of clusters and IoT nodes, and finally (one of the most important relations) between the SIoT and industry 4.0. The concept of trust is explained with the help of cool example-based scenarios and, later on, is demonstrated by using models. The current state of the art in trust using P2P and the social IoT was carefully investigated. This study aims to define classification based on two diverse paradigms, called friendliness and trust in the social IoT. We divided our classification tree into two levels. At the first level, friendliness-based approaches are stated. These methods are divided into three separate groups: service composition, service search, and the service model. In contrast, the trust-based group is divided into trust aggregation, trust updates, and trust formation. At the first level in friendliness, service composition is divided into direct and indirect trust. Service search is split into distributed and centralized searches, and finally, the service model is divided into subjective and objective models. On the other hand, trust aggregation splits into Bayesian systems, belief theory, and dynamically-weighted sums. The trust update branch is divided into event-driven and time-driven approaches. Finally, the trust formation branch splits into single- and multi-level trust. We explained these approaches by using pros and cons in detail. Based on our proposed classifications, some recent solutions from both academia and industry have been carefully surveyed. Finally, at the end of the paper, we offered an open discussion and identified major challenges and unresolved issues related to the social IoT. As future work, we plan to analyze innovative social trust metrics and the best way to combine them for SIoT trust computation. The reason is that the SIoT is inherently social-oriented.

**Acknowledgments:** This research was supported by the Ministry of Trade, Industry & Energy (MOTIE, Korea) under Industrial Technology Innovation Program. No.10063130, Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2016R1A2B4007498), and MSIT(Ministry of Science, ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2016-0-00313) supervised by the IITP(Institute for Information & communications Technology Promotion).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Tsiropoulou, E.E.; Paruchuri, S.T.; Baras, J.S. Interest, energy and physical-aware coalition formation and resource allocation in smart IoT applications. In Proceedings of the 2017 51st Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 22–24 March 2017; pp. 1–6.
2. Guo, J.; Chen, I.-R.; Tsai, J.J.P. A survey of trust computation models for service management in internet of things systems. *Comput. Commun.* **2017**, *97*, 1–14. [[CrossRef](#)]
3. Li, H.; Parlikad, A.K. Social Internet of Industrial Things for Industrial and Manufacturing Assets. *IFAC-PapersOnLine* **2016**, *49*, 208–213. [[CrossRef](#)]
4. Tsiropoulou, E.E.; Mitsis, G.; Papavassiliou, S. Interest-aware energy collection & resource management in machine to machine communications. *Ad Hoc Netw.* **2018**, *68*, 48–57.
5. Chen, I.R.; Bao, F.; Guo, J. Trust-Based Service Management for Social Internet of Things Systems. *IEEE Trans. Depend. Secur. Comput.* **2016**, *13*, 684–696. [[CrossRef](#)]
6. Lin, C.R.; Gerla, M. Adaptive clustering for mobile wireless networks. *IEEE J. Sel. Areas Commun.* **1997**, *15*, 1265–1275. [[CrossRef](#)]
7. Juhász, J.; Bányai, T. What Industry 4.0 Means for Just-In-Sequence Supply in Automotive Industry? In *Vehicle and Automotive Engineering 2*; Springer: Cham, Switzerland, 2018; pp. 226–240.

8. Chiang, C.C.; Wu, H.K.; Liu, W.; Gerla, M. Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. In Proceedings of the IEEE SICON, Singapore, 14–17 April 1997; pp. 197–211.
9. Nitti, M.; Girau, R.; Atzori, L. Trustworthiness Management in the Social Internet of Things. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 1253–1266. [[CrossRef](#)]
10. Tamás Bányai, B.I.; Bányai, A. Smart Scheduling: An Integrated First Mile and Last Mile Supply Approach. *Complexity* **2018**, *2018*, 15.
11. Nitti, M.; Atzori, L.; Cvijikj, I.P. Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies. *IEEE Internet Things J.* **2015**, *2*, 240–247. [[CrossRef](#)]
12. Abdelghani, W.; Zayani, C.A.; Amous, I.; Sèdes, F. *Trust Management in Social Internet of Things: A Survey*; Springer: Cham, Switzerland, 2016; pp. 430–441.
13. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [[CrossRef](#)]
14. Nitti, M.; Pilloni, V.; Colistra, G.; Atzori, L. The Virtual Object as a Major Element of the Internet of Things: A Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1228–1240. [[CrossRef](#)]
15. Ben Saïed, Y.; OLIVEREAU, A.; Zeglache, D.; Laurent, M. Trust management system design for the Internet of Things: A context-aware and multi- service approach. *Comput. Secur.* **2013**, *39*, 351–365. [[CrossRef](#)]
16. Chen, D.; Chang, G.; Sun, D.; Li, J.; Jia, J.; Wang, X. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Comput. Sci. Inf. Syst.* **2011**, *8*, 1207–1228. [[CrossRef](#)]
17. SENSEI. Available online: <http://www.ict-sensei.org/> (accessed on 2 August 2018).
18. Fiware Community Fiware: The Open Source Platform for Our Smart Digital Future. Available online: <https://www.fiware.org/> (accessed on 2 August 2018).
19. The Compose Project. Compose: Collaborative Open Market to Place Objects at Your Service. Available online: <http://www.compose-project.eu/> (accessed on 2 August 2018).
20. IoT-A (Internet of Things—Architecture). IoT-A (Internet of Things—Architecture). Available online: <http://www.iot-a.eu/> (accessed on 2 August 2018).
21. Rabadiya, K.; Makwana, A.; Jardosh, S. Revolution in networks of smart objects: Social Internet of Things. In Proceedings of the 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp), Changa, India, 1–2 December 2017; pp. 1–8.
22. Militano, L.; Nitti, M.; Atzori, L.; Iera, A. Enhancing the navigability in a social network of smart objects. *Comput. Netw.* **2016**, *103*, 1–14. [[CrossRef](#)]
23. Amin, F.; Ahmad, A.; Choi, G.S. Community Detection and Mining Using Complex Networks Tools in Social Internet of Things. In Proceedings of the IEEE TENCON, Region 10 Asia Conference, Jeju Island, Korea, 28–31 October 2018; pp. 1–6.
24. Atzori, L.; Iera, A.; Morabito, G. SIoT: Giving a Social Structure to the Internet of Things. *IEEE Commun. Lett.* **2011**, *15*, 1193–1195. [[CrossRef](#)]
25. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The Social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [[CrossRef](#)]
26. Amin, F.; Ahmad, A.; Choi, G.S. To Study and Analyse Human Behaviours on Social Networks. In Proceedings of the 4th Annual International Conference on Network and Information Systems for Computers (ICNISC), Wuhan, China, 14–16 April 2018; pp. 1–4.
27. Mendes, P. Social-driven Internet of Connected Objects. In Proceedings of the Interconnecting Smart Objects with the Internet Workshop, Lisbon, Portugal, 12 March 2011.
28. Nitti, M.; Girau, R.; Atzori, L.; Iera, A.; Morabito, G. A subjective model for trustworthiness evaluation in the social Internet of Things. In Proceedings of the 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC), Sydney, Australia, 9–12 September 2012; pp. 18–23.
29. Zhang, W.; Jin, Q.; Baz, D.E. Enabling the Social Internet of Things and Social Cloud. *IEEE Cloud Comput.* **2015**, *2*, 6–9. [[CrossRef](#)]
30. Wang, K.; Qi, X.; Shu, L.; Deng, D.j.; Rodrigues, J.J.P.C. Toward trustworthy crowdsourcing in the social internet of things. *IEEE Wirel. Commun.* **2016**, *23*, 30–36. [[CrossRef](#)]
31. Singh, M.P.; Chopra, A.K. The Internet of Things and Multiagent Systems: Decentralized Intelligence in Distributed Computing. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 1738–1747.

32. Yu, H.; Shen, Z.; Leung, C.; Miao, C.; Lesser, V.R. A Survey of Multi-Agent Trust Management Systems. *IEEE Access* **2013**, *1*, 35–50.
33. Christianson, B.; Harbison, W.S. *Why Isn't Trust Transitive?* Springer: Berlin/Heidelberg, Germany, 1996; pp. 171–176.
34. Guo, J.; Chen, I.R. A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems. In Proceedings of the 2015 IEEE International Conference on Services Computing, New York, NY, USA, 27 June–2 July 2015; pp. 324–331.
35. Kowshalya, A.M.; Valarmathi, M.L. Trust management for reliable decision making among social objects in the Social Internet of Things. In *IET Networks*; Institution of Engineering and Technology: London, UK, 2017; Volume 6, pp. 75–80.
36. Truong, N.B.; Lee, H.; Askwith, B.; Lee, G.M. Toward a Trust Evaluation Mechanism in the Social Internet of Things. *Sensors* **2017**, *17*, 1346. [\[CrossRef\]](#)
37. Marche, C.; Atzori, L.; Iera, A.; Militano, L.; Nitti, M. Navigability in Social Networks of Objects: The Importance of Friendship Type and Nodes' Distance. In Proceedings of the 2017 IEEE Globecom Workshops (GC Wkshps), Singapore, 4–8 December 2017; pp. 1–6.
38. Bao, F.; Chen, I.-R. Dynamic trust management for internet of things applications. In Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, San Jose, CA, USA, 16–20 September 2012; pp. 1–6.
39. Zhou, L.; Chao, H.C. Multimedia traffic security architecture for the internet of things. *IEEE Netw.* **2011**, *25*, 35–40. [\[CrossRef\]](#)
40. Chen, C.; Helal, S. A device-centric approach to a safer internet of things. In Proceedings of the 2011 International Workshop on Networking and Object Memories for the Internet of Things, Beijing, China, 18 September 2011; pp. 1–6.
41. Liu, G.; Wang, Y.; Li, L. Trust Management in Three Generations of Web-Based Social Networks. In Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, Brisbane, Australia, 7–9 July 2009; pp. 446–451.
42. Carminati, B.; Ferrari, E.; Viviani, M. *A Multi-Dimensional and Event-Based Model for Trust Computation in the Social Web*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 323–336.
43. Suryani, V. A survey on trust in Internet of Things. In Proceedings of the 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, 5–6 October 2016; pp. 1–6.
44. Chen, I.R.; Guo, J.; Bao, F. Trust Management for SOA-Based IoT and Its Application to Service Composition. *IEEE Trans. Serv. Comput.* **2016**, *9*, 482–495. [\[CrossRef\]](#)
45. Abderrahim, O.B.; Elhdhili, M.H.; Saidane, L. TMCoi-SIOT: A trust management system based on communities of interest for the social Internet of Things. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 747–752.
46. Kleinberg, J.M. Navigation in a small world. *Nature* **2000**, *406*, 845. [\[CrossRef\]](#)
47. Boguna, M.; Krioukov, D.; Claffy, K.C. Navigability of Complex Networks. *Nat. Phys.* **2009**, *5*, 7480.
48. Lan, A.; Ottino, J.M. Complex networks—Augmenting the framework for the study of complex systems. *Eur. Phys. J. B* **2004**, *38*, 147–162.
49. Chen, Z.; Ling, R.; Huang, C.-M.; Zhu, X. A scheme of access service recommendation for the Social Internet of Things. *Int. J. Commun. Syst.* **2016**, *29*, 694–706. [\[CrossRef\]](#)
50. Sawamura, S.; Barolli, A.; Aikebaier, A.; Ikeda, M.; Takizawa, M. Objective Trustworthiness of Acquaintances in Peer-to-Peer (P2P) Overlay Networks. In Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications, Singapore, 22–25 March 2011; pp. 167–174.
51. Jøsang, A. A logic for uncertain probabilities. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* **2001**, *9*, 279–311. [\[CrossRef\]](#)
52. Ganeriwal, S.; Balzano, L.K.; Srivastava, M.B. Reputation-based framework for high integrity sensor networks. *ACM Trans. Sen. Netw.* **2008**, *4*, 1–37. [\[CrossRef\]](#)
53. Yu, B.; Singh, M.P. An evidential model of distributed reputation management. In *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1*; ACM: Bologna, Italy, 2002; pp. 294–301.

54. Beynon, M.; Curry, B.; Morgan, P. The Dempster-Shafer theory of evidence: An alternative approach to multicriteria decision modelling. *Omega* **2000**, *28*, 37–50. [[CrossRef](#)]
55. Xiao, H.; Sidhu, N.; Christianson, B. Guarantor and reputation based trust model for Social Internet of Things. In Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 24–28 August 2015; pp. 600–605.
56. Chen, I.-R.; Guo, J. Hierarchical trust management of community of interest groups in mobile ad hoc networks. *Ad Hoc Netw.* **2015**, *33*, 154–167. [[CrossRef](#)]
57. Chen, I.; Guo, J.; Bao, F. Trust management for service composition in SOA-based IoT systems. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, Turkey, 6–9 April 2014; 2014; pp. 482–495.
58. Chen, I.R.; Guo, J. Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection. In Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Gwangju, Korea, 13–16 May 2014; pp. 49–56.
59. Bao, F.; Chen, I.R.; Guo, J. Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems. In Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), Mexico City, Mexico, 6–8 March 2013; pp. 1–7.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).