Northumbria
University
NEWCASTLE

Accepted Manuscript

Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open Research Challenges

Abdelmuttlib Ibrahim Abdalla Ahmed, Siti Hafizah Ab Hamid, Abdullah Gani, Suleman khan, Muhammad Khurram Khan

PII: S1084-8045(19)30243-7

DOI: https://doi.org/10.1016/j.jnca.2019.102409

Article Number: 102409

Reference: YJNCA 102409

To appear in: *Journal of Network and Computer Applications*

Received Date: 3 September 2018

Revised Date: 22 May 2019

Accepted Date: 20 July 2019

Please cite this article as: Abdalla Ahmed, A.I., Ab Hamid, S.H., Gani, A., Suleman khan, , Khan, M.K., Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open Research Challenges, *Journal of Network and Computer Applications* (2019), doi: https://doi.org/10.1016/j.jnca.2019.102409.

Trust and Reputation for Internet of Things: Fundamentals, Taxonomy, and Open Research Challenges

Abdelmuttlib Ibrahim Abdalla Ahmed [a,*], Siti Hafizah Ab Hamid [b,*], Abdullah Gani [a,*], Suleman khan [c], Muhammad Khurram Khan [d]

[a] Center for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
[b] Department of Software Engineering, Faculty of Computer Science and Information Technology, University Malaya , Malaysia
[c] Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne NE18ST, UK
[d] Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia

ABSTRACT

Internet of things (IoT) is a contemporary technology, which links a tremendous number of devices with each other to ease the life via many useful services such as information exchange, monitoring, and control. IoT comprises different types of entities such as sensors and RFID tags, which mostly deployed in unattended, sensitive, and hostile territories. Due to rapid scalability and high heterogeneity, traditional security approaches fails to provide adequate security mechanisms for the current IoT infrastructure. The possibility of insecure and unattended deployment make some of IoT's entities subject to be captured physically by the attackers. As a result, the victim device can be exploited as a gateway to compromise the entire network. Furthermore, an entity may not work correctly because of resources constraints or instability of network's link. Recently, trust and reputation (TR) extended in IoT to monitor the behaviors deviation of IoT entities. Many TR models introduced, to incorporate the trust concepts in IoT as a new security paradigm. In this study, we provide thematic taxonomy for trust in IoT, considering several issues such as understanding of trust entity roles, trust properties, trust applications, levels of trust management, trust metrics, trust computation schemes and attacks on TR. Finally, the survey presents advances and open research challenges in the IoT's trust.

Keywords: Trust; reputation; trust computing; trust management; decision-making; Internet of Things

1 Introduction

IoT is a contemporary technology that has a considerable impact on the human life in different aspects including economic, health, technical, and social issues (). Currently, IoT has revolved our life by depending on the new emergence of technologies such as transportation, manufacturing components, sensors, and various others to ease our life(Yaqoob et al., 2017). The number of IoTs devices increasing at a tremendous rate, and expected to reach 100 billion devices by 2025 and its impact on the global economy about 11 trillion USD (Rose, Eldridge, & Chapin, 2015). IoT entities can be found in different forms such as sensors, RFID tags, smartphones, data resources, and services. In the literature, the terms thing, device, and entity used interchangeably for denoting IoT components. The pervasive infrastructure and resource constraints in IoT devices raise new and cumbersome security and privacy challenges(Khan, Aalsalem, Khan, & Arshad, 2019). Due to these

circumstances and challenges, conventional security models are inadequate for IoT environment.

Trust defined as ”The firm belief in the competence of an entity to act dependably, securely and reliably within a specified context”(Grandison & Sloman, 2000). Trust known as "a degree of subjective belief regarding the behaviors of a specific entity"(Cook, 2001). The expected behavior of entities that build from self-observation or history of entity actions, known as reputation(Resnick, Kuwabara, Zeckhauser, & Friedman, 2000).Basically, the concept of trust introduced in social science to represent the state in which there are one community-member called trustor relies on the actions of another community member called trustee(Bamberger, 2010; Mayer, Davis, & Schoorman, 1995).

A trustor, delegate the trustees to perform specific actions without confirming the outcome of trustees actions. However, trustor can establish and assess expectations regard these outcomes of trustee actions(Seligman, 1998).

Security and trust are complementary to each other if we look at security tools and mechanisms like fences, locks, and gates. Consequently, the trust is a concern on when and where and why we need to put these fences, locks, and gates in IoT environments to manage the level of cooperation and integration(Harwood, 2012). Trust-based security models have emerged to enhance the level of security mechanisms for coping up with the requirements of IoT. Besides security improvement, the trust and reputation (TR) used for supporting data and service management and for boosting entities collaboration in IoT environments. Robust TR model has a crucial impact in the sustainability of IoT system that is through assisting in the selection of a high QoS and best service provider (SP) in Service Oriented Architecture IoT (SOA-IoT).

1.1 Related works

In the literature, many papers have been proposed to survey the issues of TR in cyberspace. This sub-section briefly discusses the existing survey articles of TR in converged disciplines, from which IoT extended. Namely networks technologies, Internet applications and hybrid. The scope of these survey papers in comparison to our paper illustrated in Table 1.

In networks technologies, trust studied from different aspects in the context of various networks technologies such as WSNs, MANETs and IoT. Din, Guizani, Kim, Hassan, and Khan (2018), reviewed trust management techniques for IoT, they focus on describing trust management techniques. Guo, Chen, and Tsai (2017), conducted survey on trust model for IoT. They classified trust computation models for trust-based service management based on computation schemes. The authors summarized robustness and weakness of each computation aspects and compared defense mechanisms against trust attacks models. Yan, Zhang, and Vasilakos (2014), reviewed the literature of trust management in IoT, they identified roles of trust management in IoT. Khalid et al. (2013), reviewed trust systems and their applications in WSNs. Moreover, discussed the requirements and computation schemes with the study of several types of attacks. Moreover, provided a brief comparison of various TR systems in WSNs. Chang and Chen (2012) provided a general survey on various trusts management issues such as trust evidence clustering, aggregation and reputation in WSN and IoT. Furthermore, demonstration of the bootstrap platform provided for discussing deployment solutions and challenges in IoT. Cho, Swami, and Chen (2011), reviewed trust management approaches in MANETs, they discussed trust metrics, attacks, and

performance metrics beside that the authors presented future researches directions of trust in MANETs. Han Yu, Shen, Miao, Leung, and Niyato (2010), reviewed trust applications in the fields of WSNs, MANETs, and cognitive radio networks (CRNs). The authors classified TR into: system level and individual level trust. Momani and Challa (2010), presented a survey of trust models in different network technologies with emphasize on ad-hoc and WSNs. The author summarized the factors affects trust updating. Azer, El-Kassas, Hassan, and El-Soudani (2008), reviewed TR approaches in ad hoc network, they focused on the architectures, objectives and features of the trust management systems in ad hoc networks.(Hoffman, Zage, & Nita-Rotaru, 2009; Suryanarayana & Taylor, 2004) reviewed trust schemes in Peer-to-Peer applications; they classified it into three major classes based on reputation, policy and credential, and social network.

In internet application, TR reviewed from three different perspectives such as web application, website contents and web services. Sherchan, Nepal, and Paris (2013), reviewed trust definitions and defined social trust in the perspective of Social Networks. The survey addressed three issues of social trust: evidence aggregation, trust assessment, and trust propagation. Beatty, Reay, Dick, and Miller (2011), carried-out a meta-study on the consumers trust factor in electronic-commerce websites, they concerning on websites contents and its organization as a factor of trustworthiness assurance. Management system. Golbeck (2008) ,conducted a general survey about trust on web contents, services and applications. Yao Wang and Vassileva (2007), conducted a review on different trust and reputation systems for web service selection, they provided a thematic taxonomy for classifying into three dimensions: agent's vs resources, centralized vs decentralized and global vs personalized. Jøsang, Ismail, and Boyd (2007) conducted a comprehensive review on the existing internet applications. Moreover, they covered the system that proposed for deriving measures of TR for online transactions. Grandison and Sloman (2000), surveyed trust-based applications, targeting identification of trust-based application requirements in electronic-commerce.

Some surveys focused on the robustness of TR systems against attacks: Jøsang and Golbeck (2009) focused on nine different types of trust attacks. The study identified the requirements of measuring and analyzing the robustness of a trust system. Hoffman et al. (2009), reviewed TR attacks against defense approaches. Then, classified the attacks as white washing, orchestrated, self-promoting, and denial of service and slandering.

1.2 Scope and contribution

Recently, several trust protocols, models frameworks introduced with a specific focus on Internet of things requirements. This article aims to provide comprehensive tutorial and survey of current components, protocols, models and frameworks of TR.

- Thematic taxonomy based on important parameters to help in understanding TR and its associated issues in IoT. Taxonomy parameters include entity relationships and roles, trust
- Properties, trust management levels, trust metrics, trust computation schemes and trust attacks.
- Investigation of recent advances, efforts and solutions that address TR problems in IoT environments.
- Discussion on TR challenges which paralysis the efficiency and integration of TR systems with IoT devices that is to guide for future researches.

Table 1. Related works

1.3 Organization

Survey Paper	Year	Covered Technology /Application	Comparing current research works in terms of	Category
This work	2019	IoT	Trust applications, computation schemes, metrics and attacks	Hybrid
(Din et al., 2018)	2018	IoT	Summary table, No comparison table	Networks Technology
(Guo et al., 2017)	2017	IoT	Computation models against trust attacks	
(Yan et al., 2014)	2014	IoT	Summarizing versatility of trust management in IoT	
(Khalid et al., 2013)	2013	WSN	Network initialization ,observation, trust computation and attack prevention	
(Chang & Chen, 2012)	2012	WSN/IoT	No comparison table	
(Cho et al., 2011)	2011	MANETs	Methodology , properties, management models , performance metrics, and attacks.	
(Han Yu et al., 2010)	2010	MANETs/ WSNs/ CRNs	Neighbor monitoring , reputation propagation and punishments	
(Momani & Challa, 2010)	2010	ad-hoc/ WSN	No comparison table	
(Azer et al., 2008)	2008	Ad Hoc Networks	No comparison table	
(Suryanarayana & Taylor, 2004)	2004	Conventional networks	TR models against trust threats	
(Sherchan et al., 2013)	2013	Web based Social Networks	Properties, computation models, social issues, attacks and application domains	Internet applications
(Beatty et al., 2011)	2011	Websites contents	No comparison table	
(Golbeck, 2008)	2008	Web contents, services and applications	No comparison table	
(Yao Wang & Vassileva, 2007)	2007	Web service selection	No comparison table	
(Jøsang et al., 2007)	2007	Service provisioning	No comparison table	
(Grandison & Sloman, 2000)	2000	Service provisioning	No comparison table	

The rest of this article organized as follows. Background on TR systems considering the history of TR domains given in Section 2. Section 3 presents the motivation for studying and developing TR solutions for IoT. Section 4 introduces our taxonomy of trust in IoT,

including entity roles, trust properties, trust management levels, trust metrics, trust computation schemes and trust attacks. Section 5 investigates the advances of researches regarding trust in IoT. Section 6 discusses the challenges and the open issues. The article concluded in Section 7.

2 Background

The term trust derived and explained in different perspective of different fields such as sociology, psychology, and economics and recently introduced in cyberspace as well. This section gives definitions and introduction to the journey of trust from its origin in sociology and philosophy through the communications and networks up to IoT era. The aim is to give the reader full insight that can help them to deeply understand the objectives, components and emergencies of trust computation and its management in IoT systems.

2.1 Trust in psychology

In psychology, trust is the belief of that the behaviors of a trusted community-member is up to expectation level. Simpson (2007), argued that trust is more than aspirations and hopes of peoples, but is the unique and most important item for the maintenance and development of the happiness, effectiveness and sustainable relationship.

2.2 Trust in philosophy

Baier (1986) looked to the trust from a psychology point of view, he presented the difference between reliance and trust by stating that trust relationship is more than reliance,since trust can be subject to betray, while reliance can be subject to disappointed only. Jackson (1996) illustrated that by saying "we can rely on the clock to know the time but we do not feel betrayed if it broke".

2.3 Trust in communications and networks

Baras and Jiang (2005), described trust in communications as a set of relationships such as reliability, scalability, and reconfigurability. These relationships establish among active communication entities and governs by the communication protocols. Trust decision, made according to the evidenced generated from the history of interactions between these entities within the protocol.

2.4 Trust in IoT

Trust management in IoT found in two converged architectural forms, namely social IoT (Ray Chen, Bao, & Guo, 2016; Kokoris-Kogias, Voutyras, & Varvarigou, 2016; Nitti, Girau, & Atzori, 2014) and SOA-IoT (Ray Chen, Guo, & Bao, 2016; Guinard, Trifa, Karnouskos, Spiess, & Savio, 2010). This sub-section highlighted these forms as follows:

2.4.1 Social IoT:

Social IoT is a conventional peer-to-peer network linked with social network information. In social IoT, any entity (thing) build social relationships with the other entities that based on the owner's social networks (contact list or community of interest). Recently, social IoT paradigm attracted different application as smart city and e-health (Bui & Zorzi, 2011; X. Li et al., 2011). The nature of social relationships in the social networking play crucial role in the success of IoT applications. Where human runs physical/virtual entities. Thus, the designers and developers of social-IoT's applications must considers the social-relationships and social networking among the users of social-IoT entities. For requesting a service, an

entity consults the trust system for selecting a service-provider among the service-providers from the list of friends.

2.4.2 Service-Oriented-Architecture based IoT(SOA-IoT):

Trust-based SOA-IoT (Ray Chen, Guo, et al., 2016; Guinard et al., 2010), is a paradigm of interaction between IoT entities, in which every entity either service-consumer, or service-provider, offer services and share resources as illustrated in Figure 1. The entity can mutually change their role based on the requirements of the running transaction. The interaction between SP and service consumer carried out through service APIs. SOA technologies enable IoT entities to publish, discover, select, and compose services such as smart product management and smart emergency management (Ahmed, Khan, Gani, Ab Hamid, & Guizani, 2018; X. Li et al., 2011). For requesting a service, entity consults the trust system for selecting the highly trusted entity among the provider of the desired service. SOA-IoT systems encounter trust management hurdles, which summarized as follows:

- **Resources constrain:** IoT comprises a big number of devices with restricted capabilities. Current trust computing and management solutions do not fit the rapidly changing requirements because of resources constrain such as computation capability and storage capacity.
- **High scalability**: in the SOA-IoT environments, new entities allowed to joins at any time and existing one can leaves. Therefore, trust management system has to address these issues by allowing newly-joining entities to establish-up trust as fast as possible under accurate monitoring (Guinard et al., 2010).
- **Heterogeneity:** SOA-IoT comprises a massive number of heterogeneous IoT entities that provides various services. Managing the behavior of heterogeneous entities, that provide various type of services, is a cumbersome task. The problem is that some entities perform malicious activities on behalf of its owner for self-interests; these malicious activities target the reputation of a victim entity. For instance, IoT entities collude with socially tied ones, in performing bad-mouthing attacks to destruct the reputation of the competing entities, which offer same services, that through fabricating negative recommendations. Moreover, the attackers also collude in performing ballot-stuffing attacks to enhance the reputation of each other that is through fabricating positive recommendations.

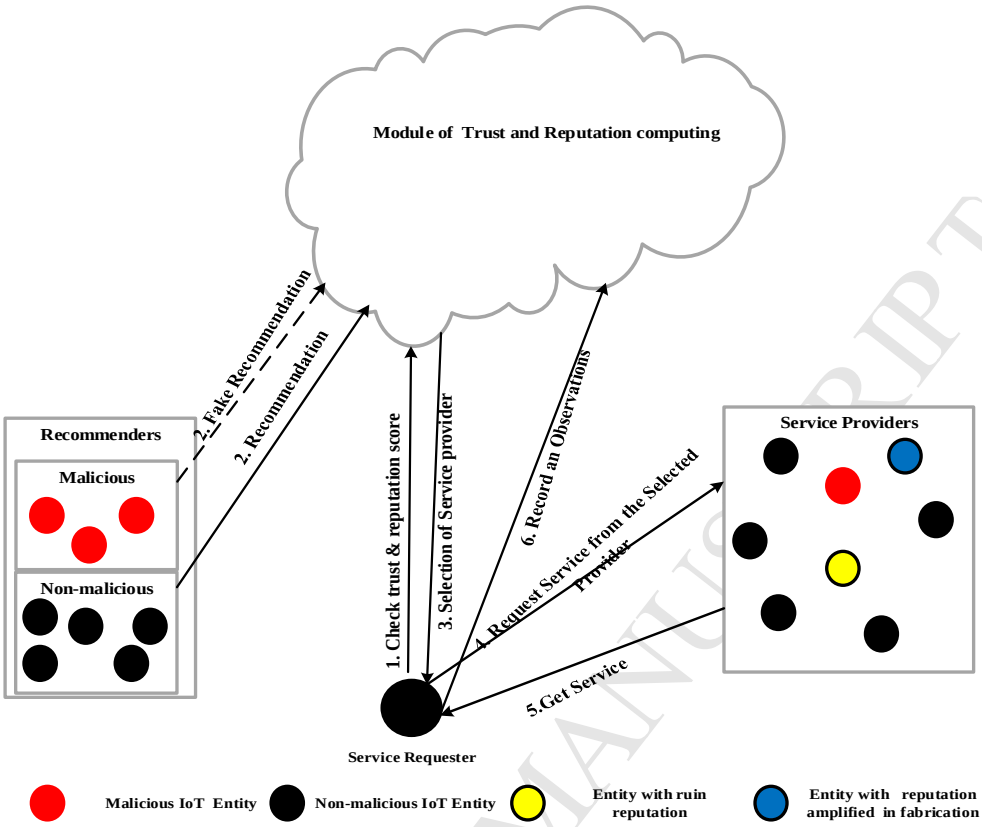

Figure *1.* Trust and Reputation in IoT

2.4.3 Hybrid IoT

Hybrid architecture is a convergence between SOA-IoT and social IoT. (Ray Chen, Guo, et al., 2016) stated that since the majority of IoT entities are human-controlled , so trust management system need to consider SOA-IoT features besides social relationships. Social relationships among the IoT entities helps in speeding up trust computation in SOA-IoT (Atzori, Iera, & Morabito, 2011). Figure 2 demonstrates The TR system in IoT, highlights flow of trust management information and different classes of entities with different behaviors (malicious, victims).

2.5 Fundamental definition and concepts

This sub-section defines several terms and concepts, which frequently used in TR discipline, and in this article, accordingly. The aim is to help the newcomers to understanding the fundamental of TR field.

Trustworthiness: According to the Oxford dictionary(Dictionaries, 2014), "Trustworthiness is the ability to be relied on as honest or truthful". The degree of trustworthiness can be represented either in discrete form or a continuous, the human nature biased to represent the rating of trustworthiness discretely. Whereas, the levels of discretization differ from one model to another, in some cases bounded with specific range and the rest allows the value, to grow infinitely (Rita Chen & Yeager, 2001; Maurer, 1996) Furthermore, these discrete values are either multinomial or binary. In the binary form, trust representation makes the judgment on the behavior of IoT entity either trusted or untrusted. The binary

representation of trust value is uncomplicated constructs, so it is not hard in term of implementation. However, multinomial form of trustworthiness representation allows entities to proceed with the transaction even the trustworthiness value of another entity is incomplete, but enough for performing the desired transaction (Jøsang et al., 2007; Pujol, Sangüesa, & Delgado, 2002)

Recommendation: The recommendation is an opinion or suggestion regarding the trustworthiness of an entity, given by other entities (Yan & Holtmanns, 2008).

Reputation: The reputation is one of the components of trustworthiness measures. The reputation establishes based on the recommendations from peers in the community of interest or contact list. An entity derives its individual's subjective trust from the other entity through combining the received recommendations and its own experiences. The existing TR systems allow the entities to generate feedbacks about each other, that after performing a complete transaction. the TR system aggregate these feedbacks to form the reputation score (Tavakolifard & Almeroth, 2012).

Collaborative filtering: this method focuses on the techniques for matching entities based on its interest and weighting these interests with similar needs to generate a recommendation for the requestor (Terveen & Hill, 2001). The source of recommendation is one of the most critical factors for weighting peers recommendations in TR systems (Jøsang et al., 2007). Besides TR systems, many applications use collaborative filtering for calculating a customized rating prediction of a provided service for the services requestor. Reputation system and collaborative filtering are similar where both are used to gather ratings from the peers.

Trust management: According to Blaze, Ioannidis, and Keromytis (2003), trust management is a mechanism that assists in automatic verification of entities behaviors against security-policies. Trust management provides a consolidated way to specify and interprets the relationships, security-policies and credentials(Blaze, Feigenbaum, & Lacy, 1996). The terms trust-management and reputation- management, used in the literature interchangeably(H. Li & Singhal, 2007). However, the difference comes when the trust management considers the current observation of trustor on the trustee where reputation management considers the calculation of trustee reputation from the global opinion on the past behaviors. Trust management helps in different aspects of decision making in IoT environment. For example authentication, intrusion detection, access control, detaching misbehaving devices, and other purposes (Cho et al., 2011).

3 Motivations

The nature of IoT application and deployment of its infrastructure raises new security and trust challenges. The conventional security, trust approaches, privacy, and governance techniques could not cope up with the IoT's requirements, that is because of the high scalability and diversity of the entities identities and the complicated relationships (Bao & Chen, 2012).

The traditional cues of TR, do not fit the requirements of IoT environments. The motivations of this article are monitoring trust information and proper dealing with trust attacks.

3.1 Monitoring trust information:

The task of monitoring the exchange and processing of trust information is a cumbersome task in IoT. Motivated by these essential facts, the establishment of trust should consider the following factors:

- Identify adequate IoT-based solution that can replace or improve conventional cues of TR systems. E.g. defining new approaches that can fit the requirements of IoT.
- Taking the advantages of cloud computing to create an efficient method for aggregating trust evidence, and deriving suitable trust measures. As a result, supporting decision-making, enhancing and sustaining IoT-based services.

3.2 Proper dealing with trust attacks:

The motivation for exploring, studying and establishing trust management system for social IoT and SOA-IoT system in the presence of misbehaving entities(Ray Chen, Guo, et al., 2016). Malicious IoT devices perform various types of trust attacks that is through exploiting their social relationships with socially close devices, for colluding in:

- Monopoly a set of services, or
- Illegally boost the trust score of each other.
- Damaging the reputation of the competing entities, which provide comparable services, that via fabricating negative recommendations.

4 Taxonomy of trust in IoT

In this section, we depicted the thematic taxonomy for trust in IoT. The thematic. The thematic taxonomy built based on seven factors: roles of trust entities, trust properties, trust management level, trust metrics, trust computation scheme, and trust attacks, as illustrated in Figure 2. These seven factors identified carefully to represent trust based-IoT environment, the process that occurs frequently. Whereas, roles of trust entities, trust properties, trust management level, represent the environment, in term of actors, properties and level of management. Each of these factors comprehensively explained in the subsequent sections as follows.

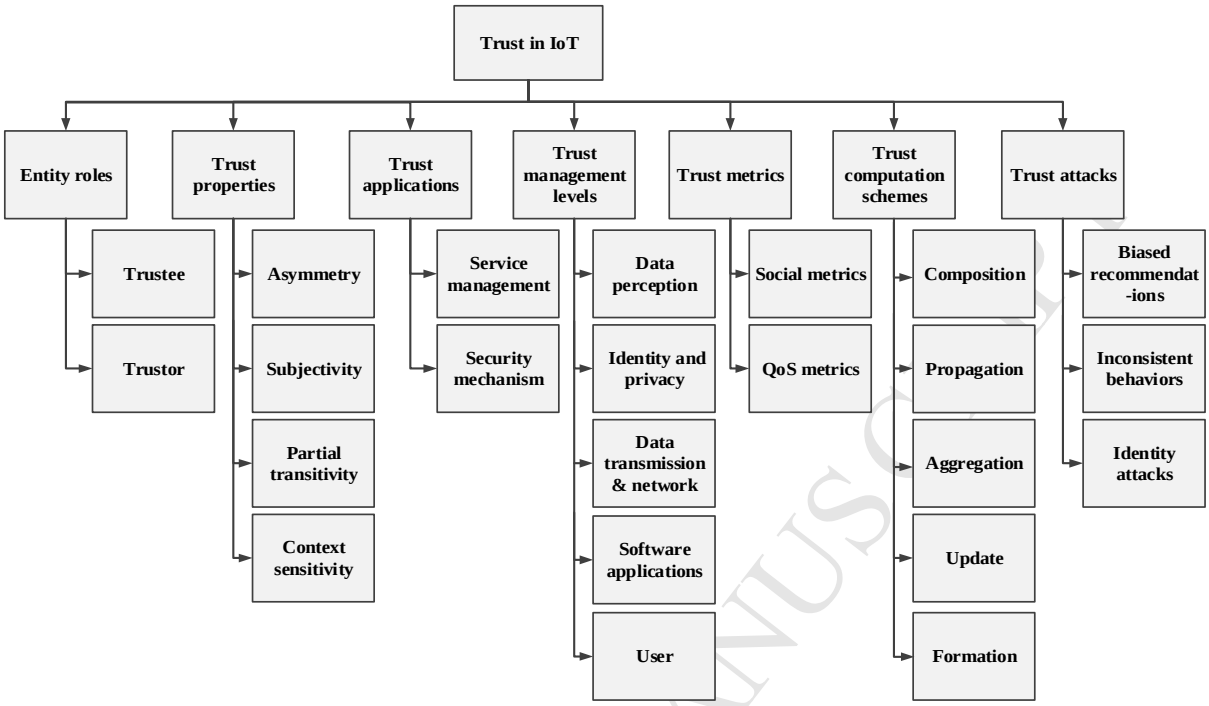

Figure 2. Taxonomy of Trust in the Internet of Things

4.1 Entity role

In In IoT, the trust relationship involves two entities/things named as trustee and trustor; These entities depend on each other to share the common interests mutually. The trustor needs to have confidence in the trustees in term of benevolence, honesty and beliefs. Therefore, it must ensure that the trustee will not betray it by performing risky behaviours(Ahmed et al., 2018). Since trust characterized by uncertainty and involves risk, so it is difficult to assure that, the trustor will be satisfied from the trustee behaviors.

4.2 Trust properties

Trust properties derived from social sciences to cyber-space, these properties such as asymmetry, subjectivity, partial transitivity, and context sensitivity (Khalid et al., 2013), these properties explained as follows:

4.2.1 Asymmetry

Trust can flow asymmetrically between IoT entities as illustrated in Figure 3. Where an entity-C trusts entity-D, which is not compulsory to imply also entity-D trusts entity-C.

$$\forall c, d \in CUD(cTb \Rightarrow \neg(dTc))$$

For all c and d in CUD, if c is related to d, then d is not related to c, Where T is trust relations.

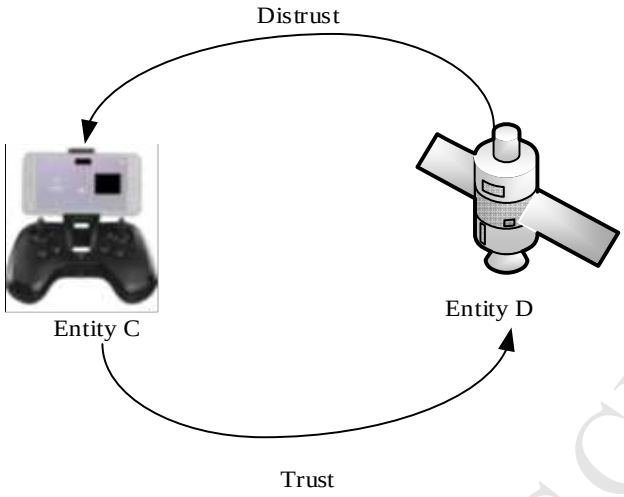

Figure 3.Trust asymmetry: one-to-one relation

4.2.2 Subjectivity

Trust is subject to evaluation by one entity with another. The reputations and observations that entity-A has about the entity-B rely on two factors:

- The level in which entity-B response to requests of entity-A, and
- The cost of extra demand from an entity-A.

Assume that the common opinion of the community of interest about an entity-B is that, an entity-B is well behaved. However, for entity-A it may still be possible to have a quite the opposite opinion about entity-B because of the demanding nature. So, entity-A trust is subject to the high expectations that entity-A has from an entity-B.

4.2.3 Partial transitivity

Trust can be transitive or non-transitive. For instance, assume an entity-A trusts entity-B, entity-B trusts entity-C, it is not compulsory for entity-A to trust entity-C. Therefore, entity-A can have a various level of trust from entity-B trust evaluations of other entities. The trust score found during trustworthiness evaluation of entity-A is also called the credibility of entity-A (Khalid et al., 2013). Credibility factor is one of the crucial factors for decision making in trust-based social IoT; it makes the difference in the decision in many cases. That is when the trustor, recommender, and recommendations are same but the credit of the trustee is different, for instance if the credit of entity-D is better than the credit of entity-C. As a result, the decision of entity-A regarding-D is "Trusted", but the decision of entity-A regarding entity-C is "Distrusted" that as illustrated in Figure 4.

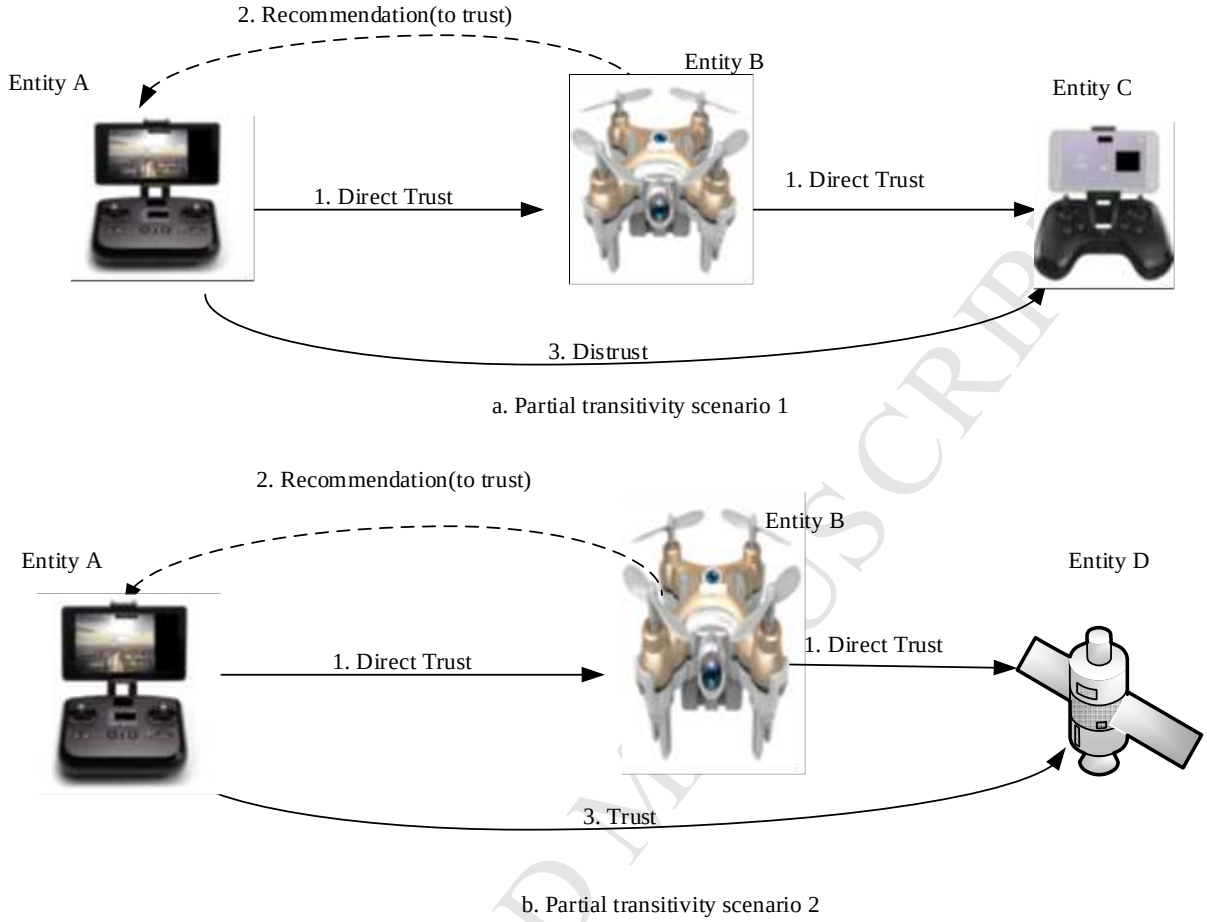

Figure 4. Trust Partial transitivity

4.2.4 Context sensitivity

The semantic characteristics of the TR attributes are essential factors for participating entity in the trust-based IoT system, that for both a trustor and trustee (Jøsang et al., 2007). For instance, if an entity-A forms a trust about an entity-B, the judgment also considers the context based on which entity-A has established that judgment (Han Yu et al., 2010). Whereas, entity-A may trust entity-B in the task (T_{n-3}). But, an entity-A may not trust entity-B in tasks (T_{n-1}) and (T_{n-2}). Consequently, the context must also be counted on the basis in which the entity-A takes a trust rating for the entity-B from other entities. The semantic measure descriptions to trust attributes are subjectivity, objectivity(Jøsang et al., 2007), as classified in Table 2.

- **Subjective:** indicates that an entity gives a recommendation/rating according to subjective judgment.
- **Objective:** indicates that the recommendation values generated according to objective evaluation on the trustee against formal criteria.

Table 2. semantic of trust attributes in IoT

Entity role	Trust attributes	Semantic
Trustee	- Reliability - Dependability - Competence - Timeliness - Ability - Security - Integrity - Behaviour - Predictability	Objective
	- Honesty - Benevolence - Goodness	Subjective
Trustor	- Standards - Assessment - Trustor's standards	Objective
	- Confidence - Expectations - Intention - Probability - Belief - Disposition - Attitude - Faith - Reliance - Willingness	Subjective

4.3 Trust application:

Trust-and-reputation concepts can be applied as an integral part in building different IoT applications. For instance, trust-based services management and trust-based security mechanisms. We discussed the categories of trust-based applications as follows:

4.3.1 Trust-based security Mechanism

Conventional security services are useful for traditional networks (Boukerche & Ren, 2008). However, IoT environments are dynamic, the number of entities is highly scalable, and service is heterogeneous. Moreover, the malicious entities threats the processes of establishing up and managing chain of IoT services. Therefore, conventional security services are inadequate for fitting the particular requirements of IoT security. The trust-based system can track the behavior of IoT entities, and then punish misbehaving entities and rewards well-behaving ones. Therefore, Trust systems can contribute to IoT security through supporting various types of security services and mechanisms such as intrusion detection, dynamic access control policy, discussed as follows.

• **Trust-based intrusion detection system:**
Dealing with intruders involves intrusion detection, prevention, and response, these tasks achieves through intrusion-prevention systems (IPs) and intrusion-detection (IDs) systems, that at entry points to IoT entity. IDS is an automated tool designed to detect unauthorized access to IoT system. An IPS involve IDS functionality but also contains mechanisms built to block intruder's traffic. TR system has been utilized to boost intrusion detection systems. Trust-based Intrusion Detection System comprises two stages; the first stage is intrusion detection, the second stage is trust evaluation among the entities. One of the IoT entities or cloud server uses Trust-based IDS for assessing the maliciousness of IoT entities (Bao, Chen, Chang, & Cho, 2011). The assessment of entity-to-entity trust involves procedures of statistical analysis on the interactions and behaviour's information.

• **Dynamic access control policy:**
In IoT environment, the entities collaborate in serving each other mutually and in sharing the common resources. However, IoT environment is dynamic, and the deployment of IoT devices make it vulnerable to several types of threats and physical capturing by the adversary. The captured device can be exploited as a gateway to compromise the entire IoT system. Robust and dynamic access control policy, which cope up the requirements of IoT environment, can assist in preserving security in the environment. That through helping in adjusting the access control to the requestor based on the context of each interaction. (Miao & Chen, 2010) introduced trust-based dynamic access control policy. Their solution comprises two major component. Namely, trust establishment and access right granting:

- **Trust establishment:** encompass two phases, initial static trust establishment and dynamic trust management. Firstly, Initial static trust establishment performed according to entity properties. The initial trust on both communication parties build based on trust properties of both sides. Secondly, Dynamic trust management: for proper dynamic trust decision, making trust management must rely on context information.
- **Granting access right:** Initially the entities granted many roles, which is based on the initial trust. Then proper role will be activated dynamically according to the change in the transaction context.

4.3.2 Trust-based services management

Service management in IoT deals with enhancing the alignment of IoT efforts with smart environments requirements. Using TR system as a complementary part of service management techniques boost the solutions regarding several issues of services management in IoT environment, for instance, Trust-based routing and SP selection.

• **Trust-based service provider selection**
The development of IoT software requires the interaction of services from diverse web SPs. According to (Consortium, 2004) "web services are a software system designed to support interoperable machine-to-machine interaction over a network". In SOA-IoT the approach of software design has new consideration such as SPs, service requestors and new services join or leave the system frequently Consequently, the selection of SP is a crucial issues. Trust-based SP Selection gives better performance when a requester needs to select the best SP (Billhardt, Hermoso, Ossowski, & Centeno, 2007).

• **Trust-based routing**
Involving trust concepts as sub-module with routing protocols enhanced the performance of routing processes through assisting in the selection of a suitable device as a next hop and

securing data-packets during the transmission process. Trust-based routing achieves by considering self-observation and recommendation of other devices. Encryption techniques widely used in routing protocols to secure data-packets during transmission process (Ray Chen, Bao, Chang, & Cho, 2014). However, encryption techniques incur a high computational cost, and it cannot identify the malicious nodes. The use of encryption techniques is not appropriate to many types of IoT devices as it has limited resources and vulnerable to many kinds of attacks and environmental impacts. In Trust-based routing, trust mechanisms can serve as an alternative to encryption techniques. Trust mechanism secure data-packet forwarding through isolating devices behaves maliciously before making routes and finding the best and trustworthy route (Brenner, 2006).

4.4 Levels of trust management

Trust management objectives achievable at multiple levels in computing environments, such as data perception, data transmission, identity trust, privacy preservation, users and applications.

4.4.1 Data Perception Trust

Is an important aspect of trust in IoT since it significantly supports overall trust on IoT service. This level of trust deals with IoT data during collection stages in the perception layer. (Javed & Wolf, 2012) discussed the verification of data that collected through multiple sensing devices. Stated that various entities using outlier detection can perform the sensors management. Moreover, they introduce a technique for automatic driving of a model for the environment, which monitored by the sensors. (Ukil, Sen, & Koilakonda, 2011) introduced a solution that resists various tamper-proofing attacks of the embedded devices, the solution applies trusted computing concept in IoT. However, the technology address security issues in hardware platform and data through supporting trusted data perception and secure data transmission as well. (Khoo, 2011) investigated security and trust issues in RFID technology through analyzing different threats against the components of RFID system, these threats such as tag cloning, relay attack, personal and location privacy, blocking and jamming devices, and intrusion detection. The study supports achievement of data perception trust and privacy protection. (Sicari, Coen-Porisini, & Riggio, 2013), combined WSNs with the wireless mesh network. This hybrid architecture support secure data collection. Whereas, secure and verifiable multilateralism technique used to allow the network to preserve the trustworthiness of collected data. This solution showed good impact regarding data reduction. The limitation of this study is that it does not consider data privacy.

4.4.2 Identity trust and privacy preservation

Identity trust and privacy preservation are essential factors in achieving optimum benefits of IoT applications since the identity of a trustee is the base level for trust-based systems. Several research carried out to enhanced identity trust and privacy. Fongen (2012), proposed a framework for supporting trust requirements in IoT environment. The framework provides proper authentication, integrity, and services protection. Jara et al. (2011), introduced a trust extension protocol for providing many services under IP-based WSNs such as connectivity, secure mobility and dependability.Evans and Eyers (2012), suggested controlling the flow of information to preserve properties of data privacy in IoT. This technique achieved data control via trusted computing based on privacy policies.

4.4.3 Data transmission and networks trust

Data transmission and networks trust are crucial element for the stability of IoT applications. Whereas, trustworthy communication and networking protocols must support the heterogeneity and scalability of IoT. Isa et al. (2012), a proposed protocol for securing the transfer of the bulk of data in IoT environments, enhanced with security framework to support trust and privacy. Raza, Wallgren, and Voigt (2013), introduced an IDS for IoT. This system showed good efficiency and less overhead when evaluated against various attack models such as selective forwarding and spoofing. Heer et al. (2011), identified the requirements and challenges for IP-based solutions. The study stated that to securing IoT, the architecture of security in IoT must fit the life-cycle of the entire transactions.

4.4.4 User trust

The concept of user trust concern with the behaviors of devices owners and users, the issue is to limit the interactions to only trusted owners and users to sustain IoT services. Køien (2011), investigated a different aspect of trust some component of IoT such as device, hardware, software, and services. This investigation carried out in term of psychological reflexivity and transitivity, risk management, dishonesty, suspicion, social relation, the human brain, and reputation. The study stated that IoT components could not be fully trusted. However, human should not distrust IoT services at all. Moreover, the study suggested using a trusted proxy and applying devices manufactured by trusted companies. Ding, Zhou, Cheng, and Lin (2013), utilized differential game in building secure communication model, which observes and evaluates user behaviors in IoT environment. That is in the presence of interaction among malicious and selfish entities. Their model wisely exploits network resources to perform secure packet forwarding and studied vulnerabilities impact on the performance. Their results showed that their model could detect malicious behavior with high probability.

4.4.5 Software applications trust

Recently, many software applications of IoT developed for supporting daily life in various aspects. The success and sustainability of these applications maintained through considering some methods that can assist in fulfilling partial trust management objectives. The methods such as commodity integrity detection algorithm, privacy preservation in smart-meter, and multi-party computation-based methods.

- **Privacy preservation in smart-meter:** this technique based on load management system, which utilizes primitives of homomorphic encryption for secure multi-party computation (Thoma, Cui, & Franchetti, 2012). The system preserves the details of user data in smart grid control and management via applying verification process.
- **Multi-party computation-based techniques:** Provides secure search service in an audio database such as music matching and considering privacy issues. Many studies discussed the tradeoff between computational complexity and privacy in audio/video matching application.

4.5 Trust metrics

Trust metrics aim to identify standards or patterns for evaluating and measuring services and values in IoT systems. The successful trust management systems rely on accurate measures and suitable trust metrics that help in monitoring the interactive services and the level of relationship between IoT entities. Trust measurements can be device-dependent or application-dependent, according to design objectives of a proposed scheme (Cho et al.,

2011). In the literature many studies form trust metric based on trust properties (Ray Chen, Guo, et al., 2016; Mendoza & Kleinschmidt, 2015; Namal, Gamaarachchi, MyoungLee, & Um, 2015). Trust metrics build based on either social properties or QoS properties (Bao, Chen, Chang, & Cho, 2012).

4.5.1 Social trust metrics

The concept of social trust indicates the attributes that used for measuring the relationships between IoT entities; the term derived from the social networks. For instance, Intimacy used as trust metric for measuring the closeness based on the observations, honesty as metric for measuring anomaly behavior during the interaction.

4.5.2 QoS trust metrics

The concept of QoS trust derived from the computer systems and networks. In QoS trust, for example, energy consumption used as metrics for measuring the competence, unselfishness used for measuring the cooperativeness.

4.6 Trust computation schemes

Trust computation is the processes that encompass techniques for extracting trustworthiness information regarding IoT entities. Trust computation schemes categorized into "trust composition, trust propagation, trust aggregation, trust update, and trust formation" (Guo et al., 2017).

4.6.1 Trust composition

The term trust composition introduced by Guo and Chen (2015), it indicates the components (trust-properties) that considered in trust computation processes. Trust components fall either under an asocial trust or QoS trust.

- **Social trust:** one of the significant factors in successful social relationships and interactions between owners of IoT entities (Ray Chen, Guo, et al., 2016). The measures of social trust are honesty, connectivity, unselfishness, and intimacy.
- **QoS trust**: indicate the belief that an IoT entity can provide services in the quality as agreed or requested by the peer (D. Chen et al., 2011). For instance, QoS in routing service measured by some factors as energy-consumption, packet-forwarding, and packet-delivery ratio.

4.6.2 Trust propagation

Trust propagation concern on the style of exchanging trustworthiness information among IoT entities. In the literature, trust propagation categorized in one of two schemes, either centralized or distributed (Guo & Chen, 2015).

- **Decentralized trust propagation**: In In this scheme, IoT entity propagates trust evidence autonomously to it is partners among IoT entities, directly without employing centralized entity as illustrated in Figure 5.
- **Centralised trust propagation:** In this scheme, the reliable centralized entity (IoT device or cloud server) is required to maintain trust information (Nitti et al., 2014). The centralized entity maintains a data structure to store trust's feedback. Moreover, the centralized entity replies to the requests come from IoT entities regards trust information as shown in figure 6. Saied, Olivereau, Zeghlache, and Laurent (2013), introduced centralized trust manager to manage and store trust information.

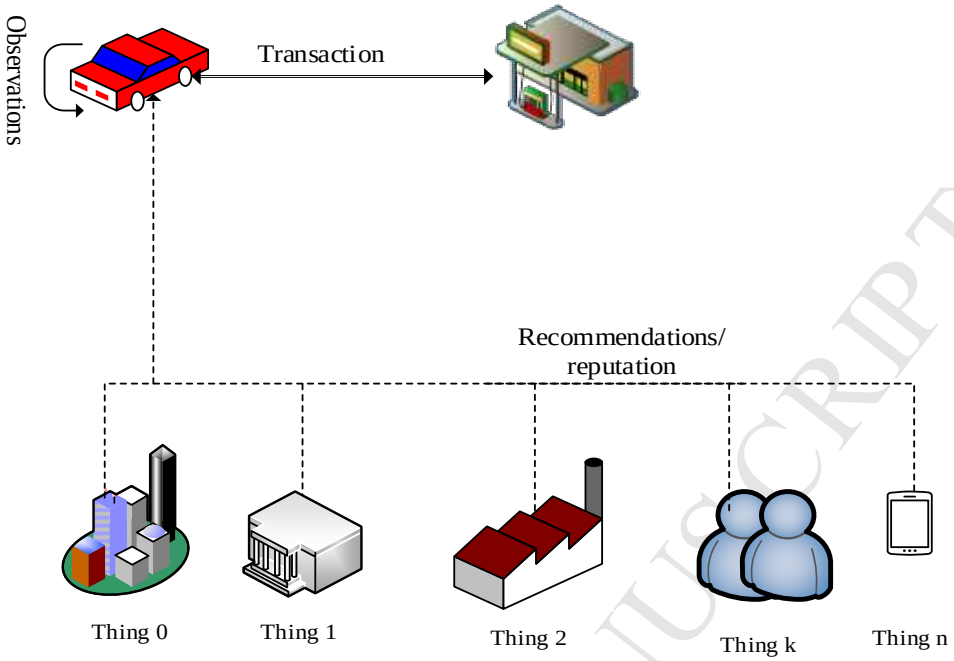

Figure 5. Decentralized trust propagation

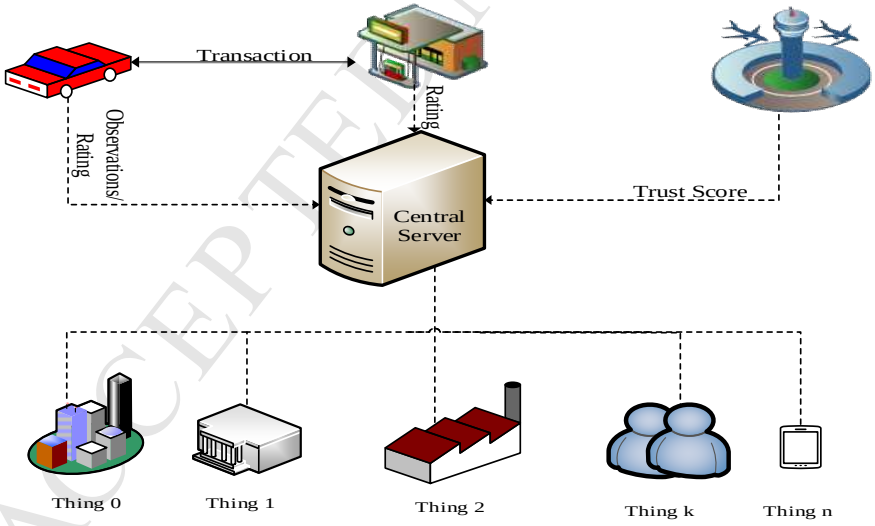

Figure 6. Centralized trust propagation

4.6.3 Trust aggregation

Trust aggregation concerns on an aggregation of trust information (observations and recommendation), through either self-experience or peers recommendations. In the

literature, many trust aggregation techniques investigated (Jøsang et al., 2007). The major categories include weighted sum, inference approaches, and regression analysis.

- **Weighted sum:** is a common evidence aggregation technique. The transactions that have a higher aggregated-weight will have more consideration. The weighted sum use for aggregating direct/ self-observations trust and recommendation /indirect trust (Nitti et al., 2014). The weight of a recommenders feedback called trust credit (Martinez-Julia & Skarmeta, 2013)
- **Inference approaches:** some trust aggregation techniques use inference approaches such as Fuzzy Logic, Bayesian Inference, and Dempster–Shafer theory (Belief Theory).Fuzzy Logic deals with uncertainty where the reasoning is approximate rather than exact, fuzzy variable value falls in the range 0 to 1. The degree of uncertainty managed by a suitable membership function. The linguistic variables used, in such cases, the specific membership function is needed to manage the degrees in the range. Trust considered as a measure of fuzziness with membership-functions to describe trust degree (Zhao & Li, 2013). Fuzzy logic have reasoning rules with fuzzy measures. Bayesian-inference allows the probability distribution for dealing with trust variables, where it updates the model parameters in case of new observations.

Commerce, Jøsang, and Ismail (2002), introduced reputations system composed of trust random variable value, between [0-1], using beta distribution for Bayesian inference. Belief Theory provide reasoning with uncertainty; it has well-defined interfaces to other theories and frameworks such as probability and possibility. Jøsang (2001), maintained opinion metric to represent subjective beliefs, where it utilized by the subjective logic.

- **Regression analysis** is statistic technique that measures the relationships among statistical variables. It can be utilized for relationships estimations between trust and the variables that represent entities behaviors (Yating Wang et al., 2014).

4.6.4 Trust update

Trust update is the process of involving new observations and recommendations into trust credit. Trust update follows either event-driven approach or time-driven approach (Guo & Chen, 2015).

- **Event-driven:** this approach, updates trust data after a transaction or event occurrence. In another word, after service rendering. Consequently, feedback regarding service quality is received either in each participating entity or in IoT cloud-server. In some environments the recommendations send upon request, where entities collaborate with each other in exchanging a recommendation about other entities behaviors,(Ray Chen, Bao, Chang, & Cho, 2010; Ray Chen et al., 2014).
- **Time-driven:** in this approach, the collection of trust evidence (self-observations and recommendations) performs periodically. In some time no evidence can be found, Therefore, trust decay over time most important because recent information is more trustworthy than old ones. The exponential decay-function is suitable for a specific application's needs (R. Chen et al., 2010; Ray Chen et al., 2014).

4.6.5 Trust formation

The term trust formation introduced by (Guo & Chen, 2015) to represent the way of computing the overall-trust. In the literature, trust formation found in either multi-trust form or single-trust form.

- **Single-trust:** in this scheme, just one trust metric considered in a trust protocol. For instance, QoS considered as the most critical metric in social IoT (Ray Chen, Guo, et al.,

2016). Thus, the evaluation of an IoT device relay on its effectiveness in showing QoS in response to requests.

- **Multi-trust:** This scheme, follows the common belief that trust is multi-issues. Therefore, this scheme followed multiple-metrics during trust formation. (Ray Chen & Guo, 2014) considered intimacy, competence, honesty, and unselfishness, in the evaluation of overall trust of an IoT device.

There are several mathematical methods used for computing single-trust and multi-trust formation such as identifying thresholds for weighted sum, and Trust-scaled-by-confidence:

- **Trust metrics with thresholds:** This method uses independent trust metrics with defining a minimum threshold for each these metric; that is depending on the context requirements. For instance, honesty is critical. Therefore, its threshold stetted to highest level. However, intimacy is not critical, so lower threshold applied on it.
- **Weighted sum**: this method combines independent trust metrics together to form overall-trust metric. The assigned weight is needed to represent the application requirements; When, the honesty is critical that it should have a higher weight. Moreover, the assigned weight can be readjusted in dynamic way to reflect the context/environment status. In malicious environments, honesty weight is higher, to overcome reputation attacks (e.g. ballot-stuffing and bad-mouthing). On the other direction, if the environment is friendly and safe such as research lab, the competence has more importance than honesty, thus the competence metric given the higher weight. (Ray Chen, Guo, et al., 2016), introduced weights readjustment for indirect and direct trust, the aim to maximize users satisfaction through the recent interval. Saied et al. (2013), introduced a dynamic change of a weight associated with positive recommendations during the process of deriving overall-trust credit. (Liu, Chen, Xia, Lv, & Bu, 2010) used the weight of penalty coefficient with the history for updating trust information.
- **Trust-scaled-by-confidence:** this method scales the most important trust metrics with lower ones, which considered as confidence. (Yating Wang, Chen, Cho, Chan, & Swami, 2013), selected two trust metrics: integrity and competence for rating an entity with competence-metrics being most important trust metric. Two scaling scheme had been considered: (a) competence-metric adjusts to zero if integrity-metric dropped under the threshold; (b) competence-metric scale either to 0 or 1, (1 represent the maximum, 0 represent minimum), that based on the level of integrity-metric, upper or under trust-threshold.

4.7 Trust attacks

Robust TR systems are essential for sustaining functionality of IoT applications. However, several types of attacks compromise TR systems themselves. Trust attacks performed by malicious entities, which behave either in non-honest form or non-cooperation form (Koutrouli & Tsalgatidou, 2012). Trust attacks categorized into a biased recommendation, inconsistent behaviors, and identity attacks as illustrated in, Figure 7. This section explores the kind attacks against TR systems and respectively defense mechanisms in IoT environment.

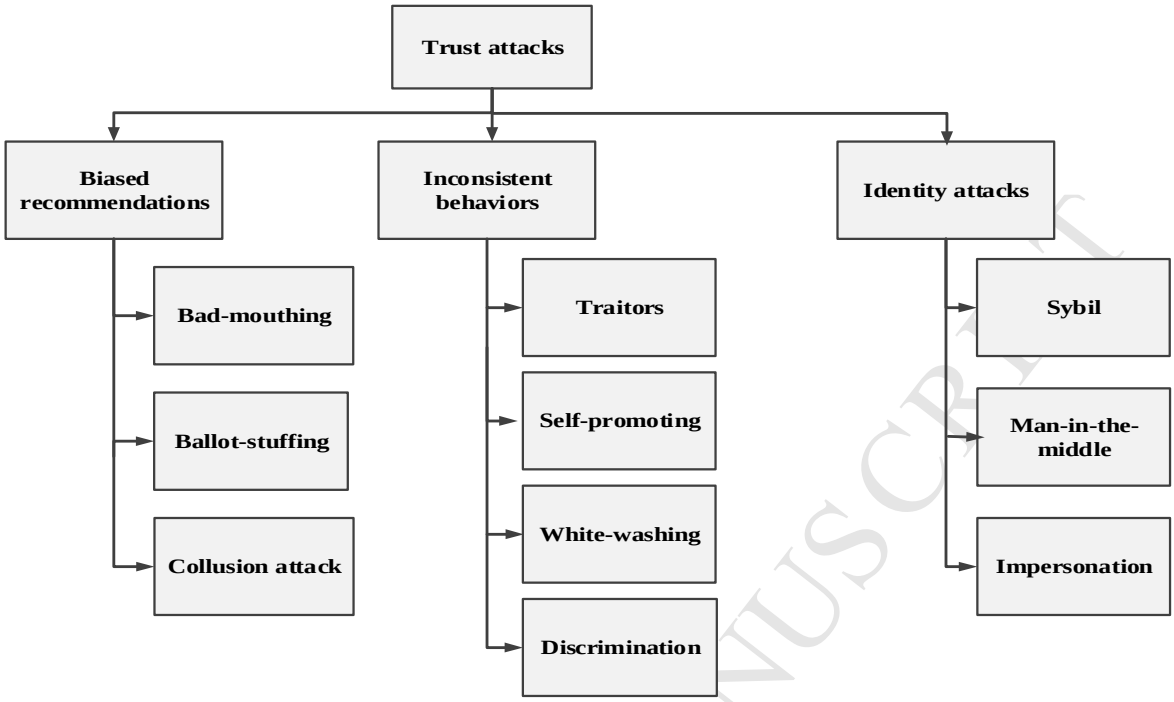

Figure 7. Taxonomy of trust attacks

4.7.1 Biased recommendations

This category of attacks targets the trust-based system via giving un-real recommendations regarding the transactional situation. Biased recommendation attacks, occurs mainly when the recommender is malicious, self-interested or having imperfect information. The attack can be performed by an individual entity or through the collusion of a group of IoT entities. There are several types of attacks categorized under biased recommendations attacks, namely ballot-stuffing, self-promoting, and bad-mouthing as depicted in Table 3. and discussed as follows:

- **Bad-mouthing attacks:** In this type of attacks, malicious entities collude in fabricating fake negative recommendations about a well-behaving entity in IoT environment. These fabricated fake recommendations aim to ruin the reputation of the target entity. As a result, the system isolates the victim entity or decreases its opportunity of being chosen as a service-provider (Banković, Vallejo, Fraga, & Moya, 2011). The malicious entities remain to provide appropriate recommendations for the other entities. Therefore, it appears as unbiased recommender in front of the other entities (Koutrouli & Tsalgatidou, 2012).

Table 3.Biased Recommendations attacks and the defence mechanism.

Attack Name	Defence Mechanisms	
	Recommendation content based	Recommendation selection based

Bad-mouthing	• Hiding entities recommendation from each other via cryptography mechanism (Jurca & Faltings, 2003). • Incorporating uncertainty and lack of information in opinion based recommendation (Can & Bhargava, 2013; Sabater & Sierra, 2002). • Enticements of honest recommendation (Fernandes, Kotsovinos, Östring, & Dragovic, 2004; Papaioannou & Stamoulis, 2006).	• Estimating recommendation reputation (Dillon, Chang, & Hussain, 2004; Patel, Teacy, Jennings, & Luck, 2005; Xiong & Liu, 2004) • Filtering technique (Dellarocas, 2000b; Grolimund, Meisser, Schmid, & Wattenhofer, 2006). • Estimating confidence for the recommendation (Can & Bhargava, 2013; Sun, Han, Yu, & Liu, 2006). • Controlled anonymity (Dellarocas, 2000b). • Threshold witnessing(Carbunar & Sion, 2006).
Ballot-stuffing	• Tying recommendations with corresponding transaction(Singh & Liu, 2003; Srivatsa, Xiong, & Liu, 2005) .	• Difficult to change identities(Douceur, 2002; Resnick, 2001).
Collusion attack	• Hiding entities recommendation from each other via cryptography mechanism (Jurca & Faltings, 2003). • Transaction costs (Bhattacharjee & Goel, 2005).	• Checking social relationship between recommenders(Sabater & Sierra, 2002). • Controlled anonymity (Dellarocas, 2000b). • Use of pre-trusted entities (Kamvar, Schlosser, & Garcia-Molina, 2003). • Sending recommendations always to the same group of entities, (Grolimund et al., 2006). • Filtering/clustering techniques to identify colluders (Dellarocas, 2000b).

- **Ballot-stuffing attacks:** In this type of attacks, the attackers collude and coordinate to increase the reputation of their friend entity by giving fabricated fake positive-recommendations. Consequently, increasing its probability for being chosen as a service-provider. this type of attacks avoided by selecting honesty as a metric in overall-trust formation phase (Ray Chen, Bao, et al., 2016).
- **Collusion attack** is a scenario of biased recommendation, where a group of malicious entities collaborates and coordinates together for illegally performing biased recommendation attacks. The malicious entities illegally increase their reputations or decrease the reputation of another entity(Abdul-Rahman, 2005). The colluding entity modifies the reputation of another entity based on either ballot-stuffing attack or bad-mouthing attack.

4.7.2 Inconsistent behaviours

In In this category of attacks, a peer tries to obtain illegal positive reputation through performing the inconsistent behavior. The inconsistent behavior attackers can come in two forms: (1) Transactional behaviors; and (2) Recommendation behaviors. Attacks types fall under t inconsistent behaviors are traitor, self-promoting, white-washing and discrimination, have been compared in Table 4.

- **Traitor/ On-off attacks:** In traitor's attacks, a malicious entity builds a high positive reputation at the beginning through behave correctly, consequently become one of the trusted entities, then start spuriousness behaviors (S. Chen, Zhang, Liu, & Feng, 2010). When the reputation gets down to a specific threshold, the malicious entity changes to perform honestly and accurately. The traitor repeats the process as mentioned above cyclically. Fast trust update mechanism can help TR system in detecting traitor's entities.
- **Self-promoting attacks:** in primary form of self-promoting, the malicious entity modifies its trust-value during recommendations propagation or fabricates positive-feedback about itself. Malicious entity exploits vulnerabilities in authentication and data integrity in IoT environment. Self-promotion threat will exist if there is the possibility of acquiring multiple identities by a single physical identity, e.g. via a Sybil attack(Douceur, 2002). The self-promoting attack avoided by considering short history, preventing the entities from switching its identities and avoiding Sybil attacks(Koutrouli & Tsalgatidou, 2012).
- **White-washing attacks**: White-washing attacks also known as a self-serving attack(Lai, Feldman, Stoica, & Chuang, 2003). It performs inconsistent behaviors based on the identity-related breach. Where, the malicious entity exit and rejoining IoT environment again to wash its bad reputations. That is occurs when the trust-value assigned with newly login is higher than its current-trust value. Some malicious entity discards its identity and rejoins using new identity periodically, such case known as pseudospoofing. Pseudospoofer prevented by avoiding Sybil attack(Marti & Garcia-Molina, 2006).
- **Discriminatory attack:** In this type of trust attacks, an entity provides high QoS to a group of entities and the same services with lower quality to other groups(Jøsang & Golbeck, 2009). This discrimination follows one of two forms, i.e. positive or negative(Dellarocas, 2000a; Jackson, 1996). In the negative discrimination form, an entity provides high-quality services to all the entities except specific entities that it is not like to serve properly. In the positive discrimination form, an entity provides exceptionally high quality of service to a limited number of selected entities and the average QoS to the rest of the entities. Discrimination different from biased recommendation since rates are providing fair/real/ actual ratings about the entities. (Dellarocas, 2000a), proposed controlled anonymity and the cluster filtering approach as a solution for avoiding discrimination.

Table 4. Inconsistent behaviours attacks and defence mechanism

Attack Name	Defence Mechanisms	
	Recommendation content based	**Recommendation selection based**
Traitors	N/A	N/A
Self-promoting	- Hiding entities recommendation from each other via cryptography mechanism (Jurca & Faltings, 2003) - Incorporating uncertainty and lack of information in opinion based recommendation (Can & Bhargava, 2013; Sabater & Sierra, 2002) - Enticements of honest recommendation (Fernandes et al., 2004; Papaioannou & Stamoulis, 2006)	- Estimating recommendation reputation(Dillon et al., 2004) -Filtering techniques (Dellarocas, 2000b; Grolimund et al., 2006) - Estimating confidence for the recommendation(Sun et al., 2006) - Controlled anonymity (Dellarocas, 2000b) - Threshold witnessing(Carbunar & Sion, 2006)
White-washing	-Self recommendation with reputation transfer (Seigneur, Gray, & Jensen, 2005)	- Difficult to change identities (Douceur, 2002; Resnick et al., 2000) - Exploring graph characteristic of P2P systems (Cheng & Friedman, 2005; Haifeng Yu, Kaminsky, Gibbons, & Flaxman, 2006)
Discrimination	N/A	- Filtering technique (Dellarocas, 2000b) , (Grolimund et al., 2006). - Controlled anonymity (Dellarocas, 2000b).

4.7.3 Identity-related attacks

Reputation and recommendation relay on the identity of an entity. Therefore, each entity should have exactly one unique identity. However, these identities could be associated with identities of the real world. Unfortunately, an entity can have one or multiple number of identities. In trust-based IoT environments, there are several types of attacks related to identity management as compared in Table 5. and discussed as follows.

- **Sybil attack:** The attacker is physical entity, which obtains multiple identities. That is through utilizing cheap or anonymous pseudonyms, to escape from the consequences of its malicious behavior (Resnick, 2001). In the literature, there are two approaches for dealing with this problem: centralized and de-centralized. A centralized paradigm has central-authority responsible for issuing and verifying the identity of every participating entity. The central-authority imposes more charges for commuting cost per every additional identity, to overcome Sybil attack(Bazzi & Konjevod, 2007). The decentralized approach binds an identifier, for instance, IP address with encryption public key (Douceur, 2002). Then, it employs network coordinator to detect the entity with multiple identities (Bazzi & Konjevod, 2007).

- **Man-in-the-middle attack:** The attacker intercepts the flow of specific service messages and replace them with non-preferable or bad-services (Mármol & Pérez, 2009). As a result, the reputation of that SP decrease. Furthermore, the malicious entity intercepts the recommendation given by an honest entity and modify it for its interest. The cryptographic authentication scheme is one of the solutions for avoiding this type of attacks.
- **Impersonation:** Attacks occurs in different forms such as device cloning, unauthorized access, address spoofing, replay and rogue access point (Barbeau, Hall, & Kranakis, 2006). The IoT device impersonated by reprogramming it with the physical-address of the victim-device. Then, this device behaves dishonestly, while acting as the original device (victim). Thus, the reputation of the original device could be affected.

Table 5. Identity Management-related attacks and defence mechanism

Attack Name	**Defence Mechanisms**	
	Recommendation content based	**Recommendation selection based**
Sybil attack	Self-recommendation with reputation transfer (Seigneur et al., 2005).	- Difficulty in changing identities (Douceur, 2002; Resnick, 2001). - Exploring graph characteristic of P2P systems(Cheng & Friedman, 2005; Haifeng Yu et al., 2006).
Man-in-the-middle	Cryptographic mechanisms for securing recommendations (Jurca & Faltings, 2003).	- Cryptographic mechanisms for securing for authenticating recommenders and mediators (Gutscher, 2007). - Estimating mediator credibility (Sherwood, Lee, & Bhattacharjee, 2006).
Impersonation	• Unique digital identity(Gupta, Judge, & Ammar, 2003).	• Unique digital identity(Gupta et al., 2003).

5 Recent Advances

This section critically present the recent advances of research effort (models, frameworks, and protocols) which directed at trust in IoT. The solutions described in Table 6a, Table 6b and discussed as follows:

Zhu, Rodrigues, Leung, and Lei Shu (2018), tried to improve the performance of Industrial IoT (IIoT), that is through improving trust-based communication in IIoT. The authors introduced three categories of trust-based communication: collaborative, independent and mutual sensor-cloud. The experiments results showed that their trust-based communication mechanism could massively boost the performance of sensor-cloud. However, they did not test the resistance of their mechanisms against trust attacks, which can hinder the entire trust-based IIoT.

Lin and Dong (2018), proposed trust model for Social IoT, depicting trust as a dynamic task. The authors clarified trust model features in five directions: mutuality of trust between service-provider (trustee) and service-requestor (trustor), inferential transfer, trust transitivity, an update of trustworthiness based on delegation results, and impact of dynamic environment on the trustworthiness. In this model, service-requestor and service-provider assess trustworthiness bilaterally. Therefore, the malicious requestor could not easily obtain any service, and the malicious service-provider could not easily involve in service-requestor tasks. The experiment's result showed considerable improvement in term of decreasing abuse rates and increasing success rates. However, their model has the overhead of bilateral computation of trust, in SP and service requestor sides, the impact of this overhead not evaluated, and the robustness not compared with the conventional trust-based models.

Al-Hamadi and Chen (2017), proposed decision-making protocol for trust-based IoT Health systems. In this system, knowledge base established to store the rates of the environment (particular place and specific time). This shared knowledge enables health IoT devices to decide for whether to visit or not visit the desired location. This decision made for health reason. The design of Trust-based health IoT protocol considered several factors such as reliability trust, risk classification, and probability of health problem as three factors for decision-making. The authors analyzed and compared the performance of their protocol with two baseline protocols; their protocol showed considerable improvement. However, social characteristics of device-to-device not considered for trust assessment.

Ray Chen, Bao, et al. (2016), introduced adaptive trust management protocol for social applications. The protocol follows distributed approach; each node adopts the event-driven way to updates trust towards others. Direct observation and indirect recommendations used in the update of trust evaluation. This protocol controls trust aggregation and propagation for the indirect recommendations and direct observation, that through two readjust-able coefficients so the protocol can cope up the dynamically changing environments, consequently boost the accuracy of trust assessment. The simulation result showed that this protocol performs service composition better than the random ways. However, statistical methods highly needed for enhancing trust convergence.

Hasan and Mouftah (2016), proposed a deployment strategy for trust-system in smart grid . The aimed to install trust system in a location that can enable it to serve as a firewall and intrusion detection system. For achieving these tasks the trust system monitor ingress and egress traffic. The proposed method built based on heuristic algorithm utilizes segmentation of minimum spanning tree to SCADA network segmentation in the smart grid. The experiment results show that the scheme provides better protection quality in the scenarios of topology-aware selection of a trusted node. Moreover, this scheme offers compatibility with cyber-security planning approaches such as the optimal deployment of trust systems, when the number of segments is unidentified. However, this trust system could get out-of-service for many reasons such as capacity problem, which lead to system failure.

Ray Chen, Guo, et al. (2016), proposed protocol for trust management in SOA-IoT environments. They used distributed collaborative-filtering for trust feedback selection from the entities, which share the same interest. Furthermore, they develop novel adaptive filtering to dynamically adjust the parameters of the protocol, that to avoid biased trust assessment and boosting application performance. The experiments result showed that the

adaptive IoT trust protocol performed better than Eigen Trust model and Peer Trust, the comparison carried out in hostile environment, where the malicious nodes performed false recommendation and opportunistic service attacks. However, the authors not tested their protocol against many types of attacks such as opportunistic collusion, random attacks.

Kokoris-Kogias et al. (2016), Introduced a hybrid TR model for social IoT(TRM-SIoT) based on the social scheme of COSMOS project. The authors combined the popular solution, which used on Peer-to-Peer and mobile ad-hoc networks, and utilized it in IoT. In TRM-SIoT an entity computes trust index of author entities based on its direct experiences. Moreover, the entity has capabilities deter its reputation either via consulting friend entities or via consulting the COSMOS Platform. The simulation results showed that TRM-SIoT could exclude the malicious nodes from the network, with lowest computation cost and high accuracy. Moreover, the adaptive nature of TRM-SIoT supports the possibility of reintegrating the excluded nodes. However, the probabilistic analysis should be considered with each of COSMOS services to determine the actual behavior of the entity that based on setting appropriate variables and thresholds.

Mendoza and Kleinschmidt (2015), proposed trust management model, in which the assessment of an entities trustworthiness conducted only using direct observations. The proposed model rewards the cooperating entity with a positive score and punishes the malicious entity with a negative score. The authors tested their model against On-Off attacks, the malicious behavior detected based on density of malicious entities, position of the entity, the traffic volume in the transmission range. The simulation results showed that the proposed model performed efficiently against On-Off attacks and considerable success in recognizing malicious nodes in the network. However, a neighbor recommendation not considered in trust assessments and the robustness of the model not tested against Ballot-stuffing and Bad-mouthing attacks.

Namal et al. (2015), proposed an automatic trust management framework. Aiming to align trust management with highly dynamic applications and services of cloud-based IoT. The framework adopted MAPE-K feedback to assess the level of trustworthiness. The author studied the framework extensively in term of capability, response time, reliability and availability in a heterogeneous cloud environment. The experiment results showed that the proposed framework consistent with trust computation level. However, this framework not tested against different types of trust attacks, which can hinder the applications and services cloud-based IoT systems.

Table 6(a). Description of recent solution for trust system in IoT

Research	Application	Computation Schemes					Metrics	Attacks Considered
		Composition	Propagation	Aggregation	Update	Formation		
Zhu et al. (2018)	Service Management	QoS	Distributed	Weighted sum	Event-driven	Single trust with trust threshold	-Throughput -Response time	N/A
Lin and Dong (2018)	Service Management	Social	Distributed	Weighted sum	Event-driven	Multi-trust	-Honesty	N/A
Al-Hamadi and Chen (2017)	Service Management	QoS	Centralized	Weighted sum	Event-driven	Multi-trust	-Reliability -Risk classification -Loss of path	-Bad-mouthing -Ballot-stuffing
Ray Chen, Bao, et al. (2016)	Security Mechanism	QoS	Distributed	Weighted sum	Event-driven	Multi-trust with weighted sum	-Honesty -Community of interest -Cooperative-ness	-Self promoting -Discrimination - White washing
Hasan and Mouftah (2016)	Service Management	QoS	Semi-centralized	Static Weighted sum	Event-driven	Single trust	-Size balancing -Geographic dispersion	N/A

Table.6(b). Description of recent solution for trust system in IoT

Research	Application	Computation Scheme					Metrics	Attacks Considered
		Composition	Propagation	Aggregation	Update	Formation		
Ray Chen, Guo, et al. (2016)	Service management	Social	Distributed	Bayesian systems	Event-driven	Single trust	- Intimacy - Closeness - Community of interest	-Bad-mouthing -Ballot-stuffing
Kokoris-Kogias et al. (2016)	Service management	Social	Hybrid	weighted sum	Event-driven	Single trust	- Response time - Reliability - Availability	-Discrimination -Collection -Inconsistent behavior
Mendoza and Kleinschmidt (2015)	Security mechanism	QoS	Distributed	weighted sum	Event-driven	Single trust	Cooperativeness	On-Off/terroirs
Namal et al. (2015)	Service management	QoS	Centralized	weighted sum	Time-driven	Single trust	- Availability, - Reliability; - Response time - Capacity	N/A
Saied et al. (2013)	Security mechanism	QoS	Centralized	weighted sum	Event-driven	Single trust	- Cooperativeness	-Ballot-stuffing -Bad-mouthing -Self-promotion

Saied et al. (2013), introduced trust system considering several IoT requirements. The authors considered the experience in assessment of function trustworthiness. The model specifies trust scores dynamically to IoT entities according to different contexts and

different functions. The design of the proposed model enables it to carefully judge the level of confidence on the node and report that to another node. The system assign scores to the recommender, based on the accuracy and trustworthiness of its recommendations. Rating of the node adjusts after each transaction during the learning stage. The simulation results showed that the proposed model has considerable performance improvements in trust management. However, the model not tested against several types of trust attacks such as opportunistic service and On-off attacks.

6 Challenges and future research directions

This section discusses the challenges and future directions of TR in the IoT environments. The aim is to provide research directions for helping the researchers in further investigations and improvements of trust models, protocols and frameworks. Among the seven factors, which we discuss in our thematic taxonomy of TR in IoT, we found that the challenges are related to trust computation schemes and trust attacks, the remaining factors describe trust-based IoT systems. Trust-computation-related challenges and attack-related challenges discussed as follows:

6.1 Trust computation challenges

Trust computation challenges interleaved with the processing of composition, propagation, aggregation, update and formation.

6.1.1 Trust Composition

One of the most crucial tasks for TR systems in trust-based IoT environment is the selection and composition of trust metrics, in addition to that the generation of honest and accurate recommendation based on trust metric used by the recommendation requestors. In the real-life, IoT devices belonged to a human being owner and connected via a social network of its owners. Therefore, the majority of recent trust-based IoT applications are social oriented as depicted in table .5. Mostly the composition of trust metrics involves social metrics to assist in assessing the trustworthiness of IoT devices that is because friendships deserve high weight in their recommendation because of social similarity and interest. However, associativity between social relation and the quality of recommendations need further investigations to boost trust computation in term of accuracy and resiliency of against trust attacks.

6.1.2 Trust propagation

In Trust-based IoT system, the distributed paradigm widely used for trust propagation. Distributed trust propagation is suitable for IoT environment, where the environment is dynamic and smart devices are highly mobile. It is a solution when there is no accessibility of central entity as cloud servers. However, data filtering and search problem remain as a challenge for distributed data propagation in IoT. Since not possible for every IoT device to deal with a massive stream of information. The usability of these entities proportionate to its ability to search on and filter the vast stream of trust data and find the requested trust recommendation and then propagate it (Malaga, 2001).

Recently, centralized trust propagation associated with cloud-based TR system. Nitti et al. (2014), Implemented centralized TR system using hash table structure. (Namal et al., 2015; J. P. Wang, Bin, Yu, & Niu, 2013) defined central trust entity and advice for further investigation on central trust propagation paradigms. The significant challenge for cloud-based central trust propagation is the design of infrastructure design that can enable propagation of trust

information between IoT devices and cloud server. Where cloud server aggregate trust feedbacks and reply to queries of IoT entities regarding services quality and trustworthiness of other entities in the IoT environment.

6.1.3 Trust aggregation:

In the literature, many trust aggregation solution has been explored, for instance, static weighted sum, Bayesian inference, fuzzy logic and dynamically weighted sum. However, regression analysis and belief theory not investigated. In the literature, no comparative study for analyzing and evaluation trust aggregation algorithms in IoT environments. Since the aggregation approach concern on the collection of trust evidence through self-observations and peers recommendations. The implementation of trust evidence aggregation faces different inherited challenges such as value imbalance problem and categorizations, detailed as follows:

- **Value imbalance problem:** this problem happens when the reputation system gives the recommendations equal weight regardless of the transaction size. This problem makes the system subject to trust attacks where an entity can exploit this opportunity by building a good trust score through performing a limited number of small transactions honestly, and then use that trust score for performing maliciously sensitive and valuable transactions (Carbunar & Sion, 2006).
- **Categorizations:** reputation and trust score is a general concept in many environments. However, there is a lack of ability to use trust score in various categories. Categorizations of reputation could boost the systems through giving proper granularity, for instance, an entity may have appropriate trust credit in one aspect (e.g. honesty) and low credit regarding another aspect (e.g. competence). Categorizations concept should be utilized in conjunction with filtering during the search.

6.1.4 Trust update:

In Event-driven approach, trust status update performed after every service or transaction completion. Event-driven is more suitable for centralized system and cloud-based propagation scheme. In the time-driven method, the update happened periodically to meet system constraints such as computation capability, network bandwidth and energy consumption. Time-driven is appropriate for distributed trust propagation system, where the system must tradeoff between energy consumption and trust accuracy. The tuning of update interval is a crucial factor in preserving the optimum level of trust accuracy, consequently maximizing the performance of IoT application, this assumption not well investigated. The primary challenge is time sensitivity for trust-updates, the time differences between performing instances of a transaction have an impact on the trust score. As a result, malicious entities can exploit the vulnerability of time difference and carry out a large number of services in low-quality before the update of the trust score (Kerr & Cohen, 2006).

6.1.5 Trust formation:

In the literature, single-trust formation with weighted-sum is widely followed in trust-based IoT system. Multi-trust formation approach considers multiple trust metrics or proprieties, each of which being evaluated individually, the overall trust score calculated from all the multiple metrics. In IoT, device-to-device communication and behavior take place on behalf of the owners of the devices. The behavior and communication paradigm considers the social relationships of these devices owners. Therefore, social trust metrics

and properties must be taken into account besides the QoS during trust computation.(Bao & Chen, 2012; Ray Chen, Bao, et al., 2016), followed multi-trust, the challenge for multi-trust formation model is to cope up with both social orientation and QoS, targeting performance maximization of IoT applications.

6.2 Attacks-related Challenges

In IoT environments, TR concepts are applicable for SOA-IoT and Social-IoT systems. Since IoT devices owned by the human being so that it could perform malicious activities for its owner interest. TR systems work as complementary subsystem aiming to boost security mechanism and preserving high QoS. Trust attacks disrupt TR sub-system; as a result, trust-based IoT applications will be hindered. Therefore, defending trust-based IoT system against trust attacks is a crucial and challenging task. The following sub-sections discuss each category of trust attacks and its associated challenges.

6.2.1 Biased recommendation attacks

Accurate and representative recommendations are crucial factors in the success of computation and judgments in TR system. The challenge is not only accuracy of computation process, but also malicious devices try to cheat the system by generating a biased recommendation (negative or positive, illegally). In ballot-stuffing, the fake positive recommendation assist another malicious entity, a friend of the recommendation generator, for being chosen as a service-provider. In bad-mouthing, the false negative recommendation aims to abuse the competing entities, so its opportunity of being chosen as a service-provider will be reduced. In some circumstances, the generation of fake negative recommendation is a hard decision for a malicious entity that is because of possible penalties. However, anonymity allows the malicious entities to escape from the punishment. The correlation between the requestee and requester recommendation indicates that there is a level of interchange of positive recommendations between entities and revenge for negative recommendations as well (Resnick & Zeckhauser, 2002).

6.2.2 Inconsistent behaviors

Inconsistency attack happens in several form such as self-promoting or white-washing attacks. In self-promotion attacks, the attacker exploits the weaknesses during trust aggregation phases that is to illegally increase its reputation score. Some attacker modifies its reputation through the propagation phase or fabricates positive recommendation about itself. The challenge is solving the lack of data authentication and integrity, which make the system unable to discern between the legitimate and fabricated recommendations. In white-washing attacks, the attacker abuse the competitors for a short-term to degrade their trust score then get off and re-enter using a new identity to escape from the penalties and fresh its reputation (Lai et al., 2003). This type of attacks enabled by cheap pseudonyms, some systems restrict the use of multiple identities but fail to reduce the reputation score of the malicious entities to its correct level and apply punishments (Hoffman et al., 2009)

6.2.3 Identity-related attacks

Inexpensive identities became a serious challenge since it affects security and performance of trust-based IoT. As an entity can create new identities at a cheap cost, the presence of multiple identities cause many problems, for example, Sybil attack and churn attacks. Treating newcomers by disallowing anonymity is not a practical/desirable solution in a wide

range of transactions. One of the promising solutions is applying entry fees with use of standard encryption techniques, during the interactions (Resnick & Zeckhauser, 2002). Several issues raised in such case, for instance considering the newly joining entity as a neutral in term of reputation. That makes the newcomers struggling at the early stages to reach a sufficient reputation for enabling them to participate as trustee or service-provider. The solution is to incorporate trust system and social networks; where considering the location and social factors of the newcomers can help in the inference of some trust properties. That helps in achieving proper initialization of trust in bootstrapping stage (Golbeck & Hendler, 2004). Some systems give low weight to a negative recommendation that comes from the newcomer and increases the weight of that come from the old entities, that to keep the consistency of the reputation difference. This approach can lead to gradual changes in the importance of the newest recommendations (Malaga, 2001).

7 Conclusion

Trust is an important concept in the Internet of Things, for making a decision regarding the misbehaving devices. The task of trust management becomes challenging issue because the number of devices in IoT is highly scalable and the environment is rapidly changing. This survey introduced several taxonomies, presented comprehensive tutorial and investigated the literature of TR systems. This study discussed in details trust properties and the level of trust management followed by trust computation schemes. Moreover, the survey presented potential attacks on TR systems, Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015beside that we highlighted defense mechanism. We concluded the survey with challenging issues in Trust-based IoT systems.

References:

Abdul-Rahman, A. (2005). *A framework for decentralised trust reasoning.* University of London,

Ahmed, A. I. A., Khan, S., Gani, A., Ab Hamid, S. H., & Guizani, M. (2018). *Entropy-based Fuzzy AHP Model for Trustworthy Service Provider Selection in Internet of Things.* Paper presented at the 2018 IEEE 43rd Conference on Local Computer Networks (LCN).

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

Al-Hamadi, H., & Chen, R. (2017). Trust-based decision making for health IoT systems. *IEEE Internet of Things Journal, 4*(5), 1408-1419.

Atzori, L., Iera, A., & Morabito, G. (2011). Siot: Giving a social structure to the internet of things. *IEEE communications letters, 15*(11), 1193-1195.

Azer, M. A., El-Kassas, S. M., Hassan, A. W. F., & El-Soudani, M. S. (2008). *A survey on trust and reputation schemes in ad hoc networks.* Paper presented at the Availability, Reliability and Security, 2008. ARES 08. Third International Conference on.

Baier, A. (1986). Trust and antitrust. *ethics, 96*(2), 231-260.

Bamberger, W. (2010). Interpersonal trust–attempt of a definition. *Scientific Report, Technical University Munich*.

Banković, Z., Vallejo, J. C., Fraga, D., & Moya, J. M. (2011). Detecting bad-mouthing attacks on reputation systems using self-organizing maps. In *Computational Intelligence in Security for Information Systems* (pp. 9-16): Springer.

Bao, F., & Chen, I.-R. (2012). *Dynamic trust management for internet of things applications.* Paper presented at the Proceedings of the 2012 international workshop on Self-aware internet of things.

Bao, F., Chen, R., Chang, M., & Cho, J.-H. (2011). *Trust-based intrusion detection in wireless sensor networks.* Paper presented at the Communications (ICC), 2011 IEEE International Conference on.

Bao, F., Chen, R., Chang, M., & Cho, J.-H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE transactions on network and service management, 9*(2), 169-183.

Baras, J. S., & Jiang, T. (2005). *Managing trust in self-organized mobile ad hoc networks.* Paper presented at the Proc. 12th Annual Network and Distributed System Security Symposium Workshop.

Barbeau, M., Hall, J., & Kranakis, E. (2006). Detecting impersonation attacks in future wireless and mobile networks. In *Secure Mobile Ad-hoc Networks and Sensors* (pp. 80-95): Springer.

Bazzi, R. A., & Konjevod, G. (2007). On the establishment of distinct identities in overlay networks. *Distributed Computing, 19*(4), 267-287.

Beatty, P., Reay, I., Dick, S., & Miller, J. (2011). Consumer trust in e-commerce web sites: A meta-study. *ACM Computing Surveys (CSUR), 43*(3), 14.

Bhattacharjee, R., & Goel, A. (2005). *Avoiding ballot stuffing in ebay-like reputation systems.* Paper presented at the Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems.

Billhardt, H., Hermoso, R., Ossowski, S., & Centeno, R. (2007). *Trust-based service provider selection in open environments.* Paper presented at the Proceedings of the 2007 ACM symposium on Applied computing.

Blaze, M., Feigenbaum, J., & Lacy, J. (1996). *Decentralized trust management.* Paper presented at the Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on.

Blaze, M., Ioannidis, J., & Keromytis, A. D. (2003). *Experience with the keynote trust management system: Applications and future directions.* Paper presented at the International Conference on Trust Management.

Boukerche, A., & Ren, Y. (2008). A trust-based security system for ubiquitous and pervasive computing environments. *Computer Communications, 31*(18), 4343-4351.

Brenner, M. (2006). *Classifying ITIL processes; a taxonomy under tool support aspects.* Paper presented at the Business-Driven IT Management, 2006. BDIM'06. The First IEEE/IFIP International Workshop on.

Bui, N., & Zorzi, M. (2011). *Health care applications: a solution based on the internet of things.* Paper presented at the Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies.

Can, A. B., & Bhargava, B. (2013). Sort: A self-organizing trust model for peer-to-peer systems. *IEEE transactions on dependable and secure computing, 10*(1), 14-27.

Carbunar, B., & Sion, R. (2006). *Uncheatable reputation for distributed computation markets.* Paper presented at the International Conference on Financial Cryptography and Data Security.

Chang, K.-D., & Chen, J.-L. (2012). A survey of trust management in WSNs, internet of things and future internet. *KSII Transactions on Internet & Information Systems, 6*(1).

Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems, 8*(4), 1207-1228.

Chen, R., Bao, F., Chang, M., & Cho, J.-H. (2010). *Trust management for encounter-based routing in delay tolerant networks.* Paper presented at the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE.

Chen, R., Bao, F., Chang, M., & Cho, J.-H. (2014). Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Transactions on Parallel and Distributed Systems, 25*(5), 1200-1210.

Chen, R., Bao, F., & Guo, J. (2016). Trust-based service management for social internet of things systems. *IEEE transactions on dependable and secure computing, 13*(6), 684-696.

Chen, R., & Guo, J. (2014). *Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection.* Paper presented at the Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on.

Chen, R., Guo, J., & Bao, F. (2016). Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing, 9*(3), 482-495.

Chen, R., & Yeager, W. (2001). Poblano: A distributed trust model for peer-to-peer networks. Sun Microsystems, inc. White Paper. In.

Chen, S., Zhang, Y., Liu, P., & Feng, J. (2010). *Coping with traitor attacks in reputation models for wireless sensor networks.* Paper presented at the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE.

Cheng, A., & Friedman, E. (2005). *Sybilproof reputation mechanisms.* Paper presented at the Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems.

Cho, J.-H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials, 13*(4), 562-583.

Commerce, B. E., Jøsang, A., & Ismail, R. (2002). *The beta reputation system.* Paper presented at the In Proceedings of the 15th Bled Electronic Commerce Conference.

Consortium, W. W. W. (2004). Web Services Architecture, W3C Working Group Note 11 February 2004. *http://www. w3. org/TR/2004/NOTE-ws-arch-20040211/*.

Cook, K. (2001). *Trust in society*: Russell Sage Foundation.

Dellarocas, C. (2000a). *Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior.* Paper presented at the Proceedings of the 2nd ACM conference on Electronic commerce.

Dellarocas, C. (2000b). *Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems.* Paper presented at the Proceedings of the twenty first international conference on Information systems.

Dictionaries, O. (2014). Language matters. *URL: www. oxforddictionaries. com [Дата обращения: 01.02. 2016]*.

Dillon, T., Chang, E., & Hussain, F. (2004). Managing the dynamic nature of trust. *IEEE Intelligent Systems*.

Din, I. U., Guizani, M., Kim, B.-S., Hassan, S., & Khan, M. K. (2018). Trust management techniques for the Internet of Things: A survey. *IEEE Access, 7*, 29763-29787.

Ding, Y., Zhou, X.-w., Cheng, Z.-m., & Lin, F.-h. (2013). A security differential game model for sensor networks in context of the internet of things. *Wireless personal communications, 72*(1), 375-388.

Douceur, J. R. (2002). *The sybil attack.* Paper presented at the International workshop on peer-to-peer systems.

Evans, D., & Eyers, D. M. (2012). *Efficient data tagging for managing privacy in the internet of things.* Paper presented at the Green Computing and Communications (GreenCom), 2012 IEEE International Conference on.

Fernandes, A., Kotsovinos, E., Östring, S., & Dragovic, B. (2004). *Pinocchio: Incentives for honest participation in distributed trust management.* Paper presented at the International Conference on Trust Management.

Fongen, A. (2012). *Identity management and integrity protection in the internet of things.* Paper presented at the Emerging Security Technologies (EST), 2012 Third International Conference on.

Golbeck, J. (2008). Trust on the world wide web: a survey. *Foundations and Trends® in Web Science, 1*(2), 131-197.

Golbeck, J., & Hendler, J. (2004). *Accuracy of metrics for inferring trust and reputation in semantic web-based social networks.* Paper presented at the International Conference on Knowledge Engineering and Knowledge Management.

Grandison, T., & Sloman, M. (2000). A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials, 3*(4), 2-16.

Grolimund, D., Meisser, L., Schmid, S., & Wattenhofer, R. (2006). *Havelaar: A robust and efficient reputation system for active peer-to-peer systems.* Paper presented at the Proc. 1st Workshop on the Economics of Networked Systems (NetEcon).

Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., & Savio, D. (2010). Interacting with the soa-based internet of things: Discovery, query, selection, and on-demand provisioning of web services. *IEEE transactions on Services Computing, 3*(3), 223-235.

Guo, J., & Chen, R. (2015). *A classification of trust computation models for service-oriented internet of things systems.* Paper presented at the Services Computing (SCC), 2015 IEEE International Conference on.

Guo, J., Chen, R., & Tsai, J. J. (2017). A survey of trust computation models for service management in internet of things systems. *Computer Communications, 97*, 1-14.

Gupta, M., Judge, P., & Ammar, M. (2003). *A reputation system for peer-to-peer networks.* Paper presented at the Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video.

Gutscher, A. (2007). *A trust model for an open, decentralized reputation system.* Paper presented at the IFIP International Conference on Trust Management.

Harwood, W. (2012). *The logic of trust.* University of York,

Hasan, M. M., & Mouftah, H. T. (2016). Optimal trust system placement in smart grid SCADA networks. *IEEE Access, 4*, 2907-2919.

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications, 61*(3), 527-542.

Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A survey of attack and defense techniques for reputation systems. *ACM Computing Surveys (CSUR), 42*(1), 1.

Isa, M. A. M., Mohamed, N. N., Hashim, H., Adnan, S. F. S., Manan, J., & Mahmod, R. (2012). *A lightweight and secure TFTP protocol for smart environment.* Paper presented at the Computer Applications and Industrial Electronics (ISCAIE), 2012 IEEE Symposium on.

Jackson, R. L. (1996). A philosophical exploration of trust.

Jara, A. J., Marin, L., Skarmeta, A. F., Singh, D., Bakul, G., & Kim, D. (2011). *Mobility modeling and security validation of a mobility management scheme based on ECC for IP-Based Wireless Sensor Networks (6LoWPAN).* Paper presented at the Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on.

Javed, N., & Wolf, T. (2012). *Automated sensor verification using outlier detection in the internet of things.* Paper presented at the Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on.

Jøsang, A. (2001). A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9*(03), 279-311.

Jøsang, A., & Golbeck, J. (2009). *Challenges for robust trust and reputation systems.* Paper presented at the Proceedings of the 5th International Workshop on Security and Trust Management (SMT 2009), Saint Malo, France.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems, 43*(2), 618-644.

Jurca, R., & Faltings, B. (2003). *An incentive compatible reputation mechanism.* Paper presented at the E-Commerce, 2003. CEC 2003. IEEE International Conference on.

Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003). *The eigentrust algorithm for reputation management in p2p networks.* Paper presented at the Proceedings of the 12th international conference on World Wide Web.

Kerr, R., & Cohen, R. (2006). *Modeling trust using transactional, numerical units.* Paper presented at the Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services.

Khalid, O., Khan, S. U., Madani, S. A., Hayat, K., Khan, M. I., Min-Allah, N., . . . Chen, D. (2013). Comparative study of trust and reputation systems for wireless sensor networks. *Security and Communication Networks, 6*(6), 669-688.

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2019). Data and Privacy: Getting Consumers to Trust Products Enabled by the Internet of Things. *IEEE Consumer Electronics Magazine, 8*(2), 35-38.

Khoo, B. (2011). *RFID as an Enabler of the Internet of Things: Issues of Security and Privacy.* Paper presented at the Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing.

Køien, G. M. (2011). Reflections on trust in devices: an informal survey of human trust in an internet-of-things context. *Wireless Personal Communications, 61*(3), 495-510.

Kokoris-Kogias, E., Voutyras, O., & Varvarigou, T. (2016). *TRM-SIoT: A scalable hybrid trust & reputation model for the social Internet of Things.* Paper presented at the Emerging Technologies and Factory Automation (ETFA), 2016 IEEE 21st International Conference on.

Koutrouli, E., & Tsalgatidou, A. (2012). Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers. *Computer Science Review, 6*(2-3), 47-70.

Lai, K., Feldman, M., Stoica, I., & Chuang, J. (2003). *Incentives for cooperation in peer-to-peer networks.* Paper presented at the Workshop on economics of peer-to-peer systems.

Li, H., & Singhal, M. (2007). Trust management in distributed systems. *Computer, 40*(2).

Li, X., Lu, R., Liang, X., Shen, X., Chen, J., & Lin, X. (2011). Smart community: an internet of things application. *IEEE Communications Magazine, 49*(11).

Lin, Z., & Dong, L. (2018). Clarifying Trust in Social Internet of Things. *IEEE Transactions on Knowledge and Data Engineering, 30*(2), 234-248.

Liu, Y., Chen, Z., Xia, F., Lv, X., & Bu, F. (2010). *A trust model based on service classification in mobile services.* Paper presented at the Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing.

Malaga, R. A. (2001). Web-based reputation management systems: Problems and suggested solutions. *Electronic Commerce Research, 1*(4), 403-417.

Mármol, F. G., & Pérez, G. M. (2009). Security threats scenarios in trust and reputation models for distributed systems. *computers & security, 28*(7), 545-556.

Marti, S., & Garcia-Molina, H. (2006). Taxonomy of trust: Categorizing P2P reputation systems. *Computer Networks, 50*(4), 472-484.

Martinez-Julia, P., & Skarmeta, A. F. (2013). Beyond the separation of identifier and locator: Building an identity-based overlay network architecture for the Future Internet. *Computer Networks, 57*(10), 2280-2300.

Maurer, U. (1996). *Modelling a public-key infrastructure.* Paper presented at the European Symposium on Research in Computer Security.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review, 20*(3), 709-734.

Mendoza, C. V., & Kleinschmidt, J. H. (2015). Mitigating On-Off attacks in the Internet of Things using a distributed trust management scheme. *International Journal of Distributed Sensor Networks, 11*(11), 859731.

Miao, C., & Chen, L. (2010). *Trust-based dynamic access control policy for ubiquitous computing.* Paper presented at the Ubi-media Computing (U-Media), 2010 3rd IEEE International Conference on.

Momani, M., & Challa, S. (2010). Survey of trust models in different network domains. *arXiv preprint arXiv:1010.0168*.

Namal, S., Gamaarachchi, H., MyoungLee, G., & Um, T.-W. (2015). *Autonomic trust management in cloud-based and highly dynamic IoT applications.* Paper presented at the ITU Kaleidoscope: Trust in the Information Society (K-2015), 2015.

Nitti, M., Girau, R., & Atzori, L. (2014). Trustworthiness management in the social internet of things. *IEEE Transactions on knowledge and data engineering, 26*(5), 1253-1266.

Papaioannou, T. G., & Stamoulis, G. D. (2006). *Enforcing truthful-rating equilibria in electronic marketplaces.* Paper presented at the Distributed Computing Systems Workshops, 2006. ICDCS Workshops 2006. 26th IEEE International Conference on.

Patel, J., Teacy, W. L., Jennings, N. R., & Luck, M. (2005). *A probabilistic trust model for handling inaccurate reputation sources.* Paper presented at the International Conference on Trust Management.

Pujol, J. M., Sangüesa, R., & Delgado, J. (2002). *Extracting reputation in multi agent systems by means of social network topology.* Paper presented at the Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1.

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad hoc networks, 11*(8), 2661-2674.

Resnick, P. (2001). The social cost of cheap pseudonyms. *Journal of Economics & Management Strategy, 10*(2), 173-199.

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation systems. *Communications of the ACM, 43*(12), 45-48.

Resnick, P., & Zeckhauser, R. (2002). Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. In *The Economics of the Internet and E-commerce* (pp. 127-157): Emerald Group Publishing Limited.

Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things (IoT): An Overview–Understanding the Issues and Challenges of a More Connected World. *Internet Society*.

Sabater, J., & Sierra, C. (2002). *Reputation and social network analysis in multi-agent systems.* Paper presented at the Proceedings of the first international joint conference on Autonomous agents and multiagent systems: Part 1.

Saied, Y. B., Olivereau, A., Zeghlache, D., & Laurent, M. (2013). Trust management system design for the Internet of Things: A context-aware and multi-service approach. *Computers & Security, 39*, 351-365.

Seigneur, J.-M., Gray, A., & Jensen, C. D. (2005). *Trust transfer: Encouraging self-recommendations without sybil attack.* Paper presented at the International Conference on Trust Management.

Seligman, A. B. (1998). Trust and sociability. *American Journal of economics and sociology, 57*(4), 391-404.

Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys (CSUR), 45*(4), 47.

Sherwood, R., Lee, S., & Bhattacharjee, B. (2006). Cooperative peer groups in NICE. *Computer Networks, 50*(4), 523-544.

Sicari, S., Coen-Porisini, A., & Riggio, R. (2013). Dare: evaluating data accuracy using node reputation. *Computer Networks, 57*(15), 3098-3111.

Simpson, J. A. (2007). Psychological foundations of trust. *Current directions in psychological science, 16*(5), 264-268.

Singh, A., & Liu, L. (2003). *TrustMe: anonymous management of trust relationships in decentralized P2P systems.* Paper presented at the Peer-to-Peer Computing, 2003.(P2P 2003). Proceedings. Third International Conference on.

Srivatsa, M., Xiong, L., & Liu, L. (2005). *TrustGuard: countering vulnerabilities in reputation management for decentralized overlay networks.* Paper presented at the Proceedings of the 14th international conference on World Wide Web.

Sun, Y. L., Han, Z., Yu, W., & Liu, K. R. (2006). *A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks.* Paper presented at the INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings.

Suryanarayana, G., & Taylor, R. N. (2004). A survey of trust management and resource discovery technologies in peer-to-peer applications.

Tavakolifard, M., & Almeroth, K. C. (2012). A taxonomy to express open challenges in trust and reputation systems. *Journal of Communications, 7*(7), 538-551.

Terveen, L., & Hill, W. (2001). Beyond recommender systems: Helping people help each other. *HCI in the New Millennium, 1*(2001), 487-509.

Thoma, C., Cui, T., & Franchetti, F. (2012). *Secure multiparty computation based privacy preserving smart metering system.* Paper presented at the North American Power Symposium (NAPS), 2012.

Ukil, A., Sen, J., & Koilakonda, S. (2011). *Embedded security for Internet of Things.* Paper presented at the Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on.

Wang, J. P., Bin, S., Yu, Y., & Niu, X. X. (2013). *Distributed trust management mechanism for the internet of things.* Paper presented at the Applied Mechanics and Materials.

Wang, Y., Chen, R., Cho, J.-H., Chan, K. S., & Swami, A. (2013). *Trust-based service composition and binding for tactical networks with multiple objectives.* Paper presented at the Military Communications Conference, MILCOM 2013-2013 IEEE.

Wang, Y., Lu, Y.-C., Chen, I.-R., Cho, J.-H., Swami, A., & Lu, C.-T. (2014). *Logittrust: A logit regression-based trust model for mobile ad hoc networks.* Paper presented at the 6th ASE International Conference on Privacy, Security, Risk and Trust, Boston, MA.

Wang, Y., & Vassileva, J. (2007). *A review on trust and reputation for web service selection.* Paper presented at the Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference on.

Xiong, L., & Liu, L. (2004). Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE transactions on Knowledge and Data Engineering, 16*(7), 843-857.

Yan, Z., & Holtmanns, S. (2008). Trust modeling and management: from social trust to digital trust. *IGI Global*, 290-323.

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications, 42*, 120-134.

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE wireless communications, 24*(3), 10-16.

Yu, H., Kaminsky, M., Gibbons, P. B., & Flaxman, A. (2006). *Sybilguard: defending against sybil attacks via social networks.* Paper presented at the ACM SIGCOMM Computer Communication Review.

Yu, H., Shen, Z., Miao, C., Leung, C., & Niyato, D. (2010). A survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE, 98*(10), 1755-1772.

Zhao, H., & Li, X. (2013). VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks. *The Journal of Supercomputing, 64*(3), 805-829.

Zhu, C., Rodrigues, J. J. P. C., Leung, V. C. M., & Lei Shu, a. L. T. Y. (2018). Trust-Based Communication for the

Industrial Internet of Things. *IEEE Communications Magazine 56*(2), 16 – 22. doi: 10.1109/MCOM.2018.1700592

ABDELMUTTLIB IBRAHIM ABDALLA AHMED (abdelmuttlib@siswa.um.edu.my)
Received the B.Sc. degree in computer science from OIU, Sudan, and the M.S. degree in computer science from IIUI, Pakistan. He is currently pursuing the Ph.D. degree with the University of Malaya, Malaysia. His research Interest areas include trust and reputation systems, Internet of Things, cloud computing security, and software defined vehicular networks.

SITI HAFIZAH BINTI AB HAMID (Hafizah@um.edu.my)
Received BS (Hons) in Computer Science from University of Technology, Malaysia., MS in Computer System Design from Manchester University, UK., and the PhD in Computer Science from University Of Malaya, Malaysia. She is currently an Associate Professor with the Department of Software Engineering, Faculty of Computer Science & Information Technology, and University of Malaya, Malaysia. She has authored over 75 research articles in different fields, including mobile cloud computing, big data, software engineering, machine learning and IoT.

ABDULLAH GANI (abdullah@um.edu.my)
Received the B.Phil. and M.Sc.degrees in information management from the University of Hull, U.K., and the Ph.D. degree in computer science from The University of Sheffield, U.K. He is currently a Professor with the School of Computing & IT, Taylor's University, Malaysia. He has authored over 250 research articles in different fields, including mobile cloud computing, big data, wireless networking, machine learning and IoT.

SULEMAN KHAN (Suleman.khan@northumbria.ac.uk)
Received the Ph.D. degree (Distinction) from the Faculty of Computer Science and Information Technology, University of Malaya, Malaysia, in 2017. He was a faculty member with the School of Information Technology, Monash University Malaysia (June 17 – March 19). Currently, he is faculty member in department of computer and information sciences, Northumbria University, Newcastle, UK. He has published more than 50 high-impact research articles in reputed international journals and conferences. His research areas include, but are not limited to, network forensics, software-defined networks, the Internet of Things, cloud computing, and vehicular communications.

MUHAMMAD KHURRAM KHAN (mkhurram@ksu.edu.sa)
Is currently a Full Professor with the Center of Excellence in Information Assurance, King Saud University, Saudi Arabia. He has authored over 450 research papers in the journals and conferences of international repute. He is a fellow of the IET, BCS, and FTRA. He is the Editor-in-Chief of the Telecommunication Systems. He is on the Editorial Board of several international journals/magazines.

Conflict of Interest and Authorship Conformation

- All authors have participated in (a) conception and design, (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.
- This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.
- The authors have **NO** affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript

Author's name	**Affiliation**
Abdelmuttlib Ibrahim Abdalla Ahmed	Center for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Information Technology, University Malaya , Malaysia
Siti Hafizah Binti Ab Hamid	Department of Software Engineering, Faculty of Computer Science and Information Technology, University Malaya , Malaysia
Abdullah Gani	Center for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Information Technology, University Malaya , Malaysia
Suleman Khan	Department of Computer and Information Sciences, University of Northumbria, Newcastle, UK
Muhammad Khurram Khan	Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia