A Trustworthy Mobile Solution for Healthcare Based on Internet of Things

Kai Kang[1,2(✉)] and Cong Wang[1,2]

[1] School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
onefish@126.com
[2] Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing 100876, China

Abstract. Healthcare services based on the Internet of Things (Health-IoT) has great potential. The popularity of intelligent mobile medical devices, wearable bio-medical sensor devices, cloud computing and big data analysis have dramatically changed the usage pattern and business rule of Health-IoT. The rapid development of mobile solutions towards Health-IoT contains the risk of security and privacy. In this paper, a comprehensive trustworthy mobile solution based on architecture modeling with fuzzy-set theory towards Health-IoT is proposed. In particular, the solution is an semantics-based and fuzzy set theory mechanism to calculate trustworthiness for every stakeholders in mobility ecosystem for Health-IoT. An analytic methodology is presented backed with theoretical metrics and evaluated experimentally. The feasibility of the implemented about trustworthy mobile solution Health-IoT has been partly proven in field trials.

Keywords: Internet of things · Fuzzy set · Trustworthy · Mobile · Healthcare

1 Introduction

The rapid development of modern Information and Communication Technologies (ICTs) has led to a new circumstance of the social environment. The Internet of Things (IoT) is heterogeneous Internet-based information architecture in the wave of development [1]. The IoT connects all the ordinary physical objects to the Internet through kinds of information perception devices. The perception devices in IoT are able to exchange information with each other, and ultimately achieve the goal of intelligent recognition, locating, tracking, monitoring and management [2].

The mobile device based on IoT has been widely used as a pervasive healthcare gateway that collects data from the medical devices. Several connected healthcare devices like body fat analyzer, blood pressure monitor, ECG and etc., have been used

Kai Kang, he is with School of Software Engineering, Beijing University of Posts and Telecommunications; Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Beijing, China (e-mail:onefish@126.com).

R. Giaffreda et al. (Eds.): IoT360 2014, Part I, LNICST 150, pp. 217–222, 2015.
DOI: 10.1007/978-3-319-19656-5_31

in conjunction with the mobile gateway of IoT [3–5]. Plenty of the mobile applications afford constant monitoring service of patient's symptoms and needs, enabling physicians to diagnose and monitor health problems wherever the patient is, either at home or outdoors.

Mobile solution for healthcare on the basis of IoT (mHealth-IoT) offers a unique opportunity to tailor and customize care services for individual patients health needs and behavioral attributes. With the convenience of mHealth-IoT, rapidly increasing demands of daily monitoring would be satisfied. However, the security and privacy risk is increasing rapidly due to its armature. In order to develop and integrate effective ubiquitous sensing for healthcare, trustworthiness as an important design goals should be taken into account in future mHealth-IoT [6].

In this paper, to tackle with the risk of security and privacy emerging in mHealth-IoT, a trustworthy mobile solution is proposed. Trustworthy fuzzy set theory evaluates trustworthiness of stakeholders in ecosystem are discussed.

The rest of this paper is organized as follow: some related works are summarized in Sect. 2, theoretical method for evaluation of stakeholders is presented in Sect. 3, and conclusion and future work are discussed in Sect. 4.

2 Related Works

Generally, an IoT system could be decomposed into three layers, which are sensor (recognition) layer, network (transformation) layer and application (services) layer. Traditional strategies, such as access control, are no longer suit for resolving security and privacy issues of distributed system because of their centre-dependence and poor scalability.

Trust is a multidimensional, multidisciplinary, and multifaceted concept. Common to these definitions are the notions of confidence, belief, and expectation on the reliability, integrity, ability, or characters of an entity. To reduce and solve the risk, a number of literature articles in terms of trust management in IoT domain were published. 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.

Trust management (TM) plays an important role in IoT [7]. It enhances user privacy and information security, and improves quality of services. A trustworthy mHealth-IoT should consist of reliable mobile devices, provides secure communications, and preserves users' privacy, part or all of the ways to gain user trust. In this paper, a trustworthy mHealth-IoT is present in order to illustrate what trust properties should be enhanced in order to achieve holistic trust management.

A number of studies pay special attention to TM in IoT. The main issues focus on the following aspects: Secure framework and architecture [8, 9]; Secure data transmission and communication [10, 11]; Privacy preservation [12, 13].Yan et al. [14] reviews and summaries the existing work as eight taxonomies: Trust Evaluation, Trust Framework, Data Perception Trust, Identity Trust and Privacy Preservation,

Transmission and communication Trust, Secure Multi-Party Computation, User Trust and Application Trust. In the domain of Health-IoT, Pang et al. [15–17] establishes special ecosystem for Health-IoT, and design a trustworthy in-home medication management solution. Yang et al. [18] upgrades the solution above and implements a comprehensive intelligent home-based platform for iHome Health-IoT. Kang et al. [18] proposes a security and privacy mechanism for rural areas in China towards Health-IoT. Their works do not attach importance to the capability of mobile devices in Health-IoT. In another word, mobility of "things" (e.g. mobile medical devices and mobile terminals) is not the kernel part of Health-IoT. Kang et al. [20] proposes an innovative ecosystem and model for Health-IoT. In his study, a mobile application market ecosystem is described, notion of application trustworthiness is defined, case study and experiment is implemented. He depicts a fundamental solution for mHealth-IoT in the view of security and privacy. However, the role of mobile terminal has not illuminates clearly; theoretical method and measurement for trustworthiness is difficult to utilize in mHealth-IoT. With advantage of his study, considering stakeholders, a trustworthy mHealth-IoT is proposed in next section, which focuses on the evaluation for stakeholders.

3 Trustworthy mHealth-IoT

A trustworthy mHealth-IoT should be operating in particular ecosystem, which consists of trustworthy devices and trustworthy services. In the ecosystem, many roles in different society domains are involved. The theory of ecosystem was introduced: "*Products and services mainly flow from means providers, through service providers, to end users. Payments (obligatory or optional, depending on different cases) flow back from end users, through financial sources, to the means providers and service providers. Thus a close-loop is established. It is exactly the "close-loop" feature that makes the ecosystem economically sustainable. Win-win cooperation is enabled only if every stakeholder's benefit is guaranteed*" [21]. In the ecosystem, many roles in different society domains are involved. The major stakeholders in the ecosystem as following: Healthcare mobile service providers; Healthcare financial sources; Content providers; Telecom operators; Mobile devices providers; Mobile medical devices providers; Mobile application broker and etc. [18, 21]. In this section, a trustworthiness evaluation for every stakeholder is proposed based on Sugeno Integral of fuzzy set theory.

3.1 Trustworthiness Evaluation for Stakeholders

In the view of TM, traditional solutions for Health-IoT, spend much effort to solve problems at some points, such as recognition, transformation, storage, processing and etc. All the key points belong to different stakeholders in ecosystem. Evaluating the trustworthiness of stakeholders in ecosystem is a direct way for build up a trustworthy mHealth-IoT. Stakeholder is abstract concept; it is difficult to calculate its trustworthiness directly. Sugeno Integral [22] always is used for evaluating reputation and

trustworthiness in TM. Hence, it helps us to solve the problem about trustworthiness evaluation for stakeholders.

Definition 1. Assume measurable space (X, Ω), $h : X \to [0, 1]$ satisfying the following conditions:

(1) $m(\emptyset) = 0, m(X) = 1$;
(2) $A \subseteq B \Rightarrow m(A) \leq m(B)$;
(3) $h_\lambda = \{x \in X : h(x) \geq \lambda\}$, whenever $\lambda \in [0, 1]$.

h is measure function.

Definition 2. Assume that the (X, Ω, m) is a fuzzy measurable space, $A \in \Omega, X = \{x_1, x_2, \cdots, x_n\}, h : X \to [0, 1]$

The Sugeno integral for h is:

$$\int_A h \circ m = \sup_{A \in [0,1]} \min\{\lambda, m(A \cap h_\lambda)\} \tag{1}$$

whenever satisfying the condition: $h(x_i) \leq h(x_{i+1}), 1 \leq i \leq n - 1$.

The Sugeno integral for h is:

$$\int_A h \circ m = \max_{i \in \{1,2,\cdots,n\}} \min\{h(x_i), m(A \cap X_i)\} \tag{2}$$

Attributes for stakeholder should be mapping to X in measurable space (X, Ω). x stands for attribute in X. $m(A \cap X_i)$ denotes as measure. Different people or institutions can describe degree of importance for each attribute denotes as *h(x)*. In this paper, the result of Sugeno Integral with attributes and measurements is equivalent to the trustworthiness of stakeholders. Trustworthiness evaluation for mobile medical device provider as an example is explained.

To simplify the condition, four attributes are mentioned for mobile medical device provider. The formula description is shown as following:

$$\begin{aligned} &x_1(product\_quality),\\ &x_2(research\_ability),\\ &x_3(enterprise\_scale),\\ &x_4(enterprise\_reputation) \end{aligned} \tag{3}$$

The value of them is calculated by questionnaire survey.

If someone evaluates mobile medical device provider for each attributes, the result should be:

$$h(x_i), \quad i = 1, 2, 3, 4 \tag{4}$$

The trustworthiness for mobile medical device provider is shown as following:

$$\int_A h \circ m = \max \left\{ \begin{array}{l} \min\{h(x_1), m(X)\}, \\ \min\{h(x_2), m(\{x_2, x_3, x_4\})\}, \\ \min\{h(x_3), m(\{x_3, x_4\})\}, \\ \min\{h(x_4), m(\{x_4\})\} \end{array} \right\}$$

t is short for trustworthiness for every stakeholders, and w represents weights. The trustworthiness for mHealth-IoT is:

$$T = \frac{\sum_n t \cdot w}{n} \tag{5}$$

4 Conclusions and Future Works

A trustworthy mobile solution based on architecture modeling with fuzzy-set theory towards Health-IoT is proposed. Fuzzy set theory and mechanism help people to calculate and evaluate trustworthiness of stakeholders. A trustworthy mobile solution for Health-IoT is still on trial, the details and experiments is taken into consideration in future works.

Acknowledgments. This work is supported by the National Key Technology R&D Program of the Ministry of Science and Technology of China (2012BAJ18B07-05).

References

1. Xu, L., He, W., Li, S.: Internet of things in industries: a survey. IEEE Trans. Ind. Inf. **10**(4), 2233–2243 (2014)
2. Li, T., Liu, Y., Tian, Y., Shen, S., Mao, W.:A storage solution for massive iot data based on nosql. In: 2012 IEEE International Conference on Green Computing and Communications (GreenCom), pp. 50–57 (2012)
3. Ghose, A., Bhaumik, C., Das, D., Agrawal, A.K.: Mobile healthcare infrastructure for home and small clinic. In: Proceedings of the 2nd ACM International Workshop on Pervasive Wireless Healthcare, Hilton Head, South Carolina, USA, (2012)
4. Paschou, M., Sakkopoulos, E., Sourla, E., Tsakalidis, A.: Health internet of things: metrics and methods for efficient data transfer. J. Simul. Model. Pract. Theory **34**, 186–199 (2013)
5. Sama, P.R., Eapen, Z.J., Weinfurt, K.P., Shah, B.R., Schulman, K.A.: An evaluation of mobile health application tools. JMIR mHealth and uHealth **2**(2), e19 (2014)
6. Zhang, Y., Sun, L., Song, H., Cao, X.: Ubiquitous WSN for healthcare: recent advances and future prospects. IEEE J. Internet Things **1**, 497–507 (2014)
7. Gu, L., Wang, J., Sun, B.: Trust management mechanism for internet of things. China Commun. **11**(2), 148–156 (2014)
8. Ning, H., Liu, H., Yang, L.T.: Cyberentity security in the internet of things. J. Comput. **46** (4), 0046–0053 (2013)

9. Li, X., Xuan, Z., Wen, L.: Research on the architecture of trusted security system based on the internet of things. In: 2011 International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 2, pp. 1172–1175 (2011)
10. Isa, M.A.M., Mohamed, N.N., Hashim, H., Adnan, S.F.S., Manan, J.A., Mahmod, R.: A lightweight and secure TFTP protocol for smart environment. In: 2012 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), pp. 302–306 (2012)
11. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S., Wehrle, K.: Security challenges in the IP-based internet of things. J. Wirel. Pers. Communic. **61**(3), 527–542 (2011)
12. Køien, G.M.: Reflections on trust in devices: an informal survey of human trust in an internet-of-things context. J. Wirel. Pers. Commun. **61**(3), 495–510 (2011)
13. Thoma, C., Cui, T., Franchetti, F.: Secure multiparty computation based privacy preserving smart metering system. In: North American Power Symposium (NAPS), pp. 1–6 (2012)
14. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for internet of things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
15. Pang, Z., Tian, J.: Ecosystem-driven design of in-home terminals based on open platform for the internet-of-things. In: International Conference on Advanced Communication Technology (ICACT), pp. 369–377 (2014)
16. Pang, Z., Chen, Q., Zheng, L., Dubrova, E.: An in-home medication management solution based on intelligent packaging and ubiquitous sensing. In: 15th International Conference on Advanced Communication Technology (ICACT), pp. 545–550 (2013)
17. Pang, Z., Zheng, L., Tian, J., Kao-Walter, S., Dubrova, E., Chen, Q.:Design of a terminal solution for integration of in-home health care devices and services towards the internet-of-things. Enterprise Information Systems, (ahead-of-print), pp.1–31. (2013)
18. Yang, G., Xie, L., Mantysalo, M., Zhou, X., Pang, Z., Xu, L., Kao-Walter, S.,Chen, Q., Zheng, L.: A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor and intelligent medicine box. IEEE Trans. Ind. Inf. **10**(4), 2180−2191 (2014)
19. Kang, K., Pang, Z.B., Wang, C.: Security and privacy mechanism for health internet of things. J. China Univ. Posts Telecommun. **20**, 64–68 (2013)
20. Kang, K., Pang, Z., Ma, L., Wang, C.: An interactive trust model for application market of the internet of things. IEEE Trans. Ind. Inf. **10**(2), 1516−1526 (2014)
21. Pang, Z., Chen, Q., Tian, J., Zheng, L., Dubrova, E. :Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things. In: 15th International Conference on Advanced Communication Technology (ICACT), pp. 529–534 (2013)
22. Sugeno, M.: Theory of fuzzy integrals and its applications. Tokyo Institute of Technology. (1974)