LIVERPOOL JOHN MOORES UNIVERSITY

LJMU Research Online

Lee, GM

A Survey on Trust Computation in the Internet of Things

http://researchonline.ljmu.ac.uk/id/eprint/2727/

Article

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

Lee, GM (2016) A Survey on Trust Computation in the Internet of Things. Information and Communications Magazine, 33 (2). pp. 10-27. ISSN 1226-4275

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

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

A Survey on Trust Computation in the Internet of Things

Nguyen B. Truong
Liverpool John Moores University
United Kingdom
n.b.truong@2015.ljmu.ac.uk

Upul Jayasinghe
Liverpool John Moores University
United Kingdom
u.u.jayasinghe@2015.ljmu.ac.uk

Tai-Won Um
Electronics and Telecommunications Research Institute
Korea
twum@etri.re.kr

Gyu Myoung Lee
Liverpool John Moores University
United Kingdom
g.m.lee@ljmu.ac.uk

Abstract

Internet of Things defines a large number of diverse entities and services which interconnect with each other and individually or cooperatively operate depending on context, conditions and environments, produce a huge personal and sensitive data. In this scenario, the satisfaction of privacy, security and trust plays a critical role in the success of the Internet of Things. Trust here can be considered as a key property to establish trustworthy and seamless connectivity among entities and to guarantee secure services and applications. The aim of this study is to provide a survey on various trust computation strategies and identify future trends in the field. We discuss trust computation methods under several aspects and provide comparison of the approaches based on trust features, performance, advantages, weaknesses and limitations of each strategy. Finally the research discuss on the gap of the trust literature and raise some research directions in trust computation in the Internet of Things.

I. Introduction

With recent advanced technologies toward a hyper-connected society from the increasing digital interconnection of humans and objects, big data processing and analyzing, the Internet of Things (IoT)-related applications and services are playing more and more significant role in the convenience of human daily life. However various problems occurred due to the lack of trust which will hinder the development of IoT. To cope with a large number of complex IoT applications and services, it is needed to create a trusted and secured environment in order for sharing information, creating knowledge and conducting transactions.

Trust concept is an abstract notion with different meanings depending on both participators and scenarios; and influenced by both measurable and non-measurable factors. 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. 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 [1]. 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. Trust revolves around ‘assurance’ and confidence that people, data, entities, information or processes will function or behave in expected ways. At the deeper level, trust is regarded as a consequence of progress towards security or privacy objectives.

Till now, most research on trust have focused on trust computation models and trust management systems for solving related-security issues such as Access Control in decentralized systems [4],[5], Identity Management [6],[7] and Public Key Certification [8],[9]. In these research works, some network environments are considered such as sensor networks, peer-to-peer networks, ad-hoc network, social networks and IoT. However, there are limited works on trust computation in the IoT environments; and most of them are related to security enhancement for dealing with malicious entities or access control. Nonetheless, the research of trust in the IoT is very decent due to the need for a trusted environment for the reach of IoT full potential.

In this survey, some existing trust computation methods are analyzed and discussed based on our classification of a trust computation in the IoT: network architecture, system layered architecture, various kind of trust models; and trust aggregation. We summarize both pros and cons of each method and make comparison among them in order to highlight the effectiveness when applying trust to offer more secure services. Finally, we discuss the gap of state-of-the-art research directions in developing trust computation in IoT, as a result, suggest some future research areas.

II. Background and Trust Computation Objectives

A. Trust Attributes

Generally trust presents the confidence and the assurance that entities, users, systems, data and process behave as it is expected to be. Therefore trust can be considered as a way of achieving extra security and privacy objectives. As trust can be interpreted in different ways, here we present various meanings from literature for more clear views on trust in terms of Information and Communication Technologies (ICT) [10].

Trust is dynamic: as it solely depending on the time and changing nature of entities. As an example from human world, one who was trustworthy for some time ago can be changed over time and completely unreliable.

Trust is context-dependent: On different contexts trust can be totally unlike and will have different trust measures for each and every dissimilar scenarios. For example one can get advice from friend about his lessons but about medical treatments as the knowledge, experience is different in two scenarios.

Trust is not transitive in nature but maybe transitive within a given context: That is, if entity A trusts entity B, and entity B trusts entity C then entity A may not trust entity C. However A may trust any entity that entity B trusts in a given context although this derived trust may be explicit and hard to be quantified.

Trust is an asymmetric relationship: Thus, trust is a non-mutual reciprocal in nature. That means if entity A trust entity B, then the statement “entity B trusts entity A” is not always true.

The nature of trust is fuzzy, dynamic and complex. Besides asymmetry and transitivity, there are additional key characteristics of trust: implicitness, antonymy, asynchrony, and gravity [11],[12].

Implicit: Trust can have different form depending on the context and entity and hence it is difficult to clearly measure the confidence, belief, capability, context, and time dependency of trust.

Gravity: The degree of seriousness in trust relationships may differ between the entities. For example, entity A may think that its trust with entity B is important, however, entity B may think it differently.

B. Trust in IoT

There are plentiful trust solutions have been proposed for many network systems such as peer-to-peer (P2P), multi-agent systems, and e-commerce. In this section, we consider trust in IoT: the networks of devices like household appliances, office appliances, sensors and vehicles which are interconnected seamlessly and with ability of self-configuring capability. 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 On board Units (OBUs). IoT is expected to enable advanced services and applications like smart home, smart grid or smart city by integrating a variety of technologies in many research areas from embedded systems, wireless sensor networks, service platforms, and automation to privacy, security and trust.

Recently, trust in IoT is intensively investigated and mostly divided into two types direct trust and third party trust [2]. The direct trust is a situation where a trusting relationship is nurtured by two entities and formed after these entities have performed transactions with each other. The third-party trust is a trust relationship of an entity that is formed from the third party recommendations which could be no previous transaction ever occurred between the two interacting entities. For example, entity A trusts entity B because B is trusted by entity C. In this example, entity A derives trust of B from C, and A also trusts entity C does not lie to him. As with any types of trust relationship, there is a link with the risk which affects the trusting relationship between the entities. Author in [3] stresses that an entity will only proceed with the transaction if the risk is perceived as acceptable.

Lately, the convergence of two emerging network paradigms Social Networks and IoT as Social Internet of Things (SIoT) 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 assessing trust is imitated by modulating Reputation, Recommendation, and Knowledge as three basic Trust Metrics (TMs).

C. Trust Computation Objectives

To provide trust among entities in the IoT environment, research on trust computation should achieve some goals in accordance with the deployment of a trust platform in the IoT system model.

- System Architecture and Network Architecture of the environment in which trust platform will be deployed. Based on this, trust computation models are developed and built.
- Trust Model: a Trust Model in accordance with TMs and TAs. This part should include Trust Composition as Credentials, TMs, Technical Attributes (TAs) and IoT properties contributed to Trust Computation such as network characteristics and social relationships.
- Trust Aggregation techniques: methods to examine a trust score or trust level once all TAs and TMs are already collected and calculated.

III. System and Network Architecture of a Trust Platform

A. Network Architecture

With heterogeneous applications and services in IoT, one must give special attention to the architecture of the trust model with respect to trust propagation. According to the literature, studies on trust architectures can be mainly categorized into centralized approach and distributed approach. Some properties of each approach are described in Table 1.

As the name implies centralized approach store all the information about TMs, TAs, protocols and algorithms and mathematical models, related to trust computation in a central database and provide the service on demand as shown in Figure 1(A). On the other hand in distributed approach Figure 1(C), trust agents do all the computation necessary locally.

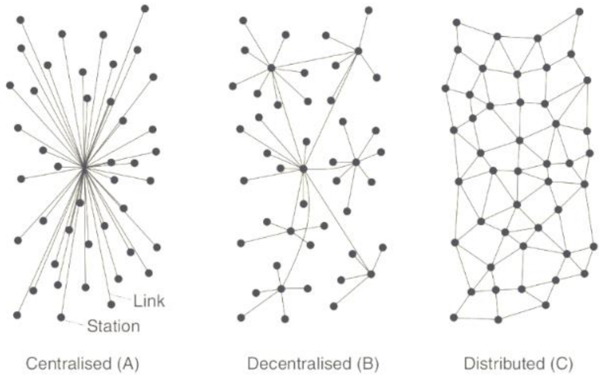


Figure 1. Centralized vs Decentralized vs Distributed Networks

Table 1. Comparison of Trust Propagation Methods

Property/behaviour	Centralized	Decentralized	Distributed
Points of failure	Single point of failure	Finite number of failures	Infinite
Maintenance	Easy	Moderate	Difficult
Stability	Highly unstable	Recovery possible	Very Stable
Scalability/ Max population	low scalability	low scalability	Infinite
Ease of development/ creation	Less Complex	Moderate	More details needed
Evolution / Diversity	Slow/little	High	High

But for IoT applications, sticking in to only one approach will not be sufficient as sometimes calculations have to be done locally and some are remotely depending on the resources availability. Therefore fully distributed model or fully centralized versions will not give satisfactory results and combined methods also to be considered in respect to trust computation. In this regard, the decentralized model shown in Figure 1(B) can be considered as an optimum model for the trust computation with the complexity of IoT services.

a. Centralized Trust

In the approach, each trust request and service will go through a central node or TA which can be accessed by all other nodes in his domain as shown in Figure 1(A). TA will be responsible for managing trust information including trust negotiation, calculation and decision making and/or assist users by providing the initial information required for trust computation.

In general, centrality based rating systems are global rating systems. One of the most prominent area where centralized trust computation has been deployed is in the social networks like Facebook™ and e-markets like Amazon™ and eBay™ [13],[14]. In here, reputation is a function of the cumulative ratings on users by others. Furthermore, [15] explains how the reputation system works in social networks using a mathematical model. Basically it introduces adjacency matrix which represent rating from node “i" to node “j” and method to solve this matrix recursively to obtain the reputation of each reputed users.

More evolved version of a reputation model called SPORAS compared to eBay™ is developed by [16] where only the most recent recommendations have been taken into the consideration. Here the mechanism is built in such a way that the reputation update will effect significantly for low reputed users and rarely for the users with high reputation. The underlying core principal is based on the standard deviation of reputation values. Also they suggest a method to incorporate reputation mechanisms in online communities to make it more reliable and more effective the way users contribute in the community.

In [17], trust computation based on a centralized cluster head is proposed. Initially cluster head is responsible for delivering trust values for every node in its domain. After that local node will combine locally calculated trust with initially learned trust value from cluster head.

In [18],[19], an agent based trust computation method is suggested for mobile ad hoc network (MANET). It uses the weighted means to measure the nodes final trust and then makes the corresponding decision.

A trust modelling scheme for a group of nodes (group trust) based on cluster head approach is proposed in [20],[21]. The entire network is divided into number of small groups and every group has a cluster head and all the cluster heads are connected to the base station. This trust value will be sent to cluster head. The cluster head will determine the trust value of other cluster heads based on interactions and then forward all the information to the base station. Base station will then decide the trust factors (fully trust, untrust or uncertain). Comparison of different centralized trust computing schemes with respect to research area, pros and cons, complexity and performance limitations is provided in Table 2.

Table 2. Comparison of different centralized trust computing mechanisms

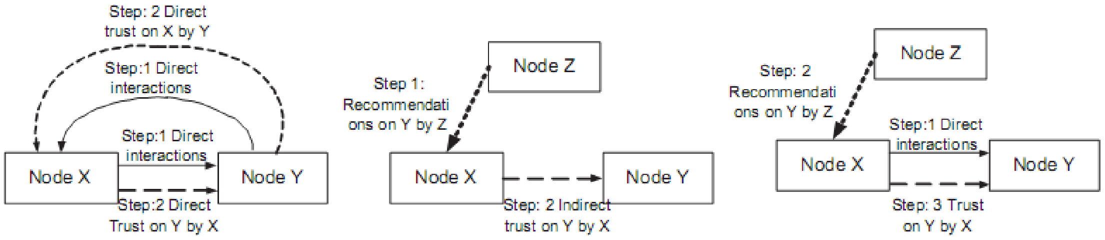
Research Work	Research Focus	Trust Measurement	Advantages	Complexity	Performance and Limitations
[17]	Clustering based trust computations.	Trust is measured in the interval [0, 1] using Beta distribution.	The computed trust is global and not biased.	Complexity in maintaining the cluster and electing the cluster heads.	The computed trust may not be precise with respect to single particular node. Cluster head can be single point of failure.
[20] [18]	Nodes query the agents for the initial trust and then calculates the final trust value based on averaging.	Trust is defined in the interval [0, 1]. Malicious node handling, security overhead and community sizes have been analyzed.	This scheme can handle collusion attack well as the trust is bootstrapped from the reputation agent.	Infrastructural complexity of maintaining more than one trust agents and the reliable communications from the agents to the nodes.	This scheme will perform well as long as number of reputation agents are high.
[19]	Cluster head aggregates the trust reports received from individual nodes and determines the final trust.	Trust is presented as fuzzy logic in the intervals [0 - 0.4, 0.4 - 0.6, 0.6 - 1]. Memory requirements have been analyzed.	Global trust value.	Complexity of maintaining high trustworthy communication between cluster heads and cluster heads to base station.	Cluster head can be single point of failure.
[21]	Based on a centralized Trust Block which collects votes and calculates the trust.	Trust is confined in the range [0, 1]. The impact on trust computations by increasing the peer numbers has been analyzed.	This trust algorithm can be made adaptive by changing the presentation unit of the Trust Block.	Infrastructural and computational cost of hosting Trust Block.	Trust Block could be single point of failure.

b. Distributed Trust

This refers to IoT users independently exchange trust matrices with neighboring users without intervention of centralized entity. In here the trust computation methods can be categorized in to three parts as direct trust, indirect Trust and hybrid methods as shown in Figure 2.

- Direct Trust

A trustor node (X) is directly in contact with trustee node (Y) and learns the trust knowledge via direct negotiation between them as shown in Figure 2(a). In an event, trustor node compares this learned knowledge with locally calculated trust values and best on that final trust value will be generated. That is, final trust value is a combination of both locally generated trust values and direct observations. Hence determination of trust factor between these two entities is vital and [23] proposes a mathematical model based on probability theory to determine optimum percentages from both entities.


Step: 2 Direct trust on X by Y
Step:1 Direct interactions
Step:1 Direct interactions
Node X
Node Y
Step:2 Direct Trust on Y by X
Node Z
Step 1: Recommendati ons on Y by Z
Node X
Node Y
Step: 2 Indirect trust on Y by X
Node Z
Step: 2 Recommendati ons on Y by Z
Step:1 Direct interactions
Node X
Node Y
Step: 3 Trust on Y by X

(a) Neighbour sensing based direct trust establishment

(b) Recommendation based indirect trust establishment

(c) Hybrid method of trust establishment

Figure 2. Distributed Trust Computation methods [22].

A direct trust computation method for wireless sensor nodes is proposed in [24] based on confidence interval concept. Final trust value will be decided after observing the behavior of adjacent node over considerable time. Here trust is represented as mean trust value and a confidence interval about the mean. Then based on the confidence interval trustor will proceed with the decision making process, i.e. if the confidence interval is sufficiently narrow enough. If not trustor will observe more knowledge from trustee before calculation of final trust value. In [25], table based trust storage mechanism is used for each neighboring node. Comparison of some other distributed trust computing mechanisms with respect to research area, pros and cons, complexity and performance limitations is provided in Table 3.

Table 3. Comparison of different direct trust computing mechanisms

Research Work	Research Focus	Trust Measurement	Advantages	Complexity	Performance and Limitations
[24]	Based on observing the neighbors behavior over the time.	Trust is a fractional value in [0, 1]. Convergence time, memory cache requirements are analyzed.	Accumulates the past behaviors and weigh them based on time. Hence the trust computation is precise. No single point failure.	Requires memory to store the past experiments. Computational complexity to determine the t-distributions.	Trust computation is completely local and biased.
[26]	Routing based direct trust calculations.	Trust is a fractional value in [0, 1]. Performance of AODV and DSR protocol have been analyzed with the proposed trust scheme.	Works based on existing request and acknowledgement schemes in AODV and OLSR protocols. No single point failure.	Additional hardware to monitor the packet drop/forward event of neighbors.	Specific to routing. Nodes should monitor neighbors all the time to construct and update trust relations. Computed trust is biased.
[27]	Past actions and present behavior are combined in Bayesian estimate to determine trust.	Trust is measured as probability value. The improvement of trust for various numbers of observations has been analyzed.	No single point failure.	Observation collection and Bayesian calculations requires memory and computational complexity.	Measurement is totally instantaneous and may not be precise.

- Indirect Trust

In a situation where direct observation is not possible with trustee node trustworthiness can be calculated based on recommendations from the peer users which have records about trustee. However relying on others recommendations involved high risk compared to direct trust method as recommenders can falsely provide dishonest information which can lead to reduce trust value of honest users and improve the trust of malicious nodes. Therefore other than calculating trust, validating them is also a key research area in this method.

In regard to determine dishonest users, [28], [29] propose trust credibility evaluation methods based on threshold values and assigning lesser weights for the dishonest users in future transactions. After filtering out the false recommendation, the next step is to calculate the effectiveness of each honest recommendation. Authors in [30] proposed several methods determine creditability of trust by using fuzzy logic. A trust calculation method based on threat reports for MANETs is proposed in [31]. In this method, an alarming system is included in each and every node. Then every node listen to its adjacent nodes and generate a trust report based on their behavior. This will be broadcast to each and every node so that if any node generate false report it can be detected by the alarming system.

B. System Layered Architecture

With the definition of IoT, it is clear that establishing trust in one particular layer is not enough and in fact trust should be defined as multidimensional property over all layers of IoT layered architecture as shown in Figure 3.

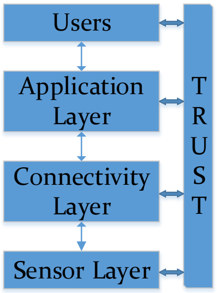


Figure 3. Trust establishment procedures

That is, the final value of trust of specific entity is determined not only by one single parameter but trust matrices distributed among users, applications, connections and devices. Moreover, these aggregated data is essential for the decision making process as shown in Figure 4.

As an example, smart city is considered to elaborate layered trust architecture mentioned above. With corresponding to three layer structure, device layer represents physical devices like various kind of sensors and physical network. In our user case, these sensors helps to gather information like weather, location and traffic condition. In similar manner, trust matrices like Quality of Service (QoS), delay and routing is considered in the network layer for trust computation and at application layer, trust for services like storage, processing, and etc. is calculated. Then the locally calculated trust in each layer will be send for the final decision making process as shown in Figure 4.

In [32] researchers propose a trust computation method in connectivity layer with respect to MANNET. Additionally they implement a cross layer protocol based on trust to improve the security of packet exchanging and delivery ratio of the network. Moreover, [33] suggests trust calculation method based QoS while [34] presents a method to predict the trust based on QoS parameters particularly considering the service providers side.

Considering sensor layer, establishing trust for IoT devices is a challenging task due to heterogeneous relations. To extract trust information in sensor layer, several mechanisms like trusted computing [35] and computational trust mechanisms proposed in [36] are required. Nevertheless it is mandatory to provide necessary trust information to every entity that matters and hence ontology based mechanisms need to be deployed as described above. Also authors in [37] provide an algorithm based on partial correlation to achieve data trust when computing trustworthiness of an entity and in decision making process.

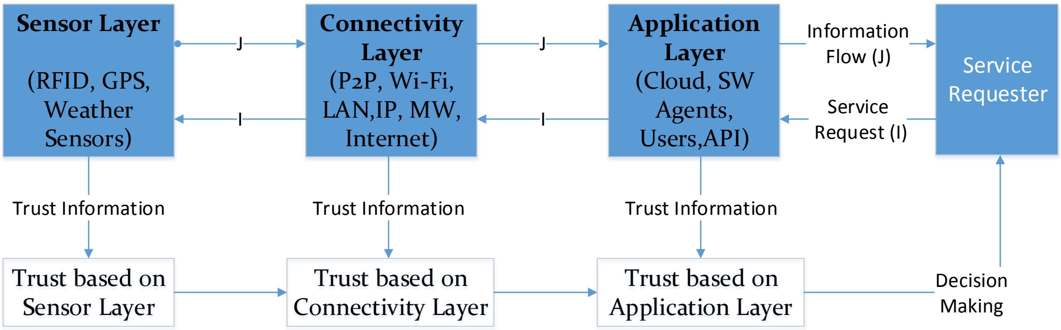

Sensor Layer
(RFID, GPS, Weather Sensors)
J
I
Connectivity Layer
(P2P, Wi-Fi, LAN,IP, MW, Internet)
J
I
Application Layer
(Cloud, SW Agents, Users,API)
Information Flow (J)
Service Request (I)
Service Requester
Trust Information
Trust Information
Trust Information
Trust based on Sensor Layer
Trust based on Connectivity Layer
Trust based on Application Layer
Decision Making

Figure 4.Trust Computation Steps in IoT

IV. Trust Computation Models

There are two conventional ways of trust models are policy-based approach (or rule-based approach) and reputation-based approach. These two trust models have been investigated under the context of different network environment including IoT with different purposes and goals.

Traditionally, policy mechanisms manage the decision of a system by describing pre-defined set of conditions (rules) and specific set of actions in accordance with each condition. In this manner, policy can assist in making decision for trust computation when a certain ambiguity level occurs while assessing trust. As a result, policy-based trust models normally involve the exchange or verification of trust-related credentials called trust negotiation process.

A reputation-based trust model is basically used in trust computation for assessing trust score or trust level based on the history of interactions of related entities. The reputation information in this scenario could be either directly with the evaluator (direct reputation) or as recommendation by other entities (indirect reputation, recommendation or third party information). The trust model based on a certain levels of reputation information is obviously since it happens in the process when people analyze and examine trust.

In recent years, most of researchers have accepted that reputation is one important factor of trust resulting in the dominance of reputation-based trust models compared to policy-based models. Some have tried to integrate both approaches in their trust models in order to leverage the advantages of them. Nevertheless, both credentials and reputations are the important information involving in the trust transitivity among entities; and each of them has its own pros and cons that have motivated researchers to work on.

A. Policy-based Trust Computation Models

This approach has been intensively investigated in the previous decade (mostly from 2000 to 2005) in which policies or rules are used in the trust computation. To establish and calculate trust, a trust management need to integrate trust negotiation protocols for creating, exchanging and managing credentials of network entities. The policy-based trust methods generally assume that a trustor after several processes of credential creation and exchange, it will obtain a sufficient amount of credentials from trustee and from other entities for trust establishment and trust calculation. There is an issues called “recursive problem” which is related to the trust of the credentials in this approach. This problem can be solved by introducing a trusted authority (a third party entity) for issuing and verifying these credentials.

The policy-based trust mechanism are usually used in the context of distributed network system as a solution for access control and authorization [38],[39],[40],[41]. The goal is simple by judging whether a user is trustful or not based on a set of credentials and predefine rules before granting rights to access network resources. The focus in this situation is how to apply policy languages, entities ontology and reasoning engines for specifying and producing additional rules and trust knowledge for trust computation procedures.

For the summary research related to policy-based mechanism, we organize the research work into sub-categories of trust computation procedures: trust credentials establishment, trust negotiation process, and policy/rules trust languages.

- Trust Credentials Establishment:

Conventionally, credential is information about an entity and context of the environment needed to evaluate trust. Although the word "credential" is frequently used in many research works, there is no common definition or standard to specify and determine it. Policies should rely on credential information and other context properties in order to judge trust. An obvious example of credentials in trust is the use of username and password to gain access control when logging to a computer. According to the system policy, having a correct username in accordance with an appropriate password proves that the user is trusted by that computer system. In a more complicated example, credentials are also automatically generated during a negotiation process by leveraging security certificates with digital signatures or using public key infrastructure (PKI). Note that only certificates that includes trust-related information of an entity or context can be used as credentials. For example, TrustBuilder [42] dealt with trust by establishing trust credentials using traditional security techniques such as authentication and encryption which is called "hard security" trust.

There is a well-known research work related to credential exchange is Kerberos protocol[43]. The protocol considers a user as the trustee and a computer as the trustor and enables them to securely exchange their own verifiable credentials. To do this, Kerberos system needs to use a third party, in this case is another computer, to facilitate the credentials exchange process. However, this approach is no longer used since the current network systems like IoT are much more complex and are facing many intelligent attacks.

Recently, many researchers consider "credentials" in a broader perspective and have used the term "trust metrics" and "technical attributes" instead of "credentials". This approach allows us to develop trust more flexible, scalable and effective.

- Trust Negotiation Process

An important issue when exchanging and generating credentials is the undesirable reveal of information to malicious entities, resulting in loss of security and privacy. The question raised is: To what extend an entity trusts other entities to see its own credential information in exchange of earning their credentials. There are many research works dealing with this trade-off between gaining trust and sacrificing privacy such as in [44],[45],[46]. These researchers considered several particular context in accordance with types of credentials and number of credentials. They analyzed the loss of privacy once any credentials are revealed to other entities. This trade-off approach has motivated some researchers to develop a trust platform by developing architecture systems based on that trade-off principles.

TrustBuilder is a typical example in which a mechanism is implemented for analyzing and choosing the reasonable solution for the trade-off in the context of web services[42]. The trustor needs to understand the risk of losing privacy information when revealing credentials in exchange of earning trust. Based on this mechanism, trust is gained when a successful trade-off is made: sufficient credentials are revealed while sacrifice privacy is still maintained in some level. The concept of trust transitivity property is also characterized in TrustBuilder in the form of "credentials chain". For example, if entity A trusts B' s credentials, and B trusts C' s credentials, then A trust in the credentials of C in some degree.

Based on the credentials chain concept, some research works designed and developed trust frameworks that perform credential chaining and credential exchange such as in PeerTrust[47], PROTUNE[41], RT10[48].

Table 4. A Comparison on Research Work related to Policy and Trust Languages

Research Work	Network Environment	Trust Context	Policy/Trust Language Features
KAoS [51]	Distributed heterogeneous environments	Access Control for KAoS services	KAoS Policy language with ability of dynamic policy changes.
Rei [52]	Semantic Webs	For Security and Privacy Issues	Use semantic representation and model for dynamic policy manipulation. Allow each entity to set their own policy,
Global Computing [53]	Global Computing system	To replace key-based security	Include observation of trustee, recommendation from others and reference to other sources of the trustee. Use a formal policy language. Trust can be proved
WS-Trust [54]	Web services	Specification and OASIS standard providing extensions to WS-Security	Security Assertion Markup Language (SAML). Trust is gained through proofs of identity, authorization, and performance. To validate the security token.
[55]	Global Computing system, Dynamic Networks	For trust-based security mechanism	Policy language that use lattices of relative trust values. Allows fine-tuned control over trust decisions
Cassandra [56]	Large scale distributed systems	Role-based access control and Context-based system for authorization	Use a policy specification language based on Datalog with constrains with five special predicates. Trust is obtained after credentials exchanged.
[57]	Open Distributed System, WWW	Trust-based access control for web resources	Use ontology for representing trust negotiation policies. Rules are used to negotiate trust. Policies are more flexible than standard policy set, allowing simplify policy specification
Policy Maker [58]	Distributed Systems	Trust-based authorization	Provide "proof of compliance" for request, credentials and policies. Allow individual system to have different trust policies. PolicyMaker assertions can be written in any programming language.
KeyNote [59] [60]	Distributed Systems	Trust-based authorization	Same principles with PolicyMaker[58]: directly authorize actions (in accordance with credentials) instead of processing both authentication and access control. Require credentials and policies be written in a specific assertion language to work with KeyNote compliance checker.

Ontologies and Context-aware mechanisms are also soon introduced when developing credentials on the context of client-server system [49] and Semantic Web[50].

- Policy Languages and Trust Languages

It is needed to design formalism for trust-related information, e.g credentials and trust metrics in order to develop a trust system. This objective can be achieved by incorporating findings from logic to automate various kinds of reasoning, such as the application of rules and policies or the relations of sets and subsets for the Trust Computation process. Most of researchers have used the Semantic Webs techniques such as semantic representation, policy languages, ontologies and reasoning mechanisms to the trust computation. The issue is how to represent and express trust information and trust knowledge. Some efforts have been made to create policy languages for trust as described in Table 4.

B. Reputation-based Trust Computation Models

This approach uses history of interactions and behaviors among trustor, trustee and related entities, combines them in accordance with a reputation model in order to make a trust decision about the trustee. The history of interactions between trustor and trustee is sometimes called personal experience or direct reputation. The history of interactions between other entities and trustor is also called indirect reputation, referral reputation or recommendation.

There are much parallel research works on both reputation-based trust model and reputation model. The confusion between a reputation system and a trust system should be clarified. Trust and reputation are sometimes in the same across multiple contexts or are treated as the same mechanism to support services. Basically, a reputation system collects feedbacks from entities after an interaction incurs. These feedbacks will be combined and calculated using several mathematical models to get a reputed score. This reputed score is sometimes misunderstood as trust level. Several reputation systems have been developed in the context of e-commerce systems and web services such as eBay [61] and Keynote [59][60]. These systems use a centralized authority to get ratings and feedbacks from users after each transaction and then update the overall reputed score by using several mathematical models as mentioned above. There are also some distributed approaches for reputation system in which each entity establishes and maintains reputed scores to its neighbors by updating once any related interaction occurs by using several heuristic algorithms. It is required to integrate these score due to the use of deterministic numbers for representing reputation.

Reputation-based trust system can be considered as a step forward compared to reputation system in which trust computation mechanism combines not only ratings or feedbacks from entities but also trustor and trustee properties and preferences; and context information to calculate trust level. In this sense, reputation system is a part of trust system. There have been a large amount of effort to investigate the reputation-based trust model and to develop reputation-based trust systems in many type of network environment such as in distributed systems, P2P networks, sensor networks, and grids. There are also some research works to build a network of trust in which trust is established and maintained between any two entities over time, resulting in creating a "web of trust".

- Reputation-based Trust in Distributed System and P2P Networks

  The trust models in this part try to create a trust system that entities are able to establish, calculate trust level, and make trust decisions rather than rely on a centralized authority. The contribution in this approach is how to create appropriate credentials, TMs and TAs that provided to each entity to produce trust. Depending on different purposes of applications in each network environment, reputation-based trust systems are utilized accordingly. For example, in distributed system, many research works focus on the detection of malicious entities and prevention of network attacks while trust system in P2P networks is to guarantee the quality of data transfer.

- Reputation-based Web of Trust

  Almost effort in this idea uses the concept of credentials chain. The majority of trust computation transitivity has been focus on using reputation. Reputation, in this scenario, is defined as a TM, and each entity maintains reputation information on other entities, thus creating a "trust network" or "web of trust".

There are two approach for trust systems in the web of trust. The first approach assumes that trust credentials and TMs are already existed, and the trust systems are trying to propagate trust among entities which may not have been evaluated for trust. The later supposes that a web of trust is given in which a link between two entities mean the trust decision with a trust value. There is no matter how these links are made as long as the trust can be quantified. If there is no link between two entities, it means no trust decision has been made, and trust transitivity should be applied in this scenario. The summary and comparisons of reputation-based trust computation in the above discussed perspectives are described in detailed in Table 5.

Table 5. Features comparisons among reputation-based trust models

Research Work	Network Environment	Trust Context	Reputation-Related Features
[62][63]	Distributed System	Malicious Node detection	Define Agent, Trust Relationships, Trust Value and Trust Categories. Define first-hand knowledge as direct reputation and second-hand knowledge as recommendation. Propose Recommendation protocol for trust propagation.
[64][65] [66]	Distributed System Social Network	Reputation Management	Reputation information is obtained from external sources. Allow entities actively determine trust using reputation information obtained from other entities. Avoid hard security by distributing reputation information allowing individuals to make trust decisions instead of a centralized trust management system. Weight the reputation information by the reputation of those sources for providing good information.
[67]	Social Networks Multi-agents system	Reputation System	Analyze the reputation information by characterizing the indirect and direct information. Considering the social relation in calculating reputation score. Put the context information into account.
[68]	Open Networks	Trust-based authentication	Provides methods for computing degrees of trust in the presence of conflicting information.
[69] [70]	P2P Networks	Reputation and Trust for Webpages ranking	Propose PageRank algorithm for ranking websites by authority. EigenTrust algorithm using PageRank to calculate global reputation value for each entity. Credentials for reputation in this work is the quality of a peer’ s uploads (e.g., did the file successfully upload?) within a peer-to-peer network.
[71]	P2P Networks	Reputation System	Propose XRep protocol which allows for an automatic vote using user’ s feedback for the best host for a given resource.
[72][73]	Web of Trust	TrustMail application	Use ontologies to express trust and reputation information, which then allows a quantification of trust for use in algorithms to make a trust decision about any two entities. Trust transitivity is considered as credentials chain. Local reputation and Global reputation is also taken into account.
[74][75]	Web of Trust P2P Network	Trusted applications in Open Network	Define controversial users who are both trusted and distrusted in particular context. Globally computed trust value (in a web of trust) for a controversial user may not be as accurate as a locally computed value due to the global disagreement on trust for that user. Propose a method that performs a global computation on reputation values but considers the individual’ s input to the evaluation as the user preferences.

V. Hybrid Trust Model and Trust Aggregation

Several research works have tried to combine both reputation and policy-based models as a hybrid trust model in order to take advantages of both approaches while may get rid of their drawbacks. This idea has recently become more popular in the context of IoT where trust is more complex because many factors contributed to the trust establishment and to the trust computation. In such IoT environment, history of interactions and behaviors of entities are not only for reputation information but also for trust-related knowledge extraction. The combination of reputation information, knowledge and relationships among entities in IoT draws a very complicated picture of trust computation.

Table 6. Summary of Trust Aggregation Techniques

Aggregation Techniques	Research Work	Importance Technique Features
Weighted Sum	[76][77]	Entities with a higher reputation or transaction relevance have a higher weight. Entities with strong relationships to trustor have higher weight. Use credibility as weight associated with indirect trust (recommendation or feedback). Use similarity as weight for indirect trust aggregation.
Fuzzy Logic-based	[78][79]	Fuzzy Logic deals with reasoning that is approximate rather than fixed and exact. Fuzzy logic variables may have a truth value that ranges in degree between 0 and 1 and produce a partial trust where the truth value may range between completely true and completely false as trust levels. Linguistic variables are used as trust levels and managed by specific membership functions. Then trust is represented as a fuzzy measure with membership functions describing the degrees of trust (trust level).
Belief Theory	[80][81]	Belief theory (evidence theory or Dempster-Shafer theory (DST)) deals with reasoning with uncertainty, with connections to other techniques such as probability, possibility and imprecise probability theories. Trust can leverage the subjective logic by operating on subjective beliefs about the network environment, and used opinion metric to denote the representation of a subjective belief. Used in trust computational model to compute trust of agents in autonomous systems by modeling the trust by belief, disbelief and uncertainty of an entity to other entities. It makes use of a base rate probability in the absence of evidence. The average trust then can be calculated as the probability expectation value between trustor and trustee. Subjective logic operators such as the discount and consensus operators can be used to combine opinions (self-observations or recommendations).
Bayesian Methods	[82][83]	Trust can be considered as Bayesian interference: a random variable following a probability distribution with its model parameters being updated upon new observations. Can be used as a trust computational model because of its simplicity and sound statistical basis. Trust value can be modeled as a random variable in the range of [0, 1] following Beta distribution in which Belief discounting can be applied to defend against malicious entities such as bad-mouthing attacks ballot-stuffing attacks.

In the hybrid model, reputation is considered as one of several TMs. The reputation TM can be obtained by using the reputation mechanisms and reputation systems that have already been developed and mentioned above. That is the content of Trust Aggregation procedure in which trust evidences (TAs, TMs) are collected through several techniques, such as self-observation or reputed information in the form of feedbacks and recommendations.

TMs can be gained from sufficient TAs by using trust aggregation techniques, for example, TMs can be computed by using Weighted Sum [76],[77], Fuzzy-based algorithms [78],[79], Belief Theory [80],[81], Bayesian mechanisms [82],[83].

To calculate the overall trust score or trust level, a policy-based mechanism with one of a trust aggregation method mentioned above or with a reasoning method is needed to combine those TMs.

It is needed to note that the trust aggregation is a dynamic process which heavily depends on context-aware information, service requirements and trustor's preferences. Each trustor needs appropriate trust data, context data and aggregation methods for producing desired overall trust score which reflects the trustor’ s perspective and context awareness. Specific trustors might use and define different trust aggregation techniques for dealing with their associated trust data. There is currently no complete trust aggregation mechanism can deal with the personalized trust in dynamic context-awareness environment, however, several researchers have proposed some solutions for particular contexts and services. The summary is described in Table 6. The trust aggregation techniques and reasoning mechanism are the crucial parts needed to investigate and develop in order to build a completed trust platform in the IoT.

VI. Discussion and Future Research

In our study, extensive range of trust computation mechanisms has been discussed. However the current research methods are only focused only on specific context and hence lacking completeness. Therefore a single unique solution is not presented for the trust computation and acquisition. Thus issues are still open for investigation and some of the ideas are discussed here.

A. Research Gaps and Discussion

Based on many papers that have been analyzed above, there are many gaps that needed to be filled in order to have a complete trust understanding and development.

One of the most important gap that we intend to discuss and go for doing research is the lack of using environment information to trust computation. The network system here is the IoT in which physical devices are owned by human-related factors and inherently socially connected by physical-cyber-social system. Moreover, trust computation methods also lack concerns on trustor’ s subjective properties, in other words, the trust results are not reflected of personalized expectation. The solutions for this gap could be two-fold approaches: The first one is to develop the trust relationships among entities in the IoT, thus creating a reliability and readiness of the trust network, based on the existing social models in the network systems. The second one is to explore other social TMs such as trustor’ s similarity and friendship behaviors, centrality, community of interest, and more appropriate reputation TM.

Along with the two approaches, trustor preferences should be taken into account in order to reflect the personalized trust and to enhance the intelligence of trust. There are possibly large number of TMs depending on each context of IoT and services requirements such as honesty, cooperativeness, QoS, community of interest, and etc. In order to explorer more TMs, it is needed to investigate the network environment ontologies and trust ontologies in which relationships among entities and the relationships’ properties are represented and clarified. Consequently, by using a reasoning mechanism or a machine learning technique, new trust information and trust knowledge could be extracted and help enhancing the effectiveness of trust computation.

Another big gap in the area of trust computation is the trust aggregation methods and trust reasoning that have been stated in the previous section. This gap incurs in both situation in the trust computation procedure: when there are several distinct TAs needed to combine into one overall TM; and when there are several TMs needed to combine into the overall trust score or trust level. There are limited literatures in this area as mentioned in Section IV. The most popular and simple method to deal with the trust aggregation and trust reasoning currently is to apply the use of static weighted sum for trust formation. However, this solution is not smart enough due to the complicated IoT environment. Thus, there is an urgent need for a novel research on the use of more effective trust formation methods including dynamic weighted sum, belief theory, fuzzy logic and regression analysis. For example, an intelligent weighted sum method can dynamically adjust the weights associated with TA and TMs based on context awareness and user preferences. The weighted sum method can also use a regression analysis that links context information with TA and TM and user preference so as to determine the best weight assignment.

B. Other Research Directions

As compared to network security, it is essential to investigate on trust validation methods to effectively combat and defend with all sort of attacks including self-promoting, good mouthing/bad mouthing attacks and other possible attacks. While defending from attacks, it is also important to investigate resilient self-healing approaches to enhance trust recovery after a positive attack. Further effectiveness of trust management when it comes to billions of devices and applications should be studied carefully. One possible direction is to investigate trust management with concepts like Big Data and Data-mining. Essentially employing trust capabilities should minimally compromise performance and process of IoT as many devices have limited resources. A possible research direction is the investigation of intelligent trust-based routing protocols which are more reliable while consuming minimum energy and traffic overhead.

Static methods for dealing with trust discussed above will not be enough to implement context-aware scheme. Thus, an autonomous or dynamic trust computation mechanism should be considered for the process involved with TMs acquisition, calculation and finally for decision making process.

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] B. A. e. al., "Towards a Decision Model based on Trust and Security Risk Management," in *Seventh Australasian Conference on Information Security*, 2009, pp. 61-70.

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

[3] Z. Y. e. al., "A Survey on Trust Management for Internet of Things," *Journal of Network and Computer Applications,* pp. 120-134, 2014.

[4] J. F. M. Blaze, J.Lacy, "Decentralized trust management," in *Proceedings of IEEE Conference on Security and Privacy*, 1996.

[5] N. Li and J. C. Mitchell, "Datalog with Constraints: A Foundation for Trust-management Languages," in *Proceedings of the Fifth International Symposium on Practical Aspects of Declarative Languages*, 2003.

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

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

[8] M. B. T. Beth, B. Klein, "Valuation of trust in open networks," in *European Symposium on Research in Computer Security*, 1994.

[9] G. Caronni, "Walking the web of trust," in *Proceedings of 9th IEEE International Workshops on Enabling Technologies (WETICE)*, 2000.

[10] G. S. Ilung Pranata, Rukshan Athauda, "A Holistic Review on Trust and Reputation Management Systems for Digital Environments," *International Journal of Computer and Information Technology,* vol. 1, pp. 2277 – 0764, September 2012 2012.

[11] E. Chang, F. K. Hussain, and T. S. Dillon, "Fuzzy nature of trust and dynamic trust modelling in service oriented environments," in *Workshop on secure web services*, Fairfax, USA, 2005.

[12] E. Chang, T. Dillon, and F. K. Hussain, "Trust Reputation for Service-Oriented Environments," ed West Sussex, England: John Wiley & Sons Ltd, 2006.

[13] G. Barbian, "Trust Centrality in Online Social Networks," in *Intelligence and Security Informatics Conference (EISIC), 2011 European*, 2011, pp. 372-377.

[14] W. Yan, L. Lei, and L. Ee-Peng, "Price Trust Evaluation in E-service Oriented Applications," in *E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services, 2008 10th IEEE Conference on*, 2008, pp. 165-172.

[15] L. Mui, "Computational models of trust and reputation : agents, evolutionary games, and social networks," ed: Massachusetts Institute of Technology, 2003., 2014.

[16] Z. G., "Collaborative reputation mechanisms for online communities," ed: Massachusetts Institute of Technology, 1999., 2005.

[17] S. S. Park, J. H. Lee, and T. M. Chung, "Cluster-

based trust model against attacks in ad-hoc networks," 2008, pp. 526-532.

[18] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," 2008, pp. 2129-2133.

[19] R. A. Shaikh, H. Jameel, S. Lee, Y. J. Song, and S. Rajput, "Trust management problem in distributed wireless sensor networks," 2006, pp. 411-414.

[20] A. Boukerche and Y. Ren, "A security management scheme using a novel computational reputation model for wireless and mobile Ad hoc networks," 2008, pp. 88-95.

[21] B. Lagesse, M. Kumar, M. Wright, and J. M. Paluska, "DTT: A distributed trust toolkit for pervasive systems," 2009.

[22] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," *Communications Surveys & Tutorials, IEEE,* vol. 14, pp. 279-298, 2012.

[23] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," presented at the Proceedings of the 2012 international workshop on Self-aware internet of things, San Jose, California, USA, 2012.

[24] M. J. Probst and S. K. Kasera, "Statistical trust establishment in wireless sensor networks," *Parallel and Distributed Systems, 2007 International Conference*, 2007, pp. 1-8.

[25] D. Chen, G. R. Chang, D. W. Sun, J. J. Li, J. Jia, and X. W. Wang, "TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things," *COMPUTER SCIENCE AND INFORMATION SYSTEMS,* vol. 8, pp. 1207-1228, 2011.

[26] A. A. Pirzada and C. McDonald, *Trust establishment in pure ad-hoc networks*.

[27] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, *A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks*.

[28] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems,* vol. 43, pp. 618-644, 1/1/2007 2007.

[29] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," *Proceedings of the 2nd ACM Conference: Electronic Commerce,* p. 150, 10/17/ 2000.

[30] N. Iltaf, A. Ghafoor, U. Zia, and M. Hussain, "An Effective Model for Indirect Trust Computation in Pervasive Computing Environment," *Wireless Personal Communications,* vol. 75, pp. 1689-1713, 2014/04/01 2014.

[31] L. Zhaoyu, A. W. Joy, and R. A. Thompson, "A dynamic trust model for mobile ad hoc networks," in *Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of*, 2004, pp. 80-85.

[32] A. Rajaram and D. S. Palaniswami, "A Trust Based Cross Layer Security Protocol for Mobile Ad hoc Networks," 11/03/ 2009.

[33] L.-H. Vu, M. Hauswirth, and K. Aberer, "QoS-Based service selection and ranking with trust and reputation management," presented at the Proceedings of the 2005 Confederated international conference on On the Move to Meaningful Internet Systems - Volume &gt;Part I, Agia Napa, Cyprus, 2005.

[34] M. H. Mashinchi, L. Lei, M. A. Orgun, and W. Yan, "The prediction of trust rating based on the quality of services using fuzzy linear regression," in *Fuzzy Systems (FUZZ), 2011 IEEE International Conference on*, 2011, pp. 1953-1959.

[35] A. Iliev and S. W. Smith, "Protecting Client Privacy with Trusted Computing at the Server," *IEEE Security and Privacy,* vol. 3, pp. 20-28, 2005.

[36] A. J, #248, sang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.,* vol. 43, pp. 618-644, 2007.

[37] S. P. D. Rotondi, G. Altomare, A. Galipò, and S.Genolini, " Final framework architecture specification " in *IoT Work* vol. WP1, ed: Siemens, 2013.

[38] P. B. a. P. Samarati, "Regulating service access and information release on the web," in *7th ACM conference on computer and communications security*, 2000.

[39] N. Li and J. Mitchell, "RT: A Role-based Trust-management Framework," in *DARPA Information Survivability Conference and Exposition (DISCEX)*, Washington D.C, 2003.

[40]W. N. R. Gavriloaie, D. Olmedilla, K. E. Seamons, M.Winslett, "How to use declarative policies and negotiation to access sensitive resources on the semantic web," in *1st European Semantic Web Symposium (ESWS)*, Crete, Greece, 2004.

[41] P. A. Bonatti and D. Olmedilla, "Driving and monitoring provisional trust negotiation with metapolicies," in *IEEE 6th International Workshop on Policies for Distributed Systems and Networks (POLICY)*, Stockholm, Sweden, 2005.

[42] T. Y. M. Winslett, K.E. Seamons, A. Hess, J. Jacobson, R. Jarvis, B.Smith, L. Yu, "Negotiating trust on the web," *IEEE Internet Computing,* pp. 30-37, 2002.

[43] B. C. N. J. Kohl, "The Kerberos network authentication service,," IETF RFC 15101993.

[44] K. E. S. W.H.Winsborough, V.E. Jones, "Automated trust negotiation," in *Proceedings of the DARPA Information Survivability Conference*, 2000, pp. 88-102.

[45] M. W. T. Yu, "Policy migration for sensitive credentials in trust negotiation," in *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society (WPES 03)*, New York, USA, 2003, pp. 9-20.

[46] M. W. T. Yu, K.E. Seamons, "Interoperable Strategies in Automated Trust Negotation," in *Proceedings of the 8th ACM Conference on Computer and Communications Security*, New York, USA, 2001, pp. 146-155.

[47] D. O. W. Nejdl, M. Winslett, "Peertrust: automated trust negotiation for peers on the semantic web,," in *Proceedings of Workshop on Secure Data Management in a Connected World in Conjunction with the 30th International Conference on Very Large Data Bases*, 2004, pp. 118-132.

[48] W. H. W. N. Li, J.C. Mitchell, "Distributed credential chain discovery in trust management," *Computer Security 11,* pp. 35-86, 2003.

[49] C. D. J. J.-M. Seigneur, "Trust enhanced ubiquitous payment without too much privacy loss," in *Proceedings of the 2004 ACM Symposium on Applied Computing*, New York, USA, 2004, pp. 1593-1599.

[50] N. M. S. F.L. Gandon, "Semantic web technologies to reconcile privacy and context awareness," in *UbiMob ' 04: Proceedings of the 1st French-speaking Conference on Mobility and Ubiquity Computing*, New York, USA, 2004, pp. 123-130.

[51] J. B. A. Uszok, R. Jeffers, N. Suri, P. Hayes, M. Breedy, L. Bunch,M. Johnson, S.Kulkarni, J. Lott, "Kaos policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement policy," in *POLICY '03 Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*, Washington DC, USA, 2003.

[52] T. W. F. L. Kagal, A. Joshi, "A policy-based approach to security for Semantic Web," in *Proceedings of the 2nd International Semantic Web Conference*, 2003, pp. 402-418.

[53] K. K. M. Nielsen, "Towards a formal notion of trust," in *Proceedings of the 5thACMSIGPLAN International Conference on Principles and Practice of Declaritive Programming*, New York, USA, 2003.

[54]OASIS, "WS-Trust 1.4," in *WS-Trust 1.4*, ed, 2012.

[55] M. N. M. Carbone, V. Sassone, "A formal model for trust in dynamic networks," in *Proceedings of International Conference on Software Engineering and Formal Methods*, 2003.

[56] P. S. M.Y. Becker, Cassandra, "Distributed access control policies with tunable expressiveness," in *International Workshop on Policies for Distributed Systems and Networks*, 2004.

[57] W. N. T. Leithead, D. Olmedilla, K.E. Seamons, M. Winslett, T. Yu, C.C. Zhang, "How to exploit ontologies for trust negotiation," in *Workshop on Trust, Security, and Reputation on the Semantic Web (ISWC)*, 2004.

[58] J. F. M. Blaze, J. Lacy, "Decentralized trust management," in *Proceedings of IEEE Symposium on Security and Privacy*, 1996, pp. 164-173.

[59] J. F. M. Blaze, J. Ioannidis, A. Keromytis,, "The KeyNote Trust Management System," University of Pennsylvania, Pennsylvania, USA1999.

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

[61] e. a. P. Resnick, "Reputation Systems " *Communications of the ACM,* pp. vol. 43, pp. 45-48, 2000.

[62] S. H. A. Abdul-Rahman, "A distributed trust model," in *The New Security Paradigms Workshop*, 1997, pp. 48-60.

[63] S. H. A. Abdul-Rahman, "Using recommendations for managing trust in distributed systems," in *Proceedings of IEEE International Conference on Communication*, 1997.

[64] M. P. S. B. Yu, "A social mechanism of reputation management in electronic communities," in *International Workshop on Cooperative Information Agents*, London, UK, 2000, pp. 154-165.

[65] M. P. S. B. Yu, "An evidential model of distributed reputation management," in *AAMAS ' 02: Proceedings of the First International Joint Conference onAutonomousAgents and Multiagent Systems*, New York, USA, 2002, pp. 294-301.

[66] M. P. S. B. Yu, "Detecting deception in reputation management," in *AAMAS ' 03: Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems*, New York, USA, 2003, pp. 73-80.

[67] C. S. J. Sabater, "Reputation and social network analysis in multiagent systems," in *AAMAS ' 02: Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems*, New York, USA, 2002.

[68] M. B. T. Beth, B. Klein, "Valuation of trust in open networks," in *Proceedings of the 3rd European Symposium on Research in Computer Security*, 1994.

[69] L. P. S. Brin, "The anatomy of a large-scale hypertextual Web search engine," *Computer Networks,* pp. 107-117, 1998.

[70] M. T. S. S.D.Kamvar, H. Garcia-Molina, "The

eigentrust algorithm for reputation management in P2P networks," in *12th International Conference on World Wide Web*, New York, NY, USA, 2003.

[71] D. C. d. V. E. Damiani, S. Paraboschi, P. Samarati, F. Violante, "A reputation-based approach for choosing reliable resources in peer-to-peer networks," in *9th ACM Conference on Computer and Communications Security*, New York, NY, USA, 2002.

[72] J. H. J. Golbeck, "Accuracy of metrics for inferring trust and reputation," in *Proceedings of the 14th International Conference on Knowledge Engineering and Knowledge Management*, 2004.

[73] J. H. J. Golbeck, "Inferring reputation on the semantic web," in *Proceedings of the 13th InternationalWorldWideWeb Conference*, 2004.

[74] P. A. P. Massa, "Controversial users demand local trust metrics: an experimental study on epinions.com community," in *25th American Association for Artificial Intelligence Conference*, 2005.

[75] W. N. P.-A. Chirita, M. Schlosser, O. Scurtu, "Personalized reputation management in P2P networks," in *Proceedings of the Trust, Security and Reputation Workshop Held at the 3rd International Semantic Web Conference*, 2004.

[76] F. B. a. I. R. Chen, "Dynamic Trust Management for the Internet of Things Applications," in *International Workshop on Self-Aware Internet of Things*, San Jose, USA, 2012.

[77] I. R. C. F. Bao, "Trust Management for the Internet of Things and Its Application to Service Composition," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Francisco, USA, June 2012.

[78] G. C. D. Chen, D. Sun, J. Li, J. Jia, X. Wang, "TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things," *Computer Science and Information Systems,* vol. 8, pp. 1207-1228, 2011.

[79] Nguyen B.Truong, Tai-Won Um, Gyu Myoung Lee, "A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things," in *Innovations in Clouds, Internet and Networks (ICIN)*, Paris, France, March 2016.

[80] A. Jøsang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 9, pp. 279- 311, June 2001.

[81] R. I. A. Jøsang, C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems,* 2007.

[82] I. R. C. F. Bao, J. Guo, "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems," in *11th International Symposium on Autonomous Decentralized System*, Mexico City, Mexico, 2013.

[83] J. G. I.R. Chen, "Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection," in *International Conference on. Advanced Information Networking and Applications*, Victoria, Canada, 2014.

Nguyen B.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, 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 interest is 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 also involved in problems of Load Balancing, Channel Utilization and Energy Efficiency Protocols.

Upul Jayasinghe, received the B.Sc. degree in electronics and telecommunication engineering (first-class honours) from University of Moratuwa, Sri Lanka in 2010 and the M.Sc. from Asian Institute of Technology, Thailand in 2013. Mr. Jayasinghe, is the recipient of The A.B. Sharma Memorial Prize in recognition having the best thesis from the fields of Information and Communication Technologies and Telecommunications, Asian Institute of Technology in 2013. Currently He is doing PhD at Liverpool John Moores University United Kingdom. He has worked as a researcher in Centre for Wireless Communication, University of Oulu, Finland and Computer Communications and Applications Laboratory, EPFL, Switzerland. His research interests include IoT, Networking and Security, Wireless Communication and Mobile Networks.

Tai-Won Um received the BS degree in electronic and electrical engineering from Hong Ik University, Seoul, Korea, in 1999, and the MS and PhD degrees from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2000 and 2006, respectively. He is currently a senior researcher with Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea.

Dr. Um has been actively participating in standardization meetings including ITU-T SG 13 (Future Networks including mobile, cloud computing and NGN), and currently serves as an editor of Q16/13.

Gyu Myoung Lee received his BS degree from Hong Ik University, Seoul, Rep. of Korea, in 1999 and MS, and PhD. degree from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Rep. of Korea, in 2000 and 2007, respectively. He joined Department of Computer Science at the Liverpool John Moores University, Liverpool (LJMU), UK, as a Senior Lecturer in 2014. He is also with KAIST Institute for IT convergence, Daejeon, Rep. of Korea, as an adjunct professor from 2012.

His research interests include future networks, Internet of Things, multimedia services, energy saving networks including Smart Grid. He has actively contributed for standardization in ITU-T as a Rapporteur (currently Q11/13, Q16/13 and Q4/20) and IETF. He is an IEEE senior member.