sensors

MDPI

Article

Toward a Trust Evaluation Mechanism in the Social Internet of Things

Nguyen Binh Truong [1], Hyunwoo Lee [2], Bob Askwith [1] and Gyu Myoung Lee [1,*]

[1] Department of Computer Science, Liverpool John Moores University, Liverpool, L3 3AF, UK; n.b.truong@2015.ljmu.ac.uk; r.j.askwith@ljmu.ac.uk; g.m.lee@ljmu.ac.uk

[2] Media Research Division, Broadcasting & Media Research Laboratory, Electronics and Telecommunications Research Institute (ETRI), Daejeon, 34129, Korea; hwlee@etri.re.kr

* Correspondence: g.m.lee@ljmu.ac.uk; Tel.: +44-151-231-2052

Academic Editor: name

Received: date; Accepted: date; Published: date

Abstract: In the blooming era of the Internet of Things (IoT), trust has been accepted as a vital factor for provisioning secure, reliable, seamless communications and services. However, a large number of challenges have been unsolved yet due to the ambiguity of the concept of trust as well as the variety of divergent trust models in different contexts. In this research, we augment the trust concept, the trust definition and provide a general conceptual model in the context of the Social IoT (SIoT) environment by breaking down all attributes influencing trust. Then, we propose a trust evaluation model called REK comprised of the triad Reputation, Experience and Knowledge trust indicators (TIs). The REK model covers multi-dimensional aspects of trust by incorporating heterogeneous information from direct observation (as Knowledge TI), personal experiences (as Experience TI) to global opinions (as Reputation TI). The associated evaluation models for the three TIs are also proposed and provisioned. We then come up with an aggregation mechanism for deriving trust values as the final outcome of the REK evaluation model. We believe this article offers better understandings on trust as well as provides several prospective approaches for the trust evaluation in the SIoT environment.

Keywords: Trust; Trust Concept; REK Trust Evaluation Model; Social Internet of Things; Knowledge; Experience; Reputation

1. Introduction

In the recent years, we have been witnessing a novel paradigm – the Internet of Things (IoT) in which billions of electronic objects are connected to the Internet. These objects range from small and low computation capability devices such as Radio Frequency Identification tags (RFIDs) to complex ones such as smartphones, smart appliances and smart vehicles. Indeed, the idea to connect and share data among physical objects, cyber-space and humans using hyperlinks over a global network was promulgated by Tim Berners Lee three decades ago. A number of efforts have been made to build upon this premise in the last ten years, for example, Semantic Web (Web 3.0) integrates humans and social information to the Web, yielding a composite Cyber-Social system. With the IoT, we are now reaching to a breakthrough of a Cyber-Physical-Social System (CPSS) that connects the Cyber-Social Webs with physical world objects [1]. With billions of sensing and actuating devices deployed, the IoT is expected to observe various aspects of human life anywhere on Earth. Observation data is aggregated, processed, and analyzed into valuable knowledge describing occurrences and events regarding to different real-world phenomena. With various types of information from cyber and social domains, it is possible for a variety of services to reveal the untapped operational efficiencies and create an end-to-end feedback loop between individual's needs and physical object responses. In

order to meet the requirements for such IoT services, a unified CPSS framework has been developed that "*takes a human centric and holistic view of computing by analyzing observations, knowledge, and experiences from physical, cyber, and social worlds*" [2].

In the early years, most of IoT-related research articles have concentrated on RFID and Wireless Sensor Networks (WSNs) that aim at building underlying networking protocols, hardware and software components in order to enable interactions and communications among physical objects and cyber-space. However, a human-centric IoT environment in which human plays an important role in supporting application and services, are more and more perceptible. This is proven by the high rate of utilization of social phenomena and crowd intelligence when developing real-world IoT services. Consequently, the so-called Social Internet of Things (SIoT) has recently been proposed for illustrating the CPSS concept in which people are envisaged as an integral part of the IoT ecosystem [3,4]. However, the merging of physical objects, cyber components and humans in the SIoT will introduce new concerns for risks, privacy and security. Consequently, managing risk and securing the SIoT are broad in scope and pose greater challenges than the traditional privacy and security triad of integrity, confidentiality, and availability [5]. In this regard, trust is recognized as an important role in supporting both humans and services to overcome the perception of uncertainty and risk when making a decision.

Trust is a multifaceted concept used in many disciplines in human life influenced by both participators and environmental factors. It is an underlying psychological measurement to help a trustor to come up with a decision whether it should put itself into a risky situation in case a trustee turns out to be misplaced. As the aim of any SIoT services is to autonomously make decisions without human intervention, trust has been highlighted as a vital factor for establishing seamless connectivity, secure systems and reliable services. A trust platform could minimize the unexpected risks and maximize the predictability, which helps both SIoT infrastructures and services to operate in a controlled manner and to avoid unpredicted conditions and service failures.

As the importance of trust in SIoT, recently, a large number of research groups have been intensively working on trust-related areas in various networking environments such as peer-to-peer (P2P) networks, wireless sensor networks, social networks, and the IoT; varying in many applications and services from access control [6] to e-Commerce [7,8]. To develop a complete trust platform, various trust-related areas are necessarily taken into considerations such as trust evaluation and trust management [9]. In this article, we mainly focus on developing a trust evaluation model. Besides, researchers have also focused on developing trust management mechanisms dealing with trust establishment, dissemination, update and maintenance processes. Some articles have been proposed trust evaluation models based on a set of information (so-called *direct trust*) by extracting trustee's characteristics or by observing trustee's behaviors. This information are used to describe some trust-related characteristics of an entity that are coined as Trustworthiness Attributes (TAs); these TAs are combined to a final value for representing the trustee's trustworthiness. The trustworthiness is then unconsciously used as trust. Other approaches have measured trust based on third-party information about a trustee that the third-parties have been already interacted with, thus, they already gained some clues of trust (so-called *indirect trust*). To do so, a mechanism needs to be created in order to evaluate opinions of an entity to another after each interaction; and to spread the opinions to others (in forms of feedback and recommendations). The final step is to aggregate the set of the third-party information to finalize an overall score which is actually the reputation of a trustee. Again, the reputation is used for quantifying trust. Reputation, which is an indicator of trust, should not be confused with trust but partially affects trust. Therefore, each of the previous research work is as a separated piece of a big picture solving a particular challenge in a specific environment.

Our on-going projects have been targeting to developing a complete platform for trust evaluation and management. The platform cooperates with applications and services to help both service consumers and providers making decisions in risky scenarios, resulting in securer activities and providing better quality of services and experiences. The platform is then considered as *Trust as a Service (TaaS)*. In this article, we aim at providing two major contributions. The first contribution is

the augmentation of trust concept, definition and evaluation model that consolidate understanding on trust in the SIoT environment. This helps to remove the confusion among trust, reputation, dependability, security and privacy. The second contribution is the introduction of a complete trust evaluation mechanism in the SIoT environment called REK which comprises of the three components Reputation, Experience and Knowledge. Conceptual models and evaluation approaches for the three components are proposed and described along with an aggregation mechanism for integrating the three components to finalize a trust value. An illustration for the REK model is also briefly presented using a specific use-case called User Recruitment in Mobile Crowd-Sensing (MCS) [10].

The rest of the paper is organized as follows. Section 2 provides important understandings and clarification of the trust concept in the SIoT. Section 3 describes related work as well as highlights a conceptual evaluation model with provisions. Section 4 is dedicated for describing the REK trust evaluation platform including conceptual model, prototype and the use-case. The last section concludes our work and outlines future research directions.

2. Augmentation of Trust Concept in the SIoT

Trust can be roughly defined as 'assurance' or 'confidence' of a trustor in a trustee to perform a task in a way that satisfies the trustor's expectation. In this sense, the trustor partly recognizes the vulnerabilities and potential risks when the trustee accomplishes the task, thus it represents the trustor's willingness to be vulnerable under the conditions of risks and interdependence [11].

2.1. Trust Concept Clarification

Trust is a complicated concept which was originally used in many disciplines in human life. In the SIoT environment, trust interplays between social sciences and computer science influenced by both objective and subjective factors from both participators and contextual characteristics [12].

The earliest variant of trust in computer science is system security and data security that cover concepts of hardware, software and communications. A system is trustworthy if it is secure and not compromised, meaning that it identifies people accessing the system and only allows authorized users; and the data security ensures that data is only accessed by those authorized users even in the presence of adversaries. More than three decades ago, Ken Thomson mentioned about trust in his Turing Award lecture when writing a Unix program to be free of Trojan horses [13]. Security gets further complex in networked worlds such as the Internet and the IoT due to the increasing participants to systems throughout the networks, resulting in introducing more threats, vulnerability and risks. System security and data security are also more complicated when privacy is taken into account. For example, personal data security could be ensured (in some degree) but providers can use the data for their own purposes or sell to a third-party. In this case, data security might be compromised if the data owner's intent for data usage is violated. One of the solutions is a trust-based access control mechanism for data sharing in the environment of Smart City that we have proposed in [14].

An advanced variant of trust for a computer system is *dependability* that is evolved from reliability, security and privacy considerations. Besides security and privacy, reliability is a factor showing whether a systems is going to perform properly. Thus, dependability is de facto property of a system representing ability of the system to deliver secure and quality services by characterizing the security, privacy and reliability schemes in terms of some attributes such as availability, safety, integrity, confidentiality and reliability. Grandison and Sloman have defined this variant of trust as "*infrastructure trust*" [15]. In our perspective, dependability is one of the most important indicator in evaluating trustee' trustworthiness (in case the trustee is a computer system). The key distinction between trust and dependability is due to the enrolment of social interactions (of both humans and devices), which is modulated in form of social capital factors (Figure 1(a)). The social capital can interpret various aspects of individuals and social networks including behaviors, norms and patterns

that have built up through social interactions over time that also help to reckon trust. In this regard, trust is an umbrella concept of dependability.

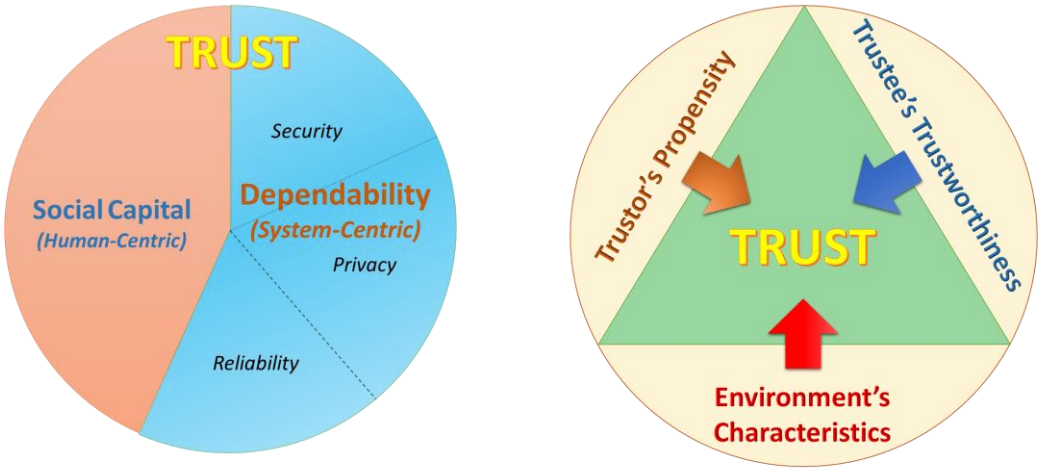


Figure 1. (a) Trust concept in the relation with dependability and social capital; (b) Three main aspects of trust in the SIoT environment

Trust is originally a foundational aspect of human social relations; and when applying trust to the SIoT environment, it should be considered under a perspective of a trustor in correlation with a society. Social interactions, subjective viewpoint of individual entity, and environments should not be neglected [16]. We have pointed out that besides trustworthiness of a trustee, trustor's propensity and environmental factors such as vulnerabilities, threats and risks also contributes to the trust evaluation (Figure 1(b)). This is obvious because trust only occurs risky scenarios in which the trustor is going to be under vulnerability.

2.2. Definition of Trust in SIoT

There are plenty of trust definitions in particular situations resulting in difficulty in establishing a standard notation of trust in computer science. In order to define trust in the SIoT environment, we tend to follow a widely-accepted approach from social science that trust is considered as *belief* which appears in many trust-related literature [11,17]. A general definition of trust in computer science has been broadly acknowledged as following:

Trust is defined as a *belief* of a *trustor* in a *trustee* that the trustee will provide or accomplish a *trust goal* as *trustor's expectation* within a *specific context* for a *specific period of time*.

In SIoT environment, trustors and trustees can be humans, devices, systems, applications and services. Measurement of trust as the belief (called trust value) can be absolute (e.g., probability) or relative (e.g., level of trust). The trust goal is in a broad understanding. It could be an action that the trustee is going to perform (trust for action); it could also be information that the trustee provides (trust for information). Trustor's expectations are deliberately considered to include specific requirements for well performing (in some degree) the trust goal. All of the terms in this definition will be described and explained in detail in the next sections.

2.3. Trust Characteristics

Some key characteristics that further interpret the trust concept are summarized as follows:

- **Trust is subjective:** With the same trustee and trust context, trust might be different from trustors. In other word, trust is dependent on trustor's perspective. For example, Alice (highly) trusts Bob but Charlie does not (for fulfilling a trust goal).

- **Trust is asymmetric:** Trust is a non-mutual reciprocal in nature although in some special cases, trust may be symmetric. For example, if Alice (highly) trusts Bob (in fulfilling a trust goal) it does not mean that Bob will (highly) trusts Alice (in fulfilling such trust goal).
- **Trust is context-dependent:** With the same trustor and trustee, trust might be different depending on context including (i) task goal, (ii) period of time, and (iii) environment. For instance, (i) Alice (highly) trusts Bob to provide a cloud storage service but not for a real-time streaming service; (ii) Alice (highly) trusted Bob to provide a cloud storage service two years ago but not for now; and (iii) Alice (highly) trusts Bob to provide a cloud storage service in the United Kingdom but not in the United States.
- **Trust is not necessarily transitive but propagative:** If Alice (highly) trusts Bob, and Bob (highly) trusts Charlie then it is not necessarily that Alice will (highly) trust Charlie. However there are some evidences from the trust relationship between Bob and Charlie that Alice can rely on in order to judge the trust in Charlie.

More details about trust characteristics can be found in [18].

2.4. Conceptual Trust Model in SIoT environment

It is important to clarify that trust is neither a property of a trustor (e.g., trustor's preferences) nor a property of a trustee (e.g., trustee's trustworthiness and trustee's reputation). It is a relationship between the trustor and the trustee that is subjective and asymmetric which is derived from the triad of trustee's trustworthiness, trustor's propensity and environment's characteristics. Based on the clarification of the trust concept, a conceptual trust model in the SIoT is proposed as illustrated in Figure 2. Then, a more specific trust definition in the SIoT associated with the conceptual trust model is proposed as follows:

Trust is the *perception of a trustor* on *trustee's trustworthiness* under a *particular environment* (within a *period of time*) so-called *perceived trustworthiness*.

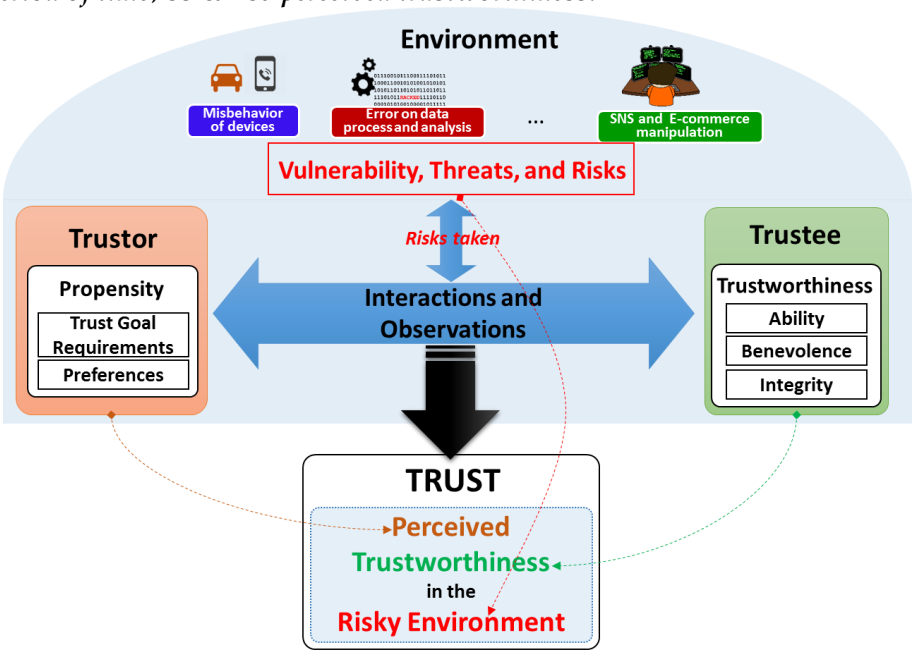


Figure 2. Conceptual Trust Model in the SIoT environment

According to the proposed model illustrated in Figure 2, trust will be obtained by harmonizing the trustor's propensity and environment conditions into the trustee's trustworthiness. The harmonization is accomplished by aggregating both the observation of a trustor toward a trustee and

the interactions between the two. It is worth to note that the environment conditions are reflected as risks taken during the observations and interactions. The trustor's propensity includes both *requirements for the trust goal* and the *trustor's preferences* about the trustee's trustworthiness whereas the environment conditions are the considerations for some factors such as vulnerabilities, threats and risks. The *trust goal requirements* with the *environmental factors* helps determining the set of TAs for deriving the *perceived trustworthiness* whereas the *trustor's preferences* is to help combining these TAs to obtain an overall trust value for making a decision. For example, *trustor's preferences* could be represented in forms of weights of TAs, indicate the levels of importance of the TAs when constructing trust. Trust as *perceived trustworthiness* is as an instance of trustee's trustworthiness respecting to a particular trustor and an environment, thus, even same a trustee and same an environment, different trustors might have different propensities of the trustee's trustworthiness. This illustrates the subjective characteristic of trust. Another important characteristic of trust is the context-dependence that can also be illustrated using this conceptual model as follows: with the same trustor and trustee, different environments might result in different TAs and different trustor's propensities.

Based on the conceptual model, the goal of any trust model is two-fold: (i) to specify and evaluate TAs of the trustworthiness of a trustee respecting to *trustor's propensity* and *environment conditions*; (ii) to combine the TAs to finalize the *perceived trustworthiness* as the *trust value*. From now on in this article, the term "*trust"* is referred to this conceptual model and it is exchangeably used with the term "*perceived trustworthiness*".

2.5. Trustworthiness and Trustworthiness Attributes

According to the proposed conceptual trust model, in order to quantify trust, it is necessary to investigate trustee's trustworthiness by specifying TAs associated with it. As mentioned above, trustworthiness is as a composite of a variety of TAs that illustrate different characteristics of the trustee. Despite a large number of TAs have been figured out in trust-related literature, TAs are mostly fallen into three categories as the three main dimensions of trustworthiness: Ability, Benevolence and Integrity. This classification is well-known and widely-accepted in the field of social organization settings [19]; and we believe it is also appropriate for consideration of trustworthiness in the SIoT environment.

- **Ability**: is a dimension of trustworthiness showing the capability of a trustee to accomplish a trust goal. An entity may be high benevolent and integrity for fulfilling a trust goal but the results may not be satisfactory if it is not capable. This term incorporates some other terms that have been used as TAs in many trust-related literature such as competence, expertness, and credibility.
- **Benevolence**: is a dimension of trustworthiness showing to what extent a trustee is willing to do good things or not harm the trustor. Benevolence ensures that the trustee will have good intentions toward the trustor. This term incorporates some TAs such as credibility, relevance, and assurance as TAs.
- **Integrity**: is a dimension of trustworthiness showing the trustee adheres to a set of principles that helps the trustor believe that the trustee is not harmful and not betray what it has committed to do. These principles can come from various sources such as fairness, or morality. This term incorporates some TAs such as honesty, completeness, and consistency.

Table 1 lists a miscellany of TAs keywords classified into the three categories.

Some of the TAs in Table 1 are frequently used in trust literature ranging from social science to computer science, the other are rarely used and only existed in specific contexts. Even though each of the three factors Ability, Benevolence and Integrity captures some unique elements of trustworthiness, many of these keywords are not necessarily separated, and the interpretations of

253 them clearly depend on particular environments and trust goals. For some specific environments and
254 goals, certain TAs are similar whereas they are different in other contexts.

255 **Table 1.** Some keywords of trustworthiness from trust-related literatures classified into three dimensions

Ability TAs	Benevolence TAs	Integrity TAs
Competence, ability, capability, expertness, credibility, predictability, timeliness, robustness, safety, stability, scalability, reliability, dependability	Good intention, goodness, certainty, cooperation, cooperativeness, loyalty, openness, caring, receptivity, assurance	Honesty, morality , completeness, consistency, accuracy, certainty, availability, responsiveness, faith, discreetness, fairness, promise fulfilment, persistence, responsibility, tactfulness, sincerity, value congeniality, accessibility

256 **3. Trust Evaluation Model: Background and Provisions**

257 Trust *can only be measured partly*. It is *impossible* to measure *trust completely* due to a huge range
258 of factors from both participants and environment contributing to the trust relationship. Moreover,
259 some of them are unable to obtain or greatly challenged to measure.

260 As implied in the conceptual model in Section 2.4, a trivial trust evaluation scheme could be as
261 the following procedure: (i) determine and calculate all TAs of a trustee's trustworthiness; (ii) specify
262 task requirements and preferences, (iii) figure out all environment conditions; then (iv) incorporate
263 these factors to build trust. This trust evaluation model is called *Direct Trust* that indeed calculates
264 trust based on direct observations on both the participants (the trustor and the trustee) and the
265 environment. However, this approach finds unfeasible to efficiently measure trust due to several
266 reasons. For example, there are variety of TAs (some of them are listed in Table 1) need to be
267 quantified in order to measure the *direct trust; and this* is an impossible mission. One reason for this
268 is due to the ambiguity and variability of natural language when defining terms for TAs that are still
269 debatable in trust literature. Another reason is the complication and limitation of data collection,
270 technologies and methodologies for valuating all the TAs as well as the complexity of incorporating
271 TAs with trustor's propensity and environment conditions to evaluate trust. Authors in [20] also
272 mentioned that TA collection might cause privacy leakage which makes involved entities reluctant
273 to provide personal evidence for a trust evaluation platform.

274 Consequently, instead of measuring trust using only the direct trust approach, a prospective
275 approach is to determine a set of indicators called Trust Indicators (TIs) that are feasible, not so
276 complicated to obtain, and cover different aspects of trust. As the word 'indicator' implies, each TI is
277 as a "*piece of a puzzle*" showing the consensus of trust. TIs could be a TA or a combination of several
278 TAs; could also be a combination some TAs with trustor's propensity and environmental factors. TIs
279 can be obtained using different approaches, for instance, the direct trust evaluation model could
280 produce a good TI. However, other TIs do not necessarily only stick to the direct trust evaluation
281 scheme. Thanks to the integration of social networks, some TIs can be determined based on social
282 interactions in the SIoT environment that effectively indicate trust such as Recommendation and
283 Reputation which are evaluated contingent on the propagation characteristic of trust. These TIs are
284 then combined to derive a portion of the *complete trust* called *computational trust*. The *computational*
285 *trust* is persuasively used on behalf of the *complete trust* (Figure 3). As many TIs are specified and
286 evaluated as more accurate the *computational trust* will get. However, as two sides of a coin, there is
287 always trade-off between computational trust accuracy and computational efforts.
288

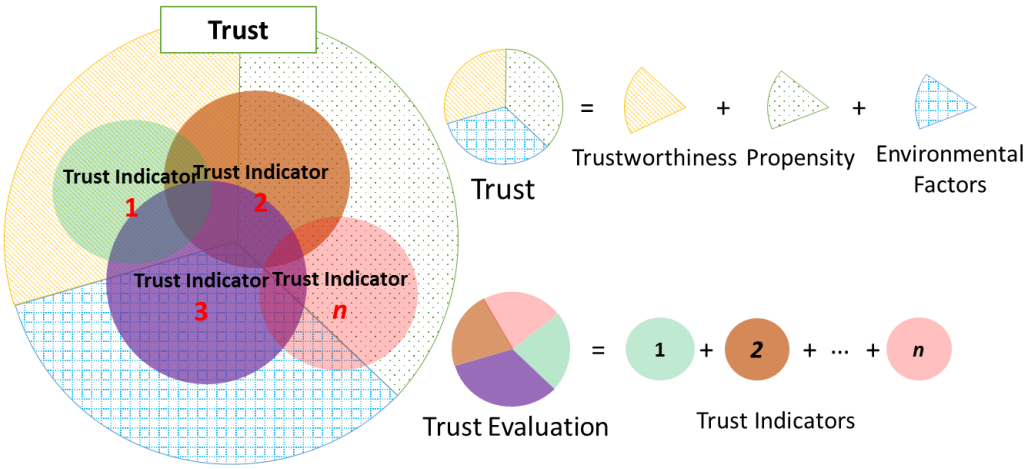


Figure 3. Concept of Computational Trust that comprised of multiple Trust Metrics

Nevertheless, any trust evaluation models in SIoT environment should determine two objectives: (i) specify a set of TIs in which each TI represents a piece of the three factors: trustee's trustworthiness, the trustor's propensity, and the environmental factor; (ii) propose mechanisms to evaluate the TIs as well as to derive the *computational trust value* from the TIs. Again, the *computational trust* should be much similar to the *complete trust* so that it can be efficiently used on behalf of the *complete trust* in most of the cases.

3.2. Related Work on Trust Evaluation

Despite the importance of trust in computer science, there are limited notable articles that clearly clarify the trust concept, trust models and evaluation mechanisms, especially in the IoT environment. A variety of models and mechanisms have been proposed for evaluating trust, however, they have mainly focused on building reputation systems in social networks for e-Commerce services [21] [22] or focused on developing trust management mechanisms in distributed systems such as WSNs [23,24], mobile ad-hoc networks (MANET) [25-27], and P2P networks [6,28]. The trust evaluation mechanisms in these articles are mostly based on insufficient information (i.e., only direct observation information or only third-party information).

Some trust models attempt to assess trustee's trustworthiness by introducing some TAs and associated evaluation mechanisms for generating a so-called trust. They indeed calculate *direct trust* that is a portion of the *perceived trustworthiness*. Researchers have pointed out that in some scenarios such as MANETs, due to high mobility, it is challenged to maintain a centralized system for managing third-party information, resulting in only direct observation information is possibly obtained; and they have to adapt the trust models based on constrains of the environments [25,26]. In these evaluation models, *direct trust* consists of a set of manifold TAs that are necessary and sufficient for a trustor to quantify trust in a particular environment. The *perceived trustworthiness* is not required to cover all TAs, instead, the set of TAs should be deliberately chosen based on *trustor's propensity* and *environmental factors* (even though in these articles, the *trustor's propensity* and *environment characteristics* are not mentioned). For example, when evaluating trustworthiness of sensor nodes in WSNs, F. Bao and I. Chen have used Cooperativeness, Community-Interest, and Honesty to judge whether a sensor node is malicious or not. These TAs help to evaluate trustworthiness of a sensor node in a WSN that contains some types of vulnerabilities and attacks [23]. The disadvantage of this approach is that the authors do not have a mechanism to combine such information to illustrate the subjectivity of trust. Thus, what they calculate is as an instance of entity's trustworthiness. Y. Yu *et al.* in [24] have analyzed various types of threats and attacks and variety of trust models in the WSN environment for secure routing protocols by characterizing many attributes of a secure system such as security mechanisms and attack preventing mechanisms. I. Li *et al.* in [27] have used only local information about a node for evaluating trust, giving an incomplete partial trust for a trust

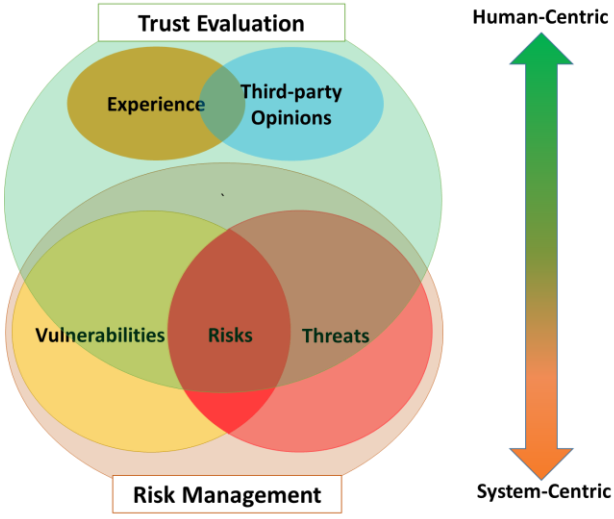
management called Objective Trust Management Framework (OTMF) in MANETs environment. The novel idea is that they apply a modified Bayesian model using different weights assigned for each information obtained from direct observations. The information is collected using a watchdog mechanism; and in order to calculate weights for each kind of information, the OTMF floods all the observation information throughout the network. A node can rely on the observation from neighbors (called second-hand information) for determining its own weights. The problem of the mechanism is the generation of a significant amount of overhead to MANETs. In [6,29], the authors have mentioned about trust-related information extracted from the three layers of a networking system namely physical, core and application layers; and they use the information for quantifying trust. An inference engine based on fuzzy logics is used to infer a trust level. However, the drawback of this approach is only focusing on objective factors only but not subjective factors of trust. As a result, values they got from the computation mechanism do not reflect some key characteristics of trust, thus cannot quantify as trust. An interesting article is about judging trust based on several features extracted from social interactions such as spatiality, relative orientation, frequency of interactions, and duration of interactions [30]. However, this information is not sufficient to accurately derive trust due to a variety of assumptions on relations between trust and behaviors of entities which are sometimes not correct.

Some trust models imitate the human cognitive process to form a belief value by considering several types of TIs such as reputation and recommendation and observation. These models have been proposed for trust evaluation and trust management in P2P networks [31], Social Networks [32], IoT [23,33] and in SIoT [34]. Most of them are based on interactions among entities in (social) networks to evaluate trust, resulting in a distributed, activity-based or encounter-based computation model. Here, trust is derived only based on social concepts such as reputation, recommendation and experience by propagating knowledge among entities. Reputation has been widely used in many applications and e-Commerce websites such as eBay, Amazon, and IMDb, however, the biggest drawback of these reputation schemes are the requirements of human participants in giving feedback as their opinions about the entities they have interacted with. In addition to the online transactions in e-Commerce, reputation schemes can be used in purely P2P, MANETs and WSNs systems that facilitate interactions among entities distributed over a network. For instance, many trust-based routing protocols in WSNs and MANETs assess trustworthiness of a node in the networks by considering third-party opinions and reputation as well as their own experiences based on their understanding to make sure that a node is not going to be mis-behavioured and compromised. Based on the trustworthiness value, a decision maker will choose whether the node is put into routing paths or not. For example, a time-sensitive and context-dependent trust scheme in MANET is proposed as a combination of self-measurement and neighbor sensing (as recommendation) for enhancing trust evaluation accuracy[35]. M. Nitti *et al*. in [34] have also proposed a trust management scheme in the SIoT that incorporates several TIs extracted from feedbacks such as *credibility*, *relationship factors*, and *transaction factors*; as well as incorporates some TIs from direct knowledge such as *computational capabilities* showing the potentiality of an object to damage other objects.

Another notion of trust is ranks among webpages introduced by Google in their PageRank™ mechanism [8]. In this example, webpages are listed in descending orders of *levels of trust* of the trust between a user and a webpage. The *trust goal* in this case is that the webpages should be the correct targets the user is searching for. The mechanism actually assesses a composite of reputation and importance of a webpage by observing network behaviors with an assumption that "*the more back-links to a webpage, the more reputation and importance it gets (and higher probability users will visit such webpage)"*. In this sense, PageRank™ value is partial trustworthiness of a webpage and it is used as a TI. Even though PageRank™ is just a portion of trust and does not carry some important characteristics (e.g., subjectiveness and transitivity); in this webpage ranking scenario, it is effectively used on behalf of trust.

3.3. Trust Evaluation versus Risk Management

375 Apart from the main content of the article, it is worth to mention the correlation between trust
376 evaluation and risk management due to the need for assessing risk (in some degree) as environmental
377 factors when evaluating trust. Managing risk for a computer system is a complex and multifaceted
378 process including (i) frame risk; (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor
379 risk. These four tasks require a full investigation of vulnerabilities, threats and risks in networking
380 systems [36]. The analysis of vulnerabilities, threats, and risks is also required in the trust evaluation
381 but it is not necessarily fully involved as in the risk management. Instead, trust evaluation takes
382 social-related factors (i.e., Experience and Third-party Opinions) into account when judging trust
383 (Figure 4). Risk management assesses an entity (i.e., a computer system) from the perspective of a
384 system (system-centric) while trust considers the entity (the trustee) under perspectives of a trustor,
385 expressing a subjective view of the trustor on the trustee in an associated social context (human-
386 centric).



387
388 **Figure 4.** Trust Evaluation and Risk Management in comparison

389 **4. REK Trust Evaluation Model in the SIoT**

390 *4.1. REK Trust Evaluation Model*

391 We propose a trust evaluation model that comprises of triad of Reputation, Experience and
392 Knowledge TIs so-called REK Trust Evaluation Model (Figure 5). The reason to come up with the
393 three TIs is that in social science, people normally base their determination of trust on three main
394 sources: (i) public opinion on a trustee (as Reputation); (ii) previous transaction with a trustee (as
395 Experience); and (iii) understandings on a trustee (as Knowledge). We believe this social cognitive
396 process could be applied to the SIoT environment.

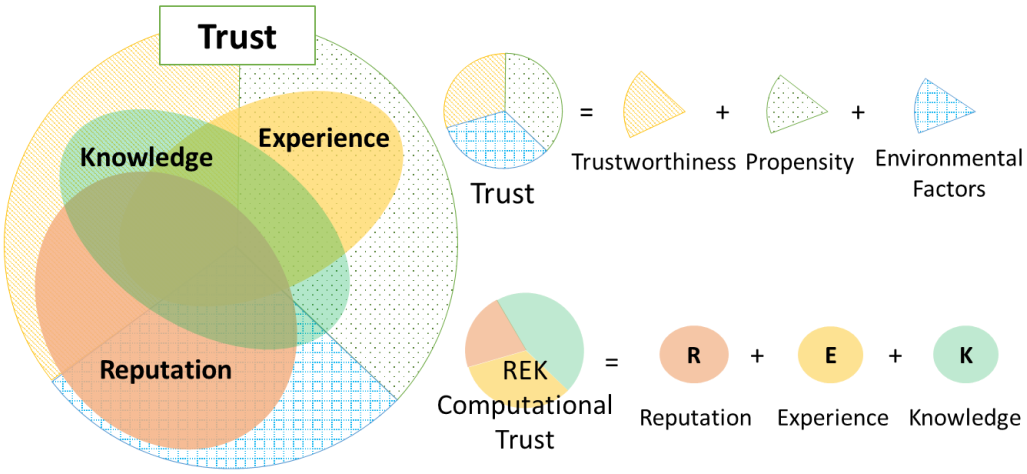


Figure 5. Reputation, Experience and Knowledge as the three indicators in the REK Trust Evaluation Model

Knowledge TI is the *direct trust* mentioned in Section 3 that renders trustor's perspective on trustee's trustworthiness in a respective environment. Knowledge TI can be obtained based on limited available information about characteristics of the trustee and the environment under the trustor's observation. Knowledge TI can reveal a portion of trust which is illustrated in Figure 5. It indicates more about trustworthiness of the trustee and trustor's propensity but not much about the environmental vulnerabilities, threats and risks.

Experience and Reputation TIs are social features and attained by accumulating previous interactions among entities in the SIoT over time. Experience TI is a personal perception of the trustee's trustworthiness by analyzing previous interactions from a specific trustor to a particular trustee in various contexts. As the personal perception, Experience TI indicates more about trustor's propensity but not trustee's trustworthiness and environmental factors due to limited knowledge obtained. Reputation TI, instead, reflects global perception about a trustee by aggregating all previous experiences from entities (in a society) with this trustee. Thus, Reputation TI is able to effectively exhibit about the trustee's trustworthiness and the environment characteristics; but not about the trustor's propensity (Figure 5). In SIoT scenarios with billions of entities, there is very high possibility that there are no prior interactions between two any entities, resulting in no Experience. Therefore, Reputation TI is a necessary indicator for trust, especially in case there are no previous interactions between a trustor and a trustee. Reputation is taken into account when evaluating trust because of the propagation characteristic of trust: Each entity (a trustor) has previous interactions with a specific entity (as the trustee) has its own opinions; and a reputation model (or a recommendation model) let it share the opinions (as its recommendations) to others. Entities, then, can refer the opinions as one of the cues of trust to personally judge trust. By doing so, trust is propagated throughout the network.

By synthesizing the three TIs, REK Trust Evaluation Model consolidates the *computational trust* so that it can be used on behalf of the *complete trust* in most of cases in the SIoT environment with high accuracy.

4.2. Knowledge TI Evaluation Model

Knowledge TI unfolds perception of a trustor toward a trustee about how trustworthy it accomplishes a trust goal in a specific context in SIoT. It leverages the direct trust evaluation model mentioned in Section 3, thus, comprises of two major tasks: (i) specify a set of TAs for the trustee's trustworthiness that reflects the trustor's propensity and the environmental factors; and (ii) an aggregation mechanism to combine these TAs for deriving the *direct trust* as the Knowledge TI value. In this section, a general TAs set is introduced which covers sufficient information to evaluate *direct trust* in the SIoT environment; then, a TAs set for the specific use-case User Recruitment in MCS is

specified and described as the detailed illustration for the general TAs set. The second task will be clarified in Section 4.4.

4.2.1. A general set of TAs for Knowledge TI

For the first task, we specify six important attributes introduced in the system dependability concept namely Serviceability, Safety, Reliability, Confidentiality, Availability, and Integrity as six TAs for the *Ability dimension* of trustworthiness illustrated as D1 to D6 in Figure 6. These six TAs could precisely indicate capability of a trustee to dependably accomplish a trust goal. Besides, the *Ability dimension* might contain other TAs according to a specific scenario. For instance, in the User Recruitment in MCS use-case, *spatial distance* between a trustor and a trustee is considered as a TA (see Section 4.2.2). The meanings of the six TAs in quantifying trustworthiness are as following:

- **Availability:** Probability of an entity in operation in a given period of time.
- **Confidentiality:** Preserving the authorized restriction on access and disclosure on data, information or system.
- **Integrity:** Ability to guard against improper modifications and destruction.
- **Safety:** A property to guarantee that an entity will not fail in a manner that would cause a great amount damage in a period of time.
- **Reliability:** Probability that a component correctly performs a required job in a specified period of time under stated conditions.
- **Serviceability:** Property indicating how easy and simply a system can be repaired or maintained.

Generally, combination of the TAs is a measure of a system's capability to accomplish a given task that can be defensibly trusted within a period of time [37]. However, it is not necessary to include all of the six TAs which could require huge effort. Instead, only some of them are necessarily taken into consideration according to a *specific trust goal* and *environmental factors*. The TAs are quantitatively or qualitatively measured based on different types of information and methodologies, which have been intensively explored over time[38]. Each TA can be slightly interpreted and attained differently depending on particular use-cases due to the variations and ambiguity of its linguistic meaning. Details of dependability models can be found on a large number of articles such as Cyber-Physical System (CPS) Framework [39] and Managing Information Security Risk [36] by National Institute of Standards and Technologies (NIST).

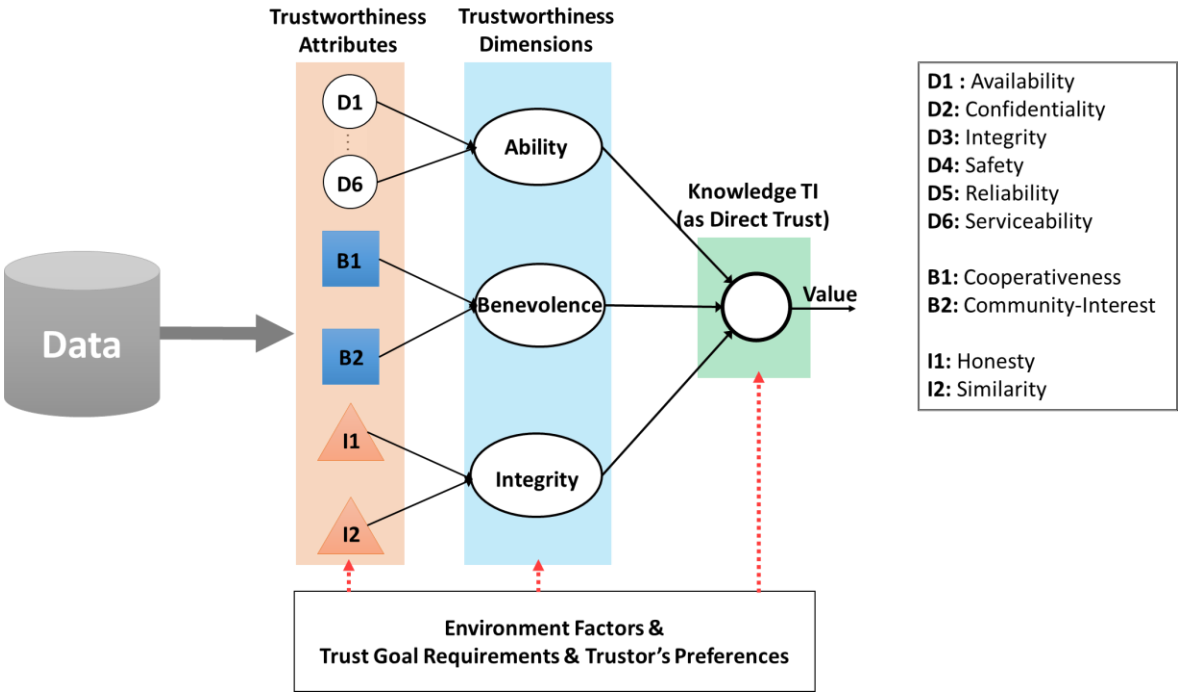


Figure 6. Evaluation Model for Direct Trust (as Knowledge TI)

As SIoT environment, we characterize two major TAs constituted the *Benevolence dimension* for Knowledge TI as *Cooperativeness* and *Community-Interest* illustrated as B1 and B2; and two TAs constituted the *Integrity dimension* as *Honesty* and *Similarity*, illustrated as I1 and I2 in Figure 6, respectively.

- **Cooperativeness:** this property indicates the level of cooperativeness between a trustor and a trustee based on the following hypothesis: "*the more cooperative between the two entities in a social network, the more trustworthy they are*". Cooperativeness can be calculated by considering the common features between the two entities such as mutual friends and same locations.
- **Community-Interest:** Due to the integration of social networks in SIoT, concept of community (of SIoT entities) is also introduced that refers to a group of entities sharing same characteristics (e.g., physical areas, a same goal, and same required tasks). This property indicates the level of community relationship between two entities based on the following hypothesis: "*the more similar among communities that entities belong to, the more trustworthy they get*".
- **Honesty:** a property indicates the level of honesty of an entity based on observation toward an entity that whether it conducts some suspicious interactions or it breaks social etiquette using a set of anomaly detection rules.
- **Similarity:** a property indicates the level of similarity between two entities (in terms of their features) using similarity measurement mechanisms between two profiles of entities [40]. This TA is taken into account because of the following hypothesis: "*a trustor tends to trust a trustee if they are similar*".

These four factors are chosen to determine an entity in a society which is trustworthy or malicious; and also to recognize the SIoT environment risks including various types of attacks in social networks such as self-promoting, bad mouthing, and ballot stuffing [41]. Therefore, the combination of these four TAs guarantee to explicitly indicate whether an entity is trustworthy in a social network or not. And by integrating the Ability, a perceived trustworthiness in the SIoT environment could be effectively achieved.

4.2.2. User Recruitment in Mobile Crowd-Sensing Use-case

Most of applications and services in IoT heavily depend on massive amount of data collected from various types of sensors. However, traditional sensor network schemes have never reached to full potential or successfully deployed in the real world due to high installation cost, insufficient spatial coverage and so on. As a prospective solution for the traditional sensor networks, recently, the new sensing paradigm MCS has attracted attentions from both academia and industry [10]. MCS is a large scale sensing mechanism leveraging smart devices integrated with built-in sensors such as mobile phones, tablets, wearable devices and smart vehicles. It expands the traditional participatory sensing by involving both participatory sensory data from devices and social information from mobile social networking services [42]. MCS offers a large number of mobile sensing devices owners to share knowledge (e.g., local information, ambient context, noise level, and traffic conditions) acquired from their devices which further aggregated in cloud for large-scale sensing and intelligent mining [43] (Figure 7), thus enables a broad range of applications such as traffic planning, public safety, environment monitoring, and mobile social recommendation.

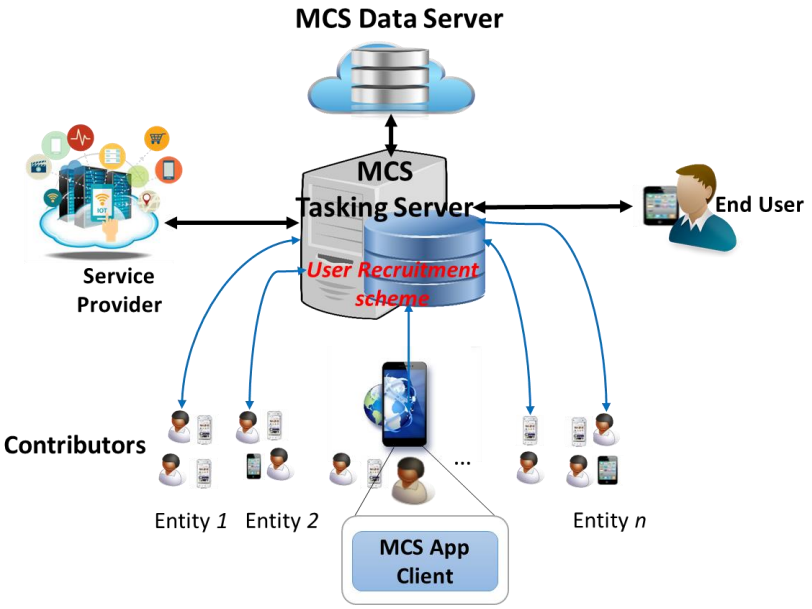


Figure 7. Mobile Crowd-Sensing System Architecture

One of the challenges in MCS is the recruitment of contributors for sensing tasks [44,45]. In a crowded urban area with high number of participants, it is critical to recruit trustworthy users to collect high quality of data as well as to guarantee security, privacy and data integrity. This challenge calls for an efficient User Recruitment scheme implemented in the MCS Tasking Server for making proper selection of contributors respecting to a specific sensing task as illustrated in Figure 7 (the sensing task requested by service providers and assigned based on a mechanism deployed at the MCS [46]). Note that in order to recruit users evolving in a sensing task, the MCS Tasking Server should manage an incentive scheme as rewards for their contributions because users sustain costs (e.g., energy consumption, data subscription, and privacy and security breach) for accomplishing assigned sensing tasks. The User Recruitment scheme specifies criteria for user eligibility to contribute to a crowd-sensing campaign by judging whether a user accomplishes a sensing task as expected. In other words, the MCS Tasking Server chooses contributors as it trusts to fulfil the sensing task. Therefore, this use-case turns to a trust scenario as follows:

Evaluate trust between the MCS Tasking Server (as the trustor) and owners of mobile devices (as the trustees), respecting to a sensing task (as the trust goal).

A sensing task called Traffic Congestion and Accident Report is considered as follows: Report accidents and traffic congestion at a specific crossroad X. The sensing task is event-based, spatial, urgent, and nearly real-time required. Contributors should report situation of the traffic situation at

the crossroad X by sending data obtained from smartphone sensors such as accelerometer, magnetometer, and GPS coordinates as well as submitting an image or a video about the traffic incidents [47,48]. Based on the proposed Knowledge TI model, a set of TAs is deliberately chosen as following:

- **Spatial Distance**: This TA shows the distance between a contributor and the crossroad X. The contributors should be close enough to the crossroad X so that it is able to report traffic situation correctly to the MCS server. The distance can be calculated based on the GPS coordinates of the smartphone and the crossroad X using the "*haversine*" formula presented in [49]. This TA belongs to the *Ability dimension* and should not exceed the distance boundary (as a threshold).
- **Availability**: Availability is a TA indicating the activeness of a user in getting connected to social activities. It shows how much a user uses his smart device for social applications and is ready to fulfil an assign task which is essential to consider for user recruitment. The Availability can be calculated based on both time spending on social network application and amount of data consumed [44,45]. This TA belongs to the *Ability dimension*.
- **Transmission Capability**: It is required to be reliable, fast, and secure when fulfilling important tasks in traffic incident reports; thus this indicator is essential for reflecting the capability of a smart device to transmit data in real-time or nearly real-time as well as in a secure and privacy manner without compromise. Therefore, this indicator includes several TAs in Ability dimension mentioned in Section 4.2.1 such as Reliability, Confidentiality and Integrity. For simplicity, we specify the level of the Transmission Capability based on some information: *signal strength, signal-to-interference-plus-noise-ratio* (*SIRN*), and the *communication technology* in use (*WiFi, LTE, 3G, WiMax*, and *Bluetooth*). For example, Transmission Capability is *high* when the user is using *4G LTE* for data transmission with high signal strength (*4G LTE Signal* ≥ *-50dBm*) and *high LTE SIRN (LTE SIRN* ≥ *12.5)* whereas it is *low* when *3G* is used with *low 3G SIRN (3G SIRN* ≤ *-5).*
- **Cooperativeness**: This TA represents the degree of a user cooperates with crowd-sensing tasks, thus, high cooperativeness indicates more opportunities that the user is willing to accomplish an assigned sensing task, and vice versa. This TA belongs to the *Benevolence dimension*. Cooperativeness can be simply calculated by using Equation (1):

$$Cooperativeness(i) = Frequency(i) \times \frac{|Number\ of\ tasks\ involved\ |}{|Number\ of\ tasks\ requested\ |} \quad (1)$$

where $Frequency(i)$ indicates how frequently the user i has involved in the crowd-sensing campaign. It is calculated based on Equation (2)

$$Frequency(i) = \frac{|Number\ of\ sensing\ tasks\ involved|}{|sampling\ period\ of\ time|} \quad (2)$$

The numbers of tasks requested is the number of times the MCS Tasking server has requested the user to participate in a sensing task; and the number of tasks involved is the number of times the user has accepted to involve in sensing tasks that the MCS has requested. The number of tasks canceled is the number of times the user cancels a sensing task when it has already accepted to involve in the sensing task. The number of requested, involved, and canceled sensing tasks of the user *i* is kept track and managed by the MCS Tasking Server.
- **Honesty**: This TA represents the degree of keeping promise once a sensing task is already assigned to a user. High honesty means that the user is not going to cancel a task once it is

assigned due to any cause whatsoever. This TA belongs to the *Integrity dimension* and it is simply measured by the equation (3).

$$Honesty(i) = 1 - \frac{|Number\ of\ tasks\ canceled|}{|Number\ of\ tasks\ involved|} \quad (3)$$

An aggregation mechanism for inferring the direct trust Knowledge TI will be prototyped in Section 4.5.

4.3. Experience TI Evaluation Model

Experience is a social concept that represents personal understandings and opinions about one entity to another based on its previous interactions to the counterpart. We propose a conceptual model for the Experience TI depicted in Figure 8 which computes experiences based on the three factors: the current value of Experience, the outcomes, and the timestamps of individual interactions. Therefore, an *outcome evaluation scheme* for the interactions is one of the important components in the Experience TI model. Various mechanisms can be used to deduce outcomes of interactions depending on particular scenarios. For instance, outcomes might be feedback (in both implicit and explicit forms) from consumers after each interaction (as used in many e-Commerce and reputation systems), might just be a Boolean value (or 0/1) generated by using an ACK message to track whether the interaction has successfully accomplished or not (as in some reputation-based trust systems). For example, in Wireless Sensor Networks, interactions are package transmissions between two nodes, if a transmission is successful, then the outcome of the interaction is 1, and 0 otherwise. In a file-sharing P2P networks, interactions are file transfer transactions. If a file is successfully transferred, then the outcome of the interaction is 1; otherwise is 0. The interaction is also in form of any types of relationship between two entities. For example, Google PageRank™ considers a hyperlink as an interaction between a source webpage and a destination webpage; and the outcome value is set as 1 [8].

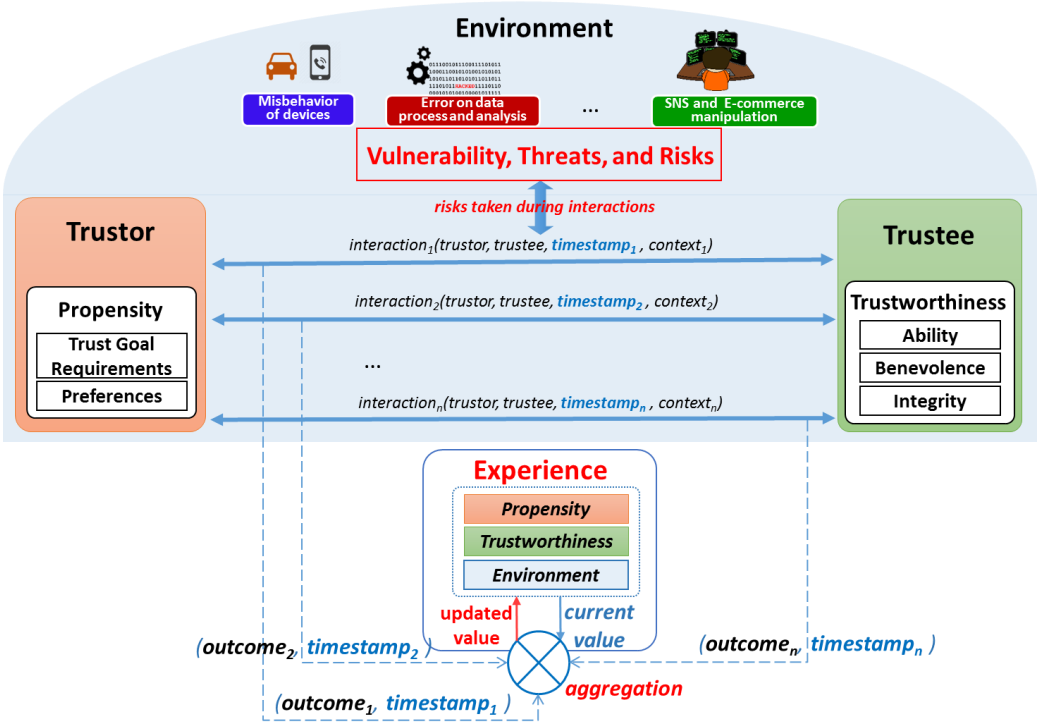


Figure 8. The Experience TI model in the REK Trust Evaluation

Another important component is an *aggregation model* for calculating Experience TI. There is an important assumption about experience relationship between humans in sociological environment: Experience accumulates for cooperative interactions and is decreased by uncooperative interactions. It also tends to decay over time if it is not maintained by interactions. This assumption has been

reasonably proven in many trust-related sociological literatures [50,51]. Thus, there are three trends of the experience relationship: Increase, Decrease, and Decay; and all of them are measured based on three features: *intensity of interactions*, *values of the interactions*, as well as *the current value of the experience*. Therefore, a mathematical linear difference equation could be used to model the trends of the Experience TI. We have proposed an Experience TI model in which an outcome of an interaction is either 0 (indicates uncooperative interaction) or 1 (indicates the cooperative interaction). The model consists of three trends is proposed as following:

- **Experience Increase (in case of a cooperative interaction occurs):**

The Experience Increase trend is modelled using a linear difference equation as following:

$$Experience_{t+1} = Experience_t + \Delta Experience_{t+1} \quad (4)$$

$$\text{where } \Delta Experience_{t+1} = \alpha - \frac{\alpha}{max_{Experience}} \times Experience_t \quad (5)$$

where $Experience_t$ indicates Experience TI at the time *t;* and $\Delta Experience_t$ indicates the increase value of Experience TI. α is a parameter indicating the *maximum increase value* of the experience. $max_{Experience}$ is a parameter indicating the *maximum value* of Experience TI (obviously $\alpha < max_{Experience}$). Usually it is more convenient for Experience TI to use the same scale with trust (i.e., the range of [0, 1]), thus, $max_{Experience}$ is 1. Consequently, the equation (4) and (5) can be rewritten as:

$$Experience_{t+1} = Experience_t + \alpha \times (1 - Experience_t) \quad (6)$$

$$\text{or } Experience_{t+1} = (1 - \alpha) \times Experience_t + \alpha \quad (7)$$

As shown in the equation (6), the *increase value* $\Delta Experience_{t+1} = \alpha \times (1 - Experience_t)$ is relatively large when the current value $Experience_t$ is small; but the *increase value* is reaching to 0 when the current value $Experience_t$ is high (approaching to 1).

- **Experience Decrease (in case of an uncooperative interaction occurs):**

The mathematical model for the Experience Decrease is as following:

$$Experience_{t+1} = Max\langle min_{Experience}, Experience_t - \beta \times \Delta Experience_{t+1}\rangle \quad (8)$$

where $\Delta Experience_{t+1}$ is specified as in equation (2); and β is as a damping factor controlling the rate of the decrease. The β parameter can be fixed or dynamic depending on situations, but it should be always greater than 1 because the experience relationship is hard to gain but easy to lose. $min_{Experience}$ is a parameter indicating the minimum value of the experience (i.e., 0), which guarantees that the experience value cannot go lower than that.

- **Experience Decay (in case of no interaction):**

Experience TI decreases if there is no interaction during a period of time. However the rate of the decrease may vary according to the level of current status of the relationship (i.e., the current experience value). If the current status is high (meaning that there is a strong tie between two entities) then the decrease is not much; but if current status is low (i.e., a weak tie between the two) then the decrease is much. Hence, experience is assumed to require periodic maintenance but strong ties tend to persist longer even without reinforcing cooperative interactions. Decay is assumed to be inversely proportional to the current experience value; thus, experience with a high value will exhibit less decay than experience with a low value. Then, the mathematical model for the Experience Decay is proposed as following:

$$Experience_{t+1} = Max\langle min_{Experience}, Experience_t - \Delta decay_{t+1}\rangle \quad (9)$$

$$\text{where } \Delta decay_{t+1} = \delta \times \left(1 + \gamma - \frac{Experience_{t-1}}{max_{Experience}}\right) \quad (10)$$

The δ is a parameter indicating the *minimal decay value* of Experience which guarantees that even strong ties still get decreased if experience is not maintained. γ is a parameter indicating the *rate of decay* which can be fixed or dynamic depending on particular situations.

According to the Experience TI model, in order to obtain a high experience value (i.e., a strong tie between a trustor and a trustee), it is required to have many cooperative interactions in a short duration of time. And when it gets high, it is not easy to decay as time goes by. However, uncooperative interactions can highly damage the experience relationship, especially when the current state is not strong. This is similar to what happens in the real human world, thus, we believe the proposed Experience TI model can effectively migrate the experience relationship from human sociology environment to entities in the SIoT.

4.4. Reputation TI Evaluation Model

Reputation is a social concept which corresponds to what is generally understood about entity's characteristics. Reputation of any entity should be public and is determined by aggregating opinions of other in its social groups. Reputation has been intensively carried out in both computer sciences and information sciences recent years [7,52-54]. A reputation system is frequently found in e-Commerce websites for encouraging online transactions by providing evidences of trust to help people interact with each other without having firsthand knowledge. Thus, in this case, reputation can serve as a basic for trust. Reputation systems are mostly based on feedback from the participants in the transactions (as the trustors) about how a trustee has accomplished a given task (trust goal), in both positive and negative opinions. This feedback is then aggregated and presented to the public as an estimate of the trustee' trustworthiness. Therefore, a reputation mechanism is necessary for managing feedback as well as for evaluating, propagating, and maintaining reputation values for each entity in SIoT. For instance, eBay, IMDb and Keynote use a centralized trust authority to establish and maintain user ratings whereas Google has developed a distributed approach for assessing reputation of webpages based on backlinks. They use several heuristic algorithms for reputation integration and update on evaluation process.

In the scenarios of the SIoT environment, as mentioned in Section 4.3, feedback is a form of outcomes of interactions; and Experience TI is considered as an aggregation of feedback from a specific entity to another. Experience TI model shows that each of entities (as the trustor) which has previous interactions with a specific entity (as the trustee) holds an opinion about the trustee as its experiences. And if all of these entities share their opinions as *recommendations* about the trustee to others, we can come up with a model that aggregates these *recommendations* to form a unique value about the trustee as the trustee's reputation. A necessary consideration is that each of the *recommendations* contributes differently to the trustee's reputation. The weight a trustor's *recommendation* contributing to the trustee's reputation depends on both Experience TI (between the trustor and the trustee) and Reputation of the trustor itself. Therefore, an appropriate reputation model should not only take the experience values into account but also the reputation values of the trustors. It is reasonable because obviously, an entity with high reputation contributes more than an entity with lower reputation to the trustee's reputation.

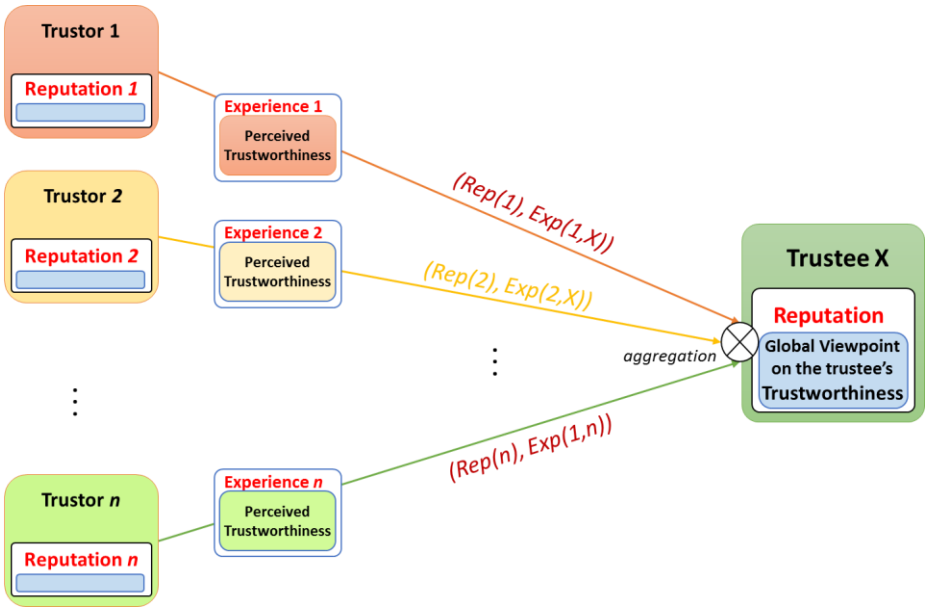


Figure 9. Conceptual Reputation Model incorporating the Experience concept

We have come up with a non-bias mechanism for calculating recommendation and reputation values of trust for all entities in a distributed network in [55]. The mechanism, however, is conducted in the centralized authority and it requires to aggregate necessary information about the social relationships of both trustors and the trustee. In this article, inspired by the PageRank™ idea in [8], we have proposed a novel approach to calculate reputation values for entities over the SIoT networks. Two challenges appeared when designing a model for the Reputation TI based on the PageRank™ algorithm: (i) Different weights of recommendations from many entities to a particular entity; and (ii) Recommendations could be both positive and negative; positive recommendations occur when Experience value $Exp(i,N) > \theta$ result in increasing reputation of the target entity N whereas negative recommendations ($Exp(j,N) < \theta$) should reduce reputation. θ is the threshold parameter indicating whether an Experience is considered as negative or positive. The original PageRank™ considers same weights for all links from a webpage to another and the mathematical model correctly works for only positive links' values (the weights for all links are assigned as 1/N where N is the total number of webpages in a network).

A modification of the PageRank™ model for the Reputation TI so-called Rep-Ranking is proposed as following:

$$Rep_{Pos}(X) = \frac{(1-d)}{N} + \mathrm{d} \times \left(\sum_{\forall i} Rep_{Pos} \times \frac{Exp(i,X)}{C_{Pos}(i)} \right);\ \forall i\ that\ Exp(i,N) > \theta \quad (8)$$

$$Rep_{Neg}(X) = \frac{(1-d)}{N} + \mathrm{d} \times \left(\sum_{\forall i} Rep_{Neg}(i) \times \frac{1 - Exp(i,X)}{C_{Neg}(i)} \right);\ \forall i\ that\ Exp(i,N) < \theta \quad (9)$$

$$Rep(X) = \mathrm{Max}\left(min_{Rep}\ , Rep_{Pos}(X) - Rep_{Neg}(X) \right) \quad (10)$$

where:

- N is total number of entities in the networks for calculating Reputation
- $Rep_{Pos}(i)$ is called positive reputation of the entity i which considers only positive recommendations.
- $C_{Pos}(i) = \sum_{Exp(i,j)>\theta} Exp(i,j)$ is the total values of all positive recommendations that the entity i is currently sharing.
- $Rep_{Neg}(i)$ is called negative reputation of the entity i which considers only negative recommendations.

- $C_{Neg}(i) = \sum_{Exp(i,j)<\theta}(1 - Exp(i,j))$ is the total values of all complements of the negative recommendations that the entity i is currently sharing.
- $Rep(i)$ is the reputation of the entity i that we are interested.
- $min_{Reputation}$ is a parameter indicating the minimal value of reputation (i.e., 0). This guarantee the reputation value will not go below the $min_{Reputation}$.
- $Experience(i, X)$ is the Experience TI from the entity i toward the entity X described in Section 4.3.
- d is the damping factor. Various studies on PageRank-related literature have tested different damping factors for ranking webpages on the Internet, and they have come up with an appropriate value around 0.85. The research on the damping factor for the Reputation TI model is left as our future work.

Similar to PageRank™, the equations (8), (9), and (10) form a normalized probability distribution of the reputations (positive reputation, negative reputation and overall reputation) after conducting a number of iterations throughout the network; as well as calculating and updating reputation values for all entities in the network after each iteration. Therefore, the reputation model can be implemented in a centralized system to calculate reputation values for all of entities in a social network. Details of the mechanism can be found in various related literature such as in [8], [56-58]. This approach could face a critical challenge when the size of a network dramatically increases (i.e., millions of entities). However, by using classification machine learning algorithms with an appropriate semi-distributed architecture, whole social network can be divided into smaller sub-populations, resulting in the feasibility of conducting the proposed reputation model [59,60].

4.5. Aggregation Mechanism for REK Trust Evaluation Model

The outcome of the REK Trust Evaluation model is aggregated based on the triad Reputation, Experience, and Knowledge TIs. It also requires to aggregate TAs to derive Knowledge TI. As clarified in the conceptual trust model as well as the REK model, these aggregations should take both environmental factors and trustor's propensity into consideration. Technically, there are two common approaches to attain TIs from associated attributes; and to finalize an overall trust value from the three TIs. The choice between the two depends on specific scenarios such as information modelling of TAs, of the trustor's preferences, and of the environmental factors.

The first approach is to use mathematical models such as weighted sum [61,62], Bayesian neutron networks [63,64], and machine learning algorithms such as linear regression [65]. These models use mathematical models to express trustor's propensity and environment conditions by assigning weights for individual features (i.e., TAs and TIs). These values can be autonomously updated depending on outcomes of the models by using a feedback mechanism. The second method makes use of an inference engine for inferring new knowledge from a knowledge-base such as reasoning mechanisms [66] and fuzzy-based mechanisms [18,67]. These inferring mechanisms are frequently used for deriving causal-consequence knowledge that is also appropriate for incorporating trustor's propensity and environmental factors. In the second approach, all trust-related information already obtained (e.g., TAs, Experience TI, and Reputation TI) are represented in form of facts; trustor's propensity and environmental factors are represented in form of logics applied upon the facts (e.g., rules in reasoning mechanisms, and membership functions in fuzzy-based mechanisms). Based on the set of logic, an inference engine can draw new knowledge that is being interested such as Knowledge TI and the overall trust value. In real implementation, a set of default logics should be already investigated and deployed for all entities. Then a trustor might have more preferences or a considering environment might have different conditions; then these factors are converted into logics that replace or supplement the default set of logics.

For example, we have used the Apache Jena framework in the trust demonstration for the User Recruitment in MCS use-case which integrates several types of inference engines including the generic rule-based reasoner that enables *predefined rules*. Before that, all TAs, Reputation TI, and

Experience TI already obtained are converted into semantic information as metadata in forms of facts in Description Logics [68] represented in RDFS/OWL languages (Figure 10). The Jena integrated rule-based reasoner supports both *forward chaining* and *tabled backward chaining* reasoning strategies as well as the hybrid approach. For example, *generic hybrid reasoner* in the Jena framework is used in the demonstration to infer *reputation value* and *experience value* in form of *levels* (i.e., *low*, *medium*, and *high*) from the actual calculated values (the calculated values are in the range [*0-1*] and obtained using the proposed Experience TI model and Reputation TI model); as well as to infer the *level of trust* which is the overall trust value we are interested.

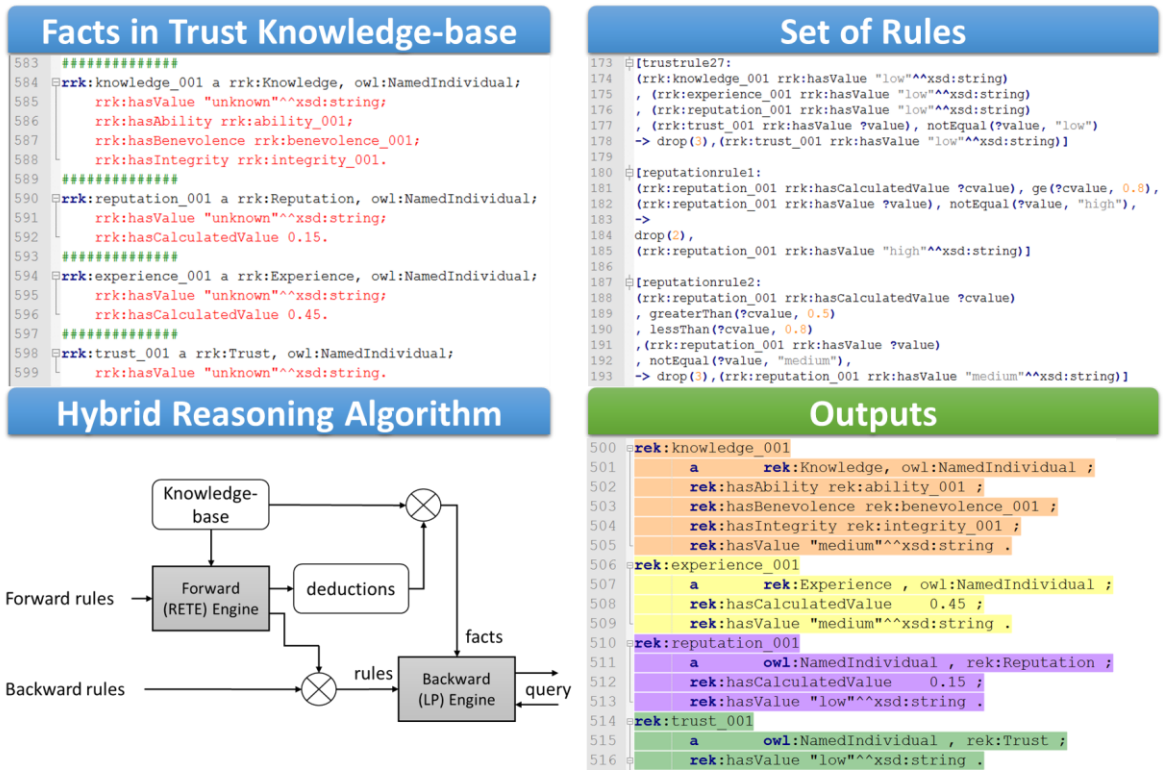


Figure 10. Reasoning mechanism used in a demonstration for inferring trust value in the REK trust model

In the User Recruitment in MCS demonstration, values of TAs such as Spatial Distance, Availability, Dependability, Cooperativeness and Honesty are already obtained and then represented in form of facts in the trust knowledge-based. Trustor's propensity is represented in form of rules upon literals introduced in the facts. For example, with a same trustee with calculated reputation value is *0.45*; a trustor could consider that Reputation TI is *low* but another trustor considers Reputation TI as *medium*. These kinds of preferences are represented using Jena syntax rules illustrated in Figure 10. Then a hybrid reasoner is used to derive the overall trust value as the *level of trust* (i.e., *low*, *medium*, and *high*). As illustrated in Figure 10, based on facts and set of rules, the reasoning engine infers the Reputation TI value as "*low*", the Experience TI value as "*medium*" and the Knowledge TI value as "*medium*". These inferred values are as new knowledge (new facts) in the Knowledge base, as a result, additional rules are triggered; new other facts are created. This process would iterate until a goal has reached or no rules can be matched (i.e., when the overall trust value (*level of trust*) is obtained). It is worth to note that different trustor profiles have different associated set of rules, resulting in different subjective level of trust inferred.

5. Conclusions and Future Work

In this article, we have provided a comprehensive understanding on trust concept in the SIoT with the REK evaluation model for trust which incorporates the three major TIs Reputation, Experience and Knowledge considering multi-dimensional trust aspects from direct observation to third-party information. We also have examined necessary TAs for covering the direct observation

of trustworthiness as the Knowledge TI considering the three dimensions Ability, Benevolence and Integrity of any entities in the SIoT environment. We have also proposed prototypes for the Experience and Reputation TIs by proposing the associated mathematical models leveraging the sociological behaviors of human in the real world as well as the Google PageRank™ ideas in the webpage ranking areas, respectively. Finally, we combine the TAs of the Knowledge TI, the Experience TI and the Reputation TI using Semantic-Web technologies for finalizing the overall trust value as the *level of trust*.

This article opens a large number of research directions in order to fulfil the trust evaluation platform. The first direction is to adapt the trust evaluation model to various scenarios and use-cases that require to figure out a set of TAs for Knowledge TI in detail as well as appropriate mathematical parameters for Experience and Reputation TIs.

The second direction could be a smart mechanism to reflect the trustor's propensity and environmental factors to the trust evaluation model such as an autonomous weighted sum mechanism with machine learning for adaptively changes the weights according to a particular context. Another solution could be a smart rules generators for the trust knowledge-base so that the final trust value will be obtained in a context-awareness manner. In the demonstration in Section 4.5, the rules are predefined using understanding of a specific service with user preferences on trust. This can be improved by using machine learning techniques for rule pattern recognition in an automatic rule creation mechanism.

Another research direction could be the improvement of the reasoning mechanism so that it can autonomously adapt with changes of the knowledge base, resulting in an autonomous trust computation framework and with real-time data streaming (stream reasoning). The usage of Semantic Web technologies such as the Ontology, RDFS and reasoning mechanism could also be improved for more complex use cases and for the support of real-time processing and scalability.

Final direction could be other mathematical models for the Experience and Reputation TIs which not only base on intensity and outcomes of interactions but also other complicated features extracted from particular contexts such as features of mutuality or difference in social environment

Acknowledgments: This research was supported by the ICT R&D program of MSIP/IITP [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system] and EU funded Horizon 2020 Wise-IoT project [Worldwide Interoperability for Semantics IoT].

Author Contributions: "Nguyen Binh Truong and Gyu Myoung Lee mainly contributed to the research work by investigating challenges, state-of-the-art trust approaches, proposing evaluation models and writing the paper; Nguyen Binh Truong also conceived and designed the use-case as well as performed the simulations; Hyunwoo Lee contributed in reviewing and improving the trust evaluation model for the use-case; Bob Askwith contributed in reviewing the paper, its structure as well as its intellectual content. Gyu Myoung Lee supervised the work.

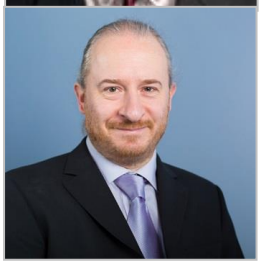
Conflicts of Interest: The authors declare no conflict of interest.

Nguyen Binh Truong received Master and Bachelor degrees in Computer Engineering from Pohang University of Science and Technology, South Korea (POSTECH) and Hanoi University of Science and Technology, Vietnam (HUST) in 2008 and 2013, respectively. He is currently doing PhD at Liverpool John Moores University (LJMU), United Kingdom. He was a Software Engineer at DASAN Networks, a leading company on Networking Products and Services in South Korea from 2012 to 2015.

His research interests are including, but not limited to, Trust in the Internet of Things, Vehicular Network, Software Defined Networking, Wireless Networks, Sensor Networks, Fog and Cloud Computing. His work is also involved in problems of Load Balancing, Channel Utilization and Energy Efficiency Protocols. He is an IEEE and ComSoc student members.

Hyunwoo Lee received his MS degree and PhD in 1995 and 2005, respectively, from the Korea Aerospace University. He is currently an assistant vice president of the Media Research Division of ETRI. His main research interests include smart media, tera-media, and open screen service platforms.

His current research interests also include trusted information infrastructure for realizing trustworthy IoT eco-system.



Bob Askwith received a BSc in Software Engineering in 1996 and a PhD in Network Security in 2000, both from LJMU. He is a Principal Lecturer in the Department of Computer Science at LJMU. He leads the development and delivery of Cybersecurity programs within the department. His research interests are focused on the security of computer networks, especially mobile, wireless, and ad hoc. He has been involved in security projects funded by UK Government and EU.

Gyu Myoung Lee received his BS degree from Hong Ik University, Seoul, Korea, in 1999 and his MS and PhD degrees from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2000 and 2007.

He is with the Liverpool John Moores University (LJMU), UK, as a Senior Lecturer from 2014 and with KAIST Institute for IT convergence, Korea, as an adjunct professor from 2012. Prior to joining the LJMU, he has worked with the Institut Mines-Telecom, Telecom SudParis, France, from 2008. Until 2012, he had been invited to work with the Electronics and Telecommunications Research Institute (ETRI), Korea. He also worked as a research professor in KAIST, Korea and as a guest researcher in National Institute of Standards and Technology (NIST), USA, in 2007.

His research interests include Internet of things, future networks, multimedia services, and energy saving technologies including smart grids. He has been actively working for standardization in ITU-T, IETF and oneM2M, etc., and currently serves as a WP chair in SG13, a Rapporteur of Q16/13 and Q4/20 as well as an Editor in ITU-T. Recently he has also appointed as the chair of newly established ITU-T Focus Group on data processing and management. He is a Senior Member of IEEE.

References

1. Xiong, G.; Zhu, F.; Liu, X.; Dong, X.; Huang, W.; Chen, S.; Zhao, K. Cyber-physical-social system in intelligent transportation. *IEEE/CAA Journal of Automatica Sinica* **2015**, *2*, 320-333.
2. Sheth, A.; Anantharam, P.; Henson, C. Physical-cyber-social computing: An early 21st century approach. *IEEE Intelligent Systems* **2013**, *28*, 78-82.
3. Atzori, L.; Iera, A.; Morabito, G. Siot: Giving a social structure to the internet of things. *IEEE communications letters* **2011**, *15*, 1193-1195.
4. 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. *Computer networks* **2012**, *56*, 3594-3608.
5. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in internet of things: The road ahead. *Computer Networks* **2015**, *76*, 146-164.
6. Mahalle, P.N.; Thakre, P.A.; Prasad, N.R.; Prasad, R. In *A fuzzy approach to trust based access control in internet of things*, Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), Atlantic City, NJ, June 2013; IEEE: Atlantic City, NJ.
7. Josang, A.; Ismail, R.; Boyd, C. A survey of trust and reputation systems for online service provision. *Decision Support System* **2007**, *43*, 618–644.

8. Brin, S.; Page, L. Reprint of: The anatomy of a large-scale hypertextual web search engine. *Computer Networks* **2012**, *56*, 3825–3833.
9. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for internet of things. *Journal of network and computer applications* **2014**, *42*, 120-134.
10. Guo, B.; Wang, Z.; Yu, Z.; Wang, Y.; Yen, N.Y.; Huang, R.; Zhou, X. Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm. *ACM Computing Surveys (CSUR)* **2015**, *48*.
11. Rousseau, D.M.; Sitkin, S.B.; Burt, R.S.; Camerer, C. Not so different after all: A cross-discipline view of trust. *Academy of management review* **1998**, *3*, 393-404.
12. Alcalde, B.; Dubois, E.; Mauw, S.; Mayer, N.; Radomirović, S. In *Towards a decision model based on trust and security risk management*, The Seventh Australasian Conference on Information Security, Wellington, New Zealand, 2009; Wellington, New Zealand, pp 61-70.
13. Thompson, K. Reflections on trusting trust. *Communications of the ACM* **1984**, *27*, 761-763.
14. Truong, N.B.; Cao, Q.H.; Um, T.W.; Lee, G.M. In *Leverage a trust service platform for data usage control in smart city*, IEEE Globecom 2016, Washington, DC USA, 2016; Washington, DC USA.
15. Grandison, T.; Sloman, M. A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, **2000**, *3*, 2-16.
16. Lewis, J.D.; Weigert, A. Trust as a social reality. *Social forces* **1985**, *63*, 967-985.
17. Schoorman, F.D.; Mayer, R.C.; Davis, J.H. An integrative model of organizational trust: Past, present, and future. *Academy of Management review* **2007**, *32*, 344-354.
18. Chang, E.; Hussain, F.K.; Dillon, T.S. In *Fuzzy nature of trust and dynamic trust modeling in service oriented environments*, The 2005 workshop on Secure web services, Fairfax, USA, 2005; Fairfax, USA.
19. Mayer, R.C.; Davis, J.H.; Schoorman, F.D. An integrative model of organizational trust. *Academy of management review* **1995**, *20*, 709-734.
20. Yan, Z.; Ding, W.; Niemi, V.; Vasilakos, A.V. Two schemes of privacy-preserving trust evaluation. *Future Generation Computer Systems* **2016**, *62*, 175-189.
21. Atif, Y. Building trust in e-commerce. *IEEE Internet Computing* **Feb., 2002**, *6*, 18 - 24.
22. Li, X.; Liu, L. In *A reputation-based trust model for peer-to-peer e-commerce communities*, IEEE International Conference on E-Commerce, New York, USA, 2003; New York, USA, pp 275-284.
23. Bao, F.; Chen, I. In *Trust management for internet of things and its application to service composition*, IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), USA, 2012; USA.
24. Yu, Y.; Li, K.; Zhou, W.; Li, P. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of network and computer applications* **2012**, *35*, 867-880.
25. Govindan, K.; Mohapatra, P. Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys & Tutorials* **2012**, *14*, 279-298.
26. Cho, J.H.; Swami, A.; Chen, R. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials* **2011**, *13*, 562-583.
27. Li, J.; Li, R.; Kato, J. Future trust management framework for mobile ad hoc networks. *IEEE Communications Magazine* **2008**, *46*.
28. Kraounakis, S.; al., e. A robust reputation-based computational model for trust establishment in pervasive systems. *IEEE Systems Journal* **2015**, 878-891.

29. Wang, J.P.; Bin, S.; Yu, Y.; Niu, X.X. Distributed trust management mechanism for the internet of things. *Applied Mechanics and Materials (Appl. Mech. Mater.)* **Aug. 2013**, 2463-2467.
30. Palaghias, N.; Loumis, N.; Georgoulas, S.; Moessner, K. In *Quantifying trust relationships based on real-world social interactions*, IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016; Kuala Lumpur, Malaysia.
31. Can, A.B.; Bhargava, B. Sort: A self-organizing trust model for peer-to-peer systems. *IEEE transactions on dependable and secure computing* **2013**, *10*, 14-27.
32. Sherchan, W.S.; Nepal; Paris, C. A survey of trust in social networks. *ACM Computing Surveys (CSUR)* **2013**, *45*.
33. Bao, F.; Chen, I. In *Dynamic trust management for internet of things applications*, International Workshop on Self-Aware Internet of Things (Self-IoT), USA, 2012; USA.
34. Nitti, M.; Girau, R.; Atzori, L.; Iera, A.; Morabito, G. In *A subjective model for trustworthiness evaluation in the social internet of things*, IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Australia, 2013; Australia.
35. Velloso, P.B.; Laufer, R.P.; Cunha, D.O.; Duarte, O.; Pujolle, G. Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE transactions on network and service management* **2010**, *7*, 172-185.
36. NIST. *Managing information security risk: Organization, mission, and information system view*; U.S. Department of Commerce: Gaithersburg, MD, United States, 2011.
37. Kumar, R.; Khan, S.A.; Khan, R.A. Revisiting software security: Durability perspective. *International Journal of Hybrid Information Technology (SERSC)* **2015**, *8*, 311-322.
38. Al-Kuwaiti, M.; Kyriakopoulos, N.; Hussein, S. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *IEEE Communications Surveys & Tutorials* **2009**, *11*, 106 - 124.
39. NIST. *Cyber-physical systems (cps) framework release 1.0*; US Department of Commerce: Gaithersburg, MD, USA, 2016.
40. Santini, S.; R.Jain. Similarity measures. *IEEE Transactions on pattern analysis and machine Intelligence* **1999**, *9*, 871-883.
41. Chen, I.; Bao, F.; Guo, J. Trust-based service management for social internet of things systems. *IEEE Transactions on Dependable and Secure Computing* **2015**, 1-14.
42. Ganti, R.K.; Ye, F.; Lei, H. Mobile crowdsensing: Current state and future challenges. *IEEE Communications Magazine* **2011**, *49*.
43. Guo, B.; Yu, Z.; Zhou, X.; Zhang, D. In *From participatory sensing to mobile crowd sensing*, IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Budapest, Hungary, 2014; Budapest, Hungary, pp 593-598.
44. Anjomshoa, F.; Catalfamo, M.; Hecker, D.; Helgeland, N.; Rasch, A. In *Sociability assessment and identification of smartphone users via behaviormetric software*, IEEE Symposium on Computers and Communications (ISCC), Messina, Italy, June 2016; Messina, Italy.
45. Fiandrino, C.; Kantarci, B.; Anjomshoa, F.; Kliazovich, D.; Bouvry, P.; Matthews, J. In *Sociability-driven user recruitment in mobile crowdsensing internet of things platforms*, IEEE Global Communications Conference (GLOBECOM), Washington DC, USA, 2016; Washington DC, USA.

46. An, J.; Gui, X.; Wang, Z.; Yang, J.; He, X. A crowdsourcing assignment model based on mobile crowd sensing in the internet of things. *IEEE Internet of Things Journal* **2015**, *2*, 358-369.
47. Bhoraskar, R.; Vankadhara, N.; Raman, B.; Kulkarni, P. In *Wolverine: Traffic and road condition estimation using smartphone sensors*, International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India 2012; Bangalore, India
48. Mohan, P.; Padmanabhan, V.N.; Ramjee, R. In *Nericell: Rich monitoring of road and traffic conditions using mobile smartphones*, ACM conference on Embedded network sensor systems, Raleigh, NC, USA, 2008; ACM: Raleigh, NC, USA, pp 323-336.
49. MovableType, L. Calculate distance, bearing and more between latitude/longitude points. Movable Type Ltd.: 2016.
50. Baumeister, R.F.; Leary, M.R. The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological bulletin* **1995**, *3*, 497.
51. Oswald, D.L.; Clark, E.M.; Kelly, C.M. Friendship maintenance: An analysis of individual and dyad behaviors. *Journal of Social and Clinical Psychology* **2004**, *3*, 413-441.
52. Kamvar, S.; Schlosser, M. In *The eigentrust algorithm for reputation management in p2p networks.*, 12th International Conference on World Wide Web, Budapest, 2003; Budapest, pp 640–651.
53. Josang, A.; Golbeck, J. In *Challenges for robust trust and reputation systems*, International Workshop on Security and Trust Management (STM), SaintMalo, France, 2009; SaintMalo, France.
54. Dellarocas, C. Reputation mechanism design in online trading environments with pure moral hazard. *Information Systems Research* **2005**, *16*, 209-230.
55. Jayasinghe, U.; Truong, N.B.; Um, T.W.; Lee, G.M. In *Rpr: A trust computation model for social internet of things*, IEEE Smart World Congress, Toulouse, France, 2016 Toulouse, France.
56. Tyagi, N.; Simple, S. Weighted page rank algorithm based on number of visits of links of web page. *International Journal of Soft Computing and Engineering (IJSCE)* **2012**, 2231-2307.
57. Ding, Y. Topic-based pagerank on author cocitation networks. *Journal of the Association for Information Science and Technology* **2011**, *62*, 449-466.
58. Backstrom, L.; Jure, L. In *Supervised random walks: Predicting and recommending links in social networks*, The fourth ACM international conference on Web search and data mining, HongKong, 2011; ACM: HongKong, pp 635-644.
59. Kotsiantis, S.B.; Zaharakis, I.; Pintelas, P. In *Supervised machine learning: A review of classification techniques*, Emerging Artificial Intelligence Applications in Computer Engineering: Real Word AI Systems with Applications in eHealth, HCI, Information Retrieval and Pervasive Technologies, Amsterdam, Netherlands, 2007; Amsterdam, Netherlands, pp 3-24.
60. Chandrashekar, G.; Ferat, S. A survey on feature selection methods. *Computers & Electrical Engineering* **2014**, *40*, 16-28.
61. Ren, Y.; Boukerche, A. In *Modeling and managing the trust for wireless and mobile ad hoc networks*, IEEE International Conference on Communication (ICC'08), Beijing, China, 2008; Beijing, China, pp 2129-2133.
62. Shaikh, R.A.; Jameel, H.; Lee, S.; Song, Y.J.; Rajput, S. In *Trust management problem in distributed wireless sensor networks*, IEEE international conference on Embedded and real-time computing systems and applications, New South Wales, Australia, 2006; New South Wales, Australia, pp 411-414.

949 63. Bao, F.; R.Chen; Guo, J. In *Scalable, adaptive and survivable trust management for community of interest*
950 *based internet of things systems*, IEEE Eleventh International Symposium on Autonomous Decentralized
951 Systems (ISADS), Mexico City, Mexico, 2013; Mexico City, Mexico.
952 64. Buchegger, S.; Jean-Yves, L.B. In *A robust reputation system for peer-to-peer and mobile ad-hoc*
953 *networks*, P2P Econ, Berkeley, U.S, 2004; Berkeley, U.S.
954 65. Jayasinghe, U.; Lee, H.W.; Lee, G.M. In *A computational model to evaluate honesty in social internet of*
955 *things*, The 32nd ACM Symposium on Applied Computing, Marrakesh, Morocco, April, 2017; Marrakesh,
956 Morocco.
957 66. Russell, S.J.; Norvig, P. Knowledge and reasoning. In *Artificial intelligence: A modern approach*, Prentice
958 Hall: New Jersey, 2014; pp 149-297.
959 67. Truong, N.B.; Won, T.U.; Lee, G.M. In *A reputation and knowledge based trust service platform for*
960 *trustworthy social internet of things*, Innovations in Clouds, Internet and Networks (ICIN), Paris, France,
961 2016; Paris, France.
962 68. Baader, F.; Calvanese, D.; McGuinness, D.; Nardi, D.; Patel-Schneider, P.F. *The description logic*
963 *handbook: Theory, implementation and applications*. Cambridge University Press: 2003.