



## LJMU Research Online

Lee, GM, Truong, NB, Lee, H and Askwith, RJ

**Toward a Trust Evaluation Mechanism for in the Social Internet of Things**

<http://researchonline.ljmu.ac.uk/id/eprint/6665/>

### Article

**Citation** (please note it is advisable to refer to the publisher's version if you intend to cite from this work)

**Lee, GM, Truong, NB, Lee, H and Askwith, RJ (2017) Toward a Trust Evaluation Mechanism for in the Social Internet of Things. Sensors, 17 (6). ISSN 1424-8220**

LJMU has developed **LJMU Research Online** for users to access the research output of the University more effectively. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LJMU Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain.

The version presented here may differ from the published version or from the version of the record. Please see the repository URL above for details on accessing the published version and note that access may require a subscription.

For more information please contact [researchonline@ljmu.ac.uk](mailto:researchonline@ljmu.ac.uk)

<http://researchonline.ljmu.ac.uk/>

1 Article

# 2 **Toward a Trust Evaluation Mechanism in the Social** 3 **Internet of Things**

4 **Nguyen Binh Truong**<sup>1</sup>, **Hyunwoo Lee**<sup>2</sup>, **Bob Askwith**<sup>1</sup> and **Gyu Myoung Lee**<sup>1,\*</sup>

5 <sup>1</sup> Department of Computer Science, Liverpool John Moores University, Liverpool, L3 3AF, UK;  
6 [n.b.truong@2015.ljmu.ac.uk](mailto:n.b.truong@2015.ljmu.ac.uk); [r.j.askwith@ljmu.ac.uk](mailto:r.j.askwith@ljmu.ac.uk); [g.m.lee@ljmu.ac.uk](mailto:g.m.lee@ljmu.ac.uk)

7 <sup>2</sup> Media Research Division, Broadcasting & Media Research Laboratory, Electronics and  
8 Telecommunications Research Institute (ETRI), Daejeon, 34129, Korea;  
9 [hwlee@etri.re.kr](mailto:hwlee@etri.re.kr)

10 \* Correspondence: [g.m.lee@ljmu.ac.uk](mailto:g.m.lee@ljmu.ac.uk); Tel.: +44-151-231-2052

11 Academic Editor: name

12 Received: date; Accepted: date; Published: date

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

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

---

## 30 **1. Introduction**

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

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

49 In the early years, most of IoT-related research articles have concentrated on RFID and Wireless  
50 Sensor Networks (WSNs) that aim at building underlying networking protocols, hardware and  
51 software components in order to enable interactions and communications among physical objects  
52 and cyber-space. However, a human-centric IoT environment in which human plays an important  
53 role in supporting application and services, are more and more perceptible. This is proven by the  
54 high rate of utilization of social phenomena and crowd intelligence when developing real-world IoT  
55 services. Consequently, the so-called Social Internet of Things (SIoT) has recently been proposed for  
56 illustrating the CPSS concept in which people are envisaged as an integral part of the IoT ecosystem  
57 [3,4]. However, the merging of physical objects, cyber components and humans in the SIoT will  
58 introduce new concerns for risks, privacy and security. Consequently, managing risk and securing  
59 the SIoT are broad in scope and pose greater challenges than the traditional privacy and security triad  
60 of integrity, confidentiality, and availability [5]. In this regard, trust is recognized as an important  
61 role in supporting both humans and services to overcome the perception of uncertainty and risk  
62 when making a decision.

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

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

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

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

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

## 110 2. Augmentation of Trust Concept in the SIoT

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

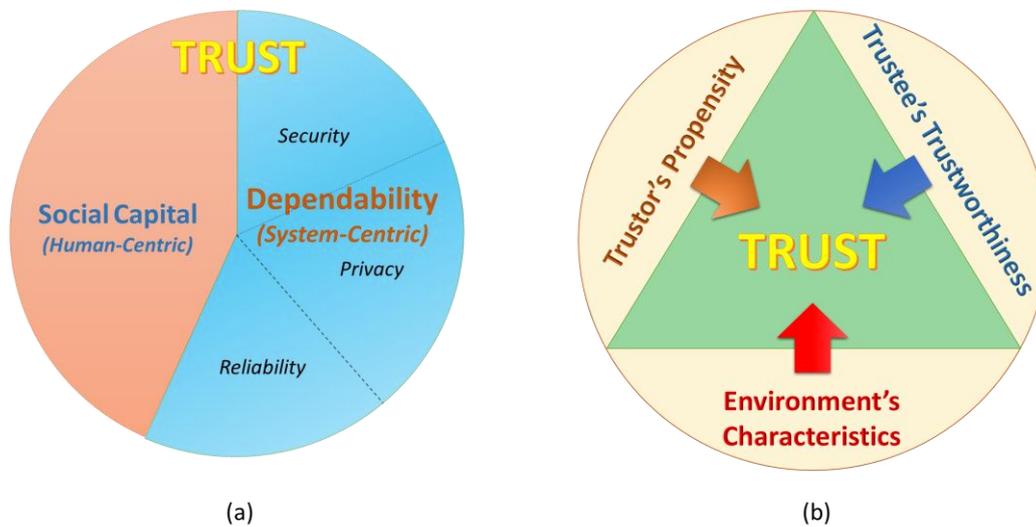
### 115 2.1. Trust Concept Clarification

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

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

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

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



146  
 147 **Figure 1.** (a) Trust concept in the relation with dependability and social capital; (b) Three main aspects of trust  
 148 in the SIoT environment

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

## 156 2.2. Definition of Trust in SIoT

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

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

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

## 171 2.3. Trust Characteristics

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

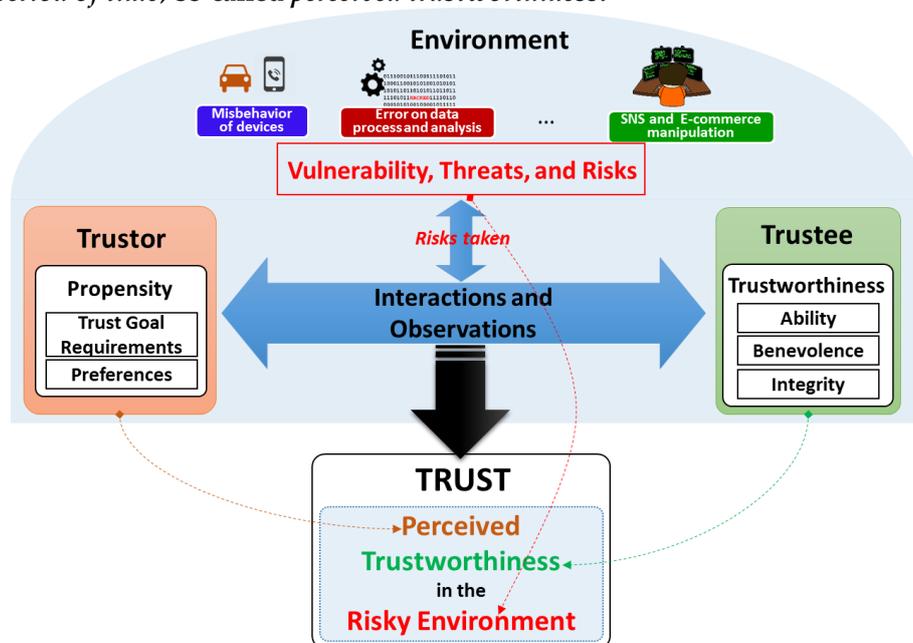
- 173 • **Trust is subjective:** With the same trustee and trust context, trust might be different from  
 174 trustors. In other word, trust is dependent on trustor's perspective. For example, Alice (highly)  
 175 trusts Bob but Charlie does not (for fulfilling a trust goal).

- 176 • **Trust is asymmetric:** Trust is a non-mutual reciprocal in nature although in some special cases,  
 177 trust may be symmetric. For example, if Alice (highly) trusts Bob (in fulfilling a trust goal) it  
 178 does not mean that Bob will (highly) trusts Alice (in fulfilling such trust goal).
- 179 • **Trust is context-dependent:** With the same trustor and trustee, trust might be different  
 180 depending on context including (i) task goal, (ii) period of time, and (iii) environment. For  
 181 instance, (i) Alice (highly) trusts Bob to provide a cloud storage service but not for a real-time  
 182 streaming service; (ii) Alice (highly) trusted Bob to provide a cloud storage service two years  
 183 ago but not for now; and (iii) Alice (highly) trusts Bob to provide a cloud storage service in the  
 184 United Kingdom but not in the United States.
- 185 • **Trust is not necessarily transitive but propagative:** If Alice (highly) trusts Bob, and Bob (highly)  
 186 trusts Charlie then it is not necessarily that Alice will (highly) trust Charlie. However there are  
 187 some evidences from the trust relationship between Bob and Charlie that Alice can rely on in  
 188 order to judge the trust in Charlie.  
 189 More details about trust characteristics can be found in [18].

#### 190 2.4. Conceptual Trust Model in SIoT environment

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

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



200  
 201

**Figure 2.** Conceptual Trust Model in the SIoT environment

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

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

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

## 225 2.5. Trustworthiness and Trustworthiness Attributes

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

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

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

249 Some of the TAs in Table 1 are frequently used in trust literature ranging from social science to  
 250 computer science, the other are rarely used and only existed in specific contexts. Even though each  
 251 of the three factors Ability, Benevolence and Integrity captures some unique elements of  
 252 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

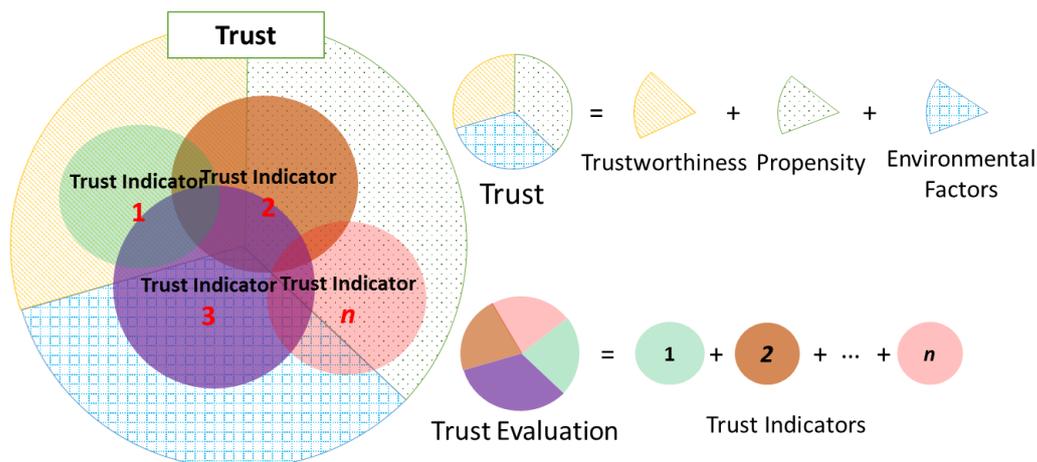
### 256 3. Trust Evaluation Model: Background and Provisions

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



289  
290 **Figure 3.** Concept of Computational Trust that comprised of multiple Trust Metrics

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

### 297 3.2. Related Work on Trust Evaluation

298 Despite the importance of trust in computer science, there are limited notable articles that clearly  
299 clarify the trust concept, trust models and evaluation mechanisms, especially in the IoT environment.  
300 A variety of models and mechanisms have been proposed for evaluating trust, however, they have  
301 mainly focused on building reputation systems in social networks for e-Commerce services [21] [22]  
302 or focused on developing trust management mechanisms in distributed systems such as WSNs  
303 [23,24], mobile ad-hoc networks (MANET) [25-27], and P2P networks [6,28]. The trust evaluation  
304 mechanisms in these articles are mostly based on insufficient information (i.e., only direct observation  
305 information or only third-party information).

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

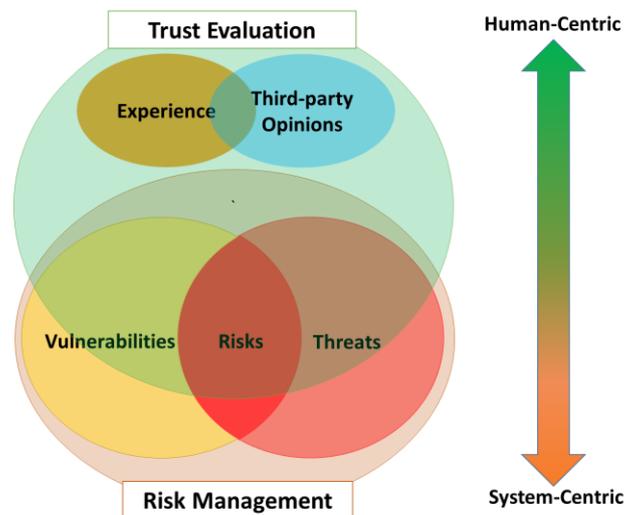
326 management called Objective Trust Management Framework (OTMF) in MANETs environment. The  
327 novel idea is that they apply a modified Bayesian model using different weights assigned for each  
328 information obtained from direct observations. The information is collected using a watchdog  
329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

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

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

374 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).



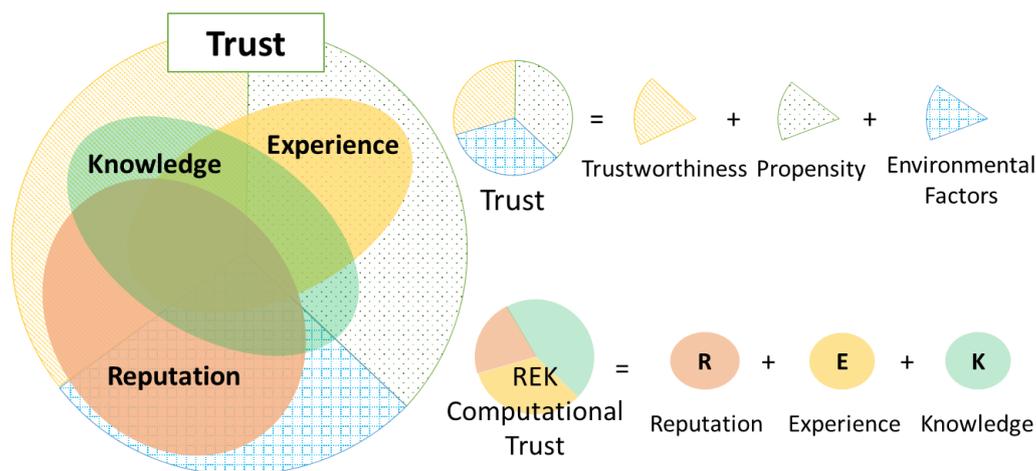
387  
 388

**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

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

#### 435 4.2.1. A general set of TAs for Knowledge TI

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

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

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

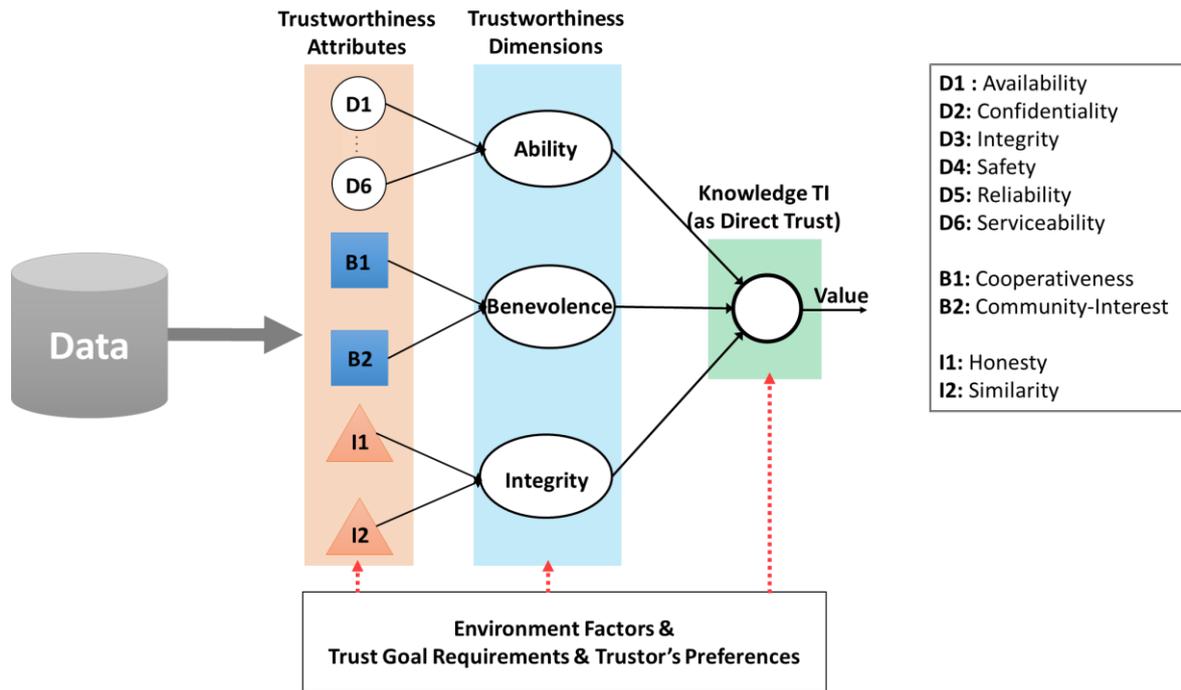


Figure 6. Evaluation Model for Direct Trust (as Knowledge TI)

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.

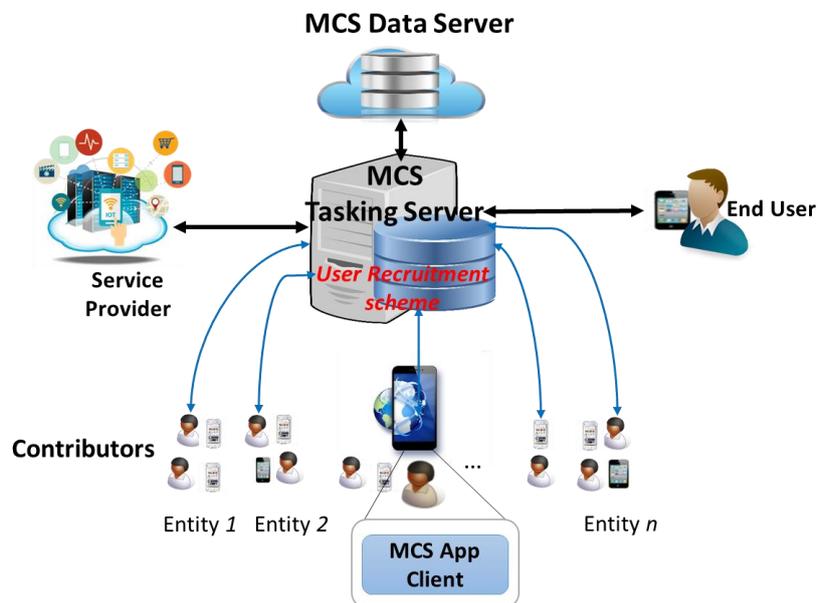


Figure 7. Mobile Crowd-Sensing System Architecture

505  
506

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

522  
523  
524

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

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

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

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

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

556 The numbers of tasks requested is the number of times the MCS Tasking server has requested  
 557 the user to participate in a sensing task; and the number of tasks involved is the number of times  
 558 the user has accepted to involve in sensing tasks that the MCS has requested. The number of  
 559 tasks canceled is the number of times the user cancels a sensing task when it has already accepted  
 560 to involve in the sensing task. The number of requested, involved, and canceled sensing tasks of  
 561 the user *i* is kept track and managed by the MCS Tasking Server.

- 562 • **Honesty:** This TA represents the degree of keeping promise once a sensing task is already  
 563 assigned to a user. High honesty means that the user is not going to cancel a task once it is

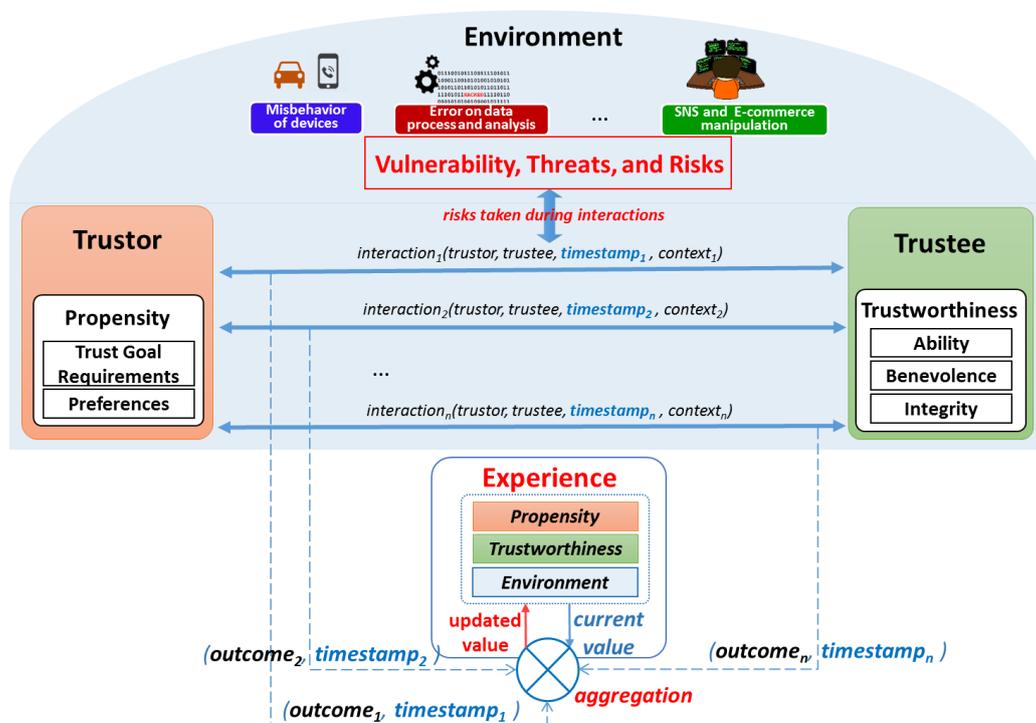
564 assigned due to any cause whatsoever. This TA belongs to the *Integrity dimension* and it is simply  
 565 measured by the equation (3).

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

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

### 568 4.3. Experience TI Evaluation Model

569 Experience is a social concept that represents personal understandings and opinions about one  
 570 entity to another based on its previous interactions to the counterpart. We propose a conceptual  
 571 model for the Experience TI depicted in Figure 8 which computes experiences based on the three  
 572 factors: the current value of Experience, the outcomes, and the timestamps of individual interactions.  
 573 Therefore, an *outcome evaluation scheme* for the interactions is one of the important components in the  
 574 Experience TI model. Various mechanisms can be used to deduce outcomes of interactions depending  
 575 on particular scenarios. For instance, outcomes might be feedback (in both implicit and explicit forms)  
 576 from consumers after each interaction (as used in many e-Commerce and reputation systems), might  
 577 just be a Boolean value (or 0/1) generated by using an ACK message to track whether the interaction  
 578 has successfully accomplished or not (as in some reputation-based trust systems). For example, in  
 579 Wireless Sensor Networks, interactions are package transmissions between two nodes, if a  
 580 transmission is successful, then the outcome of the interaction is 1, and 0 otherwise. In a file-sharing  
 581 P2P networks, interactions are file transfer transactions. If a file is successfully transferred, then the  
 582 outcome of the interaction is 1; otherwise is 0. The interaction is also in form of any types of  
 583 relationship between two entities. For example, Google PageRank™ considers a hyperlink as an  
 584 interaction between a source webpage and a destination webpage; and the outcome value is set as 1  
 585 [8].



586  
 587 **Figure 8.** The Experience TI model in the REK Trust Evaluation

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

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

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

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

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

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

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

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

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

607 As shown in the equation (6), the *increase value*  $\Delta Experience_{t+1} = \alpha \times (1 - Experience_t)$  is  
 608 relatively large when the current value  $Experience_t$  is small; but the *increase value* is reaching to  
 609 0 when the current value  $Experience_t$  is high (approaching to 1).

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

611 The mathematical model for the Experience Decrease is as following:

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

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

617 • **Experience Decay (in case of no interaction):**

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

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

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

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

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

#### 637 4.4. Reputation TI Evaluation Model

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

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

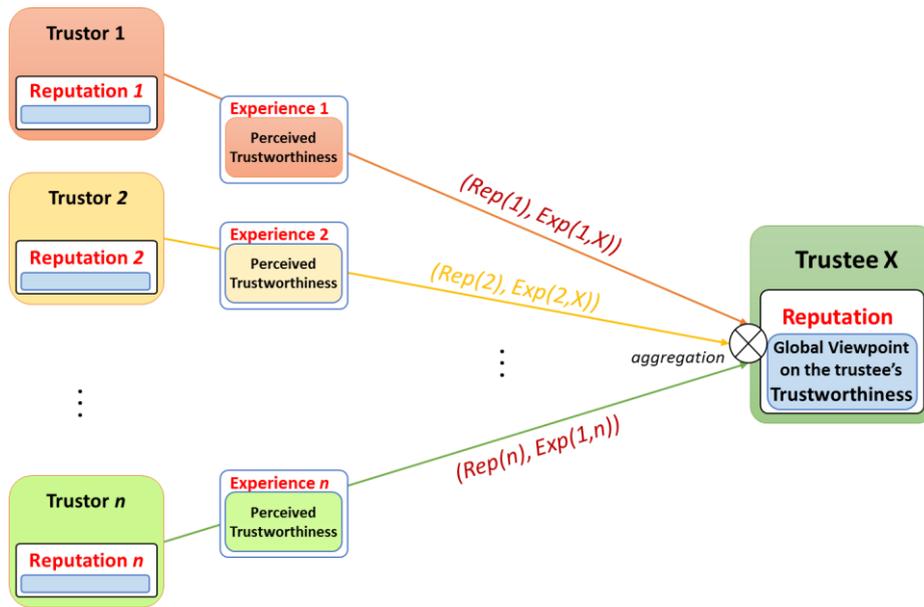


Figure 9. Conceptual Reputation Model incorporating the Experience concept

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.  $\theta$  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:

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

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

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

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.

- 693 -  $C_{Neg}(i) = \sum_{Exp(i,j) < \theta} (1 - Exp(i,j))$  is the total values of all complements of the negative
- 694 recommendations that the entity  $i$  is currently sharing.
- 695 -  $Rep(i)$  is the reputation of the entity  $i$  that we are interested.
- 696 -  $min_{Reputation}$  is a parameter indicating the minimal value of reputation (i.e., 0). This guarantee
- 697 the reputation value will not go below the  $min_{Reputation}$ .
- 698 -  $Experience(i, X)$  is the Experience TI from the entity  $i$  toward the entity  $X$  described in Section
- 699 4.3.
- 700 -  $d$  is the damping factor. Various studies on PageRank-related literature have tested different
- 701 damping factors for ranking webpages on the Internet, and they have come up with an
- 702 appropriate value around 0.85. The research on the damping factor for the Reputation TI model
- 703 is left as our future work.

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

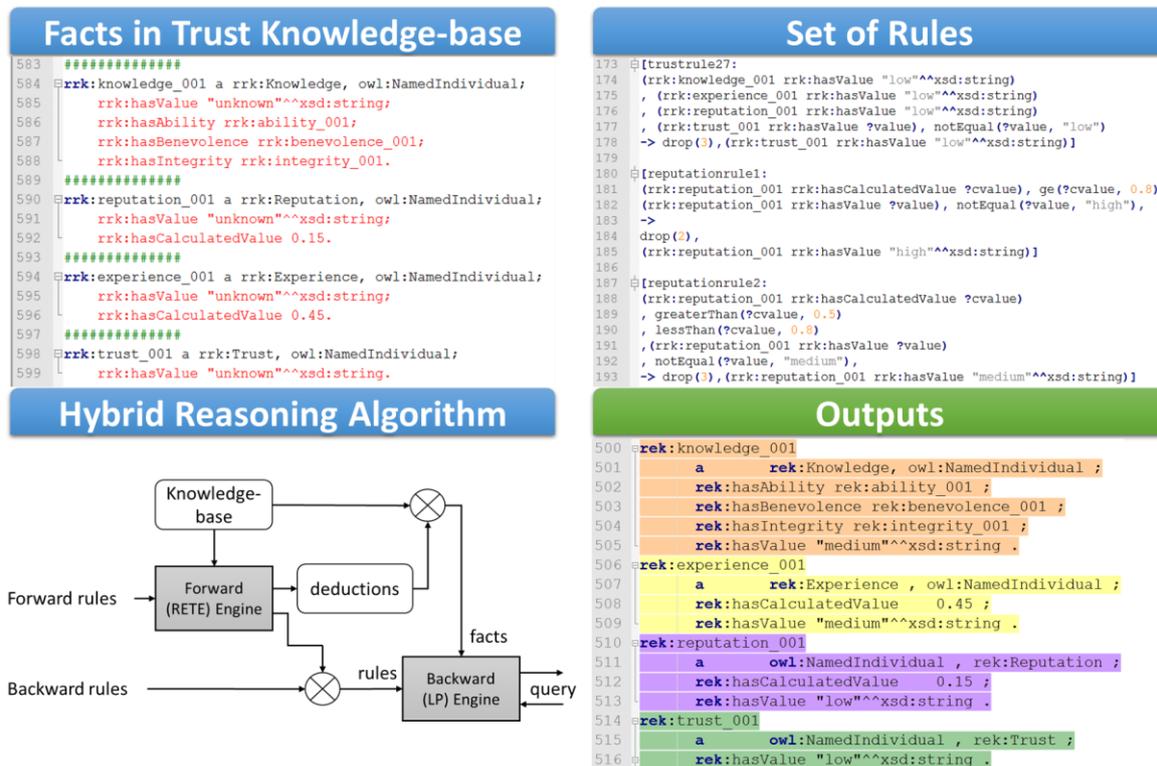
#### 714 4.5. Aggregation Mechanism for REK Trust Evaluation Model

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

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

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

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



750  
 751 **Figure 10.** Reasoning mechanism used in a demonstration for inferring trust value in the REK trust model

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

## 766 5. Conclusions and Future Work

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

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

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

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

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

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

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

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

807 **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.

## 808 References

- 809 1. Xiong, G.; Zhu, F.; Liu, X.; Dong, X.; Huang, W.; Chen, S.; Zhao, K. Cyber-physical-social system in  
810 intelligent transportation. *IEEE/CAA Journal of Automatica Sinica* **2015**, *2*, 320-333.
- 811 2. Sheth, A.; Anantharam, P.; Henson, C. Physical-cyber-social computing: An early 21st century approach.  
812 *IEEE Intelligent Systems* **2013**, *28*, 78-82.
- 813 3. Atzori, L.; Iera, A.; Morabito, G. Siot: Giving a social structure to the internet of things. *IEEE*  
814 *communications letters* **2011**, *15*, 1193-1195.
- 815 4. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The social internet of things (siot)—when social networks meet  
816 the internet of things: Concept, architecture and network characterization. *Computer networks* **2012**, *56*,  
817 3594-3608.
- 818 5. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in internet of things:  
819 The road ahead. *Computer Networks* **2015**, *76*, 146-164.
- 820 6. Mahalle, P.N.; Thakre, P.A.; Prasad, N.R.; Prasad, R. In *A fuzzy approach to trust based access control in*  
821 *internet of things*, Wireless Communications, Vehicular Technology, Information Theory and Aerospace  
822 & Electronic Systems (VITAE), Atlantic City, NJ, June 2013; IEEE: Atlantic City, NJ.
- 823 7. Josang, A.; Ismail, R.; Boyd, C. A survey of trust and reputation systems for online service provision.  
824 *Decision Support System* **2007**, *43*, 618-644.

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

- 867 29. Wang, J.P.; Bin, S.; Yu, Y.; Niu, X.X. Distributed trust management mechanism for the internet of things.  
868 *Applied Mechanics and Materials (Appl. Mech. Mater.)* **Aug. 2013**, 2463-2467.
- 869 30. Palaghias, N.; Loumis, N.; Georgoulas, S.; Moessner, K. In *Quantifying trust relationships based on real-*  
870 *world social interactions*, IEEE International Conference on Communications (ICC), Kuala Lumpur,  
871 Malaysia, 2016; Kuala Lumpur, Malaysia.
- 872 31. Can, A.B.; Bhargava, B. Sort: A self-organizing trust model for peer-to-peer systems. *IEEE transactions*  
873 *on dependable and secure computing* **2013**, *10*, 14-27.
- 874 32. Sherchan, W.S.; Nepal; Paris, C. A survey of trust in social networks. *ACM Computing Surveys (CSUR)*  
875 **2013**, *45*.
- 876 33. Bao, F.; Chen, I. In *Dynamic trust management for internet of things applications*, International Workshop  
877 on Self-Aware Internet of Things (Self-IoT), USA, 2012; USA.
- 878 34. Nitti, M.; Girau, R.; Atzori, L.; Iera, A.; Morabito, G. In *A subjective model for trustworthiness evaluation*  
879 *in the social internet of things*, IEEE International Symposium on Personal Indoor and Mobile Radio  
880 Communications (PIMRC), Australia, 2013; Australia.
- 881 35. Velloso, P.B.; Laufer, R.P.; Cunha, D.O.; Duarte, O.; Pujolle, G. Trust management in mobile ad hoc  
882 networks using a scalable maturity-based model. *IEEE transactions on network and service management*  
883 **2010**, *7*, 172-185.
- 884 36. NIST. *Managing information security risk: Organization, mission, and information system view*; U.S.  
885 Department of Commerce: Gaithersburg, MD, United States, 2011.
- 886 37. Kumar, R.; Khan, S.A.; Khan, R.A. Revisiting software security: Durability perspective. *International*  
887 *Journal of Hybrid Information Technology (SERSC)* **2015**, *8*, 311-322.
- 888 38. Al-Kuwaiti, M.; Kyriakopoulos, N.; Hussein, S. A comparative analysis of network dependability, fault-  
889 tolerance, reliability, security, and survivability. *IEEE Communications Surveys & Tutorials* **2009**, *11*,  
890 106 - 124.
- 891 39. NIST. *Cyber-physical systems (cps) framework release 1.0*; US Department of Commerce: Gaithersburg,  
892 MD, USA, 2016.
- 893 40. Santini, S.; R.Jain. Similarity measures. *IEEE Transactions on pattern analysis and machine Intelligence*  
894 **1999**, *9*, 871-883.
- 895 41. Chen, I.; Bao, F.; Guo, J. Trust-based service management for social internet of things systems. *IEEE*  
896 *Transactions on Dependable and Secure Computing* **2015**, 1-14.
- 897 42. Ganti, R.K.; Ye, F.; Lei, H. Mobile crowdsensing: Current state and future challenges. *IEEE*  
898 *Communications Magazine* **2011**, *49*.
- 899 43. Guo, B.; Yu, Z.; Zhou, X.; Zhang, D. In *From participatory sensing to mobile crowd sensing*, IEEE  
900 International Conference on Pervasive Computing and Communications Workshops (PERCOM  
901 Workshops), Budapest, Hungary, 2014; Budapest, Hungary, pp 593-598.
- 902 44. Anjomshoa, F.; Catalfamo, M.; Hecker, D.; Helgeland, N.; Rasch, A. In *Sociability assessment and*  
903 *identification of smartphone users via behaviormetric software*, IEEE Symposium on Computers and  
904 Communications (ISCC), Messina, Italy, June 2016; Messina, Italy.
- 905 45. Fiandrino, C.; Kantarci, B.; Anjomshoa, F.; Kliazovich, D.; Bouvry, P.; Matthews, J. In *Sociability-driven*  
906 *user recruitment in mobile crowdsensing internet of things platforms*, IEEE Global Communications  
907 Conference (GLOBECOM), Washington DC, USA, 2016; Washington DC, USA.

- 908 46. An, J.; Gui, X.; Wang, Z.; Yang, J.; He, X. A crowdsourcing assignment model based on mobile crowd  
909 sensing in the internet of things. *IEEE Internet of Things Journal* **2015**, *2*, 358-369.
- 910 47. Bhoraskar, R.; Vankadhara, N.; Raman, B.; Kulkarni, P. In *Wolverine: Traffic and road condition*  
911 *estimation using smartphone sensors*, International Conference on Communication Systems and Networks  
912 (COMSNETS), Bangalore, India 2012; Bangalore, India
- 913 48. Mohan, P.; Padmanabhan, V.N.; Ramjee, R. In *Nericell: Rich monitoring of road and traffic conditions*  
914 *using mobile smartphones*, ACM conference on Embedded network sensor systems, Raleigh, NC, USA,  
915 2008; ACM: Raleigh, NC, USA, pp 323-336.
- 916 49. MovableType, L. Calculate distance, bearing and more between latitude/longitude points. Movable Type  
917 Ltd.: 2016.
- 918 50. Baumeister, R.F.; Leary, M.R. The need to belong: Desire for interpersonal attachments as a fundamental  
919 human motivation. *Psychological bulletin* **1995**, *3*, 497.
- 920 51. Oswald, D.L.; Clark, E.M.; Kelly, C.M. Friendship maintenance: An analysis of individual and dyad  
921 behaviors. *Journal of Social and Clinical Psychology* **2004**, *3*, 413-441.
- 922 52. Kamvar, S.; Schlosser, M. In *The eigentrust algorithm for reputation management in p2p networks.*, 12th  
923 International Conference on World Wide Web, Budapest, 2003; Budapest, pp 640–651.
- 924 53. Josang, A.; Golbeck, J. In *Challenges for robust trust and reputation systems*, International Workshop on  
925 Security and Trust Management (STM), SaintMalo, France, 2009; SaintMalo, France.
- 926 54. Dellarocas, C. Reputation mechanism design in online trading environments with pure moral hazard.  
927 *Information Systems Research* **2005**, *16*, 209-230.
- 928 55. Jayasinghe, U.; Truong, N.B.; Um, T.W.; Lee, G.M. In *Rpr: A trust computation model for social internet*  
929 *of things*, IEEE Smart World Congress, Toulouse, France, 2016 Toulouse, France.
- 930 56. Tyagi, N.; Simple, S. Weighted page rank algorithm based on number of visits of links of web page.  
931 *International Journal of Soft Computing and Engineering (IJSCE)* **2012**, 2231-2307.
- 932 57. Ding, Y. Topic-based pagerank on author cocitation networks. *Journal of the Association for Information*  
933 *Science and Technology* **2011**, *62*, 449-466.
- 934 58. Backstrom, L.; Jure, L. In *Supervised random walks: Predicting and recommending links in social*  
935 *networks*, The fourth ACM international conference on Web search and data mining, HongKong, 2011;  
936 ACM: HongKong, pp 635-644.
- 937 59. Kotsiantis, S.B.; Zaharakis, I.; Pintelas, P. In *Supervised machine learning: A review of classification*  
938 *techniques*, Emerging Artificial Intelligence Applications in Computer Engineering: Real Word AI  
939 Systems with Applications in eHealth, HCI, Information Retrieval and Pervasive Technologies,  
940 Amsterdam, Netherlands, 2007; Amsterdam, Netherlands, pp 3-24.
- 941 60. Chandrashekar, G.; Ferat, S. A survey on feature selection methods. *Computers & Electrical Engineering*  
942 **2014**, *40*, 16-28.
- 943 61. Ren, Y.; Boukerche, A. In *Modeling and managing the trust for wireless and mobile ad hoc networks*,  
944 IEEE International Conference on Communication (ICC'08), Beijing, China, 2008; Beijing, China, pp  
945 2129-2133.
- 946 62. Shaikh, R.A.; Jameel, H.; Lee, S.; Song, Y.J.; Rajput, S. In *Trust management problem in distributed*  
947 *wireless sensor networks*, IEEE international conference on Embedded and real-time computing systems  
948 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.



© 2017 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).