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.