ELSEVIER

Available online at www.sciencedirect.com
ScienceDirect

December 2013, 20(Suppl. 2): 64–68
www.sciencedirect.com/science/journal/10058885

The Journal of China Universities of Posts and Telecommunications

http://jcupt.xsw.bupt.cn

Security and privacy mechanism for health internet of things

KANG Kai[1,3] (✉), PANG Zhi-bo[2], WANG Cong[1,3]

1. School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. ABB AB, Corporate Research, Forskargränd 7, Västerås, Västmanland, 72178, Sweden
3. Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing 100876, China

Abstract

The rapid development of technologies towards Internet of Things (IoT), has led to new circumstances at all levels of the social environment. In healthcare in particular, the use of IoT concepts and technologies make diagnose and monitor more convenient for the physicians and patients. As mobile applications solutions are widely accepted because the easy to use, secure healthcare service is a new demand for mobile solutions. To protect the privacy and security for patients in the domain of healthcare towards IoT, a systematic mechanism is needed. This article proposes a novel security and privacy mechanism for Health Internet of Things (Health-IoT) to solve above problems. Health-IoT is promising for both traditional healthcare industry and the information and communication technologies (ICTs) industry. From the view of trustworthiness, interactive vector was proposed to communicate the end-devices and application brokers. The aim is to establish a trust IoT application market (IAM), feature of application in marketplace and behavior of applications on end-devices can be exchanged in mathematical value to establish the connection between market and users.

Keywords Internet of Things, security, privacy, application market

1 Introduction

The IoT has been became a novel paradigm that is rapidly accepted by the scenario of modern wireless telecommunication. This concept is the pervasive presence of things or objects around us, such as radio-frequency identification (RFID) tags, sensors, actuators, mobile phones, and etc [1]. As a complex cyber-physical system, the IoT integrates all kinds of sensing, identification, communication, networking, and informatics devices and systems, and seamlessly connects all the people and things upon interests, so that anybody, at any time and any place, through any device and media, can more efficiently access the information of any object and any service [2].

In recent years, as a modern ICTs, combining advanced equipment and technology together, IoT is playing an important role in many different scenarios in our daily life, from smart city to smart home. In health care in particular, IoT offers potential for constant monitoring of patient's symptoms and needs in real time, enabling physicians to diagnose and monitor health problems wherever the patient is, either at home or outdoors [3]. With the development of mobile devices, the popularity of smartphones has dramatically changed the pattern of traditional healthcare. Mobile solutions based on IoT are widely accepted by physicians and patients.

IoT has made considerable progress in developing sensory devices, but it is broadly accepted that the technologies and applications of IoT are both in early stage and distant from mature. Every physical object as a virtual component in IoT brings unprecedented convenience and economy, but such extreme interconnection will cost much more our energy to concern about security and safe [4]. In addition, the privacy and its right of control is also one of the most concerned issues in IoT. In the literature, security and privacy in IoT requirements are described as following:

Received date: 13-11-2013
Corresponding author: KANG Kai, E-mail: onefish@126.com
DOI: 10.1016/S1005-8885(13)60219-8

Resilience to attacks: The system has to avoid single points of failure and should adjust itself to node failures.

Data authentication: As a principle, retrieved address and object information must be authenticated.

Access control: Information providers must be able to implement access control on the data provided.

Client privacy: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct [5].

Mobile solutions with implementation of smartphones based on Android or iOS are already intensifying users' interaction with the environment, to provide myriad dimensions of information to enrich the user experience. It faces the challenges is more severe, especially for Android, because of the open source pattern. Built on the contributions of the open-source community and hardware, software, and carrier partners, using Android OS will significantly reduce the cost and provide the flexibility of development. The advantage of the open source has also made it vulnerable to attacks. Plenty of viruses, Trojans, spywares and malwares flood into application field [6].

In this paper, to satisfy the need for security and privacy, a special systematic mechanism based on Android for Health-IoT.

2 Health internet of things

2.1 Health-IoT ecosystem

The combination of sensors, Wi-Fi, 3G, RFID and Bluetooth has improved measurement and monitoring methods of vital functions. A number of applications can be finding in the healthcare sector with IoT technologies. The revolution of IoT is reshaping the modern healthcare with promising economic and social prospects. Large user base and maturated ecosystem of traditional mobile internet service have significantly sped up the development of the IoT-powered in-home healthcare services, so-called Health-IoT. A novel ecosystem-driven design strategy has been proposed by Pang, and the implementation for it was finished in the design of an open-platform based solution [7–9]. The relations of product and service among different stakeholders, capital flows and information flows are shown in Fig. 1. In this ecosystem, many roles in different society domains are involved. Many stakeholders in the ecosystem such as healthcare service providers, healthcare financial sources, content providers, telecom operators and etc. are not on focus. In order to adapt to the development of mobile medical treatment, this paper pay more attention on application domain in healthcare. Application designer, platform provider, and application store can be given a joint name, so-called Application Broker. Application broker, the distribution of the applications for healthcare is one of the most important parts. It determines the user's experience and service quality. Therefore the applications are distributed through application market which can offer consumers and application developers more fairness in the ecosystem.

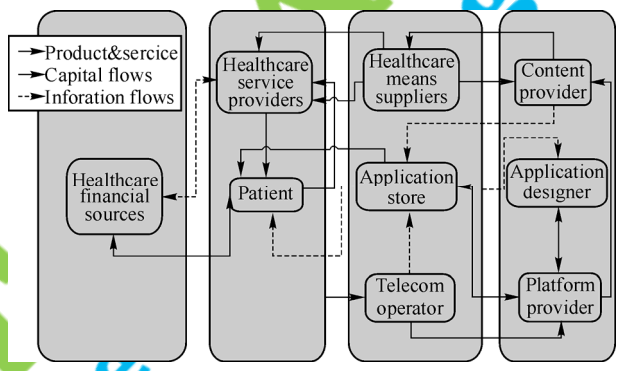

Fig. 1 Application broker in Health-IoT ecosystem

Application broker includes application designer, platform provider and application store. Application Broker codetermines the channel for distribution of applications.

In view of application broker, application store which so-called application marketplace as normal, is the major part to control the distribution of application. So, the application marketplace for Health-IoT will be mentioned next chapter.

2.2 Health-IoT application marketplace

In the Health-IoT ecosystem, application marketplace is key note for patient and other stakeholders. As is shown in Fig.1, application store as the marketplace, it is directly linked to application designer and patient. Application on terminal device is the actual form of the service which is provided to patient. The proliferation of smartphones is driving the rapid growth of mobile application market (MAM) where various applications are distributed and traded. Apple app store and the google android market are important channels for distribution [10]. According to

researches on MAM, distribution of applications presents two forms:

Independent mode: This mode is widely used for corporation which has independent hardware platform. Apple Inc. and its business model is a significant and typical example. Apple application store applies centralized authentication of apps for Apple's devices.

Non-independent mode: This mode receives more support than the independent one. It attracts hardware, software and carrier partners. Google and the open-source mobile operating system (OS) is the most successful one. Google Android market just one of markets for Android applications, many third-party markets contributes on the distribution of applications.

A dedicated application market for IoT, so-called the IAM, is expected to be an effective approach for service distribution in the era of IoT [11]. Based on the above cooperative ecosystem, the development of applications will be an important driving force to improve healthcare services. In different health issues, many specific applications are in vogue at Android market. Patient can get help with applications which assist measure, monitor and record physical signs, such as blood pressure, blood glucose, heart rate, and etc. Smartphones are often used by patient and medical personnel, because it facilitates the capability of mobility and privacy protection.

3 Model and mechanism

3.1 Model for health-IoT

Apps on users' smartphone require permissions to utilize smartphone system functionality to read and write user data. Users are often confused by the complexity of fine-grained permissions. App declares the required permissions, but users seem not to care about that. Many applications have been started to help users to observe authorized permission and monitoring their behavior. The principle of those apps is out the scope of our research. It is believe that detecting and reporting behavior of app is not a difficult thing.

TaintDroid [12] is used to detecting what app has done with the privacy on users' smartphone. On the smartphone, the following aspects are concerned:

Identification: IMEI; IMSI; SIM card identifier; Device serial number; phone number.

Content: User account information; SMS; Address Book; Location.

Using TaintDroid can be convenient and quickly observe the results for monitor the real-time privacy on users' smartphones. Interactive vector, it is a vector that indicates the trustworthiness of applications. Interactive vector plays the role as a bridge to communicate the end-users and IAM. Interactive vector includes evaluation vector and feedback vector. PA and Health-IoT IAM decide the privacy regulation together [13].

3.2 Mechanism for health-IoT

The implementation of IAM with model for Health-IoT is convenient and trusted application distribution way. The application for a particular Health-IoT service should be distributed through the application market, because the healthcare services deal with privacies of end users which are much more sensitive than other type of apps. All devices and applications for the patient should be controlled and trusted, the privacy regulations should be applied to each participant of healthcare means provides.

Security and privacy mechanism is one of the technical means to project the benefits of all stakeholders, and it will balance the right of control in the ecosystem. PA as third party supervisor is to empower the patients to believe service providers, content providers and telecom operators can really protect their privacy. Based on above consideration, under the model for IAM, the security schemas with IAM are proposed in Fig. 2 [13].

As illustrated by the step 1~10 in Fig. 2, to launch a particular Health-IoT app to the IAM, the enterprises as service providers should get authentication from the PA first. PA handover cryptography credential to each actor. During the period of monitoring, end-users generates feedback vector, and send it to PA and IAM. IAM collects the feedback vectors, and calculate the next evaluation vector should be published. The information from service provider to patient are illustrated in step 20~23. Each transmit step encrypt by different secret diffused from PA. Content provider and telecom operator have no access to the messages. In step 31~35, application broker redesign, rebuild and redistribute for application which is not satisfied for patient.

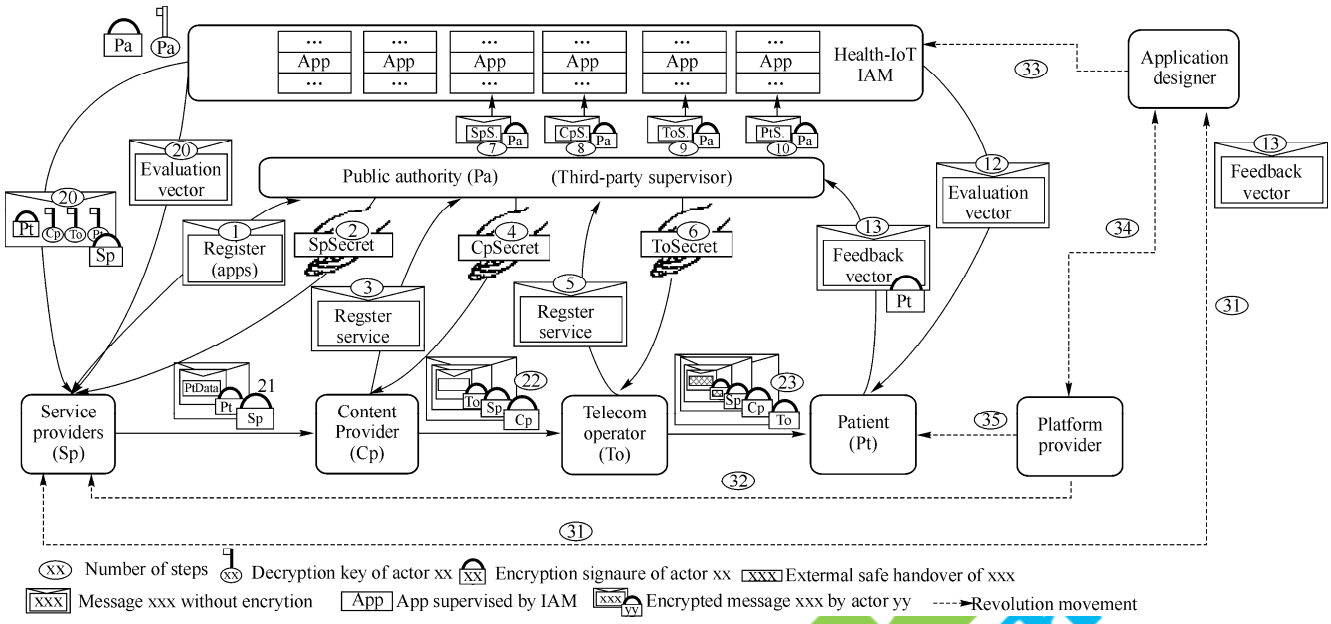

Fig. 2 The proposed security and privacy mechanism for Health-IoT

4 Vision for rural health service

In rural areas, especially in China, the development of healthcare lags far behind in cities. Although there is lack of medical equipment and staffs, the telemedicine give patient more opportunities to get help from hospital in cities. The popularity of telecom networks and smartphones, reduce the difficult and cost for patient.

The aim of our work is to establish suitable solution for rural medical and healthcare. The technologies and architecture is listed as following:

Medical cloud data center (MCDC): rely on the abundant resources of the city, Set up large-scale data center.

Health application market (HAM): the market offer trusted application for patient.

Intelligent medical terminal (IMT): based on Android, let smartphone be telecommunication terminal and the personal data center.

HAM should realizes model and mechanism have mentioned above. Platform provider affords IMT to satisfy special usage. Application designer publishes application in HAM with authorization from PA. The accepted application will be supervised by HAM. Patients, who live in rural areas, will choose application from HAM to install for IMT. With application, patient can monitor and upload physician data to MCDC, download health report and prescription from MCDC. According to the feedback from patients, application designer and platform provider improve their works.

5 Conclusions

Trust assessment of application is necessary and important for users who concern with their devices' security and privacy. Therefore, more and more security vendors and app market holders spend energy on it. Interactive vector as an important and primary indicator in application marketplaces will help people to choose the right ones.

This paper reviewed the current state of art in Health-IoT and proposes security and privacy measurement and new strategy. Security and privacy influences the users' experience and the quality of services, to protect it as the major mission in Health-IoT. It is a credible way to make both hardware (mobile devices) and software (application marketplaces) are trust.

Future research will focus on the improvement the model for IAM. Improving the quality of the model and promoting the IAM is short-term goal will be realized in the next step.

Acknowledgements

This work was supported by the National Key Technology R&D Program of the Ministry of Science and Technology of China (2012BAJ18B07-05). This work relies on the Rural Three-level Health Service Comprehensive Demonstration Research

References

1. Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer Networks, 2010, 54(15): 2787–2805
2. The internet of things-executive summary. ITU Internet Reports 2005. http://www.itu.int/osg/spu/publications/internetofthings/Internet ofThings _summary.pdf
3. Paschou M, Sakkopoulos E, Sourla E, et al. Health Internet of Things: metrics and methods for efficient data transfer. Simulation Modelling Practice and Theory, 2012
4. Roman R, Najera P, Lopez J. Securing the Internet of Things. Computer, 2011, 44(9): 51–58
5. Weber R H. Internet of Things–New security and privacy challenges. Computer Law & Security Review, 2010, 26(1): 23–30
6. Enck W, Ongtang M, McDaniel P. Understanding android security. Security & Privacy, IEEE, 2009, 7(1): 50–57
7. Pang Z, Chen Q, Tian J, et al. Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things. Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013: 529–534
8. Pang Z, Zheng L, Tian J, et al. Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. Enterprise Information Systems, DOI:10.1080/17517575.2013.776118, April 2013
9. Pang Z, Tian J, Chen Q. Ecosystem-Driven Design of In-Home Terminals Based on Open Platform for the Internet-of-Things. ICACT Transactions on Advanced Communications Technology (TACT), 2013
10. Butler M. Android: changing the mobile landscape. Pervasive Computing, IEEE, 2011, 10(1): 4–7
11. Munjin D, Morin J H. Toward Internet of Things Application Markets. Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, 2012: 156–162
12. Enck W, Gilbert P, Chun B G, et al. TaintDroid: an Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. OSDI. 2010, 10: 255–270
13. Kang K, Pang Z, Xu L, et al. An Interactive Trust Model for Application Market of the Internet of Things. Industrial Informatics, IEEE Transactions on, 2013. submitted

From p. 53

Acknowledgements

This work was supported by the 'Twelve Five' National Cryptography Development Fund for Cryptography Theoretical Research (MMJJ201101025).

References

1. Atzori L, Iera A, Morabito G. The Internet of Things: a survey. Computer Networks, 2010, 54(15): 2787–2805
2. Yang Z. The system of the internet of Things. Beijing: Beijing University of Posts and Telecommunications Oress, 2012 (in chinese)
3. Wu C K. Preliminary study on security architecture of the Internet of Things. Bulletin of Chinese Academy of Sciences, 2010, 25(4): 411–419 (in chinese)
4. Trusted Computing Group. ISO/IEC 1189-1~4. Version 1.2, Revision 103, 2009
5. State Commercial Cryptography Authority. Functionality and interface specification of cryptographic support platform for trusted computing. 2007. (in chinese)
6. Bente I, von Helden J. Towards trusted network access control. Proceedings of the First International Conference Future of Trust in Computing 2008, 157–167
7. Nuno Santos, Rodrigo Rodrigues, Krishna P et al. Policy-sealed data: a new abstraction for building trusted cloud services. Proceedings of the 21st USENIX Conference on Security symposium (Security'12). USENIX Association, Berkeley, CA, USA: 2012: 10–10