A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things

Nguyen B.Truong
Department of Computer Science
Liverpool John Moores University,
Liverpool, L3 3AF
n.b.truong@2015.ljmu.ac.uk

Tai-Won Um
Broadcasting &
Telecommunications Media
Research Laboratory, ETRI,
Daejeon, 305-700, Korea
twum@etri.re.kr

Gyu Myoung Lee
Department of Computer Science
Liverpool John Moores University,
Liverpool, L3 3AF, UK
g.m.lee@ljmu.ac.uk

***Abstract*—The Internet of Things has attracted a plenty of research in this decade and imposed fascinating services where large numbers of heterogeneous-features entities socially collaborate together to solve complex scenarios. However, these entities need to trust each other prior to exchanging data or offering services. In this paper, we briefly present our ongoing project called Trust Service Platform, which offers trust assessment of any two entities in the Social Internet of Things to applications and services. We propose a trust model that incorporates both reputation properties as Recommendation and Reputation trust metrics; and knowledge-based property as Knowledge trust metric. For the trust service platform deployment, we propose a reputation system and a functional architecture with Trust Agent, Trust Broker and Trust Analysis and Management modules along with mechanisms and algorithms to deal with the three trust metrics. We also present a utility theory-based mechanism for trust calculation. To clarify our trust service platform, we describe the trust models and mechanisms in accordance with a trust car-sharing service. We believe this study offers the better understanding of the trust as a service in the platform and will impose many trust-related research challenges as the future work.**

Keywords—Social Internet of Things; Trust as a Service; TaaS; Trust Model; Trust Metric; Trust Management; Recommendation; Reputation; Knowledge; Fuzzy; Utility Theory; User Preference

I. INTRODUCTION

The Internet of Things (IoT) is considered as the network of devices like home appliances, office appliances, and vehicles embedded with computing system, sensors, connectivity with self-configuring capability [1]. These electronic devices, which are billions in number and varied in size and computing capabilities, are ranging from Radio Frequency Identification tags (RFIDs) to vehicles with Onboard Units (OBUs). IoT is expected to enable advanced services and applications like smart home, smart grid [2, 3] or smart city [4, 5] by integrating a variety of technologies in many research areas from embedded systems, wireless sensor networks, service platforms, automation to privacy, security and trust. Recently, the convergence of two emerging network paradigms Social Networks and IoT as Social Internet of Things (SIoT) [6, 7, 8] has attracted many researchers as a prospective approach for dealing with challenges in IoT. The benefit of SIoT is the separation in terms of the two levels of humans and devices; allowing devices to have their own social networks; offering humans to impose rules on their devices to protect their privacy, security and maximize trust during the interaction among objects. Indeed, some SIoT systems are currently taking advantages of social relationship models to offer secure and reliable services by using the reputation and trust such as eBay, Amazon and Google's Web Page Rankings [9, 10].

Trust concept itself is a complicated notion with different meanings depending on both participators and situations; and based on both measurable and non-measurable factors. Nevertheless, trust is an important feature in the decision-making process not only used by humans in daily life but also by applications and services in networking system like SIoT. Until now, approaches on trust have almost focused on building a trust management system and proposing reputed mechanisms for related-security issues such as in a Recommendation System, Access Control or Identity Management [11, 12]; but do not lend themselves to develop a complete trust service including the establishment of trust model, trust metrics (hereafter TMs), trust-related ontology and trust calculation methodologies. Moreover, most of approaches are built for wireless sensor networks (WSN), peer-to-peer networks (P2P), ad-hoc network, or social networks but not SIoT [13-15]. On the other hand, most SIoT trust-related research has focused on entities definitions, interactions or on design of reference architectures and protocols; but lack of some basic aspects that leverage the social relations, interactions and information provided by the entities when developing trusted systems and services [16].

With these issues in mind, we aim at developing a trust service platform that cooperates with applications and services to evaluate the trust between two entities in SIoT, in order to support them for better quality of services and experience. The proposed platform could be considered as a core service to secure computing systems, networking applications and services in SIoT (which can be defined as Trust as a Service (TaaS)). To build the trust service platform, a semi-centralized trust management approach is used by incorporating a proposed reputation system with three new types of components Trust Agent, Trust Broker and Trust Analysis and Management into SIoT. These modules are able to cover different geographical locations and different trust purposes.

The catalyst for figuring out trust features is that when judging whether a trustee (a person, a device or a service) is trustable or not, the trustor "thinks" like human by taking its knowledge, recommendations from trustor's relations; and trustee's reputation into account. Thus, the human processing

when assessing trust is imitated in our proposed trust model by modulating Reputation, Recommendation, and Knowledge as three basic TMs. Basically, our trust service platform continuously manages and updates the Reputation and Recommendations TMs of all entities in the SIoT network by the proposed reputation system. For the Knowledge TM, the trust service platform will cooperate with each application or service for specific trust information such as Knowledge trust ontology and trustor preferences. Then, the final stage, called Trust Calculation, is to calculate the trustworthiness or trust score of the trustor to the trustee, based on all three TMs, the user preferences and the application/service context. It can be done by using an appropriate algorithm assigned by the trust analysis and management system.

In this paper, we mainly focus on trust model, Knowledge TM model; a functional architecture of the trust service platform and a Trust Calculation method in a trust car-sharing service demonstration. In this example, a Knowledge trust ontology for car-sharing service is proposed, a fuzzy-based mechanism is used for Knowledge TM evaluation and a personalized multi-criteria utility theory-based system for the Trust Calculation stage.

The rest of our article is organized as follow. The following section provides background and discussion on related research. The system model and platform architecture are presented in Section III. Section IV is for car-sharing service use case in which detail describe TMs formulation and trust score calculation. Then, we summarize our work and discuss some prospective research directions in the final section.

II. BACKGROUND AND RELATED WORK

A. *SIoT Environment*

SIoT concept is eventually formalized in some ways, mostly bases on the idea that objects in IoT belong to humans in the network [6, 7] and people offer services through their owned objects. SIoT, thus, is considered as social networks in which any device is capable of establishing social relationships with others according to its owners. These entities expose their characteristics to public areas through not only themselves but also the owners' behaviors.

Among several SIoT models proposed, we consider the SIoT environment developed by Atzori et al. [6]; and the acronym SIoT we use in this paper refers to this model. In SIoT, every device has one or more owners who could also have some other devices. The model applies some pre-defined rules and mechanisms by utilizing the social relationships among humans in reality. For example, each user in SIoT maintains its social relationship by considering the term "friends". If two users are "friends", then the devices they owned tend to be cooperative with each other. The term "community-interest" is taken into account as the environment in which devices are tent to be carried or operated (e.g. office, home, work place, public/social places). As a consequence, devices in similar communities likely share their information each other. These entity in SIoT are expected to communicate through overlay social network protocols, or underlying standard device-to-device communication network protocols like Machine-to-Machine (M2M) or P2P, forming an social network of devices which is potential for the SIoT. As a result, forms of socialization among objects are foreseen; and types of social relationships are also established [6, 7] as illustrated in Fig.1.

According to the SIoT model, our proposed trust service platform is able to instantiate a collaborative environment, allowing entities to share their trust related information, as induced from their knowledge and experience, by submitting their opinions to a reputation system.

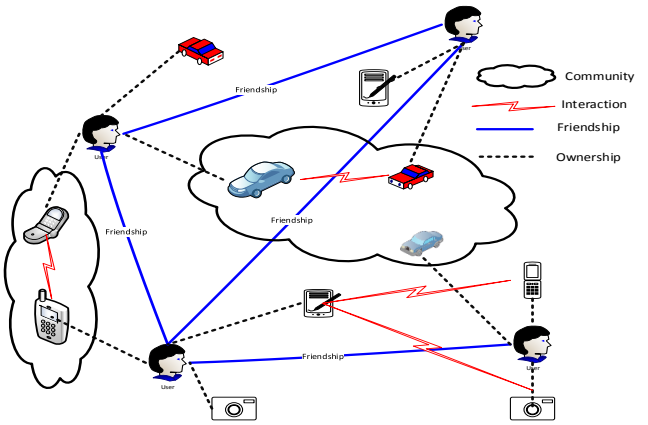

Fig. 1. Social structures of the Internet of Things

B. *Trust in the Internet of Things*

There are various kinds of trust definitions leading to difficulties in establishing a common, general notation that holds, regardless of personal dispositions or differing situations. Generally, trust is considered as a computational value depicted by a relationship between trustor and trustee, described in a specific context and measured by trust metrics and evaluated by a mechanism. Some important properties of trust are stated and discussed in [17, 18]. Previous research has shown that trust is the interplay among human, social sciences and computer science, affected by several subjective factors such as social status and physical properties; and objective factors such as competence and reputation [20]. The competence is measurement of abilities of the trustee to perform a given task which is derived from trustee's diplomas, certifications and experience. Reputation is formed by the opinion of other entities, deriving from third parties' opinions of previous interactions with the trustee.

A trust system covers a large number of trust-related research aspects ranging from Trust Relationship and Decision (TRD), Data Perception Trust (DPT) to Identity Trust (IT) [19]. Several works focus on trust evaluation and trust assessment in IoT [21, 22] and in SIoT [13]. The authors assume that entities in the systems are human-related or human-carried which are capable of establishing relations depending and cooperatively working together in accordance with their owners' relationships. They proposed distributed, encounter-based, and activity-based trust management protocols in which entities compute and update trustworthiness of the partners once mutual interactions occur. The entities also share trust evaluations to their friends as recommendations to help friends in their trust-related processes. Thus, a reputation-based mechanism is needed to incorporate with the trust systems. However, malicious entities (dishonest or socially uncooperative entities) could exploit the principal reputation-based properties to break the functionalities of the system using trust-related attacks such

as self-promoting, ballot-stuffing, discriminatory, bad-mouthing, good-mouthing, and whitewashing [23]. Several solutions were proposed to try to deal with these kinds of attack by validating identity and recommendation information through some trust compositions such as honesty, cooperativeness, community-interest [23], relationship factor and centrality [13] in the environment of WSN, P2P or ad-hoc networks.

Other works proposed fuzzy approaches to calculate trust levels from some TMs such as Experience, Recommendation, and Knowledge, or based on technical properties extracted from physical layer, core layer[1], and application layer in IoT system [12, 24] as a mechanism for access control. Each trust level is mapped to permission; the access requests are then accompanied accordingly. This approach of trust calculation is, however, impossible to deal with the scenarios that TMs are crossed-domain. Several TMs are derived from both physical layer and core layer and other TMs could only be extracted from both core layer and application layer. For instance, to reckon the Knowledge TM, it is needed to extract valuable information from data of both physical layer and application layer, which describes the trustee. This will be mentioned in the next section.

C. *Trust Car-Sharing Service*

We propose a trust car-sharing service, a popular car rental model in Europe and the U.S, in the SIoT environment that uses our proposed trust service platform. The cars rentals could be a commercial business or individuals who want to rent their spare cars. Thus, it is attractive to both customers and providers who occasional use a vehicle. The benefit of car-sharing is that car renters can use private cars without costs and responsibilities of ownership [25] whereas the owners can earn money when they do not use their car. However, currently there is no car-sharing mechanism that helps customers to choose car as they wish, except feedback ratings. Generally, customers tentatively want to rent a car that they trust the most, not only based on other feedback opinions but also based on each situation, their own knowledge of the vehicle and the vehicle owner. By using our trust service platform, the car-sharing service can show a customer a list of car sorted by the trust level based on customer's preferences.

III. SYSTEM MODEL AND ARCHITECTURE

A. *Trust Models and Trust Metrics*

We aim to develop a generalized trust definition for all entities in SIoT in which trust can be formalized and produced within our platform. Till now, it is challenged to determine the necessary and sufficient information that should be used for deriving measures of trust [9]. Technically, trust is based on several TMs which are generally defined as the information used in trustworthiness evaluation process between trustor and trustee. Each TM is derived from some Technical Attributes (TAs) as illustrated in Fig.2 [17].

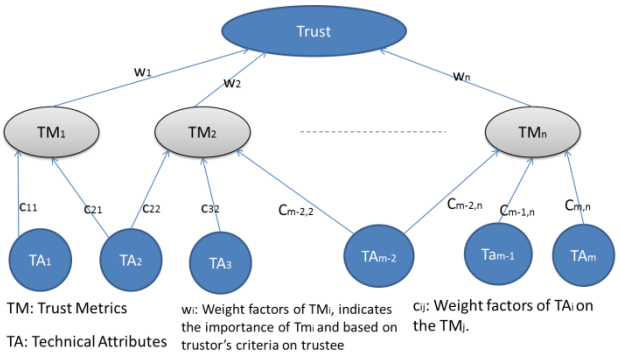

Fig. 2. General Trust Model with Trust Metrics and Technical Attributes

Following this approach with the catalyst of imitating human trust processing as discussed above, we propose a trust model that comprises of three TMs namely Reputation, Recommendation, and Knowledge [Fig. 3].

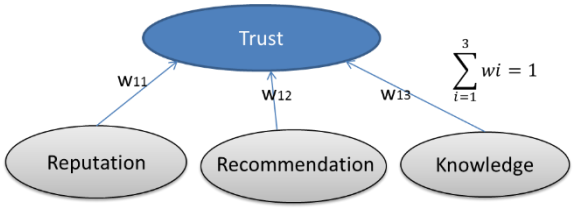

Fig. 3. The proposed Trust Model with three Trust Metrics

B. *Reputation and Recommendation TMs*

Reputation is third-party information and is considered as both social product and social process. It is a social product because it is produced by opinions of entities; on the other hand, reputation is as an information flow influencing in the SIoT. Reputation should not to be confused with trust but partially affects the trust. Several well-known reputation systems have been developed such as eBay [29] and Keynote [30-32]. These systems use a centralized trust authority to establish and maintain user feedbacks as ratings. There are also some distributed approaches for reputation mechanisms in which reputation has been built over time based on feedbacks from both customers and entities behaviors. Such systems use heuristic algorithms for reputation integration and update.

In this sense, Recommendation is considered as the opinion of trustor-related entities to trustee to help the trustor judge the trust to trustee. The reason to separate Reputation and Recommendation is that natural human information processing usually relies on both surrounding suggestions (e.g. from friends, relatives, and colleagues) and global opinions (e.g. ranking/ratings levels in public media).

Therefore, a reputation system is needed to build for managing Reputation and Recommendation TMs. It is one of the most important parts in the trust service platform which consists of three basic modules called Reputation Measurement and Evaluation (which is also called Feedback Mechanism), Propagation and Maintenance. A reputation ontology with a SIoT relationship map is proposed in order to put all the reputation-related knowledge of SIoT services together and presented in a structured form. A machine

[1] Core layer in layered IoT architecture covers key functionalities to support control and management for networking and services.

learning algorithm and a reasoning mechanism are used for the measurement and evaluation process. Then a propagation process is conducted to deal with many aspects of transmission of the reputation; and a propagation maintenance is used for the modifications in both reputation structure and content through the network and over time.

The reputation system should deal with some typical challenges such as bootstrap new services and feedback motivation and customers support. In some scenarios, customers do not need to understand the whole complicated feedback evaluation process, the system can automatically calculate feedbacks on behalf. For example, feedback of a web service could be derived from some quality of services technical properties such as reliability, availability, capability, delay and jitter [33]. The system also needs to deal with some post-processing phases such as matching, unfair feedbacks, risk remedies (unexpected events occur), self-adjustment, bias detection, reward and punishment [34].

Finally, the value of Reputation or Recommendation TM is simply converted as a number between 0 and 1, representing how high reputation and recommendation of/to the trustee is. Details of the reputation system is out of scope of this our article.

C. *Knowledge TM*

Knowledge is the first party information provided by trustee to evaluate its trustworthiness [35] and composed by some TAs depending on services and entities. Service providers are supposed to register their own information including both Knowledge TM ontology and requirements to the platform prior to use. This trust data has many dimensions and should be normalized and unified in order to be suitable for software oriented architecture (SOA) environment by using an ontology manager and an information model.

In this paper we consider our platform is for service-to-service SIoT environment in which humans offer services through their owned items. Thus, when judging Knowledge TM of a service, a user needs to assess both device and device's owner as illustrated in Fig.4.

The Human-to-Human knowledge is comprised of four TAs: Honesty, Cooperative, Community-Interest and Experience, inspired by ideas in [12, 23].

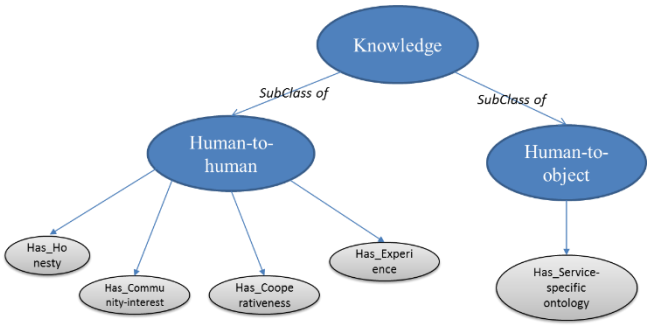

Fig. 4. The Knowledge TM is divided into two sub-ontologies

- The honesty represents whether an entity is honest. In SIoT, an entity can be dishonest when providing services or trust-related information that lead to disrupting the service continuity including trust management. Thus, honesty is chosen as a TA to prevent an entity from trusted-related attacks.
- The cooperativeness represents the level of the social cooperation from the trustee to the trustor. The higher cooperativeness means the higher trust level in the SIoT system. The cooperativeness of an entity can be evaluated based on its social relations and its social behaviors.
- The community-interest represents whether two entities have close relationship in terms of social communities, groups, and capabilities. Higher degree of community-interest can lead to high opportunities to interact with each other, resulting in higher trust level.
- The experience from an entity to another entity represents how well they previously interacts with each other. If a previous interaction is successful then, experience value is +1; or -1 if failure. High value of experience can result in high level of trust judgment.

The detailed calculations of the three TAs Honesty, Cooperativeness and Community-Interest are presented in [23] whereas the Experience TA is achieved from the interaction record conducted by Trust Agent. By considering these TAs, our proposed trust service platform is able to deal effectively with several types misbehaviour entities and attacks [21, 23].

The Human-to-Object knowledge depends on both service and object; and can be calculated using sufficient information provided from the service with appropriate reasoning methods and machine learning technique. This process will be clarified in the car-sharing use case in the next section.

D. *Trust Components and Platform Architecture*

Depending on trust model and trust-related information processing mechanisms, the choice between centralized and distributed trust management is needed to investigate. In centralized approach, trust information can be computed on demand whereas distributed approach computes trust on a regular basis and propagates throughout the network topology. We are also concerned that an entity itself in the large scale network like SIoT possibly lacks knowledge to evaluate trust. It certainly needs help from others such as trusted authorities. Moreover, a real-time trust data flow may lead to communication overhead, detrimental to both network performance and entities battery life. However, the traditional strategies for centralized system are difficult to suit for solving trust issues of a large scale distributed network like SIoT because of their poor scalability as well as center-dependence leading to single point of failure. Thus, we considered Fog computing architecture [26-28] which could be considered as semi-distributed system.

In order to deploy the trust service platform, besides the Reputation System mentioned above, we define and incorporate three new basic components to the SIoT: Trust Agent, Trust Broker and Trust Analysis and Management. We briefly present these components by describing their responsibilities and interactions in the system [Fig.5].

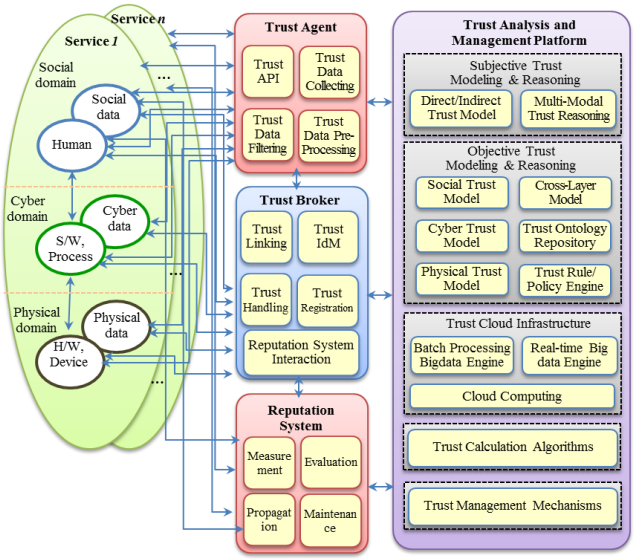

Fig. 5. Trust components interactions in the trust service platform

- Trust Agent: used to collect trust-related data from physical, cyber and social SIoT domains. The data could be TAs or opinions of entities as recommendation or feedbacks to other entities, applications or services.
- Trust Broker: used to provide the trust knowledge to various type of applications and services in SIoT. It is required to register information such as knowledge TM ontology or service requirements prior to use the trust service platform.
- Trust Analysis and Management: Beside a part for collaborating with the Reputation System, all trust-related mechanisms such as ontology-related manager, information model, reasoning mechanisms, trust cloud infrastructure, Knowledge TM evaluation mechanisms, and trust calculation algorithms are implemented at this module.

IV. TRUST CAR-SHARING USE CASE

Generally, the Reputation and Recommendation TMs in the trust car-sharing example are similar to any other services; and can be get from the reputation system. The Human-to-Human knowledge can be also calculated depending on four TAs mentioned in the previous section. The Human-to-Object knowledge extraction algorithm and Trust Calculation mechanism are service-and-object specific; and are described in this section.

A. Fuzzy-based System for Human-to-Object Knowledge Calculation

As the trust platform perspective, Human-to-Object, in this case is Human-to-Vehicle, ontology and vehicle data are provided by the car-sharing service and users. We propose that the ontology is comprised of three TAs: Reliability, Pricing and Quality as depicted in Fig. 6. To identify these TAs, it is crucial to explore what information is necessary and sufficient; and this process is a service level agreement between the trust platform, services and users. For example, vehicle owners are asked to show the TM Reliability by supplying the maintained schedule of their vehicles, the vehicle accident history or the insurance policy [Fig. 6].

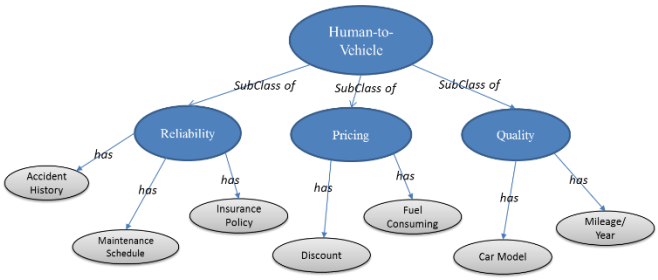

Fig. 6. Knowledge in Human-to-Vehicle of trusted car sharing service

To deal with wide range data of the Knowledge components which is ambiguous in some cases, fuzzy-based approach is a prospective solution. Fuzzy Logic-based mechanisms provide ability to treat ambiguous data that is resolved only at runtime [36, 37, 38]; offering flexible, adaptive and extensive abilities for the system. Furthermore, fuzzy logic is able to represent vague terms like "*low*" or "*high*", "*bad*", "*acceptable*" or "*good*", which obviates the need to choose a specific value. With these advantages, fuzzy logic is widely used in control theory, pattern recognition and digital image processing.

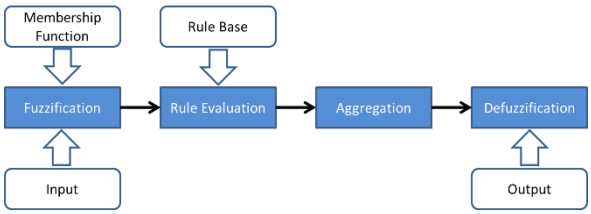

Fig. 7. Mamdany Fuzzy Interference System procedures

To this purpose, fuzzy approach is used for the Human-to-Vehicle Knowledge calculation. The ambiguous TAs parameters are easily represented (both by range of values or linguistic values where vagueness is associated). There are two well-known type of a Fuzzy Information Systems (FIS): Mamdani FIS [39] and Sugeno FIS [40]. Mamdani FIS is used in our research work due to greater expressive power and interpretability compared to Sugeno FIS [41].

The Mamdani FIS mechanism consists of four processes: Fuzzification, Rule Evaluation, Aggregation and Defuzzification as illustrated in Fig.7. To implement the fuzzy-based mechanism, several important factors such as input metrics, membership functions, and fuzzy rules are defined in accordance with service requirements that registered to the trust platform. In Fuzzification step, the input for FIS is put as real value, and then evaluated by applying appropriate membership functions. We take an example to demonstrate the evaluation of Pricing, a trust attribute of Human-to-vehicle Knowledge, using Mamdani FIS. The TA Pricing comprises of two properties Discount and Fuel Consuming. These two properties are translated into fuzzy sets using associated membership functions in the Fuzzification process which are illustrated in Fig. 8. For example, consider the Discount , which is *25%*, as the input, the associated membership function then evaluates and maps it to a value in the fuzzy set, in this case is "*poor*", instead of "*normal*" or "*good*". If the Fuel Consuming is *45 Miles per Gallon* (*MPG*), the associated membership function maps the input factor to as "*low*", instead of "*medium*", "*high*", or "*extremely high*". The evaluated result in this step is transferred as the input to the Rule Evaluation process. In this

step, the evaluated results with the membership values passed from the Fuzzification step are evaluated using fuzzy rules stored in the Rule base.

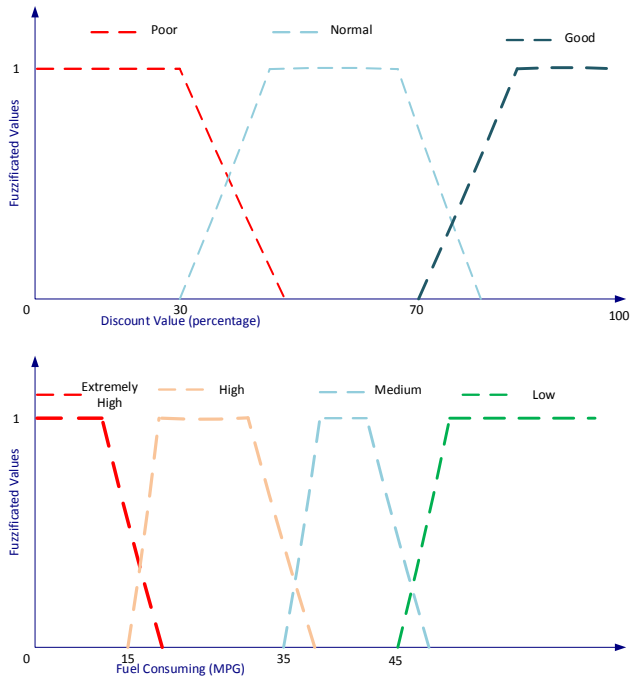

Fig. 8. Membership functions for Discount and Fuel Consuming

The Mamdani Fuzzy Logic scheme is relational model meaning that fuzzy rules are represented by an If–Then relationship in the form below:

WHEN *event_clause*
IF *condition_clause* THEN *actions*
ELSE *other_actions*

In our case, the rules are similarly defined as follow:

IF "Discount" is "good" AND "Fuel Consumption" is "LOW" THEN "Pricing" is "very good"

In this case, "*good*" is denoted as linguistic label of the input variable "*Discount*", associated with the rule. "*Very good*" is linguistic label of output variable "*Pricing*", associated with same rule. Similarly, the set of fuzzy rules for Knowledge are defined in the same way, for example:

Rule1: IF "reliability" is "very high" AND "Pricing" is "very good" AND "Quality" is "excellent" THEN "Knowledge" is "highly trust"

...

Rule m: IF "reliability" is "very poor" AND "Pricing" is "very expensive" AND "Quality" is "very poor" THEN "Knowledge" is "highly distrust"

As a result, output of the Mamdani fuzzy model is represented by a fuzzy set. In order to normalize the Knowledge TM, the outputs, in form of fuzzy values, need to be converted into crisp values, which is the final process of the system called Defuzzification. Center-of-Gravity (CoG) [36] is usually used a defuzzification method. Two below equations (1) and (2) are CoG based defuzzification formulae in continuous and discrete form, respectively.

$$COG(A) = \frac{\int_x \mu_A(x).x.dx}{\int_x \mu_A(x).dx} \quad (1) \qquad COG(A) = \frac{\sum_{q=1}^{Nq} \mu_A(x).x}{\sum_{q=1}^{Nq} \mu_A(x)} \quad (2)$$

Note that membership functions and fuzzy rules could be automatically raised by a reasoning mechanism based on a machine learning technique with information model from a ontological model of entities in SIoT. For simplicity, in the car-sharing example, these functions and rules are pre-defined.

B. Utility Theory for Personalized Trust Calculation

Trust Calculation is a dynamic process which heavily depends on trustor's preferences. Each trustor needs both appropriate trust data and aggregation methods for producing desired information which reflects the trustor perspective. Specific trustors might use and define different trust computation methodologies for dealing with their associated trust data. For example, in our proposed trust infrastructure, the weights for TM (Recommendation, Reputation, Knowledge) reflect the trustor's preferences, resulting in the calculation of overall trust value. Trustor could assign weight for Knowledge is highest since he/she is expertise in vehicle rental, the other could choose the highest weight for both Recommendation and Reputation because he/she believes in opinions from others. We denote the entity profile as the triple tuple UP($W_{recommendation}$, $W_{reputation}$, $W_{knowledge}$).

To build the entity profile for the calculation, which is usually called user profiling process, utility theory with multi-criteria utility is normally used [42]. John von Neumann and Oskar Morgenstern in their research on game theory have used the assumption of expected utility maximization as the fundamental form of utility theory [42, 43]. The utility theory is also used in demand-and-supply problem in which different consumers have different preferences for same product, resulting in imposing utility function. In this scheme, individual preferences are considered in the utility evaluation procedure. For example, a utility function can be defined as U(w; x) whereas x is from a set of product criteria and w is user preferences.

In our trust service platform, the weighted sum additive aggregates utility function UP is defined to calculate the overall trust [44]. The function aggregates multiple criteria in a composite criterion, using information given by a subjective ranking. The UP then is used as subjective ranking:

Trust Score = vector UP($W_{recommendation}$, $W_{reputation}$, $W_{knowledge}$) x vector TM(Recommendation, Reputation, Knowledge)

UP could be predefined for basic users or manually chosen for advanced users who understand the complex trust system. For a better profiling mechanism, our system should take these challenges into account:

- Profiling process is typically either knowledge-based or behavior-based. The former creates static models of entities and dynamically match the entities to the closest model whereas the latter uses the entities' behavior as a model, typically using machine learning techniques to discover useful patterns in the behavior.
- Knowledge must be acquired in order to create the entity profile. The model is then refined by monitoring subsequent behavior.

- Entity profile should be organized by the system using some mechanisms in order to easily to find similar items.

V. CONCLUSION AND FUTURE WORK

In this paper, we have briefly introduced the proposed trust service platform that offers trust evaluation of two any entities to SIoT services. We modulate the human trust information process and social relationship to create a trust model by incorporating both reputation properties (in terms of Recommendation and Reputation TMs) as well as knowledge-based property (in terms of Knowledge TM). To deploy the trust service platform, all basic components and mechanisms are mentioned or described in detail in accordance with the trust car-sharing service. They are reputation-based system for Reputation and Recommendation TMs, fuzzy-based algorithm for Knowledge TM and a personalized multi-criteria utility theory-based mechanism for calculating overall trust score.

There is a large number of research challenges needed to investigate in order to fulfill our trust service platform. The first direction could be the mechanisms for managing reputation system that can motivate entities to publish their feedbacks in a secure way whereas eliminate the risk of trust-related attacks. The second direction could be a new intelligent Fuzzy Expert System for dealing with Knowledge TM that automatically chooses the best algorithm for any kind of services while autonomously adapt with changes of context. In this paper, we restrict the trustor's preferences that only take part in the final process of trust calculation. However, it is required that a trustor has a chance to reflect their perspective in terms of personal preferences in all TMs and TAs evaluation processes, as the third future research direction.

ACKNOWLEDGEMENT

This research was supported by the ICT R&D program of MSIP/IITP [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system].

REFERENCES

[1] M. Weiser, "The Computer for the 21st Century," Scientific American, vol. 265, pp. 66-75, Sept. 1991.

[2] O. Monnier, "A Smarter Grid with the Internet of Things," Texas Instruments, 2013.

[3] E. Kosmatos, N. D. Tselikas, and A. C. Boucouvalas, "Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture," Advances in Internet of Things, vol. 1, no. 1, pp. 5–12, 2011.

[4] A. Zanella et al., "Internet of Things for Smart Cities," IEEE Internet of Thing, vol.1, no.1, Feb. 2014.

[5] J.S Hwang and Y.H Choe, "Smart Cities Seoul: a Case Study," ITU-T Technology Watch Report, Feb. 2013.

[6] L. Atzori, A. Iera and G. Morabito, "SIoT: Giving a Social Structure to the Internet of Things," Communications Letters, vol. 15, no. 11, pp. 1193-1195, Nov. 2011.

[7] L. Atzori et al., "The Social Internet of Things (SIoT)-When Social Networks meet the Internet of Things: Concept, Architecture and Network Characterization," Computer Networks, vol. 56, pp. 3594-3608, Nov. 2012.

[8] J. Breslin and S. Decker, "The Future of Social Networks on the Internet," IEEE Internet Computing, vol. 11, no. 6, pp. 86-90, Jun. 2007.

[9] A. Josang, R. Ismail and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, pp. 681-644, 2007.

[10] L.Page et al., "The PageRank Citation Ranking: Bringing Order to the Web," Technical Report, Stanford InfoLab, 1999

[11] R. Lacuesta et al., "Internet of Things: Where to be is to Trust," EURASIP Journal on Wireless Communications and Networking, pp. 1-16, 2012.

[12] P.N Mahalle et al., "A Fuzzy Approach to Trust Based Access Control in Internet of Things," Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, 2013.

[13] M. Nitti et al., "A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things," IEEE International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC, pp. 18-23, Australia, 2013.

[14] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities," IEEE Trans. Knowl. Data Eng., vol. 16, pp. 843–857, Jul. 2004.

[15] A. Selcuk, E. Uzun and M. Pariente, "A Reputation-based Trust Management System for P2P Networks," CCGRID, pp. 251-258, USA, 2004.

[16] S. Sicari et al., "Security, Privacy and Trust in Internet of Things: the road ahead," Computer Networks, vol. 75, pp. 146-164, Jan. 2015.

[17] Z. Yan and C. Prehofer, "Autonomic Trust Management for a Component based Software System," IEEE Transactions Dependable Secure Computing, vol.8, pp. 810-823, 2011.

[18] Z. Yan and S. Holtmanns, "Trust Modeling and Management - from Social Trust to Digital Trust," Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, IGI Global, pp. 290-323, 2008.

[19] Z. Yan et al., "A Survey on Trust Management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120-134, 2014.

[20] B. Alcalde et al., "Towards a Decision Model based on Trust and Security Risk Management," Seventh Australasian Conference on Information Security, vol. 98, pp. 61-70, 2009.

[21] F. Bao and I. Chen, "Dynamic Trust Management for Internet of Things Applications," International Workshop on Self-Aware Internet of Things, Self-IoT, pp. 1-6, USA, 2012.

[22] F. Bao and I. Chen, "Trust Management for Internet of Things and its Application to Service Composition," IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM, pp. 1-6, US, 2012.

[23] I. Chen, F. Bao and J. Guo, "Trust-based Service Management for Social Internet of Things Systems," IEEE Transactions on Dependable and Secure Computing, 2015.

[24] J. Wang et al., "Distributed Trust Management Mechanism for the Internet of Things," Appl. Mech. Mater., Aug. 2013.

[25] Carsharing,Wikipedia, https://wikipedia.org/wiki/Carsharing

[26] F. Bonomi, "The smart and Connected Vehicle and the Internet of Things," Invited Talk, Workshop on Synchronization in Telecommunication Systems, 2013.

[27] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, "Fog computing and its role in the internet of things," MCC workshop on Mobile cloud computing, Aug., 2012.

[28] I. Stojmenovic, S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues", Federated Conference on Computer Science and Information Systems (FedCSIS), 2014.

[29] P. Resnick et al., "Reputation Systems," Communications of the ACM, vol. 43, pp. 45-48, 2000.

[30] M. Blaze, J. Feigenbaum, J. Ioannidis and A. Keromytis, "The KeyNote Trust Management System," University of Pennsylvania, 1999.

[31] L. Xiong and L. Liu, "A Reputation-based Trust Model for Peer-to-Peer E-Commerce Communities," IEEE International Conference on E-Commerce Technology (CEC), 2003, pp. 275-284.

[32] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Managament," IEEE Symposium on Security and Privacy, 1996.

[33] W. D. Yu et al., “Modeling the Measurements of QoS Requirements in Web Service Systems,” Simulation Journal, vol. 83, pp. 75–91, 2007.

[34] Z. Aljazzaf, M. Perry and M. Capretz, “Towards a unified trust framework for trust establishment and trust based service selection,” Canadian Conference on Electrical and Computer Engineering (CCECE), 2011.

[35] S. Ganeriwal, L. K. Balzano and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," ACM Transactions on Sensor Networks, vol. 5, 2007.

[36] L. Zadeh, “Fuzzy Sets,” Information and Control Journal, vol. 8, pp. 338-353, 1965.

[37] L. Zadeh, “Fuzzy Logic, Neural Networks, and Soft Computing," Communications of the ACM, vol. 37, 1994

[38] L. Zadeh, “Fuzzy Logic = Computing with Words," IEEE Transactions on Fuzzy Systems, vol. 4, 1996.

[39] E. Mamdani et al., “Application of Fuzzy Algorithms for Control of Simple Dynamic Plant," Institutions of Electrical Engineers, vol. 121, no. 12, pp. 1585-1588, 1974.

[40] M. Sugeno, “Industrial Applications of Fuzzy Control”. Elsevier Science Inc., USA, 1985.

[41] A. Hamam and N. Georganas, “A Comparison of Mamdani and Sugeno Fuzzy Inference Systems for Evaluating the Quality of Experience of Hapto-Audio-Visual Applications," IEEE International Workshop on Haptic Audio Visual Environments and Games (HAVE), pp. 87-92, 2008.

[42] Utility, Wikipedia, https://en.wikipedia.org/wiki/Utility

[43] J. Neumann, O. Morgenstern, A. Rubinstein, and H. Kuhn, “Theory of Games and Economic Behavior,” Princeton Univ. Press, 2007.

[44] E. Jacquet-Lagreze and J. Siskos, “Assessing a Set of Additive Utility Functions for Multi-criteria Decision-Making, the UTA Method," European Journal of Operational Research, vol. 10, no. 2, pp. 151-164, 1982.