A Survey on Trust Management for Internet of Things

Article *in* Journal of Network and Computer Applications · June 2014

DOI: 10.1016/j.jnca.2014.01.014

CITATIONS
448

READS
6,248

3 authors:

Zheng Yan
Xidian University
197 PUBLICATIONS **2,183** CITATIONS
SEE PROFILE

Peng Zhang
20 PUBLICATIONS **763** CITATIONS
SEE PROFILE

Athanasios Vasilakos
680 PUBLICATIONS **23,051** CITATIONS
SEE PROFILE

Journal of Network and Computer Applications 42 (2014) 120–134

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A survey on trust management for Internet of Things

Zheng Yan [a,b,*,1], Peng Zhang [c], Athanasios V. Vasilakos [d]

[a] The State Key Laboratory of ISN, Xidian University, PO Box 119, No. 2 South Taibai Road, 710071 Xi'an, China
[b] Department of Comnet, Aalto University, Otakaari 5, 02150 Espoo, Finland
[c] The Institute of Mobile Internet, Xian University of Posts and Telecommunications, Weiguo Road, Changan District, 710121 Xi'an, China
[d] Department of Computer Science, Kuwait University, P.O. Box 5969, Safat -13060, Kuwait

ARTICLE INFO

Article history:
Received 9 October 2013
Received in revised form
12 December 2013
Accepted 13 January 2014
Available online 25 March 2014

Keywords:
Internet of Things
Trust management
Security
Privacy
Trust
Secure multi-party computation

ABSTRACT

Internet of Things (IoT) is going to create a world where physical objects are seamlessly integrated into information networks in order to provide advanced and intelligent services for human-beings. Trust management plays an important role in IoT for reliable data fusion and mining, qualified services with context-awareness, and enhanced user privacy and information security. It helps people overcome perceptions of uncertainty and risk and engages in user acceptance and consumption on IoT services and applications. However, current literature still lacks a comprehensive study on trust management in IoT. In this paper, we investigate the properties of trust, propose objectives of IoT trust management, and provide a survey on the current literature advances towards trustworthy IoT. Furthermore, we discuss unsolved issues, specify research challenges and indicate future research trends by proposing a research model for holistic trust management in IoT.

1. Introduction

Internet of Things (IoT) is going to create a world where physical objects are seamlessly integrated into information networks in order to provide advanced and intelligent services for human-beings. The interconnected "things" such as sensors or mobile devices senses, monitors and collects all kinds of data about human social life. These data can be further aggregated, fused, processed, analyzed and mined in order to extract useful information to enable intelligent and ubiquitous services. IoT is evolving as an attractive next generation networking paradigm and service infrastructure. Various applications and services of IoT have been emerging into markets in broad areas, e.g., surveillance, health care, security, transport, food safety, and distant object monitor and control. The future of IoT is promising (Agrawal and Das, 2011).

Trust management (TM) plays an important role in IoT for reliable data fusion and mining, qualified services with context-aware intelligence, and enhanced user privacy and information security. It helps people overcome perceptions of uncertainty and risk and engages in user acceptance and consumption on IoT services and applications. Trust is a complicated concept with regard to the confidence, belief, and expectation on the reliability, integrity, security, dependability, ability, and other characters of an entity. Reputation is a measure derived from direct or indirect knowledge or experiences on earlier interactions of entities and is used to assess the level of trust put into an entity.

However, the IoT poses a number of new issues in terms of trust. Generally, an IoT system contains three layers: a physical perception layer that perceives physical environments and human social life, a network layer that transforms and processes perceived environment data and an application layer that offers context-aware intelligent services in a pervasive manner. Each layer is intrinsically connected with other layers through cyber-physical social characteristics (Ning et al., 2013). A trustworthy IoT system or service relies on not only reliable cooperation among layers, but also the performance of the whole system and each system layer with regard to security, privacy and other trust-related properties. Ensuring the trustworthiness of one IoT layer (e.g., network layer) does not imply that the trust of the whole system can be achieved.

Unlike other networking systems, new issues are raised in the area of IoT caused by its specific characteristics. First, data collection trust is a crucial issue in IoT. If the collected huge volumes of data from the physical perception layer are not trustworthy enough, e.g., due to the damage or malicious input of some sensors, the IoT service quality will be greatly influenced and hard to be accepted by users even though the network layer trust and the application layer trust can be fully provided. Second, data process trust should be ensured. Trustworthy data fusion and

* Corresponding author at: The State Key Laboratory of ISN, Xidian University, PO Box 119, No. 2 South Taibai Road, 710071 Xi'an, China. Tel.: +86 18691958048.
E-mail addresses: zhengyan.pz@gmail.com, zyan@xidian.edu.cn, zheng.yan@aalto.fi (Z. Yan), pzhang@xupt.edu.cn (P. Zhang), th.vasilakos@gmail.com (A.V. Vasilakos).
[1] Tel.: +358 50 4836664.

http://dx.doi.org/10.1016/j.jnca.2014.01.014
1084-8045/

mining require efficient, accurate, secure, privacy-preserved, reliable and holographic data process and analysis in a holistic manner. However, achieving all trust properties in IoT data process is an arduous task hard to fulfill. On the other hand, IoT services are based on data process, analysis and mining. This fact actually greatly intrudes user privacy. At the same time when the users enjoy advanced services they also need to disclose or have to share their personal data or privacy. Intelligently providing context-aware and personalized services and at the same time preserving user privacy to an expected level introduces a big challenge in current IoT research and practice. More specifically, due to the cyber-physical and social characteristics of IoT, how to provide trustworthy services through social computing is a hot but uneasy topic.

In the literature, trust and reputation mechanisms have been widely studied in various fields. However, current IoT research has not comprehensively investigated how to manage trust in IoT in a holistic manner. There is little work on the trust management for IoT. A number of issues, such as big data trust in collection, process, mining and usage; user privacy preservation; trust relationship evaluation, evolution and enhancement; user-device trust interaction, etc. have not been extensively studied. IoT introduces additional challenges to offer ubiquitous and intelligent services with high qualification in practice, especially when user privacy and data trust should be seriously considered and stringently supported.

In this paper, we study trust properties and propose the objectives of IoT trust management. We explore the literature towards trustworthy IoT in order to point out a number of open issues and challenges and suggest future research trends related to trust management. We further propose a research model in order to achieve comprehensive trust management in IoT and direct future research. Thus, the contributions of this survey paper can be summarized as follows:

(1) a comprehensive literature review about IoT TM technologies regarding trust properties and holistic trust management objectives;
(2) a summary of open research issues and challenges in IoT TM based on in-depth literature study and analysis;
(3) a research model to instruct future research directions that seamlessly integrates cyber-physical social trust into IoT TM.

The rest of the paper is organized as follows. Section 2 explores the properties that influence trust and proposes an IoT system model in order to specify the objectives of holistic trust management. Section 3 gives an overview of the literature towards trustworthy IoT. Then, we specify a number of trust related open research issues, summarize challenges and instruct future research in Section 4. Furthermore, a research model for comprehensively managing trust in IoT with social trust relationship integration is proposed in Section 5. We conclude the paper in Section 6.

2. Trust properties and objectives of trust management

2.1. Trust properties

Trust is a very complicated concept that is influenced by many measurable and non-measurable properties. It is highly related to security since ensuring system security and user safety is a necessity to gain trust. However, trust is more than security. It relates not only security, but also many other factors, such as goodness, strength, reliability, availability, ability, or other characters of an entity. The concept of trust covers a bigger scope than security, thus it is more complicated and difficult to establish, ensure and maintain, in short manage trust than security.

Another important concept related to trust is privacy that is the ability of an entity to determine whether, when, and to whom information about itself is to be released or disclosed (Yan and Holtmanns, 2008). A trustworthy digital system should preserve its users' privacy, which is one of the ways to gain user trust. Trust, security and privacy are highly related crucial issues in emerging information technology areas, such as IoT.

Although the richness of the concept, we can still summarize the subjective and objective properties that are relevant to a decision of trust. As shown in Table 1, the properties influencing trust can be classified into five categories (Yan and Holtmanns, 2008; Yan and Prehofer, 2011)

- Trustee's objective properties, such as a trustee's security and dependability. Particularly, reputation is a public assessment of the trustee regarding its earlier behaviors and performance.
- Trustee's subjective properties, such as trustee honesty, benevolence and goodness.
- Trustor's subjective properties, such as trustor disposition and willingness to trust.
- Trustor's objective properties, such as the criteria or policies specified by the trustor for a trust decision.
- Context that the trust relationship resides in, such as the purpose of trust, the environment of trust (e.g., time, location, activity, devices being used, their operational mode, etc.), and the risk of trust. It specifies any information that can be used to characterize the background or situation of the involved entities (Dey, 2001). Context is a very important factor influencing trust. It specifies the situation where trust exists. Dey defined the ability of a computing system to identify and adapt to its context as context-awareness (Dey, 2001). Notably, the influencing properties of trust could be different or paid different attention by a trustor in different situations and contexts.

IoT trust management concerns part or all of above trust properties in different contexts for different purposes. In what follows, we present an IoT system model in order to illustrate what trust properties should be enhanced in order to achieve holistic trust management.

Table 1
Properties influencing trust (Yan and Holtmanns, 2008).

Trustee's objective properties	Competence; ability; security (confidentiality, integrity, availability); dependability (reliability, maintainability, usability, safety); predictability; timeliness; (observed) behaviors; strength; privacy preservation.
Trustee's subjective properties	Honesty; benevolence; goodness.
Trustor's objective properties	Assessment; a given set of standards; trustor's standards.
Trustor's subjective properties	Confidence; (subjective) expectations or expectancy; subjective probability; willingness; belief; disposition; attitude; feeling; intention; faith; hope; trustor's dependence and reliance.
Context	Situations entailing risk; structural; risk; domain of action; environment (time, place, involved persons), purpose of trust.

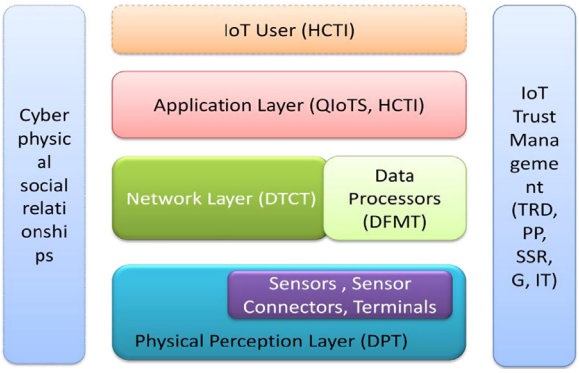

Fig. 1. A system model of IoT.

2.2. A system model of IoT

We consider an IoT system involving three layers, as illustrated in Fig. 1: a physical perception layer that contains a huge number of sensors, actuators, mobile terminals and sensor connectors and applies sensing technologies to sense physical objects (including human beings) and social environments by collecting huge amount of data in order to convert them into the entities in the cyber world; a network layer that includes all network components with heterogeneous network configurations (e.g., wireless sensor networks, ad hoc networks, cellular mobile networks and the Internet) for data coding, transmission, fusion, mining and analyzing at data processors in order to provide essential information to an application layer that pervasively and intelligently offers expected services or applications to IoT end users. This system model is compatible with the reference architecture model proposed by EU FP7 IoT-A project, especially the IoT-A tree structure (Architectural Reference Model for the IoT – (ARM), 2013). Meanwhile, various cyber-physical social relationships exist crossing the above three layers, which can be explored and mined to offer advanced services for human-beings. IoT trust management is concerned with: collecting the information required to make a trust relationship decision; evaluating the criteria related to the trust relationship; monitoring and reevaluating existing trust relationships; as well as ensuring the dynamically changed trust relationships and automating the process in the IoT system (Grandison and Sloman, 2000; Yan and Prehofer, 2011).

2.3. Objectives of trust management

To provide trustworthy IoT under the aforementioned model, research on trust management in IoT should achieve the following goals as marked in Fig. 1:

(1) Trust relationship and decision (TRD): trust management provides an effective way to evaluate trust relationships of the IoT entities and assist them to make a wise decision to communicate and collaborate with each other. Trust relationship evaluation (in short trust evaluation) concerns all IoT system entities in all layers and plays a fundamental role for intelligent and autonomic trust management.
(2) Data perception trust (DPT): data sensing and collection should be reliable in IoT. In this aspect, we pay attention to the trust properties like sensor sensibility, preciseness, security, reliability, and persistence, as well as data collection efficiency, i.e., the trustee's objective properties in the IoT physical perception layer.
(3) Privacy preservation (PP): user privacy including user data and personal information should be flexibly preserved according to the policy and expectation of IoT users. This objective relates to the IoT system objective properties in general.
(4) Data fusion and mining trust (DFMT): the huge amount of data collected in IoT should be processed and analyzed in a trustworthy way with regard to reliability, holographic data process, privacy preservation and accuracy. This objective also relates to trusted social computing in order to mine user demands based on their social behaviors and social relationship exploration and analysis. DFMT concerns the objective properties of the data processor in the IoT network layer.
(5) Data transmission and communication trust (DTCT): data should be transmitted and communicated securely in the IoT system. Unauthorized system entities cannot access private data of others in data communications and transmission. This objective is related to the security and privacy properties of IoT system wherein light security/trust/privacy solution is needed. Trusted routing and key management in IoT networks are two important issues required to be solved for achieving this objective (Liu and Wang, 2010).
(6) Quality of IoT services (QIoTS): Quality of IoT services should be ensured. “Only here, only me and only now” services are expected (Chen, 2012), which implies that the IoT services should be personalized and precisely offered at exactly right place and time to a right person. This objective is mainly about the trust management in the IoT application layer, but required to be supported by other layers. The QIoTS TM objective concerns not only the objective properties of IoT services (the trustee), but also the objective and subjective properties of users (the trustor), as well as context.
(7) System security and robustness (SSR): trust management in IoT should effectively counter system attacks to gain sufficient confidence of IoT system users. This objective concerns all system layers, focusing on system security and dependability (including reliability and availability), which are about the trustee's objective properties.
(8) Generality (G): trust management for various IoT systems and services is preferred to be generic that can be widely applied, which is a system objective property.
(9) Human–computer trust interaction (HCTI): trust management provides sound usability and supports human–computer interaction in a trustworthy way, thus can be easily accepted by its users. This requirement pays more attention to the subjective properties of trustor (i.e., IoT users) at the application layer.
(10) Identity trust (IT): The identifiers of IoT system entities are well managed for the purpose of trustworthy IoT. Scalable and efficient identity management in IoT is expected. This objective relates all layers and need crossing-layer support. It concerns the objective properties of IoT system (e.g., identity privacy) and subjective properties of IoT entities (e.g., user hope) and context that may influence identity management policies.

We would like to emphasize that vertical trust management that supports TRD, PP, SSR, G and IT is crucial for achieving trustworthy IoT as a whole. It is essential for trust management to cover all layers of IoT, not only just enhancing security, privacy and trust in each layer. Reliable cooperation among trust management techniques in all layers is required in IoT trust management. A comprehensive and holistic trust management for IoT requires that all above objectives can be well achieved.

3. Trust management in IoT

In this section, we survey the literature advances towards trustworthy IoT. We review the papers published in recent decade

from the following database: IEEE Explorer, ACM library, Springer library, and ScienceDirect based on the key words: trust, trust management, trust model, reputation systems, security, privacy, trust data, secure data access, secure multi-party computation, quality of data process/analysis in the area of IoT. We review the existing work based on eight taxonomies (Trust Evaluation, Trust Framework, Data Perception Trust, Identity Trust and Privacy Preservation, Transmission and Communication Trust, Secure Multi-Party Computation, User Trust, IoT Application Trust) and then compare their versatility for trust management by referring to the above described ten objectives, as shown in Table 2. For unifying our survey, after reviewing existing work in each of above taxonomies, we outline the aspects that can be considered as done or with satisfactory solutions and point out where we still have some gaps that need further research. The ten TM objectives, especially such vertical TM objectives as TRD, PP, SSR, G and IT for IoT as presented above will play as the criteria of our analysis and comments.

3.1. Trust evaluation

Trust evaluation is a technical approach of representing trust relationships for digital processing, in which the properties influencing trust will be evaluated. Bao and Chen proposed a trust management protocol considering both social trust and QoS trust metrics and using both direct observations and indirect recommendations to update trust (Bao and Chen, 2012). Concretely, three trust properties: honesty, cooperativeness, and community-interest are considered in the trust evaluation of IoT nodes ("things"). The honesty trust property represents whether or not

Table 2
Comparison of versatility for trust management in IoT.

	TRD	DPT	PP	DFMT	DTCT	QIoTS	SSR	G	HCTI	IT
Bao and Chen (2012), Bao et al. (2013)	x					x (no context considered)	x (considered)			
Chen et al. (2011)	x					x				
Nitti et al. (2012)	x									
Liu et al. (2010)						x				
Ning et al. (2013)		x	x		x	x				x
Suo et al. (2012)			x		x		x	x		x
Zhou et al. (2012)		x			x					
Xiong et al. (2011)		x			x			x		x
Gessner et al. (2012)	x		x		x	x partially				x
de Leusse et al. (2009), Alam et al. (2011)					x support					
Yan et al. (2010), Jun et al. (2011)			x							
Roman et al. (2013)			x partially		x partially		x partially			x (some aspects)
Kothmayr et al. (2013)			x partially		x		x			x
Javed and Wolf (2012)		x								
Ukil et al. (2011)		x			x partially					
Khoo (2011)		x	x		x					
Feng and Fu (2010)		x	x		x					x
Sicari et al. (2013)	x	x		x (fusion only)			x partially			
Huang et al. (2013)		x								
Fongen (2012)										x
Hu et al. (2011)			x location privacy							x
Jara et al. (2011)										x
Sarma and Girão (2009)			x identity privacy							x
Zhang and Tian (2010)			x role privacy							x
Isa et al. (2012)					x					
Granjal et al. (2012)					x					
Raza et al. (2013)			x somehow		x					
Evans and Eyers (2012)			x	x considered						
(Huang et al. (2012), Gusmeroli et al. (2013)			x							
SMC			x (partially)	x						
Mishra and Chandwani (2008) in SMC				x			x (zero hacking)			
Pass (2004), Yao et al. (2008), Tang et al. (2011) in SMC			x (partially)	x			x			
Køien (2011)									x	
Li and Wang (2012)			x			x integrity support				
Petroulakis et al. (2013)			x		x					x
Thoma et al. (2012)			x	x						
Portelo et al. (2012)				x						

Note: SMC refers to the following references: (Mishra et al., 2009, 2010; Bickson et al., 2008; Wee, 2010; Ye et al., 2009; Yao, 1982; Goldreich, 2004; Atallah and Du, 2001; Du and Atallah, 2001a, 2001b; Du et al., 2004; Bunn and Ostrovsky, 2007; Amirbekyan and Estivill-Castro, 2006, 2007a, 2007b, 2009; Estivill-Castro, 2004; Vaidya and Clifton, 2002; Vaidya et al., 2008; Shaneck et al., 2006; Du, 2001; Du and Zhan, 2002; Chiang et al., 2005; Xu et al., 2010; Deitos and Kerschbaum, 2009; Melchor et al., 2009; Wu et al., 2012; Pathak and Joshi, 2009; Mishra and Chandwani, 2007, 2008; Kerschbaum, 2009; Liu et al., 2011; Jurczyk and Xiong, 2011; He and Wang, 2012; Huang et al., 2010; Wang and Ishwar, 2011; Zhu et al., 2008, 2009a, 2009b; Wang and Luo, 2009; Li et al., 2009; Wang et al., 2008; Zhong et al., 2010; Liao et al., 2011; Xiong et al., 2012; Wang and Zhang, 2009; Shen et al., 2010; Liu and Zhang, 2010; Zheng et al., 2009; Wang, 2010; Luo et al., 2010; Tong et al., 2010; Luo and Li, 2004; Frikken et al., 2004; Sanil et al., 2004; Pass, 2004; Atallah et al., 2003; Liu et al., 2012; Ester et al., 1996; Kantarcioglu and Clifton, 2004; Zhang and Zhao, 2009; Lin et al., 2009; Yao et al., 2008; Wan et al., 2007; Yang et al., 2006; Tang et al., 2011; Goldwasser and Lindell, 2005; Aggarwal et al., 2010; He et al., 2012; Dolev et al., 2012).

a node is honest. The cooperativeness trust property represents whether or not the trustee is socially cooperative with the trustor. The community-interest trust represents whether or not the trustor and trustee are in the same social communities/groups (e.g., in a co-location or co-work relationship) or have the similar capabilities. In this work, trust was defined and quantified using social network theory (Daly and Haahr, 2009) and evaluated based on both direct observations and indirect recommendations. The effectiveness of the trust management protocol was demonstrated in a service composition application. It is one of the first to consider social relationships in trust management for IoT. Bao et al. further studied the scalability, adaptability and survivability of the trust management protocol in a dynamically changed IoT system (Bao et al., 2013). A trust model was proposed to protect user security by evaluating a user's trust in a service based on service classification (Liu et al., 2010). Authentication history and penalty are also concerned in the evaluation (Liu et al., 2010).

Chen et al. (2011) proposed a trust management model based on fuzzy reputation for IoT that considers a specific IoT environment consisting of only wireless sensors with QoS trust metrics containing such elements as packet forwarding/delivery ratio and energy consumption. But this QoS study is far from satisfying the objective of QIoTS as described above.

Based on a social Internet of Things (SIoT) paradigm, according to which the objects are capable of establishing social relationships in an autonomous way with respect to their owners, Nitti et al. studied how the information provided by other members of the SIoT has to be processed so as to build a reliable system on the basis of the behavior of the objects (Nitti et al., 2012). They defined a subjective model for trust management. Each node computes the trust of its friends on the basis of its own experience and the opinion of common friends with potential service providers. A feedback system is employed and the credibility and centrality of the IoT nodes are applied to evaluate the trust level.

Existing work in this taxonomy considered some objective and subjective properties of trustee (e.g., QIoTS) for trust evaluation and decision (TRD) in the context of IoT. But context-aware TRD based on social computing has not yet been seriously investigated. TRD has not been applied to achieve the objective of QIoTS, i.e., “only here, only me and only now” services mostly cannot be supported. The above work only provided TRD and supported QIoTS, some considered SSR. Obviously, none of above achieves all TM objectives in IoT.

3.2. Trust framework

Trust framework is the system architecture designed to achieve trust management of a whole. Ning et al. (2013) proposed an IoT system architecture that offers a solution to the broad array of challenges in terms of general system security, network security, and application security with respect to the basic information security requirements of data confidentiality, integrity, and availability, authority, non-repudiation, and privacy preservation. But some specific trust issues such as TDR, DFMT, SSR, G, and HCTI were not considered.

Zhou et al. (2012) proposed a trusted architecture for a farmland wireless sensor network. The architecture contains a perception logical layer, a mark recognition logical layer, a decision-control logical layer and a trusted interface logical layer. The trusted interface logical layer is consisted of cross-layer trusted protocols by which the network architecture interacts with the perception logical layer, the mark-recognition logical layer and the decision-control logical layer. This architecture can afford trusted and reliable data transmission in wireless sensor networks. However, this work mainly focused on the physical perception layer and the sensor network part of the network layer of the IoT system. It supports the trust management objectives regarding DPT and DTCT.

Suo et al. (2012) briefly reviewed the research progress of IoT, paying special attention to security. By means of deeply analyzing the security architecture and features, security requirements were given in each layer of IoT, such as lightweight cryptographic algorithm and protocol, integrity and authenticity of sensor data, key agreement in the physical perception layer; identity authentication, anti-DDoS, encryption mechanism and communication security in the network layer; secure multi-party computation, secure cloud computing and anti-virus for data processing; authentication and key management, security education and management, and privacy preservation in the application layer. Key technologies including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms were discussed. In addition, challenges such as security structure, key management, security law and regulations were briefly outlined. But this work did not consider privacy preservation in the layers of physical perception and network (e.g., DPT), TRD, DFMT, QIoTS, and HCTI. Li also studied security requirements based on IoT layers and indicated that information processing security and individual privacy are inevitable problems (Li, 2012).

A general architecture of trusted security system for IoT was proposed by Xiong et al. (2011), which mainly includes trusted user module, trusted perception module, trusted terminal module, trusted network module and module agent module. However, this architecture has not been evaluated in practice. Due to openness and the immature development of IoT, how to resolve security problems of IoT requires further study. This architecture concerns such objectives as DPT, DTCT, G, and IT.

An IoT architecture investigated by EU FP7 IoT-A project aims to take into account service privacy and IoT access security aspects throughout the architecture design for dealing with service accommodation, identification and IoT-A platform realizations (Architectural Reference Model for the IoT – (ARM), 2013). But this architecture model does not consider trust management as a whole. Most TM objectives except PP and DTCT had not been considered.

Gessner et al. (2012) proposed a comprehensive set of trust-enhancing security functional components for the resolution infrastructure as a crucial part of IoT. These components cover not only basic IoT resource access control, but also essential functions such as identity management, key exchange and management and trust and reputation management. This component composition with its interdependencies provides compulsory mechanisms for securing communications between subjects to guarantee an inviolable interaction and therefore ensure data integrity and confidentiality, service trust and privacy of users. But this composition does not satisfy all objectives listed in Section 2.3, e.g., DPT, DFMT, SSR, G, and HCTI.

de Leusse et al. (2009) identified the requirements (i.e., interoperability, automation, decentralization and contextualization) for resources to be more resilient in IoT and proposed an architectural model of Self Managed Security Cell, which leverages on current knowledge in large scale security systems, information management and autonomous systems. This model supports policy based access control on IoT resources, which is one target of DTCT. Alam et al. (2011) addressed secure access provision to IoT-enabled services and interoperability of security attributes between different administrative domains. They proposed a layered architecture of IoT framework where a semantically enhanced overlay interlinks the other layers and facilitates secure access provision to IoT-enabled services by reasoning security through ontology and semantic rules, as well as a machine-to-machine platform. We analyzed that this architecture somehow supports DTCT.

Wu et al. (2011) proposed a virtualization and abstract model based on IoT to build the data security mechanism that could protect the privacy of user data and the security of personal information. Thus it supports the objective of PP.

Roman et al. (2013) provided an explicit analysis of the features and security challenges of the distributed approach of IoT. Their study showed numerous challenges that must be solved, such as assuring interoperability, reaching a business model, and managing the authentication and authorization of entities and multiple strengths as well. It was pointed that additional trust and fault tolerance mechanisms can be specifically created for distributed IoT solutions; both centralized and distributed approaches can coexist with each other, providing the foundations of a full-fledged IoT. This work only indicated that some aspects of IT, DTCT, SSR and PP should be considered in the distributed IoT system design. However, other TM objectives were not considered.

A standard-based security architecture with two-way authentication for the IoT was developed by Kothmayr et al. (2013). The authentication is performed during a fully authenticated Datagram Transport Layer Security (DTLS) handshake and based on an exchange of X.509 certificates containing RSA keys. The extensive evaluation, based on real IoT systems, showed that the proposed architecture provides message integrity, confidentiality and authenticity with affordable energy, end-to-end latency and memory overhead. However, this architecture only supports IT, DTCT, SSR, and PP partially.

In a brief summary, none of the proposed security frameworks for IoT as described above can achieve holistic trust management with regard to all listed trust management objectives. They only focus on some aspects of trust, such as security and privacy in IoT data transmission and communications. Some of them support identity trust. However, most of them lack concern on such trust objective as TRD, DFMT, QIoTS, SSR, G and HCTI. Particularly, DFMT and HCTI were ignored in most of above work. A comprehensive trust framework is still needed to achieve all objectives of IoT trust management.

3.3. Data perception trust

Data perception trust concerns IoT data trust during collection and pre-process in the physical perception layer. Javed and Wolf addressed one data perception trust problem: how to verify sensor information that is gathered from multiple sensors that are managed by different entities using outlier detection (Javed and Wolf, 2012). They developed a technique for automatically deriving a model of the physical phenomenon that is measured by the sensors. This model is then used to compare sensor readings and to identify outliers through spatial and temporal interpolation. The system was evaluated in the context of weather sensing and is applicable to any application domains where the underlying phenomenon is continuous. This work proposed a concrete scheme for achieving DPT.

Ukil et al. (2011) provided the solutions and technologies to resist different attacks temper proofing of the embedded devices in IoT by applying the concept of trusted computing. The illustrated technologies address the issue of security for data and hardware platform, and support DPT and securing data in transit (one aspect of DTCT).

Khoo (2011) studied the serious security and privacy issues rose by RFID technology and analyzed various threats of the RFID system components (e.g., blocking and jamming devices, relay attack, eavesdropping, replay attack, tag cloning, personal and location privacy intrusion) and elucidated how these issues can be resolved or risks can be mitigated. This work supports achieving such trust objectives as DPT, PP, and DTCT.

Feng and Fu (2010) studied the approaches recently developed for solving security and privacy issues in IoT, especially in RFID systems, such as physical security mechanisms, anti-collision algorithm mechanisms, encryption & authentication protocols and many mechanisms based on architecture to solve the security and privacy problem of the IoT (e.g., HIP-tags architecture implementation for IoT, self-managed security cell, mobile proxy – a novel RFID privacy protection mechanism, and LKC-privacy and its anonymization algorithm – a protection method of RFID data privacy). Obviously, it is a challenge in IoT to support interoperability for data collection and develop privacy enhancing technologies (PET) that are suitable for IoT, e.g., lightweight authentication and access management. This work supports DPT, DTCT, PP, and IT.

Sicari et al. (2013) proposed DARE, a hybrid architecture combining wireless sensor networks (WSNs) with wireless mesh networking paradigm in order to provide secure data aggregation and node reputation in WSNs. DARE uses a secure verifiable multilateration technique that allows the network to retain the trustworthiness of aggregated data even in the presence of malicious node. DARE can effectively reduce the amount of data exchanged over the wireless medium and achieve battery lifetime improvement to the wireless sensors. This work is advanced in supporting TRD, DPT, DFMT, and SSR. But it did not consider data privacy although data trustworthiness during fusion is enhanced efficiently.

After carefully examining the characteristics of body sensor networks (BSNs), Huang et al. (2013) proposed human interactive empirical channel-based security protocols to protect sensitive personal information collection. Using these protocols, dynamically distributing keys and IDs become possible without predeployment of keys or secrets. Therefore compromised and expired keys or IDs can be easily changed. These protocols exploit human users as temporary trusted third parties, which are applied to design secure BSNs. The proposed protocols enhance DPT in the context of BSNs.

DPT is inevitably crucial in IoT. It plays a fundamental role for supporting IoT service trust since most IoT services rely on data mining and analysis. Various system attacks could be maliciously attempted to break DPT. Current research only focuses on proposing concrete solutions in a specific context. None of them investigated how to embed the solution into reality with sound quality and how to make the solution cooperate with other trust management mechanisms for achieving other goals on trust. Few existing pieces of work completely support TRD, DFMT, SSR, G, IT and concern power efficiency (except Du and Atallah, 2001b). In particular, DPT performance should be further evaluated based on IoT service quality. However, this research method was seldom applied due to practical difficulties. Future research in this area should solve these open issues and focus more on lightweight solutions that are suitable for IoT “things” (e.g., sensors) with limited computing and processing capabilities.

3.4. Identity trust and privacy preservation

A number of studies aim to improve identity trust and achieve privacy preservation in IoT. Fongen proposed a framework for authentication and integrity protection suited for an IoT environment in order to satisfy scalability and lightweight requirements of IoT trust management (Fongen, 2012). Hu et al. (2011) studied identity management for user location privacy adapted to situations such as emergency and non-emergency cases based on policy management and user authentication, as well as access control on user location information. Jara et al. (2011) proposed a trust extension protocol to support secure mobility management for extending and adapting the network to changes of location and infrastructure, increase fault tolerance capacity, connectivity,

dependability and scalability in IP-based Wireless Sensor Networks (6LoWPAN). Yan et al. (2010) analyzed the threat of unauthorized tracking by a compromised RFID discovery service in the current industrial standard and proposed a pseudonym-based RFID discovery service architecture that provides practical privacy protection against unauthorized tracking to mitigate this threat. This design protects against database reading attack by a semi-trusted discovery service and provides efficient key management and access control. Sarma and Girão (2009) proposed using identities, more precisely virtual identities, as representations of all kinds of IoT entities. They applied digital shadows to represent projections of the entities involved in a communication or in sessions for privacy preservation. But this concept has not yet been validated.

Data privacy preservation is an important aspect for achieving data trust in IoT. Evans and Eyers (2012) applied information flow control techniques and tagged data in IoT with their privacy properties, which allows a trusted computing base to control data access based on privacy policies. In addition, computing performance issue about tagging within resource-constrained sensors was also assuaged in this study. This work is significant with regard to data trust and privacy preservation. However, it relies on trusted computing technologies. Its execution performance in the physical perception layer needs extensive investigation. A privacy protection solution was proposed by Huang et al. (2012) for IoT. It contains a user controlled privacy-preserving access control protocol, context aware k-anonymity privacy policy and filter and privacy protection mechanisms in order to control which of personal data is being collected and accessed, who is collecting and accessing such data, and when these are happening. An extended role based access control model linked to context information was proposed by Zhang and Tian (2010), which can effectively enhance the security for web services and produce access control for IoT. But data fusion and mining trust (DFMT) was not considered in this work. A capability based access control system was proposed that enterprises, or even individuals, can use it to manage their own access control processes to services and information (Gusmeroli et al., 2013). This mechanism supports right delegation and sophisticated access control customization.

Most of the above studies aim to achieve the objectives of IT and/or PP, some of them supports DTCT. But none of them fully concern DFMT and DPT. HCTI and QIoTS have not been touched in the existing work. The interoperation or integration with other TM mechanisms for achieving vertical TM objectives in different contexts has not been studied in the current literature. This requires further exploration in future research. Thus, current IoT privacy preservation and identity trust solutions are imperfect and incomprehensive.

3.5. Transmission and communication trust

Data transmission and communication trust is crucial of importance for achieving IoT trust. Existing advances in networking and communications can be applied in order to achieve DTCT. In particular, the trustworthy IoT networking and communication protocols should support the heterogeneous and specific IoT networking context, which rises new issues and challenges. We review some existing work as below.

A security protocol for bulk data transfer amongst the “things” was proposed by Isa et al. (2012), together with a security framework for enhancing security, trust and privacy for embedded system infrastructure. Lightweight symmetric encryption (for data) and asymmetric encryption (for key exchange) in Trivial File Transfer Protocol (TFTP) were suggested in order to make the proposed protocol applicable in the context of IoT.

Granjal et al. (2012) described mechanisms to enable security at the network layer and at the application layer and performed an extensive experimental evaluation study with the goal of identifying the most appropriate secure communication mechanisms and the limitations of current sensing platforms for supporting end-to-end secure communications in the context of Internet-integrated sensing applications.

SVELTE, an intrusion detection system for the IoT was designed, implemented, and evaluated against routing attacks such as spoofed or altered information, sinkhole, and selective-forwarding (Raza et al., 2013). SVELTE's overhead is small enough to deploy it on constrained IoT nodes with limited energy and memory capacity.

Heer et al. (2011) discussed the applicability and limitations of existing Internet protocols and security architectures in the context of IoT. They presented challenges and requirements for IP-based security solutions and highlighted specific technical limitations of standard IP security protocols. It was indicated that for supporting secure IoT, its security architecture should fit the lifecycle of a thing and its capabilities, and scale from small-scale ad-hoc security domains of things to large-scale deployments, potentially spanning several security domains. Security protocols should further take into account the resource-constrained nature of things and heterogeneous communication models. Lightweight security mechanisms and group security that are feasible to be run on small things and in IoT context should be developed, with particular focus on possible DoS/DDoS attacks. In addition, cross layer concepts should be considered for an IoT-driven redesign of Internet security protocols.

As the foundation of IoT, DTCT plays a role of backbone for achieving IoT trust. Current research in this area focuses on proposing proper security protocols or schemes that fit into IoT scenarios by considering its specific requirements and constraints. Again, analysis on the interoperation or integration with other TM mechanisms for achieving vertical TM objectives in different contexts is missed in the existing research. Further and insight study is required to achieve DTCT and at the same time support vertical trust management objectives (such as TRD, PP, SSR, G and IT). That is a future research direction in DTCT of IoT.

3.6. Secure multi-party computation

Secure multi-party computation (SMC) deals with the problem of secure computation among participants who are not trusted with each other, particularly with the preference of privacy preserving computational geometry. SMC refers to the parties, who participate in the computation with their own secret inputs, wish to cooperatively compute a function. When the computation is over, each party can receive its own correct output (correctness), and know its own output only (privacy). It is an important research topic in IoT. We found around 70 papers in SMC studies in the scope of our survey. The problems of SMC are specifically different in different scenarios. Based on the problems solved, SMC mechanisms can be classified into the following four categories (Shaikh and Mishra, 2010) as surveyed below. This part of research mainly focuses on supporting DFMT in various IoT scenarios. Some work partially provides PP and considers SSR. Thus, our survey in this part pays attention to the SMC technologies and their current status.

3.6.1. Privacy-preserving database query (PPDQ).

Secure data statistics is a specific SMC problem, particularly on database query privacy preservation. Jurczyk and Xiong reviewed and analyzed existing representative secure union protocols as well as anonymous communication protocols as a potential solution for the secure set operations (Jurczyk and Xiong, 2011).

They also proposed an alternative simple yet effective protocol based on an approach of random shares. It was demonstrated that simple solutions exist if a tradeoff between security, efficiency and accuracy can be made based on a certain practical situation. Huang et al. (2010) proposed a secure solution based on an oblivious transfer protocol and a homomorphic encryption scheme in order to preserve database user privacy when analyzing query statistics.

A protocol for sequence comparisons of the string-edit kind was proposed by Atallah et al. (2003), such that neither party reveals anything about their private sequence to the other party. This protocol is but a first step for applications in an area of privacy preserving bio-information check in a biological database.

Private data matching between the data sets of two potentially distrusted parties has a wide range of applications. However, malicious parties could spoof their private inputs in practice, which makes many existing solutions impractical. Yang et al. (2006) addressed this problem by forcing the matching parties to "escrow" the data they use for matching to an auditorial agent, and in the "after-the-fact" period, they undertake the liability to attest the genuineness of the escrowed data. Privacy-preserving set pattern matching is a cryptographic technique, which allows one appointed party to know which elements in his set appearing in the intersection of other parties without leaking any information. An efficient technique for privacy-preserving set pattern matching in the cryptographic model was proposed by using homomorphic encryption and oblivious polynomial evaluation (Zheng et al., 2009).

Aggarwal et al. (2010) considered the problem of securely computing the kth-ranked element of the union of two or more large, confidential data sets. They investigated two-party and multi-party protocols for both the semi-honest and malicious cases and proved that the problem can be solved in a number of rounds that is logarithmic in k in the two-party setting where each round requires communication and computation cost that is linear in b, the number of bits needed to describe each element of the input data. In the multiparty setting, they proved that the number of rounds is linear in b, where each round has overhead proportional to b multiplied by the number of parties. Thus their solution is computationally reasonable, while protocols do exist for computing the kth-ranked element, they require time that is at least linear in the sum of the sizes of their combined inputs.

Tang et al. (2011) applied a secret sharing scheme to construct an efficient and secure multi-party computation protocol for sequencing problems, which is also an essential issue for privacy preserving database query. This scheme is secure against both a passive adversary that can corrupt at most $t \leq (n-1)/2$ participants, and an active adversary that can corrupt at most $t < n/3$ participants. Dolev et al. (2012) investigated an extension of the k-secret sharing scheme, in which the secret shares are changed on the fly, independently and without (internal) communications, as a reaction to a global external trigger.

Current work in PPDQ is still in its infancy. Some of PPDQ operations are studied, but definitely not all. Various joint database queries comprising different conditions introduce a big research challenge if privacy preservation and efficiency should be stringently ensured. Considering the computation complexity of cryptographic schemes, practical solutions prefer simple schemes without using cryptography. A lightweight and generic solution beyond concrete database operations is expected in practice.

3.6.2. *Privacy-preserving scientific computations (PPSC).*

Current research on PPSC includes statistical computations, numerical computations, area/scope computation, vectors' scalar product, quadratic function's extreme minimal value, computational geometry, secure multi-party sampling, steganography, universally composable, etc., with privacy preservation. Most PPSC studies focus on specific computing scenarios targeting to solve a concrete scientific computation problem under the sketch of SMC.

A novel secure multi-party computation protocol for statistical computations was proposed and implemented using a Token Ring Network by Mishra et al. (2010). Bickson et al. (2008) proposed an efficient framework for enabling secure multi-party numerical computations in a Peer-to-Peer network using a privacy preserving computation without loss of accuracy. Wee presented round-efficient protocols for secure multi-party computation with a dishonest majority that relies on black-box access to the underlying primitives (Wee, 2010). Ye et al. (2009) proposed an efficient secure protocol, which is based on numerical computation, for the problem of determining the meeting points of two intersected circles. The communicational complexity of the protocol can be lowered to just $O(12*(\log R1+\log R2))$, where $R1$ and $R2$ are the radius of the two circles respectively. Mishra et al. proposed a protocol named Extended_Encrypto_Random, which itself was an extension of its initial work Encrytpo_Random for joint-computations undertaken by multiple parties for a more secure multi-party computational process (Mishra et al., 2009). A scheme to solve the two-party weighted average problem (WAP) under a hybrid security model (not a semi-honest model without collusion with the semi-trusted third party, as applied in most work but (Kerschbaum et al., 2010) was proposed by Xiong et al. (2012). This scheme is secure and can be extended to work under a malicious model using any fair exchange scheme. Luo and Li investigated secure multi-party elementary function computation protocols that support a number of private preserving operations (e.g., exponential, power, logarithmic concern functions, and compound functions) in a cooperative environment (Luo and Li, 2004).

An important building block of SMC is secure scalar product protocol (SSPP), which is supported by a wide range of theoretical research (Yao, 1982; Goldreich, 2004). SSPP privately compute two vectors' scalar product without disclose any participants' unintended information. It is widely used in privacy preserving collaborative computation: privacy preserving computational geometry (Atallah and Du, 2001), privacy preserving statistic analysis (Du and Atallah, 2001b), privacy preserving matrix computation (Du et al., 2004), privacy preserving scientific computation (Du and Atallah, 2001a), especially privacy preserving data mining (Bunn and Ostrovsky, 2007; Amirbekyan and Estivill-Castro, 2006; Estivill-Castro, 2004; Vaidya and Clifton, 2002; Vaidya et al., 2008). But, the current challenge of SSPP study is to reduce high communication and computation complexity and preserve intermediate information, thus most of proposed schemes are impractical for real deployment (Amirbekyan and Estivill-Castro, 2007b; Shaneck et al., 2006; Du, 2001; Du and Zhan, 2002; Chiang et al., 2005). Some efforts have been made in order to improve the performance of SSPP with improved security (Xu et al., 2010; Deitos and Kerschbaum, 2009; Melchor et al., 2009; Kerschbaum, 2009; Mishra and Chandwani, 2008). He et al. (2012) presented a secure two-party quantum scalar product scheme via quantum entanglement and quantum measurement with the help of a non-colluding third party. Zhong et al. (2010) presented two protocols to the problem about how to decide the areas, i.e., a polygon is divided into two parts by a line based on Scalar Product Protocol, Monte Carlo Method and Oblivious Transfer.

Wu et al. introduced a secure two-party computation protocol for the quadratic function's extreme minimal value on the secret interval by using the technologies of the Secure Comparison Protocol and the homomorphic encryption (Wu et al., 2012). Pathak and Joshi (2009) proposed a scalable and efficient protocol to perform secure multi-party computations on encrypted data. In this protocol, modifier tokens are generated along encryption,

which are used in the computation. The computation function uses the acquired data and modifier tokens to compute a result without revealing the input plain data, thus privacy of the parties is maintained. The above protocol can be applied in conducting banking computations and collaborative computation that requires stringent privacy enhancement.

Privacy preserving computational geometry (PPCG) is a special area in SMC. Ye et al. investigated the problem of judging whether a point is in a convex hull or not by proposing a secure protocol to determine the position of a private point and a private line with two efficient point-inclusion schemes (Ye et al., 2009). Zhu et al. presented an effective protocol to privately find the approximate convex hulls (Zhu et al., 2009a, 2008. Wang et al. (2008) gave two solutions for two dimensional convex hulls. Li et al. (2009) provided a practical protocol to find the approximate intersection area of two private convex hulls and solved the three dimensional approximate convex hulls problem (Wang et al., 2008). He and Wang (2012) proposed a private determination protocol of position relation between line and circle, and also present a private determination protocol of position relation between line and hyperbola. Wang and Zhang (2009) proposed a protocol of determining a line by two secret points and further presented a new scheme to determine convex hull based on privacy protection for planar point set. Luo et al. (2010) proposed a protocol for the Points-Rectangle Area Inclusion problem, which is based on multiplication protocol and a probability algorithm for Points-Hyperspace Inclusion problem, using random technology to improve efficiency. A privacy-preserving line-ellipse position relation determination protocol was developed and a private-preserving segment-ellipse intersect-determination protocol was presented by Tong et al. (2010). These protocols have potential applications in engineering, military, on-line transactions and many other fields.

The problem of secure multi-party sampling is a subclass of SMC, in which n parties wish to securely sample an n-variant joint distribution, with each party receiving a sample of one of the correlated variables. The objective is to correctly produce the samples using a distributed message passing protocol, while maintaining privacy against a coalition of passively cheating parties. Wang and Ishwar (2011) studied this problem and gave necessary conditions and sufficient conditions for distributions that can be securely sampled. They indicated that the exact characterization of the distributions that can be securely sampled remains open.

Steganography is a technique for conveying secret messages under the cover of digital media, such that the existence of secret data is concealed. The issue of "distributed steganography" known as many cooperative computations with distributed parties in covert communications was studied by Liao et al. (2011) and a model of distributed steganography was presented aiming to carry out a steganographic technique on the union of two-party private inputs, without revealing any information.

Lin et al. (2009) presented a unified framework for the construction of Universally Composable (UC) secure protocols both with, and without, trusted set-up. This framework not only provides a conceptually simple solution for essentially all general UC-feasibility results, but also allows us to significantly improve the round-complexity and the complexity theoretic assumptions.

Pass showed how to securely realize any multi-party functionality in a way that preserves security under an a-priori bounded number of concurrent executions, regardless of the number of corrupted parties (Pass, 2004). This is one of few efforts to ensure the robustness of SMC in the literature.

The fundamental theoretical research in PPSC is still on-going. The above reviewed research results mostly solved specific issues in a dedicated context. Whether and how they can be practically applied into IoT applications and services is still an open question. We suggest future research should study the applicability of PPSC schemes in real IoT applications by taking practical requirements and restrictions into account.

3.6.3. *Privacy-preserving intrusion detection (PPID).*

PPID is a significant topic although there are few studies in this specific area. It is very useful for IoT nodes to avoid disclosing such private information as "being intruded or not" even though they share intrusion detection information with other parties.

Frikken et al. (2004) studied such a scenario that Alice gets the resource only if she satisfies Bob's policy, Bob does not learn anything about Alice's credentials (not even whether Alice got access or not), and Alice learns neither Bob's policy structure nor which credentials caused her to gain access. They proposed an efficient protocol that protects both sensitive credentials and policies. Yao et al. (2008) studied the notion of quantitative policies for trust management and gives protocols for realizing them in a disclosure-minimizing fashion. Concretely, they solve the privacy preserving credential check before granting access to any resources. A fingerprint method was also developed to recover an optimal knapsack solution, once the computed optimal value is given and also enables verification of the integrity of the optimal value. Thus the objective of SSR is somehow supported. Goldwasser and Lindell (2005) presented a mild relaxation of the definition of secure computation allowing abort. It captures all the central security issues of secure computation, including privacy, correctness and independence of inputs by decoupling the issue of agreement from these issues.

However, current literature has not seriously studied how to preserve privacy of intrusion detection information. The data or information used for intrusion detection is generally not protected from the third party and controlled for access based on the data owner's policy and expectation. The applicability of PPID schemes has not been seriously studied with regard to concrete intrusion detection systems. Future research should either propose PPID schemes based on a real intrusion detection system or analyze their applicability in real IoT scenarios.

3.6.4. *Privacy-preserving data mining (PPDM)*

PPDM is a "must-solve" problem in IoT for securely and intelligently providing various IoT services in a pervasive and personalized way. In practice, it is also a challenge, considering computation complexity and communication cost. PPDM belongs to PPSC. But different from PPSC, PPDM focuses on supporting data mining related computations, processes or operations with privacy preservation.

A new architecture was proposed by Mishra and Chandwani (2007) to enable SMC by hiding the identity of the parties by taking part in the process of Business Process Outsourcing. A class of functions was proposed to provide additional abilities to a party to split its huge data before submitting it for computation, making it almost intractable for other parties to know the actual source of the data in order to support secure and privacy-preserved data mining.

A privacy-preserving sequential pattern mining solution was designed based on secure multi-party sum protocol and secure multi-party multi-data ranking protocol for privacy-preserving consumptive action analysis of multi-marketplace, privacy-preserving disease diagnose of multi-hospital and so on (Liu et al., 2011).

A number of operations on securely input data should be supported in PPDM. Zhu et al. (2009b) proposed schemes for securely extracting knowledge from two or more parties' private data. They studied privacy-preserving Add and Multiply Exchanging Technology and presented three different approaches to privacy-preserving Add to Multiply Protocol, as well as further

extended it to privacy-preserving Adding to Scalar Product Protocol. Wang and Luo studied a private-preserving shared dot product protocol that is a main building block of various data mining algorithms with privacy concerns, and provides fundamental security guarantee for many PPDM algorithms (Wang and Luo, 2009). They constructed a privacy-preserving two-party shared dot product protocol based on some basic cryptographic techniques, which is provably secure in a malicious model in the semi-honest model. Shen, Han and Shan proposed a Horizontal Distribution of the Privacy Protection DK-Means (HDPPDK-Means) algorithm based on Horizontal partitioned database and DK-means idea to realize distributed clustering and applied a secure multi-party computation protocol to achieve the PP objective (Shen et al., 2010).

Statistical hypothesis test is an important data analysis technique. Liu and Zhang (2010) investigated nonparametric Sign Test (NST) theory in such a context that two parties, each with a private dataset, would like to conduct a sign test on their joint dataset, but neither of them is willing to disclose its private dataset to the other party or any other third party. Their proposed protocol does not make use of any third party nor cryptographic primitives.

Association rule mining is one of the hottest research areas that investigate the automatic extraction of previously unknown patterns or rules from large amounts of data. Zhan et al. (2007) developed a secure protocol for multiple parties to conduct this desired computation in a distributed way and by using homomorphic encryption techniques to exchange the data while keeping it private. Kantarcioglu and Clifton (2004) propose two protocols to implement privacy-preserving mining of association rules over horizontally partitioned data and Zhang and Zhao (2009) further revised its security proof. Privacy-preserving association rule mining was surveyed by Wang (2010) with regard to basic concepts, general principles and methods. The drawback of the existing methods was impractical, ineffective, inaccurate, unavoidable and inflexible.

In the case that agencies want to conduct a linear regression analysis with complete records without disclosing values of their own attributes, Sanil et al. (2004) described an algorithm that enables agencies to compute the exact regression coefficients of the global regression equation and also perform some basic goodness-of-fit diagnostics while protecting the confidentiality of their data. This work can be applied for distributed computation for regression analyses used in data mining.

Liu et al. presented privacy preserving algorithms for DBSCAN clustering for the horizontally, vertically and arbitrarily partitioned data distributed between two parties (Liu et al., 2012). DBSCAN (Ester et al., 1996) is also a popular density-based clustering algorithm for discovering clusters in large spatial databases with noise.

Wan et al. (2007) presented a generic formulation of secure gradient descent methods with privacy preservation. Gradient descent is a widely used method for solving many optimization and learning problems. It underlies many commonly used techniques in data mining and machine learning, such as neural networks, Bayesian networks, genetic algorithms, and simulated annealing.

Finding the nearest k objects to a query object (k-NN queries) is a fundamental operation for many data mining algorithms to enable clustering, classification and outlier-detection tasks. Efficient solutions for k-NN queries for vertically partitioned data were proposed by Amirbekyan and Estivill-Castro (2009). These solutions include the $L\infty$ (or Chessboard) metric as well as detailed privacy-preserving computation of all other Minkowski metrics, privacy-preserving algorithms for combinations of local metrics into a global metric that handles the large dimensionality and diversity of attributes common in vertically partitioned data, a privacy-preserving SASH (a very successful data structure for associative queries in high dimensions) for managing very large data sets.

Although there are a lot of efforts made in the literature to support various data mining operations, calculations or processes in a privacy-preserving manner, current solutions of PPDM are still not practical. Seldom, a PPDM protocol can satisfy all essential requirements for practical usage, such as accuracy, flexibility, efficiency, security and trustworthiness. Particularly, existing studies have not analyzed all data mining related operations with privacy preservation in an integrated way. Thus, one open question is "can privacy be preserved if data mining in one application or service requires cooperation of a number of protocols?" or new schemes are expected to be proposed in a concrete IoT service. In addition, whether the PPDM schemes can support vertical TM objectives is still an open issue that worth our further investigation. In particular, how to ensure SSR, G and IT objectives of PPDM is an interesting research topic that could attract efforts on generic PPDM study for flexible application, robust PPDM study against potential attacks and verifiable PPDM study for auditing the correctness and accuracy of PPDM.

3.6.5. SMC applications

SMC together with homomorphic encryption is widely applied into many areas, such as distributed electronic contract management (Herrmann et al., 2006), smart meter based load management (Thoma et al., 2012), healthcare frauds and abuses (Jangde and Mishra, 2011), policy-agile encrypted networking for defense, law enforcement, intelligence community, and commercial networks (Krishnan and Sundaram, 2010), privacy preserving path inclusion (Huang et al., 2012), privacy preserving string matching (Luo et al., 2010), privacy-enhanced recommender system in a social trust network (Erkin et al., 2011), user profile matching in social networking (Li et al., 2013), credit check applications (Frikken et al., 2005), private collaborative forecasting and benchmarking (Atallah et al., 2004), privacy-preserving genomic computations (Wang et al., 2009), protection against insider threats (e.g., business partners) (Kerschbaum and Deitos, 2008), privacy preserving supply chain management (Kerschbaum et al., 2010), cloud application for collaborative benchmarking (Kerschbaum, 2011), joint decision-making and benefit sharing in a simple supply chain setting (Pibernik et al., 2011), privacy preserving electronic voting (Pang et al., 2012), and so on.

We found that various applications applied different SMC schemes. Most existing work has not yet considered SSR, G and IT. Verifiable, generic and robust SMC is still an open question.

3.7. User trust

User trust in IoT devices and services is essential for the success and longevity of IoT. Køien (2011) investigated trust in an IoT setting in considerable depth by presenting a multi-faceted view of trust in software, hardware, devices and services: transitivity and reflexivity, psychological aspects of risk and risk assessment, distrust, deception, retaliation and altruism, reputations, association and brands, and human brain. Køien pointed that it is obvious that one cannot fully trust any of the IoT components (e.g., software, hardware, communications, etc.), but this does not mean that humans cannot or should not trust IoT services at all. The human heuristic handling of risks, threats and opportunities is not without its faults, but use of trusted proxy devices and the trust we have in recognized brands and companies will enable us to trust many services without too much hesitation. Ding et al. (2013) proposed a security communication differential game model to study user behaviors in IoT interactions between selfish and malicious nodes. They obtained optimal amount of network

resource to invest in information security and packet forwarding and studied how the vulnerability of information and the potential loss from such vulnerability affects the optimal amount of resources that should be devoted to securing that information. The simulation result showed that malicious behaviors can be discovered with a high probability.

Little work in the literature pays attention to the HCTI issues (Yan et al., 2011) in IoT and investigates user behavioral trust in IoT systems. Obviously, user trust and HCTI play a decisive role in the final acceptance and success of IoT services and applications. It could be a very interesting and significant research topic.

3.8. IoT application trust

There are quite a number of IoT applications in a variety of areas of our life with some support on trust by satisfying partial TM objectives, e.g., PP, DFMT, DTCT, and IT. We introduce some examples as below.

A commodity integrity detection algorithm (CIDA) based on Chinese remainder theorem (CRT) was proposed to compare the hash value of each commodity identifier and the product of these values with those values that have been stored in a database in advance in order to detect the integrity of commodities and provide efficient security and privacy protection in IoT warehouse management (Li and Wang, 2012). A privacy preserving smart meter based load management system was proposed by using secure multi-party computation and homomorphic encryption as its security primitives (Thoma et al., 2012). It fully achieved preservation of the detailed user data, kept the data resolution for proposed smart grid control and management functionalities with a verification process, and did not need the support of a trusted third party. Secure multi-party computation based techniques are often used to perform audio database search tasks, such as music matching, with privacy preservation. Portelo et al. (2012) explained the security flaws of secure multi-party computation and analyzed the resulting tradeoff between privacy and computational complexity in the music matching application. Petroulakis et al. (2012, 2013) developed a lightweight framework for ensuring security, privacy and trustworthiness of life-logging in smart environments including the use of lightweight versions of IP protocols. The efficiency of the lightweight framework and the impact of the security attacks on energy consumption were also tested in an experimental test-bed including two interconnected users and one smart attacker.

The above work only concerned some TM objectives. Obviously, existing IoT applications have not yet fully considered all aspects of trust issues and fulfilled all objectives of trust management as described in Section 2.3. Future research should concern holistic TM in IoT in order to achieve all ten objectives in an integrated and rational manner.

4. Discussions and future research

4.1. Open issues

Based on the above survey, we can find a number of open issues in the area of IoT. First, trust evaluation lacks concern on context awareness and user's (trustor's) subjective properties. The trust evaluation result is not personalized, thus hard to intelligently provide IoT services. “Only here, only now and only me” services are still an unachieved target.

Second, the literature still lacks a comprehensive trust management framework that can support all proposed trust objectives. Previous concerns mostly focus on security and privacy issues for supporting DPT, PP, DTCT, QIoTS and IT. However, TRD, DFMT, SSR, G, and HCTI are seldom considered in the framework design. Current advance of DFMT have not yet been applied in practice or can be practically used in products or real systems. SSR, Generality and HCTI are mostly ignored in prior arts, but they are essential aspects of trust management. Obviously, trust management covers more objectives than security management. Thus, previous solutions for IoT security and privacy cannot holistically solve trust management issues.

Third, although Trusted Computing Platform based DPT solutions have been proposed, they could be too heavy or complicated for capability-constrained wireless sensors to adopt. Lightweight security and trust mechanisms that are feasible to be run on small things in the context of IoT should be developed, with particular focus on fighting against possible DoS or DDoS attacks. In addition, cross layer concepts should be considered for an IoT-driven redesign of Internet trust solutions, and lightweight & heterogeneous solutions for DTCT among “things”. DPT cooperation with other TM mechanisms should be investigated in order to support vertical trust management objectives. Applying advanced research method to evaluate the performance of DPT mechanisms is expected in the literature.

Forth, prior arts of privacy preservation in IoT are not comprehensive. Little work in the literature provides a complete PP solution to ensure PP in difference layers of IoT systems. We think cross-layer solutions should be developed to integrate and harmonize privacy protection mechanisms in each layer of IoT with regard to data, identities, location, time, behaviors, business processes and other types of information. Since few existing studies fully concerned DFMT and DPT and none touched HCTI and QIoTS in the category of research, the interoperation or integration of PP techniques with other TM mechanisms for achieving vertical TM objectives in different contexts should be explored in the future research.

Fifth, the interoperation or integration of DTCT technologies with other TM mechanisms has not been studied and should be a future research direction for achieving vertical TM objectives in different contexts.

Sixth, current SMC research is still in its infancy. Most solutions are not practical with regard to computation complexity, communication costs, flexibility, generality and integrity, thus hard to be really applied. They are generally system or scenario specific, which cannot satisfy all SMC requirements in a real system. For PPDQ, lightweight and generic solutions beyond concrete database operations have not yet been deeply investigated. On the other side, whether and how existing PPSC schemes can be practically applied into IoT applications and services is still an open question. The influence of practical requirements and restrictions of IoT applications and services should be taken into account in this study. PPID is significant for hiding IoT nodes' security status from other parties, thus crucial for the system acceptance of IoT stakeholders. However, it was seldom explored and investigated. The applicability of PPID schemes is open for our research efforts. Additionally, effective deployment of PPDM schemes in real IoT systems is an open research topic with practical significance. How to make PPDM schemes support vertical TM objectives is still an open issue that worth our further investigation. In order to ensure SSR, G and IT objectives of PPDM, new researches about generic, robust and verifiable PPDM should be initiated. In a brief summary, generic, robust and verifiable SMC that support vertical TM objectives of IoT is an open and challengeable research issue.

Last but not the least, HCTI is almost ignored in the current research, but it is one of decisive aspects that impact the final success of IoT. Holistic TM in IoT with good user experience determines the final success of IoT.

4.2. Challenges and future research trends

Except for the above open issues in the literature, we are still facing a number of challenges related to trust management towards the final success of IoT.

First, in heterogeneous IoT, new demands for trust are in need. How to transmit and compute trust between different networks is a difficult problem. Notably, the trust management in different networks of the nodes should follow the same criteria, either subjective or objective. Then, how to make use of the advantage resources from the Internet to help Wireless Sensor Network (WSN) compute trust is also a problem although transferring parts of the trust computing in WSN to the Internet can reduce the load of WSN.

Second, power efficiency, making trust management algorithms and mechanisms faster and less energy-consuming to support small things, is a big challenge in IoT. Current research has not yet fully investigated this issue. This research requires lightweight trust mechanisms, e.g., avoiding cryptographic schemes. It could be a multi-disciplinary study.

Third, performance improvement will remain the major research challenge for SMC and homomophic encryption, as well as key technologies of trust management in IoT (Kerschbaum, 2011). How to make key distribution efficient, how to work out lightweight privacy preserving solutions, how to avoid complicated and energy-consuming cryptographic calculations are big challenges.

Forth, privacy of the humans and confidentiality of the business processes are still big issues and it is challenging practical solutions that can be adopted in reality. Privacy-preserving technology is still in its infancy: the systems that have proposed are generally not designed for resource-restricted devices, and a holistic view on privacy is still to be developed (e.g., the view on privacy throughout one's life crossing all layers of IoT structure model). The technologies for data anonymity, authentication of devices and trust establishment and management are mainly supported by rather powerful devices, in terms of computing power and bandwidth. The heterogeneity and mobility of "things" will add complexity to the situation. In our opinion, it is not easy to study seamless integration and cooperation of PP schemes with other TM mechanisms for completely achieving vertical TM in IoT.

Fifth, autonomic trust management is hard to be realized because the cloud of things is hard to control due to the scale of deployment, their mobility and often their relatively low computation capacity. Based on the above survey, we have not yet found any existing work in this area.

Sixth, trustworthy data fusion is not easy to achieve. It is expensive to transmit huge volume of raw data produced by numerous "things" to the Internet (Sheng et al., in press-b). Thus data fusion becomes essential to reduce such a cost (Sheng et al., in press-a). However, trustworthy data fusion and mining with the support of efficiency, accuracy, security, privacy, reliability and holographic data process and analysis are not an easy task.

Seventh, as we have mentioned already, seamless integration and cooperation of all TM mechanisms for achieving holistic TM in IoT is a big job. So far, no work has achieved the goal specified in Section 2.3. Without a doubt, it is the most difficult issue challenging us.

Last, some legal issues remain far from clear and need interpretation, e.g., the impact of location on privacy regulation, the issue of data ownership in the network of collaborative clouds of "things". The nature of the IoT requests a heterogeneous and differentiated legal framework that adequately takes into account the scalability, verticality, ubiquity and interoperability of the IoT.

We anticipate that future research in the IoT trust management will focus on solving many existing open issues and overcome challenges towards technology adoption in practice and gaining user favorite and acceptance. More crucially, research should be oriented and driven by practical needs and demands, e.g., power-efficient technologies, lightweight trust management, IoT user trust, etc. User driven solutions should be paid specially attention. IoT services and applications with seductive user experiences are expected in market. "Only here, only now and only me" IoT services are far from practically applied with high user satisfactory. Thus trust management should be usably designed for easy user acceptance and favorite.

5. A research model

In this section, we propose a research model – a holistic trust management framework of IoT based on its system model in order to advance the state-of-the-art through integration and extension and at the same time instruct future research. As shown in Fig. 2, it comprises two aspects: one is IoT trust management composing modules for achieving holistic trust management in each layer and cross-layers; the other is supporting modules for achieving intelligent and trustworthy IoT application/service based on social trust

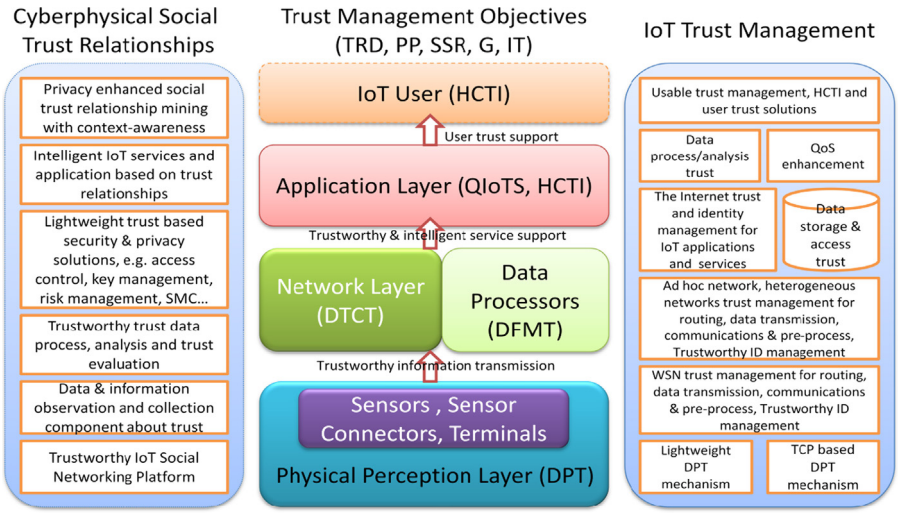

Fig. 2. A research model of IoT: a holistic trust management framework.

relationships. Herein, trust management aims to achieve all objectives listed in Section 2.3.

Starting from the bottom of the right side in Fig. 2, two kinds of DPT mechanisms should be explored: lightweight DPT mechanisms for "things" with constrained capabilities and TCP based DPT mechanisms for "things" (e.g., mobile devices) that can support TCP technologies. For supporting trustworthy data collection, fusion, transmission, communications and pre-process (related to DTCT and DFMT), trust management in heterogeneous "things" based networks (e.g., WSN, ad hoc networks, cellular mobile networks and the Internet) should be researched in a generic manner. Meanwhile, trustworthy identity (ID) management should support inter-layer and cross-layer information transition and process. Ensured data trust and identity trust in the physical perception layer and the network layer are essential for providing trustworthy IoT applications and services, in which we should study solutions for data storage and access trust over the Internet, context-aware QIoTS and data process/analysis trust. The trust relationship between users and IoT service/application should be ensured by usable trust management solutions driven by users that support HCTI and are built upon the above described modules.

Looking at the left side of Fig. 2, from the bottom to the top, a trustworthy IoT based social networking platform should be developed in order to observe and collect data related to trust relationships (in short trust data) of the objects in social life that can be sensed by "things". At the network layer, we should investigate solutions for trustworthy trust data process and analysis, as well as trust relationship evaluation. We would like to argue that lightweight security & privacy solutions for, e.g., access control, key management, risk management, SMC etc., should be developed based on trust relationship evaluation. This could be a future research direction and a very interesting research topic towards usable trust management. In addition, we think intelligent IoT services and applications based on trust relationships and privacy-enhanced social trust mining with context-awareness are also important and significant research issues.

6. Conclusions

In this survey, we pointed out the importance of trust management in IoT. In order to conduct holistic IoT trust management, we explored the trust properties that impact trust relationships, classified them into five categories and indicated that holistic trust management should concern part or all of them in different contexts and for different purposes. Based on a general IoT system model, we proposed ten objectives for holistic IoT trust management and indicated their supporting IoT layers by emphasizing vertical trust management is crucial for achieving trustworthy IoT. Applying the objectives as criteria, we survey the literature advances towards trust management by reviewing the existing work based on eight taxonomies and then comparing their versatility for trust management in order to find open issues, specify challenges and suggest future research trends. Furthermore, we proposed a research model – a holistic trust management framework of IoT that comprises not only modules for IoT inter-layer and cross-layer trust management, but also modules for offering practical and intelligent IoT services and applications based on trustworthy social trust relationships. Thus, cyber-physical social trust can be seamlessly integrated into IoT trust management.

References

Aggarwal G, Mishra N, Pinkas B. Secure computation of the median and other elements of specified ranks. J Cryptol 2010;23(3):373–401.

Agrawal S, Das ML. Internet of Things – a paradigm shift of future Internet applications. In: Proceedings of the Nirma University International Conference on Engineering (NUiCONE); 2011. p. 1–7.

Alam S, Chowdhury MMR, Noll J. Interoperability of security-enabled Internet of Things. Wirel Pers Commun 2011;61(3):567–86.

Amirbekyan A, Estivill-Castro V. Privacy preserving DBSCAN for vertically partitioned data. In: Proceedings of the IEEE international conference on intelligence and security informatics. ISI 2006, Springer Verlag Lecture Notes in Computer Science: vol. 3975; 2006. p.141–53.

Amirbekyan A, Estivill-Castro V. The privacy of *k-nn* retrieval for horizontal partitioned data-new methods and applications. In: Proceedings of the eighteenth conference on Australasian database: vol. 63; 2007a. p. 33–42.

Amirbekyan A., Estivill-Castro V. A new efficient privacy-preserving scalar product protocol. In: Proceedings of the sixth Australasian Data Mining Conference (AusDM 2007); 2007b. p. 209–14.

Amirbekyan A, Estivill-Castro V. Practical protocol for Yao's millionaires problem enables secure multi-party computation of metrics and efficient privacy-preserving k-NN for large data sets. Knowl Inf Syst 2009;21(3):327–63.

Architectural Reference Model for the IoT – (ARM). Introduction booklet. Retrieved from: ⟨http://www.iot-a.eu/public/public-documents/copy_of_d1.2/view⟩ [09.12.13].

Atallah M, Bykova M, Li J, Frikken K, Topkara M. Private collaborative forecasting and benchmarking. In: Proceedings of the 2004 ACM workshop on privacy in the electronic society; 2004. p. 103–14.

Atallah MJ, Du W. Secure multi-party computation geometry. Lecture notes in computer science, vol. 2125. Berlin: Springer; 165–79.

Atallah MJ, Kerschbaum F, Du W. Secure and private sequence comparisons. In: Proceedings of the 2003 ACM workshop on privacy in the electronic society; 2003. p. 39–44.

Bao F., Chen I. Trust management for the Internet of Things and its application to service composition. In: Proceedings of the IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM); 2012. p. 1–6.

Bao F., Chen I., Guo J. Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems. In: Proceedings of the IEEE eleventh International Symposium on Autonomous Decentralized Systems (ISADS); 2013. p. 1–7.

Bickson D., Dolev D., Bezman G., Pinkas B. Peer-to-peer secure multi-party numerical computation. In: Proceedings of the eighth international conference on peer-to-peer computing; 2008. p. 257–66.

Bunn P., Ostrovsky R. Secure two-party *k*-means clustering. In: Proceedings of the 14th ACM conference on Computer and Communications Security CCS07; 2007. p. 486–97.

Chen D, Chang G, Sun D, Li J, Jia J, Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. Comput Sci Inf Syst 2011;8(4):1207–28.

Chen, Y., Keynotes. In: Proceedings of the IEEE international conference on green computing and communications (GreenCom); 2012. p. xliv–xlviii.

Chiang YT, Wang DW, Liau CJ, Hsu TS. Secrecy of two-party secure computation. Lect Notes Comput Sci 2005;3654:114–23.

Daly EM, Haahr M. Social network analysis for information flow in disconnected delay-tolerant MANETs. IEEE Trans Mob Comput 2009;8(5):606–21.

de Leusse P, Periorellis P, Dimitrakos T, Nair SK. Self managed security cell, a security model for the Internet of Things and services. In: Proceedings of the first international conference on advances in future Internet; 2009. p. 47–52.

Deitos R, Kerschbaum F Improving practical performance on secure and private collaborative linear programming. In: Proceedings of the 20th international workshop on database and expert systems application; 2009. p. 122–6.

Dey AK. Understanding and using context. J Pers Ubiquitous Comput 2001;5(1):4–7.

Ding Y, Zhou X, Cheng Z, Lin F. A security differential game model for sensor networks in context of the Internet of Things. Wirel Pers Commun 2013;72:375–88.

Dolev S, Lahiani L, Yung M. Secret swarm unit: reactive *k*-secret sharing. Ad Hoc Netw 2012;10(7):1291–305.

Du, W., Atallah, M.J., Privacy preserving cooperative scientific computations. In: Proceedings of the 14th IEEE Computer Security Foundations Workshop CSFW 01; 2001a. p. 273–82.

Du W, Atallah MJ. Privacy preserving cooperative statistical analysis. Proc ACSAC 2001;01:102–10.

Du W, Zhan Z. A practical approach to solve secure multi-party computation problems,. In: Proceedings of the NSPW'02; 2002. p. 127–35.

Du W, Han YS, Chen S. Privacy preserving multivariate statistical analysis: linear regression and classification. In: Proceedings of the 4th SIAM international conference on data mining; 2004. p. 222–33.

Du WL A study of several specific secure two party computation problem [Ph.D. dissertation]. USA: Purdue University; 2001.

Erkin Z, Veugen T, Lagendijk RL. Generating private recommendations in a social trust network. In: Proceedings of the international conference on Computational Aspects of Social Networks (CASoN); 2011. p. 82–7.

Ester M, Kriegel HP, Sander J, Xu X. A density-based algorithm for discovering clusters in large spatial databases with noise,. In: Proceedings of the KDD 1996; 1996. p. 226–31.

Estivill-Castro V. Private representative-based clustering for vertically partitioned data. In: Baeza-Yates R, Marroquin J, Chavez E, (editors.), Proceedings of the

fifth Mexican international conference on computer science (ENC 04), SMCC; 2004. p. 160–7.
Evans D, Eyers DM. Efficient data tagging for managing privacy in the Internet of Things. In: Proceedings of the IEEE international conference on green computing and communications (GreenCom); 2012. p. 244–8.
Feng H, Fu W. Study of recent development about privacy and security of the Internet of Things. In: Proceedings of the 2010 International Conference on Web Information Systems and Mining (WISM): vol. 2; 2010. p. 91–5.
Fongen A. Identity management and integrity protection in the Internet of Things. In: Proceedings of the third international conference on Emerging Security Technologies (EST); 2012. p. 111–4.
Frikken, K., Atallah, M., Li, J., Hidden access control policies with hidden credentials, in Proc. of the 2004 ACM workshop on Privacy in the electronic society, (2004) pp.27-27.
Frikken K, Atallah M, Zhang C. Privacy-preserving credit checking. In: Proceedings of the 6th ACM conference on electronic commerce; 2005. p. 147–54.
Gessner D, Olivereau A, Segura AS, Serbanati A. Trustworthy infrastructure services for a secure and privacy-respecting Internet of Things. In: Proceedings of the IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom); 2012. p. 998–1003.
Goldreich O. Foundations of cryptography: volume, basic applications. Cambridge: Cambridge University Press; 2004.
Goldwasser S, Lindell Y. Secure multi-party computation without agreement. J Cryptol 2005;18(3):247–87.
Grandison T, Sloman M. A survey of trust in Internet applications. IEEE Commun Surv 2000;3(4):2–16.
Granjal J, Monteiro E, Silva JS. On the effectiveness of end-to-end security for internet-integrated sensing spplications. In: Proceedings of the IEEE international conference on green computing and communications (GreenCom); 2012. p. 87–93.
Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the Internet of Things. Math Comput Model0895-7177 2013, http://dx.doi.org/10.1016/j.mcm.2013.02.006.
He F, Wang T. Research and application of secure multi-party computation in several computational geometry problems. In: Proceedings of the International Conference on Industrial Control and Electronics Engineering (ICICEE); 2012. p. 1434–7.
He L, Huang L, Yang W, Xu R. A protocol for the secure two-party quantum scalar product. Phys Lett A 2012;376(16):1323–7.
Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K. Security challenges in the IP-based Internet of Things. Wirel Pers Commun 2011;61(3):527–42.
Herrmann F, Khadraoui D, Lanuel Y., Secure multi-party computation problem for distributed electronic contract management. In: Proceedings of the Information and Communication Technologies, ICTTA'06: vol. 1; 2006. p. 274–9.
Hu C, Zhang J, Wen Q. An identity-based personal location system with protected privacy in IOT. In: Proceedings of the 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT); 2011. p. 192–5.
Huang H, Zhong Hong H, Shi R. A secure scheme for data statistics. In: Proceedings of the International Conference on E-Business and E-Government (ICEE); 2010. pp. 1289–91.
Huang M, Lin B, Yang Y. Privacy-preserving path-inclusion protocol through oblivious automata. In: Proceedings of the IEEE international conference on Intelligent Control, Automatic Detection and High-End Equipment (ICADE); 2012. p. 128–32.
Huang X, Fu R, Chen B, Zhang T, Roscoe AW. User interactive Internet of things privacy preserved access control. In: Proceedings of the international conference for Internet technology and secured transactions; 2012. p. 597–602.
Huang X, Chen B, Markham A, Wang Q, Yan Z, Roscoe AW. Human interactive secure key and ID exchange protocols in body sensor networks. IET Inf Secur 2013;7(1):30–8.
Isa MAM, Mohamed NN, Hashim H, Adnan SFS, Manan JA, Mahmod R. A lightweight and secure TFTP protocol for smart environment. In: Proceedings of the IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE); 2012. p. 302–6.
Jangde P, Mishra DK. A secure multiparty computation solution to healthcare frauds and abuses. In: Proceedings of the second international conference on Intelligent Systems, Modelling and Simulation (ISMS); 2011. p. 139–42.
Jara AJ, Marin L, Skarmeta AFG, Singh D, Bakul G, Kim D. Mobility modeling and security validation of a mobility management scheme based on ECC for IP-based wireless sensor networks (6LoWPAN). In: Proceedings of the fifth international conference on innovative mobile and Internet services in ubiquitous computing (IMIS); 2011. p. 491–6.
Javed N, Wolf T. Automated sensor verification using outlier detection in the Internet of Things. In: Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW); 2012. p. 291–6.
Jun Wu, Lei Mei, Luo Zhong. Data security mechanism based on hierarchy analysis for Internet of Things. In: Proceedings of the 2011 international conference on innovative computing and cloud computing; 2011. p. 68–70.
Jurczyk P, Xiong L. Information sharing across private databases: secure union revisited. In: Proceedings of the IEEE third international conference on privacy, security, risk and trust (passat) and IEEE third international conference on social computing (SocialCom); 2011. p. 996–1003.
Kantarcioglu M, Clifton C. Privacy-preserving distributed mining of association rules on horizontally partitioned data. IEEE Trans Knowl Data Eng 2004;16(9):1026–37.
Kerschbaum F. Adapting privacy-preserving computation to the service provider model. In: Proceedings of the international conference on Computational Science and Engineering (CSE'09); 2009. p. 34–41.
Kerschbaum F. Secure and sustainable benchmarking in clouds. Bus Inf Syst Eng 2011;3(3):135–43.
Kerschbaum F, Deitos, RJ. Security against the business partner. In: Proceedings of the 2008 ACM workshop on Secure web services; 2008. p. 1–10.
Kerschbaum F, Oertel N, Chaves LWF. Privacy-preserving computation of benchmarks on item-level data using RFID. In: Proceedings of the third ACM conference on wireless network security; 2010. p. 105–10.
Khoo B., RFID as an enabler of the Internet of Things: issues of security and privacy. In: Proceedings of the 2011 international conference on Internet of Things and 4th international conference on cyber, physical and social computing (iThings/CPSCom); 2011. p. 709–12.
Kothmayr T, Schmitt C, Hu W, Brünig M, Carle G. DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Netw1570-8705 2013, . http://dx.doi.org/10.1016/j.adhoc.2013.05.003.
Krishnan R, Sundaram R. Policy-agile encrypted networks via secure function computation. In: Proceedings of the Military Communications Conference MILCOM 2010; 2010. p. 954–9.
Køien GM. Reflections on trust in devices: an informal survey of human trust in an Internet-of-Things context. Wirel Pers Commun 2011;61(3):495–510.
Li C, Wang G. A light-weight commodity integrity detection algorithm based on Chinese remainder theorem. In: Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2012. p. 1018–23.
Li D, Huang L, Yang W, Zhu Y, Luo Y, Li L, et al. A practical solution for privacy-preserving approximate convex hulls problem. In: Proceedings of the WRI international conference on Communications and Mobile Computing, CMC'09: vol. 3;(2009. p. 539–44.
Li L. Study on security architecture in the Internet of Things. In: Proceedings of the international conference on Measurement, Information and Control (MIC): vol. 1; 2012. p. 374–7.
Li M, Yu S, Cao N, Lou W. Privacy-preserving distributed profile matching in proximity-based mobile social networks. IEEE Transa Wirel Commun 2013;12(5):2024–33.
Liao X, Wen Q, Shi S. Distributed steganography. In: Proceedings of the seventh international conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP); 2011. p. 153–6.
Lin H, Pass R, Venkitasubramaniam M. A unified framework for concurrent security: universal composability from stand-alone non-malleability. In: Proceedings of the 41st Annual ACM symposium theory of computing; 2009. p. 179–88.
Liu J, Huang JZ, Luo J, Xiong L. Privacy preserving distributed DBSCAN clustering. In: Proceedings of the 2012 Joint EDBT/ICDT Workshops; 2012. p. 177–85.
Liu M, Zhang N. A solution to privacy-preserving two-party sign test on vertically partitioned data (P22NSTv) using data disguising techniques. In: Proceedings of the International Conference on Networking and Information Technology (ICNIT); 2010. p. 526–34.
Liu W, Luo S, Wang Y, Jiang Z. A protocol of secure multi-party multi-data ranking and its application in privacy preserving sequential pattern mining. In: Proceedings of the fourth international joint conference on Computational Sciences and Optimization (CSO11); 2011. p. 272–5.
Liu Y, Wang K. Trust control in heterogeneous networks for Internet of Thing. In: Proceedings of the International Conference on Computer Application and System Modeling (ICCASM); 2010. p. 632–6.
Liu Y, Chen Z, Xia F, Lv X, Bu F. A trust model based on service classification in mobile services,. In: Proceedings of the IEEE/ACM international conference on cyber, physical and social computing (CPSCom); 2010. p. 572–7.
Luo W, Li X. A study of secure multi-party elementary function computation protocols. In: Proceedings of the 3rd international conference on information security; 2004. p. 5–12.
Luo Y, Shi L, Zhang C, Zhang J. Privacy-preserving protocols for string matching,. In: Proceedings of the 4th international conference on Network and System Security (NSS); 2010. p. 481–5.
Luo Y, Zhang C, Shi L, Cheng W. A security solution to the points–hyperspace inclusion problem. In: Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT): vol. 8; 2010. p. 288–91.
Melchor CA, Ait-Salem B, Gaborit P. A collusion-resistant distributed scalar product protocol with application to privacy-preserving computation of trust. In: Proceedings of the eighth IEEE international symposium on network computing and applications; 2009. p. 140–7.
Mishra DK, Chandwani M. Anonymity enabled secure multi-party computation for indian BPO. In: Proceedings of the IEEE region 10 conference TENCON 2007; 2007. p. 1–4.
Mishra DK, Chandwani M. A zero-hacking protocol for secure multiparty computation using multiple TTP. In: Proceedings of the IEEE region 10 conference TENCON 2008; 2008. p. 1–6.
Mishra DK, Koria N., Kapoor N, Bahety R. Malicious computation prevention protocol for secure multi-party computation,. In: Proceedings of the IEEE region 10 conference TENCON; 2009. p. 1–6.
Mishra DK, Pathak R, Joshi S, Ludhiyani A. Secure multi-party computation for statistical computations using virtual parties on a token ring network. In: Proceedings of the seventh international conference on Wireless And Optical Communications Networks (WOCN); 2010. p. 1–6.
Ning H, Liu H, Yang LT. Cyberentity security in the Internet of Things. Computer 2013;46(4):46–53.

Nitti M, Girau R, Atzori L, Iera A, Morabito G. A subjective model for trustworthiness evaluation in the social Internet of Things. In: Proceedings of the IEEE 23rd international symposium on Personal Indoor and Mobile Radio Communications (PIMRC); 2012. p. 18–23.
Pang L, Sun M, Luo S, Wang B, Xin Yang. Full privacy preserving electronic voting scheme. J China Univ Posts Telecommun 2012;19(4):86–93.
Pass R. Bounded-concurrent secure multi-party computation with a dishonest majority. In: Proceedings of the thirty-sixth annual ACM symposium on theory of computing; 2004. p. 232–41.
Pathak R, Joshi S., SMC protocol for privacy preserving in banking computations along with security analysis. In: Proceedings of the first Asian Himalayas International Conference on Internet (AH-ICI 2009; 2009. p. 1–5.
Petroulakis NE, Askoxylakis IG, Tryfonas T. Life-logging in smart environments: Challenges and security threats. In: Proceedings of the 2012 IEEE International Conference on Communications (ICC); 2012. p. 5680–4.
Petroulakis NE, Tragos EZ, Fragkiadakis AG, Spanoudakis G. A lightweight framework for secure life-logging in smart environments. Inf Secur Techn Rep 2013;17(3):58–70.
Pibernik R, Zhang Y, Kerschbaum F, Schröpfer A. Secure collaborative supply chain planning and inverse optimization – the JELS model. Eur J Oper Res 2011; 208(1):75–85.
Portelo J, Raj B, Trancoso I. Attacking a privacy preserving music matching algorithm. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); 2012. p. 1821–4.
Raza S, Wallgren L, Voigt T. SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw1570-8705 2013, http://dx.doi.org/10.1016/j.adhoc.2013.04.014.
Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. Comput Netw1389-1286 2013, http://dx.doi.org/10.1016/j.comnet.2012.12.018.
Sanil AP, Karr AF, Lin X, Reiter JP. Privacy preserving regression modelling via distributed computation. In: Proceedings of the tenth ACM SIGKDD international conference on knowledge discovery and data mining; 2004. p. 677–82.
Sarma AC, Girão J. Identities in the future Internet of Things. Wirel Pers Commun 2009;49(3):353–63.
Shaikh Z, Mishra DK. A study on secure multiparty computation problems and their relevance. In: Proceedings of the second international conference on Computational Intelligence, Modelling and Simulation (CIMSiM); 2010. p. 95–9.
Shaneck M, Kim Y, Kumar V. Privacy preserving nearest neighbor search. In: Proceedings of the sixth IEEE international workshop on data mining; 2006. p. 541–5.
Shen Y, Han J, Shan H. The research of privacy-preserving clustering algorithm. In: Proceedings of the third international symposium on Intelligent Information Technology and Security Informatics (IITSI); 2010. p. 324–7.
Sheng Z, Yang S, Yu Y, Vasilakos A, Mccann J, Leung K. A survey on the IETF protocol suite for the Internet-of-Things: standards, challenges and opportunities. IEEE Wirel Commun Mag 2013;20(6):91–8 http://dx.doi.org/10.1109/MWC.2013.6704479.
Sheng Z, Wang H, Gu D, Vasilakos AV. Surfing the internet-of-things: a restful approach to enable easy access to wireless sensor networks, IEEE Sensors Journal Special Issue on Internet of Things: architecture. Protoc Serv 2014 (in press-b).
Sicari S, Coen-Porisini A, Riggio R. DARE: evaluating Data Accurancy using node REputation. Comput Netw, Elsevier 2013;57(15):3098–111.
Suo H, Wan J, Zou C, Liu J. Security in the Internet of things: a review. In: Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE): vol. 3; 2012. p. 648–51.
Tang C, Shi G, Yao Z. Secure multi-party computation protocol for sequencing problem. Sci China Inf Sci 2011;54(8):1654–62.
Thoma C, Cui T, Franchetti F. Secure multiparty computation based privacy preserving smart metering system. In: Proceedings of the North American Power Symposium (NAPS); 2012. p. 1–6.
Tong L, Luo W, Fu Z, Peng C. Privacy-preserving segment-ellipse intersect-determination protocol. In: Proceedings of the 2nd international conference on e-Business and Information System Security (EBISS); 2010. p. 1–5.
Ukil A, Sen J, Koilakonda S. Embedded security for Internet of Things. In: Proceedings of the 2nd National Conference on Emerging Trends and Applications in Computer Science (NCETACS); 2011. p. 1–6.
Vaidya J, Clifton C, Kantarcioglu M, Scott Patterson A. Privacy-preserving decision trees over vertically partitioned data. ACM Trans Knowl Discov Data (TKDD) 2008;2(3) (article No. 14).
Vaidya, JS, Clifton, C. Privacy preserving association rule mining in vertically partitioned data. In: Proceedings of the eighth ACM SIGKDD international conference on knowledge discovery and data mining; 2002. p. 639–44.
Wan, L, Ng, WK, Han, S, Lee, VCS., Privacy-preservation for gradient descent methods. In: Proceedings of the 13th ACM International conference on knowledge discovery and data dining SIGKDD; 2007. p. 775–83.
Wang P. Research on privacy preserving association rule mining a survey. In: Proceedings of the 2nd IEEE International Conference on Information Management and Engineering (ICIME); 2010. p. 194–198.
Wang Q, Zhang Y. A convex hull algorithm for planar point set based on privacy protecting. In: Proceedings of the first international workshop on Education Technology and Computer Science, ETCS'09: vol. 3; 2009. p. 434–7.
Wang Q, Luo Y, Huang L. Privacy-preserving protocols for finding the convex hulls. In: Proceedings of the third international conference on Availability, Reliability and Security, ARES 08; 2008. p. 727–32.
Wang R, Wang X, Li Z, Tang H, Reiter MK., Dong Z.Privacy-preserving genomic computation through program specialization. In: Proceedings of the 16th ACM conference on computer and communications security; 2009. p. 338–47.
Wang T, Luo W. Design and analysis of private-preserving dot product protocol. In: Proceedings of the international conference on electronic computer technology; 2009. p. 531–5.
Wang Y, Ishwar P. On unconditionally secure multi-party sampling from scratch1. In: Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT); 2011. p. 1782–6.
Wee H. Black-box, round-efficient secure computation via non-malleability amplification. In: Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS); 2010. p. 531–40.
Wu, F, Zhong, H, Shi, R, Huang, H., Secure two-party computation of the quadratic function's extreme minimal value. In: Proceedings of the 9th international conference on Fuzzy Systems and Knowledge Discovery (FSKD); 2012. p. 2975–8.
Xiong H, Zhang EP, Chim TW, Yiu SM, Hui LCK. Weighted average problem revisited under hybrid and malicious model. In: Proceedings of the 8th International Conference on Computing Technology and Information Management (ICCM): vol. 2; 2012. p. 677–82.
Xiong L, Zhou X, Liu W. Research on the architecture of trusted security system based on the Internet of Things,. In: Proceedings of the International Conference on Intelligent Computation Technology and Automation (ICICTA): vol. 2; 2011. p.1172–5.
Xu F, Zeng S, Luo S, Wang C, Xin Y, Guo Y. Research on secure scalar product protocol and its' application. In: Proceedings of the 6th international conference on Wireless Communications Networking and Mobile Computing (WiCOM); 2010. p. 1–4.
Yan Q, Deng R, Yan Z, Li Y, Li T. Pseudonym-based RFID discovery service to mitigate unauthorized tracking in supply chain management. Proc ISDPE 2010;10: 21–6.
Yan Z, Holtmanns S. Trust modeling and management: from social trust to digital trust. In: Subramanian R, editor. Computer Security, privacy and politics: current issues, challenges and solutions. IGI Global; 2008. p. 290–323.
Yan Z, Prehofer C. Autonomic trust management for a component based software system. IEEE Trans Dependable Secure Comput 2011;8(6):810–23.
Yan Z, Kantola R, P. Zhang, A research model for human–computer trust interaction. In: Proceedings of the IEEE TrustCom 2011; 2011. p. 274–81.
Yang Y, Deng RH, Bao F. Practical private data matching deterrent to spoofing attacks. In: Proceedings of the 15th ACM international conference on information and knowledge management; 2006. p. 852–3.
Yao AC. Protocols for secure computations. In: Proceedings of the 23rd Annual IEEE symposium on foundations of computer science; 1982. p. 160–4.
Yao D, Frikken KB, Atallah MJ, Tamassia R. Private information: to reveal or not to reveal. ACM Trans Inf Syst Secur (TISSEC) 2008;12(1):1–27.
Ye Y, Huang L, Yang W, Zhou Z. A secure protocol for determining the meeting points of two intersected circles. In: Proceedings of the international conference on information technology and computer science: vol. 2; 2009. p. 40–4.
Ye Y, Huang L, Yang W, Zhou Z. Efficient secure protocols to determine whether a point is inside a convex hull. In: Proceedings of the international symposium on Information Engineering and Electronic Commerce (IEEC'09); 2009. p. 100–5.
Zhan J, Matwin S, Chang L. Privacy-preserving collaborative association rule mining. J Netw Comput Appl 2007;30(3):1216–27.
Zhang F, Zhao G. A more well-founded security proof of the privacy-preserving distributed mining of association rules protocols. In: Proceedings of the first international workshop on model driven service engineering and data quality and security; 2009. p. 25–8.
Zhang G, Tian J. An extended role based access control model for the Internet of Things. In: Proceedings of the 2010 International Conference on Information Networking and Automation (ICINA): vol. 1; 2010. p. 319–23.
Zheng Q, Luo S, Xin Y, Yang Y. Protocol for privacy-preserving set pattern matching. In: Proceedings of the International conference on Multimedia Information Networking and Security, MINES'09: vol. 1; 2009. p. 168–72.
Zhong H, Huang H, Shi, R. Two protocols for computing the sub-polygon's areas divided by a line. In: Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE): vol. 1; 2010. p. 83–6.
Zhou Q, Gui F, Xiao D, Tang Y., Trusted architecture for farmland wireless sensor networks. In: Proceedings of the IEEE 4th international conference on cloud computing technology and science (CloudCom); 2012. p. 782–7.
Zhu Y, Huang L, Yang W., Chen Z, Li L, Yu Z, et al. Privacy-preserving practical convex hulls protocol. In: Proceedings of the Japan–China joint workshop on Frontier of Computer Science and Technology, FCST'08; 2008. p. 10–6.
Zhu Y, Huang L, Yang W, Li D, Luo Y, Dong F. Three new approaches to privacy-preserving add to multiply protocol and its application. In: Proceedings of the second international Workshop on Knowledge Discovery and Data Mining, WKDD 2009; 2009a. p. 554–8.
Zhu Y, Huang L, Yang W; Li D, Li L, Luo Y, et al. Privacy-preserving approximate convex hulls protocol. In: Proceedings of the First international workshop on Education Technology and Computer Science, ETCS'09: vol. 2; 2009b. p. 208–14.