# A Review on Trust Evaluation for Internet of Things

Pu Wang
The State Key Lab of Integrated Services Networks
School of Cyber Engineering
Xidian University
Xi'an China
wangpulhy@163.com

Peng Zhang
The State Key Lab of Integrated Services Networks
School of Cyber Engineering
Xidian University
Xi'an China
pengzhangzhang@gmail.com

## ABSTRACT
The Internet of Things (IoT) has been widely used in various application domains to provide advanced and intelligent services for human beings, such as environmental monitoring, intrusion detection. In IoT networks, senor nodes are normally low capability devices that are vulnerable for numerous security attacks. In order to address this issue, many security schemes and solutions have been proposed in recent years. The security and privacy requirements including privacy and trust management among users and things have played a fundamental role to detect malicious nodes in IoT, thus to better promote the applications of IoT. In this paper, we focus on the security problems in IoT networks, and provide a survey on trust evaluation towards trustworthy IoT with specified criteria. Moreover, we present research challenges of trust evaluation in IoT and provide future research direction in this area.

## CCS Concepts
**•General and reference Surveys and overviews • General and reference • Evaluation**

## Keywords
Internet of Things (IoT); Security; Trust evaluation; Trust management; Privacy-preserving.

## 1. INTRODUCTION
Throughout the past decade, with the emergence of various wireless communication technologies (e.g., RFID, Wi-Fi, ZigBee, and IEEE 802.15.x), the Internet of Things (IoT) has gradually become more popular in our daily lives. The 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 being. The interconnected "things", such as sensors or mobile devices sense, monitor and collect 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. The IoT forms a closed loop that includes context sensing, information processing and feedback control to the physical world, together with building the information bridge between things and things, things and people, and people and people. The rapid development of the IoT brings great changes to our traditional thinking of the Internet security.

In an IoT network, a resource-constrained sensor node as a part of the Internet is able to establish secure end-to-end communications with external nodes, which do not belong to the same network. However, the node is limited in terms of computing power and/or radio range, the setup of any secure channel could be either unaffordable or prohibitively expensive, which has envisaged new security challenges to IoT networks.

Trust management (TM) plays an important role in the IoT for reliable data fusion and mining, qualified services with context-aware intelligence, and enhanced user privacy and information security [20]. Trust is a complicated concept with regard to confidence, belief, and expectation on the reliability, integrity, security, dependability, ability, and other characters of an entity. It is a relationship between a trustor and a trustee and has some basic characteristics: subjective, dynamic, context-aware and so on [24].

In this paper, we conduct a literature review towards trustworthy IoT in order to point out a number of open issues and challenges and suggest future research trends related to trust management.

The rest of the paper is organized as follows. Section II describes the IoT and its architecture, and also introduces the criteria of assessment on trust evaluation in IoT. An overview of literature about trust evaluation in IoT is presented in Section III. Section IV specifies a number of trust related open research issues and discusses research challenges and future trends. Conclusion is given in Section V.

## 2. II. CONCEPT AND CRITERIA ON TRUST EVALUATION

### 2.1 Basic Concepts
**Trust:** The concept of trust has been studied in disciplines ranging from economics to psychology, from sociology to medicine, and to information and computer science. Herein, we take the natural definition of ''trust''. Trust is the confidence, belief, and expectation regarding the reliability, integrity, ability, and other characteristics of an entity, and is a substantive evaluation of subjective probability of another entity will perform a behavior of a specific. This assessment is observed before actual behaviors, which is context-dependent [19]. 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 [20]. Trust can be classified into two types according to different information

MOBIMEDIA 2016, June 18-19, Xi'an, People's Republic of China

DOI 10.4108/eai.18-6-2016.2264183

sources: one is direct trust; the other is indirect trust [21, 22]. Direct trust is a kind of independent trust of the node's credibility on the other nodes. Indirect trust is some node trust other nodes in some degree, trust the source of information is information from other nodes, and the information can be in the form of their own direct trust and can also be the information they collected from other node.

Although the richness of the concept of trust, we can still see that trust is subjective and measurable. Different people hold different opinions on trust value on the same entity even in the same situation. And the trust value represents the different degrees of trust that an entity may have in another and is a quantified expression of trust.

**Trust management:** trust management is the technology to collect information required to make a trust relationship decision; evaluate the criteria related to the trust relationship; monitor and reevaluate existing trust relationships; as well as ensure the dynamically changed trust relationships and automate the above process. It plays as a useful means to control and maintain trust in digital systems. Transforming from a social concept of trust to a digital concept, trust modeling and management help in designing and implementing a trustworthy digital system, especially in mobile and distributed computing. Nowadays, trust management is emerging as a promising technology to facilitate collaboration among entities in an environment where traditional security paradigms cannot be enforced due to lack of centralized control and incomplete knowledge of the environment.

## 2.2 Internet of Things

The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

A British visionary, Kevin Ashton, first documented the term “Internet of Things” in 1999. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications [1]. The interconnection of these embedded devices (including smart objects) is expected to usher in nearly all fields, while also enabling advanced applications like Smart Grid [2].

Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, and automobiles with built-in sensors, or field operation devices that assist fire fighters in search and rescue. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. A foundational technology for the IoT is RFID technology, which allows devices to transmit identification information to a reader through wireless communication. With RFID readers, people can identify, track, and monitor any objects attached with RFID tags automatically. Another foundational technology is wireless sensor networks (WSNs) consisting of spatially distributed autonomous sensors to monitor physical or environmental conditions and to cooperatively pass their data to a main location. The advance of RFID and WSNs significantly contribute to the development of the IoT. In addition, many other Internet technologies and devices such as smart phones, social networks and cloud computing have been also used to construct an extensive network for supporting IoT [24]. The technologies associated with IoT are illustrated in Fig. 1.

Moreover, the IoT is expected to generate large amounts of data from diverse locations that is aggregated very quickly, thereby it is important to increase the need to better index, store and process such data [3][4].

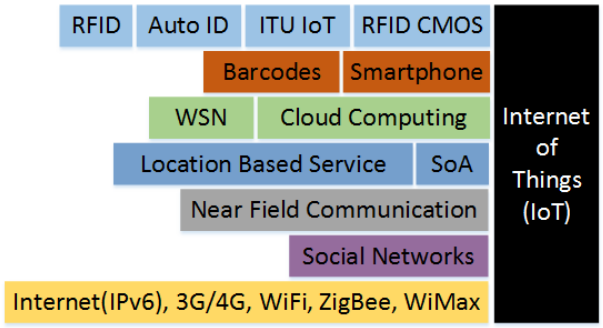


**Fig. 1. Technologies associated with IoT**

## 2.3 IoT Architecture

Generally, the IoT system is divided into three layers: perception layer, network layer and application layer [20]. The perception layer is mainly about information collection, it perceives physical environments and human social life, object perception and object control. Network layer transforms and processes data in order to provide ubiquitous access environment for perception layer and application layer can load its related businesses. Application layer offers all sorts of context-aware services in a pervasive manner and realizes intelligent computation and the allocation of resources. A trustworthy IoT system needs not only reliable cooperation among layers, but also the performance of each system layer and the whole system with regard to privacy and security. The Architecture of IoT is shown in Fig.2.

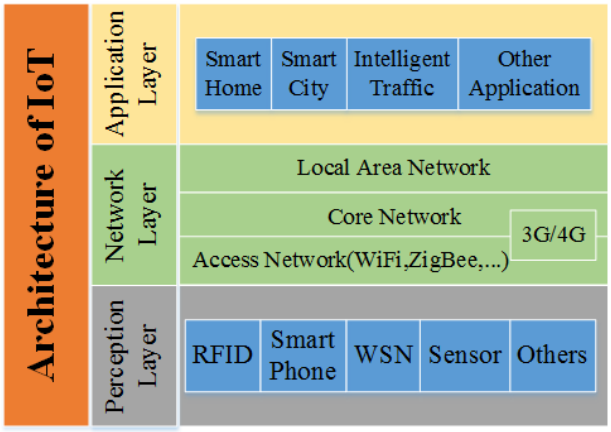


**Fig. 2. Architecture of IoT**

The IoT must ensure the security of whole system among all layers. The Perception layer includes RFID, WSNs security and any others security issue. The Network Layer includes access network security, core network security and local area network security, such as 3G/4G access network security, WiFi security, ZigBee network security. The Application Layer security is application specific security that has to be addressed in the application layer.

## 2.4 Criteria on Trust Evaluation in IoT

To ensure the trustworthy in the IoT, we propose the following criteria on trust management in the IoT based on our literature study.

- *Trustworthiness* (*T*): A trust evaluation mechanism in the IoT should be robust to overcome various potential attacks. The research should prevent the IoT systems from various attacks, for example, DoS, node control, counterfeit original attack and so on.
- *Adaptability* (*Ad*): A trust evaluation mechanism in the IoT should be adaptive to context changes with dynamic support. In the IoT application scene, the relationship is dynamic changing between nodes, such as nodes joining and leaving a system in very short time.
- *Usability* (*Us*): A trust evaluation mechanism in the IoT should be usable for users with regard to user-device interaction in order to provide more intelligent services interacting with humans.
- *Privacy* (*P*): A trust evaluation mechanism in the IoT should preserve user privacy when user data is collected for trust evaluation. It should allow legitimate users to preserve their privacy to the maximum extent.
- *Accuracy* (*Ac*): A trust evaluation mechanism in the IoT should be accurate to evaluate trust/reputation.
- *Efficiency* (*E*): A trust evaluation mechanism in the IoT should be efficient to dynamically manage trust relationships in the IoT systems in order to ensure network layer security.
- *Uniformity* (*Un*): A trust evaluation mechanism in the IoT should be uniform for users' voting with trustworthy credibility to evaluate objects' trust values.
- *Comprehension* (*C*): A trust evaluation mechanism in the IoT should support various trust influencing factors to achieve accurate evaluation.
- *Generality* (*G*): A trust evaluation mechanism in the IoT should be suitable for various IoT systems and services that can be commonly used in different application scenarios.

# 3. CURRENT LITERATURE ABOUT TRUST EVALUATION IN IOT

## 3.1 Literature review

In this section, we review the literature in past five years towards trustworthy IoT from the following databases: IEEE Explorer, ACM library, Springer library, Engineering Village and Web of Science TM based on the key words: trust, trust evaluation, trust management, trust model, reputation generation, reputation assessment, reputation evaluation, reputation system and Internet of Things.

Babar et al. [5] described a cube structure model of security and threat taxonomy for the IoT networks and applications. This model has three dimensions: security, trust and privacy, which clearly shows the intersection among the dimensions. It presents a new entrance to solve potential security issues in the IoT systems.

Dong et al. [6] proposed a trust and reputation model TRM-IoT to enforce cooperation among nodes based on their behaviors in a wireless sensor network. Meanwhile, the paper proposed a generalized and unified mechanism to address the trust and reputation issue. In the mechanism, each node develops a direct reputation for each other node by making direct observations and indirect reputation. These two kinds of reputations are used together to help a node evaluate the trustworthiness of other sensor nodes, detect malicious nodes, and assist decision-making within the wireless network. However, their trust management model only considered a specific IoT environment consisting of only wireless sensors with QoS trust metrics like packet forwarding/delivery ratio and energy consumption, and did not take into account social relationship that is important in social IoT systems. This work proposed a model for achieving the T, Ac, E and G, but others not considered.

Bao et al. [7] proposed a dynamic trust management protocol to manage misbehaving nodes whose status or behavior may change dynamically in the IoT systems, and it is capable of adaptively adjusting the best trust parameter setting in response to dynamically changing environments to maximize application performance and takes social relationships in account. But this paper only considers increasing hostility over time as instance of changing environment conditions and is short of testing the dynamic trust protocol's resiliency toward a multitude of changing environment condition. The protocol supports the characteristic of Ad and Us.

An et al. [8] proposed a new cognitive model for social relations of mobile nodes in the IoT, and defined the location factor, interconnection factor, service evaluation factor and feedback aggregation factor to solve the shortcomings in existing quantitative models. The proposed cognitive model has better dynamic adaptability and validity. This paper considers the aspects of Ad, Us and E, but not others.

Saied et al. [9] designed a context-aware and multi-service trust management system fitting the new requirements of the IoT and effectively fine-tunes nodes trust levels, even in presence of erroneous or malicious witnesses. Thus it only meets requirements of T and Ad.

Gusmeroli et al. [10] described a capability based access control system (CapBAC) for managing access control to service and information. The proposed mechanism supports rights delegation and a more sophisticated access control customization. The paper considers only access control.

Veltri et al. [11] proposed a novel centralized approach to efficiently distribute and manage a group key in generic ad hoc networks and the IoT, while reducing the computational overhead and network traffic due to group membership changes caused by users' joins and leaves. The proposed protocol considers both the cases in which a member leaves the group in a predictable manner or in an unpredictable manner, and split time into time-intervals to optimize the number of exchanged messages for handing group member changes and group key rekeying. So the Key Distribution Center (KDC) can handle all membership changes that occur in the same interval. Only in case of key revocation events explicit communication between KDC and group member is required. This system supports Ad and E.

Han et al. [12] presented a data driven quantitative trust model, which is suitable to provide timely, neutral and quantitative trust evaluation of foods in the Internet of agricultural things (AIoT). A Bayesian network is used to combine factors and evaluate the final trust of the product. However it doesn't consider the data veracity that could negatively affect this model and cannot clean the data before evaluation. This model shows its advantages in T, Ad and C.

Chen et al. [13] designed and analyzed an adaptive and survivable trust management protocol for user-centric IoT systems. In this protocol, users performs trust evaluation based on its past direct user satisfaction experiences and trust feedbacks, selected by a distributed collaborating filter. So each node can adaptively select its best trust parameter to minimize convergence time and trust bias. But the paper does not consider more sophisticated attack behaviors,. This protocol supports Ad, Us and Ac.

Liu et al. [14] presented two certificate-less remote authentication protocols to preserve the privacy of potential WBAN users. When the users access a network medical service through WBANs terminals, the protocols apply a novel certificate-less signature scheme as a cryptographic primitive. With the signature scheme, the private information and the real identities can be prevented from illegal user. So it satisfies the item P. Meanwhile, it is efficient to meet the needs of WBANs.

Kang et al. [15] proposed an interactive trust model (ITM) based on interaction between application market and end users. In this model, application trustworthiness (AT) is quantitatively evaluated by the similarity through the similarity between the application's behavior and behavior expected by the user, and by using the evaluation vector and feedback vector. The behavior-based detecting agent on users' device gives strong evidence about what applications have done to your privacy and security issues. This model fulfills Us, Un and C.

Liu et al. [16] proposed a node behavior detection-based trust evaluation model for data aggregation in Internet of Things. The model incorporates a trust record queue by recording trust information of nodes and malicious detection that captures the nature of trust evaluation. The communication cost between the nodes and storage overhead can be largely reduced to support the item of high efficiency. Similarly, the secure data aggregation scheme can satisfy most application scenarios of IoT.

Nitti et al. [17] defined two models for trustworthiness management starting from the solutions proposed for P2P and social networks: The subjective model and the objective mode. In the subjective model, each node computes the trustworthiness of its friends on the basis of its own experience and on the opinion of the friends in common. In the objective model, the information about each node is distributed and stored by making use of a distributed hash table structure. The subjective and objective model support robust trust establishment and trust social relationship to isolate almost any malicious nodes. So it satisfies the characteristic of trustworthiness.

Zhu et al. [18] described a CC-WSN (cloud computing and wireless sensor network) integration paradigm. In this paradigm, sensor network provider (SNPs) provides the sensory data collected by the deployed WSNs to the cloud service providers (CSPs). CSPs utilize the powerful cloud to store and process the sensory data and then further on demand offer the processed data to the cloud service users (CSUs). Then the paper explored an authentication as well as trust and reputation calculation and management of CSPs and SNPS, and proposes a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration to help CSU choose accurately desirable CSP and assisting CSP in selecting appropriate SNP. The whole system applying this paradigm is trustworthy.

## 3.2 Comparison of These Articles Based on Criteria

In this section, we present the comparison among all literatures for trust management by referring to the above described nine criteria, as shown in Table 1.

**Table 1. Comparison of Existing Work Based on the Proposed Review Criteria**

| Paper | T | Ad | Us | P | Ac | E | Un | C | G |
|---|---|---|---|---|---|---|---|---|---|
| [6] | Y | | | | Y | Y | | | Y |
| [7] | | Y | Y | | | | | | |
| [8] | | Y | Y | | | Y | | | |
| [9] | Y | Y | | | | | | | |
| [10] | | | | | | | | | |
| [11] | | Y | | | | Y | | | |
| [12] | | Y | | | Y | | | Y | |
| [13] | | Y | Y | | Y | | | | |
| [14] | | | | Y | | Y | | | |
| [15] | | | Y | | | | Y | Y | |
| [16] | | | | | | Y | | | Y |
| [17] | Y | | | | | | | | |
| [18] | Y | | | | Y | | | | |

# 4. PROBLEM OF CURRENT RESEARCH AND FUTURE RESEARCH TRENDS

## 4.1 Problem of Current Research

In the IoT networks, more attention should be paid to the security of the entire system, rather than just the security of a single IoT layer or a single piece of software. It is crucial to keep the entire IoT system as an integrated entity and figure out how to construct an integrated security solution, deal with all kinds of security issues, and securely compute and process heterogeneous data coming from different sources.

Based on above review in Section 3, we find out that most of the papers just focus on the security of a single piece of software or a single IoT layer. Only a few schemes meet the requirement of generality while others are designed for more particular situations. On the other hand, with various security requirements of numerous application scenarios, it is unlikely to come up with a single security architecture to handle all cases. It is more likely to provide different solutions to solve the corresponding security problem. However, it is very important to abstract all similarities of all IoT applications and design an abstract security framework to provide the basic security property for the IoT applications.

Last but not least, very few papers consider privacy and anonymity even though they play an important role in the IoT.

## 4.2 Challenges and Future Research Trends

The rapid growth of the IoT requires that customized trust, privacy and security should be insured. There are still plenty of challenges of the IoT, especially related to security, privacy and trust management. In order to address theses challenges, we propose some research trends of trust management in the IoT as follows:

1) Lightweight and efficient security solutions.

Devices in the IoT networks are normally tiny wireless devices relatively easier to be captured and cloned. Thus, study on lightweight and efficient security solutions would be one

important future research direction [25]. The security solutions should satisfy the designated requirements of the IoT in specific application context. It is necessary to study existing lightweight solution for the IoT in aspects of access control, key management, and trust authentication., which may provide an overall abstract framework for IoT security.

2) Privacy-preserving technology.

As a matter of fact, it is essential for enhancing public confidence and promoting novel IoT systems to satisfy the privacy requirement [26]. It is an important research area, including defining a model and its privacy policies to deal with dynamic environment and scalability in various IoT scenarios.

3) Mobile security in IoT

In many IoT systems, mobile devices often move from one location to another location. It is important to provide rapid handling of trust management, authentication and privacy protection. For example, in a mobile RFID system, not only the security and privacy of readers and tags, but also issues such as reader corruption, tags corruption, multiple readers and mutual authenticated key exchange protocols should be considered. Based on the characteristics of device mobility and network variability, it is important to study secure and scalable mobility trust management schemes that can support secure location update and solve the possible security and privacy vulnerabilities.

## 5. CONCLUSIONS

In this paper, we defined the unified review criteria on trust Evaluation in the IoT. We provided a literature study on trust management in IoT by comparing a number of trust management schemes. The study showed that most schemes focused on specific application scenarios, which are not applicable in general environments. Although there are a lot of researches about trust management in the IoT, it still lacks of a fully suitable distributed and dynamic solution for the flexible and scalable IoT context. Based on the analysis and comparison, we discussed the challenge and security issue of IoT and gave some future research trends.

## 6. ACKNOWLEDGMENTS

This work is sponsored by NSFC with grant number U1536202, 111 project (Grant No. B08038), the PhD grant (JY0300130104) of Chinese Educational Ministry, the Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016ZDJC-06), and Aalto University.

## 7. REFERENCES

[1] Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S. and Boyle, D. 2014. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Elsevier, 2014, ISBN 978-0-12-407684-6.

[2] Monnier, O. 2013. A smarter grid with the Internet of Things. Texas Instruments, 2013.

[3] Violino, B. 2014. The 'Internet of things' will mean really, really big data. InfoWorld. Retrieved 9 July 2014.

[4] Hogan, M. 2014. The 'The Internet of Things Database' Data Management Requirements. Scale DB. Retrieved 15 July 2014.

[5] Babar, S., Mahalle, P., Stango, A., Prasad, N. and Prasad, R. 2010. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In *Recent Trends in Network Security and Applications*, N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai, Eds. Springer, Berlin, Heidelberg, 420-429. DOI= 10.1007/978-3-642-14478-3_42.

[6] Chen, D., Chang, G. R., Sun, D. W., Li, J. J., Jia. J., and Wang. X. W. 2010. TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things. *Computer Science and Information Systems*. 8 (October 2010), 1207-28, DOI= https://eudml.org/doc/253429.

[7] Bao, F. and Chen, I. R. 2012. Dynamic trust management for internet of things applications. In *Proceedings of the 2012 International Workshop on Self-aware Internet of Things*. (San Jose, California, USA, September 17-21, 2012). ACM New York, NY, USA, 1-6. DOI= 10.1145/2378023.2378025.

[8] An, J., Gui, X. L., Zhang, W. D., Jiang, J. H and Yang, J. W. 2013. Research on social relations cognitive model of mobile nodes in Internet of Things. *Journal of Network and Computer Applications*. 36, 2 (March 2013), 799-810. DOI= 10.1016/j.jnca.2012.12.004.

[9] Saied, Y. B., Olivereau, A., Zeghlache, D. and Laurent, M. 2013. Trust management system designs for the Internet of Things: A context-aware and multi-service approach. *Computers & Security*. 39, B (November 2013), 351-365. DOI= 10.1016/j.cose.2013.09.001.

[10] Gusmeroli, S., Piccione, S. and Rotondi, D. 2013. A capability-based security approach to manage access control in the Internet of Things. *Mathematical and Computer Modelling*. 58, 5-6 (September 2013), 1189-1205. DOI= 10.1016/j.mcm.2013.02.006.

[11] Veltri, L., Cirani, S., Busanelli, S. and Ferrari, G. 2013. A novel batch-based group key management protocol applied to the Internet of Things. *Ad Hoc Networks*. 11, 8 (November 2013), 2724-2737. DOI= 10.1016/j.adhoc.2013.05.009.

[12] Han, W. L., Gu, Y., Zhang, Y. and Zheng, L. Data driven quantitative trust model for the Internet of Agricultural Things. 2014. In *2014 International Conference on the Internet of Things*. (Cambridge, MA, United states, October 6-8, 2014), IOT 2014, IEEE, Washington, DC, 31-36. DOI= 10.1109/IOT.2014.7030111.

[13] Chen, I. R., Guo, J. and Bao, F. 2014. Trust management for service composition in SOA-based IoT systems. In *Wireless Communications and Networking Conference* (Istanbul, the Republic of Turkey, April 6-9, 2014), WCNC 2014, IEEE, Washington, DC 3444-3449. DOI= 10.1109/WCNC.2014.6953138.

[14] Liu, J. W., Zhang, Z. H., Chen, X. F. and Kwak, K. S. 2013. Certificateless Remote Anonymous Authentication Schemes for WirelessBody Area Networks. *IEEE Transactions on Parallel and Distributed Systems*. 25, 2 (May 2013), 332-342. DOI= 10.1109/TPDS.2013.145.

[15] Kang, K., Pang, Z. B., Xu, L. D., Ma, L. Y. and Wang, C. 2014. An interactive trust model for application market of the Internet of Things. *IEEE Transactions on Industrial Informatics*. 10, 2 (February 2014), 1516-1526. DOI= 10.1109/TII.2014.2306799.

[16] Liu, Y. B., Gong, X. H. and Xing, C. C. 2014. A novel trust-based secure data aggregation for Internet of Things. In *9th International Conference on Computer Science and Education* (Vancouver, BC, Canada, August 22-24, 2014), ICCCSE'14, IEEE, Washington, DC, 435-439. DOI= 10.1109/ICCSE.2014.6926499.

[17] Nitti, M., Girau, R. and Atzori, L. 2014. Trustworthiness management in the social Internet of Things. *IEEE Transactions on Knowledge and Data Engineering*. 26, 5 (May 2014), 1253-66. DOI= 10.1109/TKDE.2013.105.

[18] Zhu, C. S., Nicanfar, H., Leung, V. C. M. andYang, L. T. 2015. An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration. *IEEE Transactions on Information Forensics and Security*. 10, 1 (January 2015), 118-131. DOI= 10.1109/TIFS.2014.2364679.

[19] Garg, P., K. and Misra, M. 2011. Opinion Based Trust Evaluation Model in MANETs. In *Proceedings of the 4th International Conference on Communications in Computer and Information Science* (Noida, India, August 8-10, 2011). CCSIS'12. Spring, Berlin, H. Ber, 301-312. DOI=http://dx.doi.org/10.1007/978-3-642-22606-9_32.

[20] Yan, Z., Zhang, P. and Vasilakos, A. V. 2014. A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*. 42 (June 2014), 120-134. DOI= doi:10.1016/j.jnca.2014.01.014.

[21] Boukerche, A. and Ren, Y. 2008. A Security Management Scheme Using a Novel Computational Reputation Model for Wireless and Mobile Ad hoc Networks. In *Proceedings of the Fifth ACM International Symposium on Performance Evaluation of Wireless Ad-Hoc, Sensor, and Ubiquitous Networks* (Dublin, Ireland, March 22 - 26, 2014). PE-WASUN'08. ACM, New York, NY, 27-28. DOI=http://dx.doi.org/10.1145/1454609.1454628.

[22] Liu, Y., Li, K., Zhang, J. Y., and Qu, W., 2010. A novel reputation computation model based on subjective logic for mobile ad hoc networks. In *Third International Conference on Network and System Security* (Gold Coast, QLD, October 19-21, 2009). NSS'09. IEEE, Washington, DC, 294-301. DOI=http://dx.doi.org/10.1109/NSS.2009.68.

[23] Jia, X. L., Feng, Q. Y., Fan, T. H. and Lei, Q. S. 2013. RFID technology and its applications in internet of things (IoT). In *2012 2nd International Conference on Consumer Electronics, Communications and Networks* (Yichang, China, April 21-23, 2013). CECNet'12, IEEE, Washington, DC, 1282–1285. DOI= 10.1109/CECNet.2012.6201508.

[24] Xu, L., He, W. and Li. S. 2014. Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*. 10, 4 (November 2014), 2233-2243. DOI= 10.1109/TII.2014.2300753

[25] Shahid, R. 2013. Lightweight Security Solutions for the Internet of Things. Doctoral Thesis. UMI Order Number: ID Code: 5548. Mälardalen University. ISSN 1651-4238.

[26] Sicari, S., Rizzardi, A., Grieco, L. A. and Coen-Porisini. 2015. A. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*. 76, 15 (January 2015), 146-164. DOI= 0.1016/j.comnet.2014.11.008.

[27] Jing, Q., Vasilakos, A., Wan, J. F., Lu, J. W. and Qiu, D. C. 2014. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*. 20, 8 (November 2014), 2481-2501. DOI= 10.1007/s11276-014-0761-7.

[28] Chang, K. D. and Chen, J. L. 2012. A Survey of Trust Management in WSNs, Internet of Things and Future Internet. *KSII Transactions on Internet and Information Systems*. 6, 1 (January 2012), 5-23. DOI: 10.3837/tiis.2012.01.001.

[29] Gu, L., Wang, J. and Sun, B. 2014. Trust management mechanism for Internet of Things. *China Communications*. 11, 2 (February 2014), 148-156. DOI= 10.1109/CC.2014.6821746.