International Journal of Smart Home
Vol. 9, No. 6 (2015), pp. 141-150
http://dx.doi.org/10.14257/ijsh.2015.9.6.16

Dynamic Data Binding Protocol between IoT Medical Device and IoT Medical Service for Mobile Healthcare

Byung Mun Lee

Department of Computer Engineering, Gachon University, Seongnam City, Gyeonggi-do, 461-701, South Korea
bmlee@gachon.ac.kr

Abstract

In this paper, the author suggests a binding protocol which enables users to use public medical devices as if they are their own medical devices through IoT Healthcare. Binding protocol provides customized real-time transmission function enabling interwork between mobile phones, medical devices and monitoring services. In particular, the author defines a protocol to support streaming date transmission, and verifies the operating effectiveness of the protocol by measuring the transmission time through simulation.

Keywords: *Mobile Healthcare, Binding Protocol, IoT Platform, Health Monitoring Service*

1. Introduction

Since 2010, interest in and research of IoT technologies have surged [1-2]. IoT can be classified into five categories - IoT services, IoT platform, IoT network, IoT devices and IoT security - but they are closely associated with each other [3-4]. For example, IoT devices are connected to an IoT platform using an IoT network. In the course of this process, IoT security guarantees the privacy, integrity and availability of information [5-6]. A new IoT service model has been introduced on the basis of such an infrastructure [7]. Moreover, the rapid penetration of smartphones turns them into IoT devices through which users interface, playing a critical role in interacting with the platform [8].

For this reason, smartphone manufacturers such as Google, Apple and Samsung and telecommunication services companies are building IoT devices and platforms using their own products and technologies [9-11]. If it were not for an IoT service model like the killer application, they cannot be developed. Of IoT services, health applications receive the most attention and provide services which improve the living quality and health of humans (*e.g.*, Healthcare, Life care and Sleep care). In particular, wearable devices that have been developed in various forms are used to manage sleep and various activities [12-13], interacting with smartphones [14-15], but they have a limitation in that they can be used only in daily life [16-17].

However, in order to be more effective as a killer application, the IoT platform must allow the user to freely choose from a variety of devices and services to suit the individual environment and preferences, and IoT devices and mobile phones must be able to interact with each other autonomously [18-21]. To facilitate this, a conventional IoT-based healthcare service model [8] [22], a medical IoT device registration protocol required to implement the healthcare service model and an IoT device discovery protocol are suggested [23-24]. However, to use these protocols, users and devices are to be bound with each other and there must be a protocol which transmits medical data measured by bound services seamlessly.

Thus in this paper, the author suggests a transmission protocol in which medical IoT devices dynamically transmit data to the bounded medical services following

ISSN: 1975-4094 IJSH

the registration protocol and protocols which have been studied previously. This supports the transmission of medical data to the bounded services at the time of use in a system where multiple users share one device.

In Section 2 the author addresses IoT-based healthcare services and the authentication, registration and discovery protocols which support the foregoing services. In Section 3, the author suggests a service model for transmitting the measured data to the bounded services. In Section 4, the author lays out the data-binding protocol, and in Section 5, the author verifies the validity of the suggested protocol through simulation and testing

2. Related Research

Healthcare is a user-customized service for personal healthcare, so that devices and services must be capable of dynamic change according to user environment and requirements. Thus medical devices used at home or the hospital must be able to recognize users and operate according to user environment. In other words, uses must be able to purchase medical devices at stores near home and use healthcare services by connecting such devices to the healthcare platform. Furthermore there is a need for intelligent autonomous services which enable transmission of data measured by the medical devices at a nearby hospital or a public institution to users' healthcare services. IoT-based healthcare services using the foregoing mobile devices have been studied and the platform structure to provide such services has been defined [23] [25-26].

To provide such services, first user identification and authentication technology are required. To interwork medical devices and mobile devices like smartphones, users must be able to be identified and authenticated. Currently most smartphones have NFC (Near Field Communication) function, which facilitates use of an authentication server as shown in Figure 1 [23].

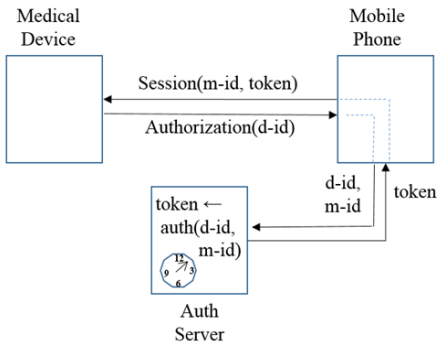

Figure 1. Authorization Model between Medical Device and Mobile Phone

In Figure 1, mobile devices transmit d-id (device id), consisting of unique identification information, to the authentication server via mobile device. The authentication server generates a token using the identification number of the smartphone: m-id (mobile id) and d-id. The token generated is used to authenticate the session for the transmission and receipt of data between medical device, mobile phone and the service platform. This plays a critical role in identifying the users of medical devices, and can be used to identify the owner of such information when the session is activated.

In such an authenticated session, the medical device is registered with the platform. For the registration process, when the mobile device is held near the medical device by the user, the device information (d-id and device metadata) and mobile phone information (m-id and user meta-information) are cross-registered with the platform and the Meta information of the device and mobile phone are also registered [27].

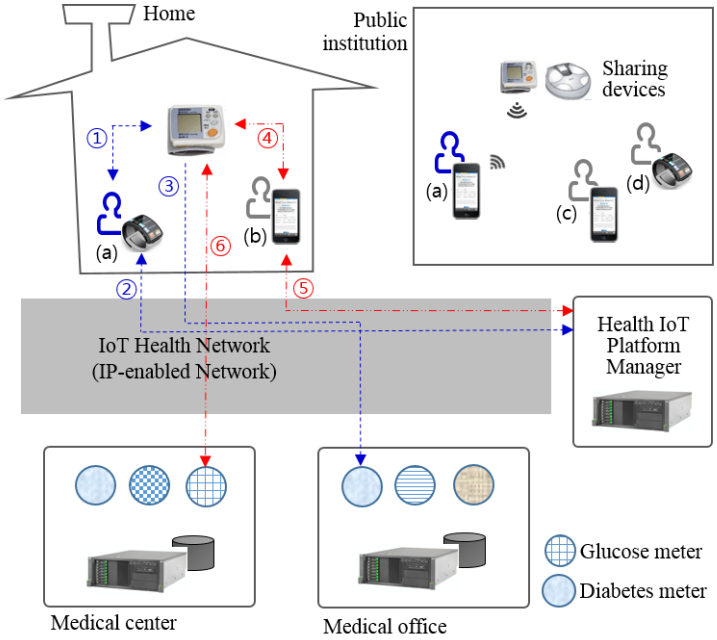

Figure 2. Service Model for Sharing Medical Device [27]

With this method, medical devices are enabled to manage user data. As shown in Fig 2, user (a) and user (b) share the device by registering themselves and the device with the platform. When user (a) uses the device, the user is connected to the service being bound with user information from the mobile device, and when user (b) uses the device, the user is connected to the service interworking with the mobile device

Thus, this model is able to provide user-customized healthcare services even if the medical device is shared by multiple users, and users also can enjoy transparent services. For this type of service, there is a need for data-binding and date transmission protocols following the service architecture, platform structure and device/user registration protocols suggested in the previous studies. Thus, in this paper, the author suggests and designs two protocols and suggests a mobile application using these protocols in the next section

3. Data binding protocol for the device to the server

Binding service activates when the user, device and monitoring service are registered with the platfom. In data-binding protocol, mobile phone and medical device interact to map user data automatically, which facilitates a continuous and dynamic monitoring service. Figure 3 shows the sequence diagram of a data-binding protocol. The mobile phone (MP) transmits the Bind.req messsage to the medical device (MD). This process is to identy users using the MD by trasmitting identification information (m-id) of the user of the MD process, notifying the user. In order for users to use the MD, they must be close to each other, so NFS provides Bind.req and Bind.res.

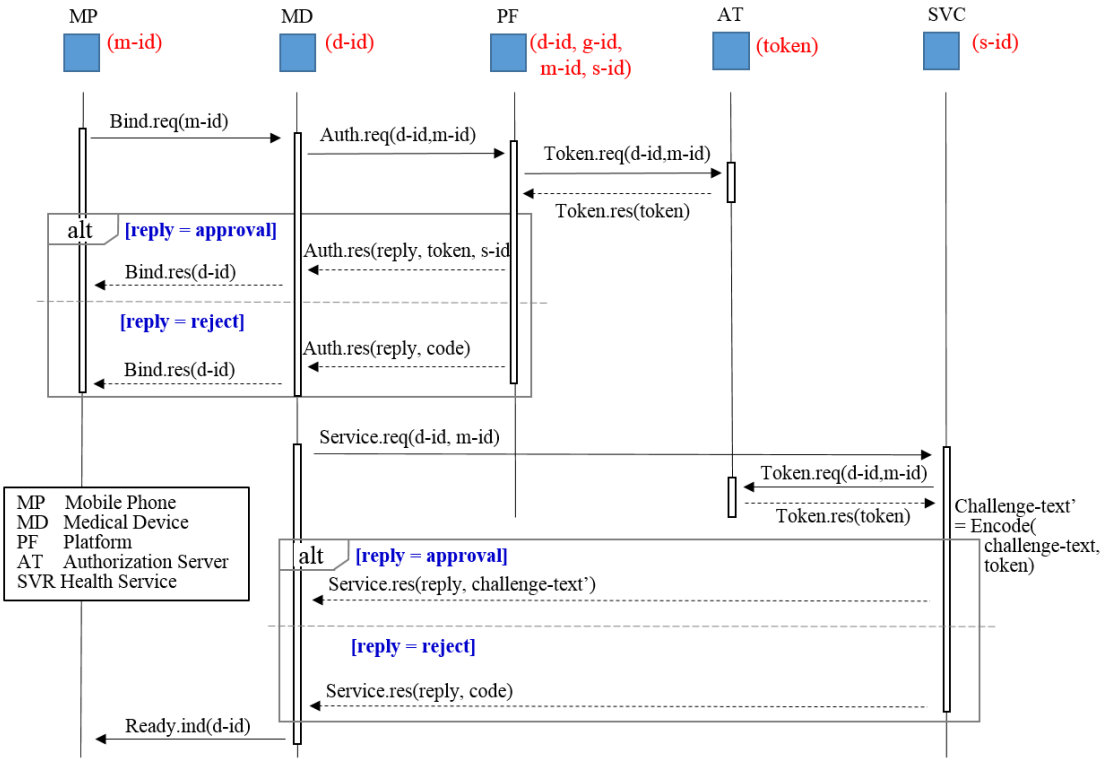

Figure 3. Sequence Diagram for Data-Binding Protocol

To confirm user access authorization, the MD transmits Auth.req to the platform to get a token and service information (s-id). If a user or device is not registered with the platform, access is not granted. Furthermore if the user did not set the services in such a way as to suit the corresponding platform, access is not granted, and the token or set s-id cannot be acquired. The s-id includes the attributes of service and URI. With user access, the MD requests service SVC for Service.req and attempts a binding between device and service.

The SVC which receives the Service.req requests the Auth server for a token and receives it. At this time, the Token is the same as the Token of the platform PT. The token plays a critical role in providing cross-authentication between MD and SVC. It encrypts predetermined random challenge texts as the token and transmits them after including them in Service.res. If SVC did not receive a token or the type of MD does not match the type of monitoring service, the request for service is rejected. For example, a glucose meter device and weight-monitoring devices do not match each other. In this case, SVC transmits 'reject' with the cause for rejection (code) to Service.res.

When the data-binding process is completed, the MS is able to transmit the measured date to the SVC as shown in Figure 4. The data to be transmitted is divided into two types: one-time data such as blood pressure or blood glucose levels, and streaming data to be measured and transmitted continuously such as electrocardiogram or pulse. In the case of one-time data, MD Data.req includes the Meta data (i.e. date type, date attributes, measurement period, measurement time and model name of measuring device) in d-header message, and transmits the data with the token. SVC verifies the received data and replies the results as Data.res.

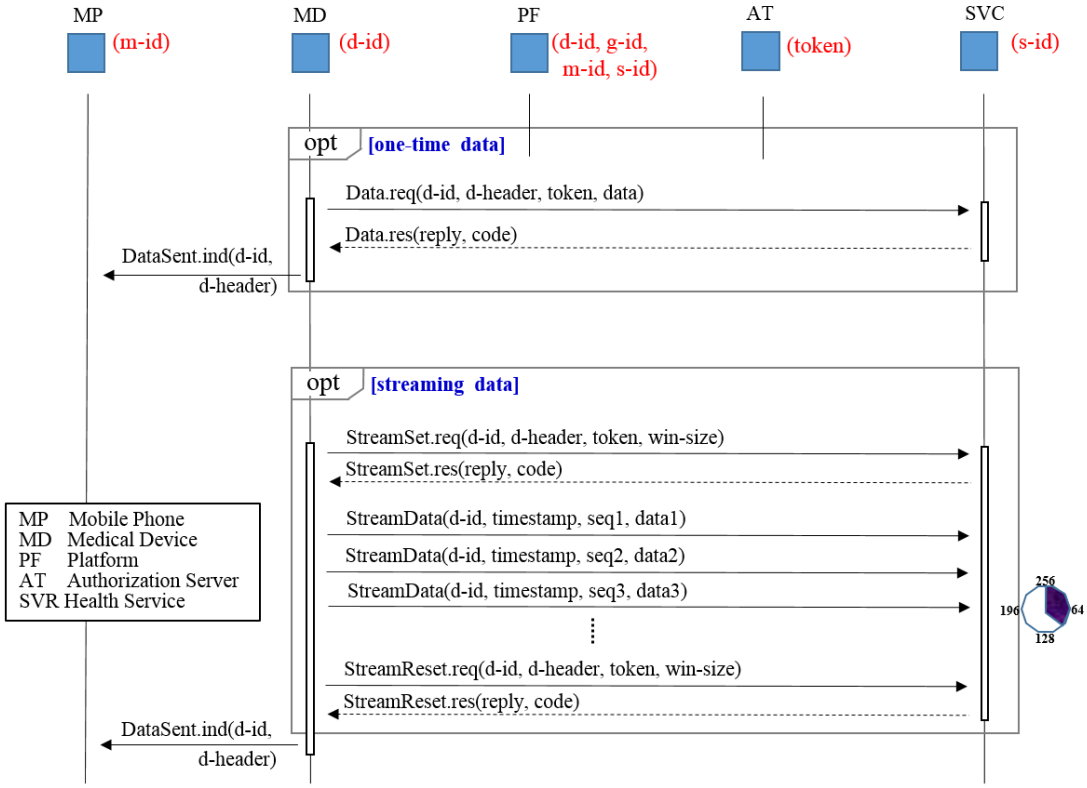

Figure 4. Sequence Diagram for Data Transfer Protocol

In the case of streaming data, the MD transmits Data.req, requesting the SVC to receive data continuously. If the SVC is in a state of not being able to receive the date, therequest may be rejected. If it is in a state of being able to receive the data, StreamSet.req transmits 'approval'. The MD which receives approval includes the streaming data in StreamData.reg message and transmits the streaming data together with timestamp including information on the time of data measurement. To increase transmission efficiency, StreamSet.req sets win-size, the size of the buffer which can be received by the SVC. The MD is able to transmit the data up to win-size without SVC reception response

4. Mobile Application for Health Service Using Data Binding Protocol

In order for users to use the set device and medical device after binding them, there is a need for an application to manage the settings. Mobile devices are easy to carry and use in conjunction with medical devices because of their user identification function. The health device (a) in Figure 5 provides a function to register and manage the medical device and its users, and the heath service provides a function to configure and manage monitoring

services provided by medical institutions. MyHealth provides a feedback service for healthcare using the data measured by the medical device.

Figure 5. Mobile Application for Binding Device and Service

When users place the mobile phone near the medical device to measure their own health information, they can see the notice message (b) in Figure 5, which confirms that the user and device are bound with each other. If users activate 'Proceed', the SVC in the MD in Figure 3 transmits Service.req and the results are seen in the mobile phone as shown in Figure 5 (c). Such a procedure is able to prove that the data to be transmitted is the data of the mobile phone user by the interaction between the medical device and mobile phone.

When the data-binding process is complete, data transmission between the medical device and monitoring service becomes possible. As shown in Figure 6 (b), the bound glucose meter transmits the data to a blood-glucose-monitoring service. After that the service sends a message confirming the reception of data to the user. This way the service provides a user-customized monitoring service through the accumulated data. My Health in Figure 6 (a) provides this function. As shown in (c), the monitoring services for blood glucose, weight, blood pressure and melliturıa are configured. As users set the service to receive the glucose service from Paris MC (Medical Center), the data measured by the glucose meter is stored in the glucose service provided Paris MC. If users want to view the detailed glucose monitoring information, they are able to see the feedback from practitioners or see their own accumulated data. In addition, users are able to customize theses services to their own preferences. Since the medical device interacts with the service dynamically, the data transmission location can change dynamically when the service is changed. Since the change of services does not lead to the stoppage of services, users can enjoy services more conveniently and effectively.

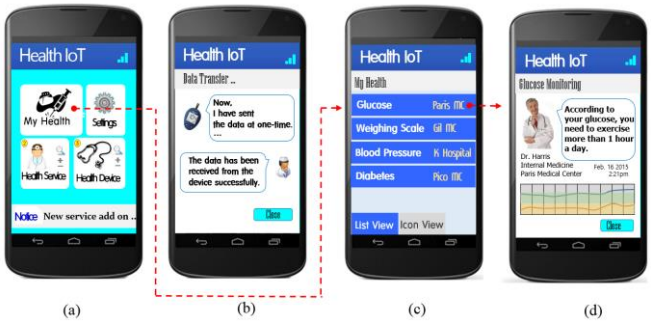

Figure 6. Mobile Application for Data Transfer and Health Service

5. Evaluation

Let's analyze the binding protocol running time. The time spent in transmitting the one-time data from the medical device via binding protocol can be calculated as the following expression (1). In this expression, the processes required to transmit the data shall be considered as shown in Figure 3 and t. Thus the time to receive the response for bind.req, service.req and data.req and $a_{0,}$ the time for the internal processing by the system shall be considered. However a_0 is regarded as a constant value since the amount is too small compared to the network time.

$$time_{onetimedata} = a_0 + \sum_{i=1}^{3} ResponseTime_i \qquad \begin{matrix} i=1 \text{ ; response for bind.req} \\ i=2 \text{; response for service.req} \\ i=3 \text{; response for data.req} \end{matrix} \qquad (1)$$

The time spent in transmitting not only one-time data but also streaming data may ray depending on the attributes (data amount, occurrence rate and sampling period) of the streaming data to be transmitted. To conduct an experiment to measure the time spent in transmitting one-time data, the author made a program for simulation in a Linux environment, implemented the protocol suggested in this paper as C for the factors of this experiment (*i.e.*, MD, PF, AT and SVC), and measured the response time of a total of 50 data entries in occurrence and processing.

Figure 7 shows the time spent in receiving bind.res from bind.req and the time spent in receiving service.res after transmitting service.req. It also shows the time spent in receiving data.res as a response after transmitting data including the data to transmit to data.res. As shown in Figure 7, relatively more time was spent for measurement in the initial stage, which is likely because of the overhead due to the time spent in identifying the location information on each network service as it is with network ARP cache update. Furthermore, the author could obtain the transmission time within the range of 60-90ms because the experiment was conducted in the same LAN environment.

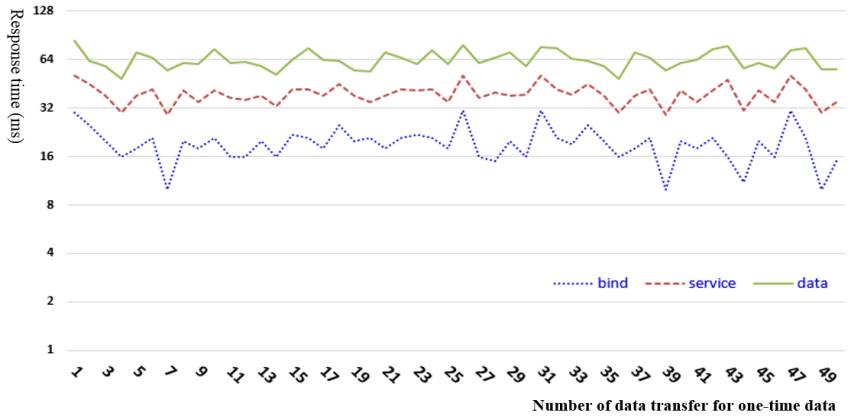

Figure 7. Time for Data Transfer of One-Time Data in Experiment

6. Conclusion

When the medical device is shared between multiple users within an IoT-based healthcare platform, users can enjoy user-customized monitoring serve using their mobile phone to interlock with the medical device for authentication. To this end, in this paper the author suggests a binding protocol enabling interaction between medical device, mobile phone and platform server. The suggested binding protocol is divided into two types of data transmission: the transmission of one-time data which varies every time the

data is measured (*e.g.*, blood pressures and weight) and the transmission of streaming data which occurs and is continuously transmitted (*e.g.*, heart rate or oxygen saturation).

This paper focuses on the transmission of data. However, since the data to transmit is important personal medical information, more detailed studies of security mechanisms are required to ensure the confidentiality and integrity of information. In particular, as the services are provided in an open platform, the personal security management is paramount

Acknowledgements

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under supervised by Incheon Information Service.

References

[1] A. Sarita, L. D. Manik, "Internet of Things – A Paradigm Shift of Future Internet Applications", Institute of technology Nirma university, **(2011)**, pp. 1-7.
[2] Gartner, http://www.gartner.com/newsroom/id/2636073
[3] S. S. Prasad and C. Kumar, "A Green and Reliable Internet of Things", Communications and Network **(2013)**, vol. 5, pp. 44-48.
[4] F. Mattern and C. Floerkemeier, "From the Internet of Computers to the Internet of Things Buchmann Festschrift", LNCS 6462, **(2010)**, pp. 242–259
[5] C. Min, W. Jiafu and L. Fang, "Machine-to-Machine Communications", Architectures Standards and Applications, KSII Trans. on Internet and Information Systems, pp. 480-497.
[6] T. Cohen, "Medical and Information Technologies Converge", IEEE Engineering Medicine and Biology Magazine, vol. 23, no. 3, **(2004)**, pp. 59-65.
[7] B. M. Lee and J. Ouyang, "Application Protocol adapted to Health Awareness for Smart Healthcare Service" International Workshop of Multimedia 2013, Advanced Science and Technology Letters, vol. 43, (**2013)**, pp. 101-104.
[8] B. M. Lee and J. Ouyang, "Intelligent Healthcare Service by using Collaborations between IoT Personal Health Devices", International Journal of Bio-Science and Bio-Technology, vol. 6, no. 1, (**2014)**, pp. 155-164.
[9] Google fitness platform service web, https://developers.google.com/fit/
[10] Samsung simband and SAMI, http://www.voiceofthebody.io/simband/
[11] Apple healthkit, https://developer.apple.com/healthkit/
[12] D. Li, D. Liu, X. Wang and D. He, "Self-reported habitual snoring and risk of cardiovascular disease and all-cause mortality", Atherosclerosis, (**2014)**, pp. 189-195.
[13] A. S. Shirazi, J. Clawson, Y. Hassanpour, M. J. Tourian, A. Schmidt, E. H. Chi, M. Borazio, and K. V. Laerhoven, "Already up? Using mobile phones to track & share sleep behavior", Int. J. Human-Computer Studies, **v**ol. 71, (**2013)**, pp. 878-888.
[14] Z. Chen, M. Lin, F. Chen, N. D. Lane, G. Cardone, R. Wang, T. Li, Y. Chen, T. Choudhury, and A. T. Campbell, "Unobtrusive Sleep Monitoring using Smartphones", Int. Conference on Pervasive Computing Technologies for Healthcare and Workshops, (**2013)**, pp. 145-152.
[15] http://www.jowbone.com
[16] http://www.fitbit.com
[17] http://www.hello.is
[18] J. V. Sorribes, J. C. Cano, C. T. Calafate and P. Manzoni, "UbiqBIOPARC, A Wireless and Sensor Based Context-Aware System for an Enhanced Guide Experience", The Journal of Multimedia Information System, vol. 1, no. 1, (**2014)**, pp. 11-22.
[19] S. Meyer, A. Ruppen and C. Magerkurth, "Internet of Things-Aware Process Modeling", Integrating IoT Devices as Business Process Resources, Advanced Information Systems Engineering, LNCS, **(2013),** pp. 480-497.
[20] D. Niewolny, "How the Internet of Things Is Revolutionizing Healthcare", White paper, (**2013).**
[21] V. M. Rohokale, "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control", International Journal of Bio-Science and Bio-Technology, vol. 6, no. 1, (**2014)**, pp. 155-164.
[22] B. M. Lee, "Healthcare Framework on the IoT open Platform", Service Model, Architecture, International Journal of Applied Engineering Research, **v**ol. 9, no. 24, (**2014)**, pp. 29783-29792.
[23] B. M. Lee, "Authorization Protocol using a NFC P2P mode between IoT device and Mobile phone, International Workshop Mobile and Wireless 2015, (**2015)**, pp. 85-88.
[24] B. M. Lee, "Requirements for a Mobile Service Model on a Personal Bio Record System for the elderly", International Workshop Ubiquitous Science and Engineering 2015, (**2015)**, pp. 81-84.
[25] R. Shahriyar, F. Bari, G. Kundu, S. Ahamed and M. Akbar, "Intelligent Mobile Health Monitoring System, Int. Journal of Control and Automation, vol. 2, no. 3, **(2009),** pp.13-28.

[26] C. S. Ryu, "IoT-based Intelligent for Fire Emergency Response Systems", Int. Journal of Smart Home, vol. 9, no. 2, **(2015)**, pp.161-168.
[27] B. M. Lee, "Personalized Service Model for Sharing Medical Devices in IoT Health Platform", Information Technology and Computer Science 2015, **(2015)**.

Author

Byung Mun Lee, He received a B.S. degree in 1988 from Dongguk University, Seoul, Korea and a M.S. degree from Sogang University and a Ph.D. degree from University of Incheon Korea, in 1990 and 2007. He had worked for LG Electronics for 7 years and was a visiting scholar professor for a year at California State University Sacramento, USA. He is currently a professor in the department of Computer Science, Gachon University, South Korea. His research interests are pervasive healthcare, its network protocol, IoT for healthcare, wireless sensor networks, operating system, etc.