International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.59-70
http://dx.doi.org/10.14257/ijsia.2015.9.10.05

Security of Personal Bio Data in Mobile Health Applications for the Elderly

[1]Jong Tak Kim, [2]Un Gu Kang, [2]Young Ho Lee and [2]Byung Mun Lee[†]

[1]*Research and Development Center, Medical Solution for People C & S, Incheon, Korea*
Department of Computer Engineering, Gachon University, Seognam-si, Gyeonggi-do, 461-701, South Korea
[1]*{ jongtakkim }@gmail.com ,* [2]*{ ugkang, lyh, bmlee }@gachon.ac.kr*

Abstract

Mobile devices used for heath can be used anywhere including homes or offices, thanks to their mobility and portability. Moreover since they are used for monitoring bio-information as well as medical services in hospital, there is an increasing possibility of the leakage of personal bio data, which in turn increases the possibility of spoofing that data. Therefore, it is critical to establish countermeasures for privacy protection. More specifically, there is an increasing need for secure transmission of personal bio data between mobile health applications and health servers which archive personal bio data. Thus in this study, the authors implemented a system which transmits personal bio data (e.g. blood pressure, blood pressures and weight, etc.) to the server safely without saving it in the mobile devices using MD5 and Spritz. To verify the security of the implemented system, the authors spoofed data and succeeded in detecting all spoofed data.

Keywords: *Mobile heath, Personal bio information, Encryption, MD5, Security, Threat*

1. Introduction

As of Mar 2015, the United Arab Emirates recorded the top mobile phone penetration rate in the world (90%), whereas South Korea ranked in 4th place (83%). Considering that the average penetration rate of all 56 countries measured was 60%, these countries ranked quite highly [1]. This implies that applications and services are developed and distributed for mobile devices [2-4]. Various contents and services (e.g. personal bio data monitoring, information on exercise, measuring activity/amount of exercise medical/health information, etc.) using mobile platforms are being studied in the healthcare industry [5][6].

However, unlike other fields, mobile health deals with personal bio data as well as privacy, so there is a significant risk of leakage of personal bio data and privacy issues. In the past, various technologies were developed to enhance security in wired network [7], but the development of mobile devices increases the importance of data security in wireless environments which are more vulnerable [8].

In general, medical institutions protect hospital information system (e.g. OCS (Order Communication System), EMR (Electronic Medical Record) and EHR (Electronic Health Record)) using firewall or intrusion detection systems [9-10]. Most privacy and personal bio data were managed and maintained safely in hospitals in the past. However, in recent years, privacy and personal bio data tend to be distributed though mobile devices, so there is no guarantee that such data will be used only in hospitals; furthermore, there is a high likelihood of data leak during

[†] Corresponding author

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

transmission. It is convenient to show personal bio data using mobile devices; however, this will increase the possibility of data leaks or spoofing. Thus, it is critical to seek countermeasures for information security.

The personal bio data stored in mobile devices can at least be protected from unexpected intrusion or malicious code.

In other words, it will be safer if the personal bio data received from the server are not saved in the devices after it is provided to users. In this context, there is a need for a process to handle personal bio data securely while transmitting and receiving it. In general, the degree of data security is determined by the presence of the guarantee of confidentiality and integrity.

Thus in this study, we intended to develop a secure data transmission method to guarantee the confidentiality and integrity of personal bio data against any intrusion when transmitting it data between mobile health applications and the health server; and to, implement and apply the healthcare mobile application and server so as to verify the extent to which they are capable of responding to intrusions upon confidentiality and integrity. In addition, the authors intended to verify the effectiveness of the suggested system through a test in which the authors eavesdropped and spoofed/falsified http messages during personal bio data transmission between the mobile application and the server in order to verify how the server identified and handled such intrusion.

In Section 2, we address the configuration and contents of the mobile health applications and PBR (Personal Bio Record) server which were studied in the past as well as the vulnerability of this system. In Section 3, we suggest a security model to resolve issues relating to the confidentiality and integrity of personal bio data. In Section 4, we implement the mobile health system with the suggested security model applied and perform a test to prove the effectiveness of the system in responding to this intrusion on confidentiality and integrity. In Section 5, we derive conclusions from this study.

2. Related Research

2.1. Mobile Healthcare System for the Elderly

A bad lifestyle degrades our physical activities and the quality of our life as well as inducing chronic diseases (e.g. obesity, hypertension and diabetes, etc.) [11-12]. In particular, as the ageing of population increases the percentage of the population with chronic diseases, health care for the elderly becomes a critical social issue[13-14]. In addition, to reduce increasing medical expenses for the elderly, it is essential that we make efforts to prevent or treat their diseases. To resolve the health issues of the elderly population, there is a need for moderate exercise, dietary prescription appropriate for health conditions, and regular healthcare, including regular health checks. Furthermore, since the mobile healthcare can sufficiently motivate the elderly to take care of themselves on a continuous basis, a mobile health system for the elderly is more meaningful.

These days, mobile health systems for the elderly are being studied and developed [15]. These systems provide the elderly with mobile health services by medical professionals and dietitians [16]. As shown in Figure 1, this system is composed of the mobile health applications used by doctors, dietitians and the elderly respectively as well as a PBR (Personal Bio Record) server. In this system, the elderly themselves measure their personal bio data (e.g. blood pressure, blood glucose, body weight and height, etc.) on a continuous basis, input the data and transmit it to the server. GPs check this personal bio data on a regular basis and write medical feedback [17-18]. The elderly and dietitians are able to check the medical feedback written by doctors and the dietitians then prescribe a

 Copyright ⓒ 2015 SERSC

customized dietary to suit each elderly person [19-20]. The elderly themselves are able to check their own bio data and maintain a healthy lifestyle with customized dietary menu. The use case diagram of a system that works this way is shown in Figure 2 [15].

Figure 1. Mobile Health System

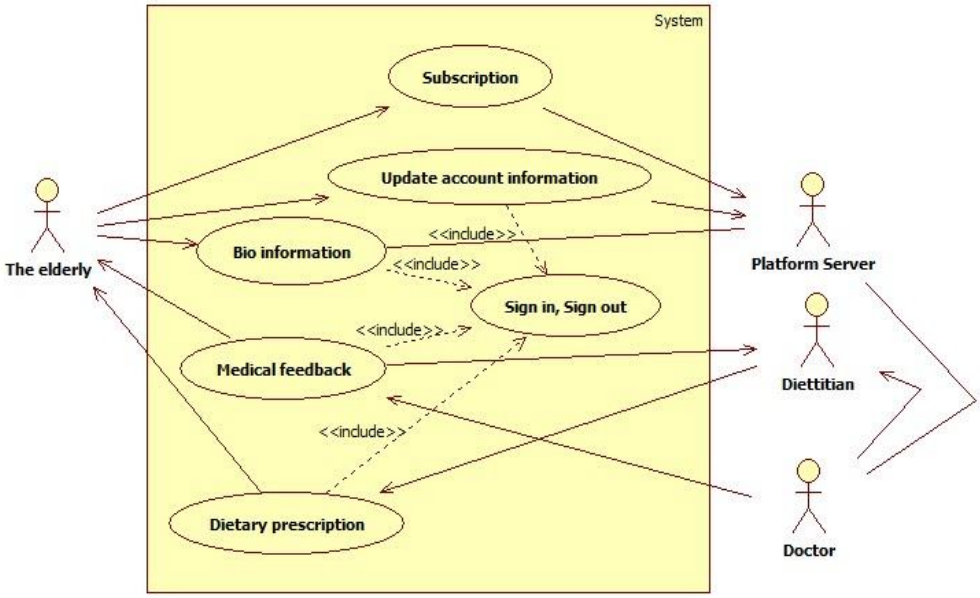


Figure 2. Use Case Diagram for Mobile Health System

In this system, the elderly receives services through mobile devices, so it is difficult to restrict their bio data to a limited space, such as home. Moreover since personal bio data is very sensitive, it must be protected from intrusion and attack. Thus, to protect personal bio data, it is necessary to understand the basic - principles of privacy protection. In the next chapter, we will address the basic principles and conditions required for privacy protection as well as vulnerabilities with the mobile health system.

2.2. Vulnerability of Personal Bio Data and Mobile Health Application

In general, to protect information, 3 conditions - confidentiality, integrity and availability - must be guaranteed. To protect confidentiality, specific information must be

Copyright ⓒ 2015 SERSC

provided only to authorized users, while unauthorized users must be prohibited from accessing these information. To protect integrity, only authorized users must be able to create and modify specific information, so unauthorized users must be prohibited from intentionally accessing data and forging or falsifying it. To provide availability, the devices and application which provide specific information and services must perform their intended functions without interruptions. Since availability greatly depends on the limited ability or capacity of the device, we will only address the confidentiality and integrity of personal bio data.

Vulnerability of User Authentication,

In order to distinguish whether or not a user is authorized, there is a need for a function to identify and authenticate the user. Most mobile applications require a user ID and password. This ID is used for recognizing users and the password for authenticating users. However if an unauthorized user appropriates someone else's ID or password, confidentiality and integrity can no longer be protected. In Figure 1, the system is vulnerabilities to user authentication, so there is a need for authentication of mobile devices.

Violation of Confidentiality

Personal bio data saved in mobile devices is more vulnerable to hacking or eavesdropping. Thus the sensitive personal information must not be saved on mobile devices. If the network traffic is sniffed, while mobile devices transmit the personal bio data to the health server, the data is likely to be leaked. As shown in Figure 3 (a), a height of 160 and the weight of 60 were input in the application. This data is sniffed using a tool such as Burp while it is being transmitted to PBR server. Since the data is transmitted as web messages (e.g. http) or network messages, it is possible to eavesdrop on all types of text.

Violation of Integrity

When transmitting bio information received from the mobile applications to the PBR server, there is the possibility of intrusion upon the integrity of the information. This is shown in Figure 3(b), in which the height and weight are spoofed from 160 and 60 to 167 and 75.

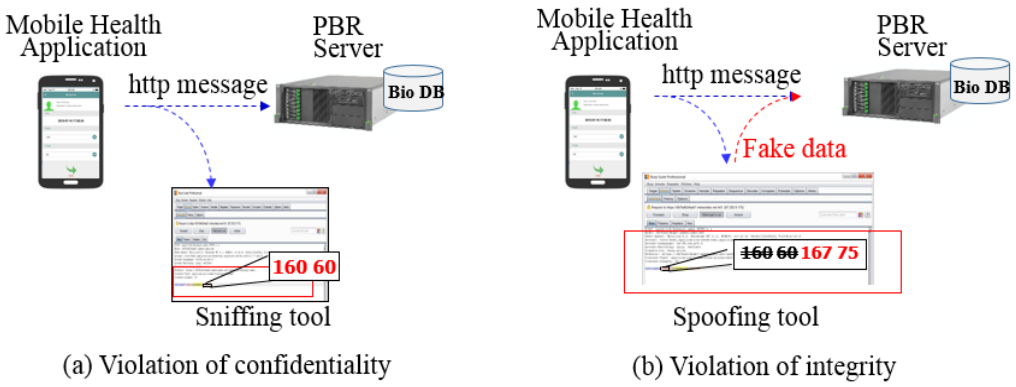


Figure 3. Scenario Showing of Data Violation during Transmission [15]

The spoofed information can be saved in the Bio DB. Most mobile applications uses http protocol packets in a text format; thus, the contents are at high risk of being spoofed

Copyright ⓒ 2015 SERSC

or falsified unless they are specially protected. Thus in the next chapter, we suggest a mobile device with a countermeasures against the violation of device authentication, confidentiality and integrity.

3. Security for the Mobile Healthcare System

3.1. Integrated Authentication for Mobile Healthcare System

The purpose of mobile health applications is to obtain the user's health information and state from the server and transmit it to the user. To do this, the user must first be registered. Before user authentication, ID and password (e.g. cell phone number) of the mobile device (e.g. mobile phone) must be registered with the server in advance. ID and password can be changed by the user at his or her discretion, but device ID is impossible to change since it was granted at the time the mobile service was first turned on. Therefore if device ID and user ID are integrated for authentication, it is possible to authenticate both the user and device at the same time.

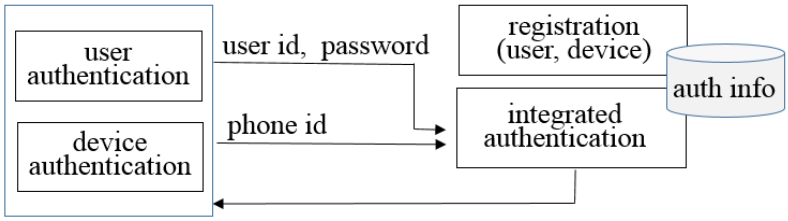


Figure 4. Integrated Authentication

As shown as Figure 4, the password contained in the auth info is converted to a hashing code using MD5 to be saved, implying that the password must be encrypted before transmission. Therefore this authentication model is very safe.

3.2. Confidentiality and Integrity for Mobile Healthcare System

To maintain the confidentiality of the bio-information input in the mobile application, it must be encrypted just before it is transmitted to the server.

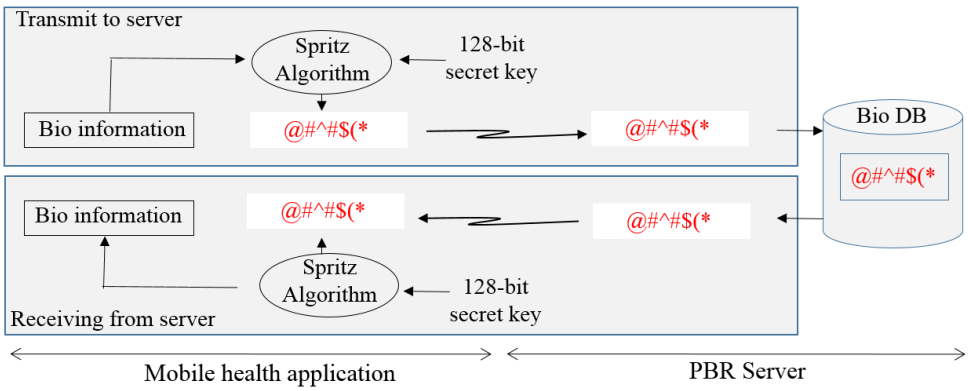


Figure 5. Encryption and Decryption

As shown in Figure 5, a Spritz encryption algorithm was applied to this system. Spritz has superior features and a similar structure that the RC4 algorithm used for TLS and WEP. In addition, it transmits the encrypted value using a 128-bit key and saves it in the Bio DB, which implies that the bio information is not leaked even if the server DB is

Copyright ⓒ 2015 SERSC

attacked or intruded upon. Furthermore the saved encryption is protected in mobile applications.

However, with the method presented in Figure 5, it is impossible to detect or block the data falsified during a man-in-the-middle attack. Thus, there is a need for additional security technique to ensure data integrity. More specifically, there is a need for a signature code which will guarantee that the encrypted information is neither spoofed nor falsified, which can be achieved by using MD5 hashing.

As shown in Figure 6, $E(m_i)$ should be obtained from Spritz encryption algorithm by using m_i and K. The $E(m_i)$ is a kind of cipher text, and it is provided to an MD5 hashing algorithm, and placing it before the encrypted $E(m_i)$ and composes a message to transmit

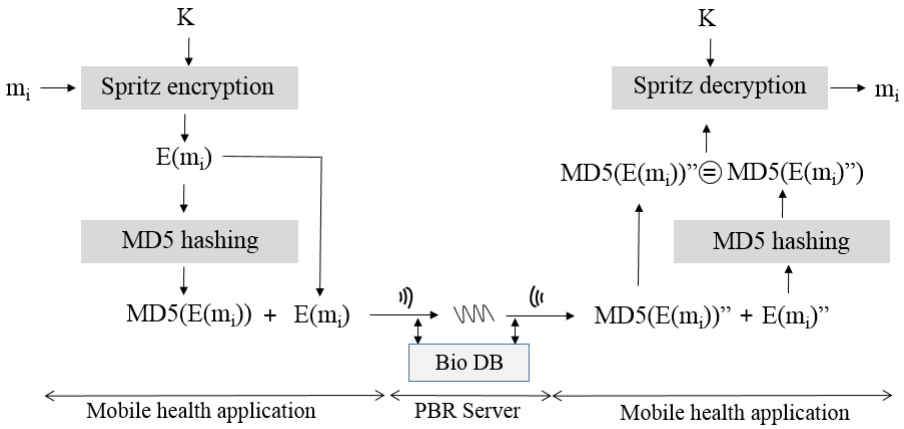


Figure 6. Integrated Encryption and Decryption with MD5

The reason for placing MD5 code before $E(m_i)$ is that parsing, which is required for decryption, is easy because the hashing code values are created at a the consistent length.

In the next chapter, the authors test the validity of security using a mobile health applications with 3 implemented security features (user authentication, mobile device authentication and an encryption technique to ensure integrity and confidentiality), and valuates the results.

4. Evaluation

4.1. Experiment Scenario by Using a Secured Mobile Health System

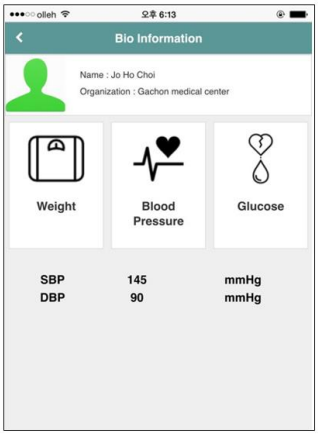
The mobile health applications implemented in this paper has the following features: log-in, bio-information input, bio-information retrieval, query referral and configuration. Figure 7 (a) shows an application user interface to input measured blood pressure. There is a window in which to input a simple profile, SBP (Systolic Blood Pressure) and DBP (Diastolic Blood Pressure) of the corresponding elderly user and two values are input. If the "SEND" button is clicked, the SBP and DBP value are encrypted as suggested in Section 3.2 and transmitted to the PBR server.

In Figure 7 (c), the blood pressure information transmitted is eavesdropped on via a sniffing attack. The sniffing attack tool used in (c) is Burp Suite. This tool extracts and indicates the http message information and is capable of modifying the information before transmitting it, thus; it is used in this test. As shown on the tool screen, an iPhone mobile device sends an http 1.1 message to the PBR server with the IP address of 192.9.44.51 and that is transmitted to an action variable for insertion in the DB. In addition, SBP and DBP values are encrypted (blue dotted line) and saved with hash code values (red solid line) in smaxpress and sminpress, respectively.

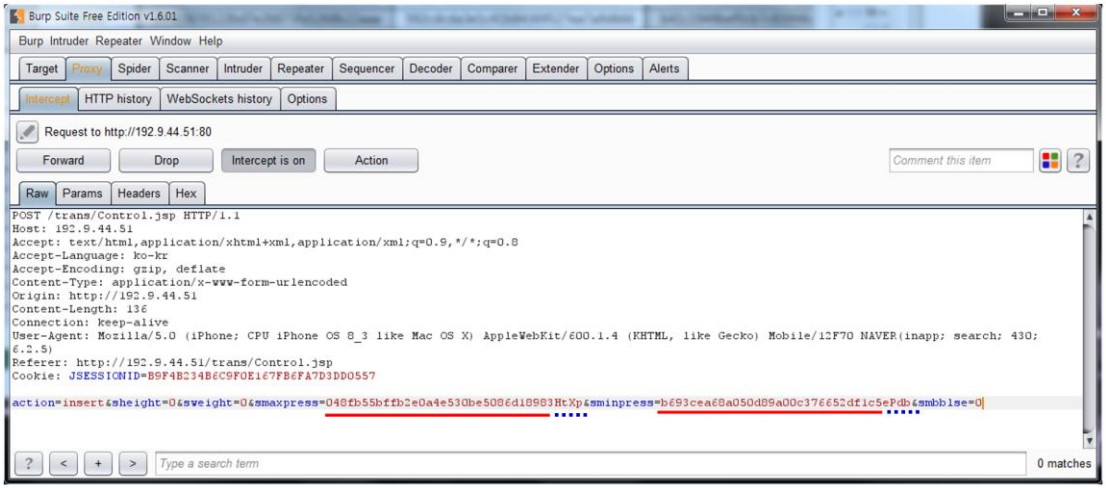
 Copyright ⓒ 2015 SERSC

The PBR receives http message and confirm its falsification using MD5 technique before saving it. If the message is not falsified, it saves the encrypted information in the DB. Figure 7 (d) shows the contents of the Oracle DB table. It confirms that HtXp and Pdb are saved in the MAX_PRESS and MIN_PRESS fields, meaning 145 and 90, respectively. Since the encrypted values are saved, they cannot be identified even through eavesdropping.

(a) Input SBP and BDP on the mobile



(b) Retrieve SBP and DBP from server



(c) Hash code and encrypted bio data in the http message

HEIGHT	WEIGHT	MAX_PRESS	MIN_PRESS	MB_BLSE	CHEK_DATE
0	0	HtXp	Pdb	0	15/07/16

(d) Stored SBP and DBP data in the Bio DB (Oracle)

Figure 7. Transmission of Blood Pressure between Mobile Application and Server

However, this requires a feature enabling a doctor or a dietitian to identify the health information of the corresponding the elderly person. In the result of decryption, 145 and 90, are presented in screen (b).

Copyright ⓒ 2015 SERSC

4.2. Evaluation Results

We tested weight, blood pressure and blood glucose as in Section 4. A single value is measured for weight whereas for blood glucose the measurement may be taken 6 times: before and after breakfast, before and after lunch and before and after dinner. However, the blood glucose was taken only before breakfast for this test.

The weight test was performed 10 times and the values were taken by stage (e.g. the values obtained by Epritz encryption of the weight input by users and MD5 hash code obtained using the former values (A); and the values of intentionally falsified weight for the integrity test and the hash code value obtained using the former values(B)). If (A) and (B) are different, that indicates a falsification whereas if (A) and (B) are identical, that indicates no falsification. The results in Table 1 indicate that (A) and (B) are not identical, implying that they were falsified. In the case of the 5th example, value 98 was encrypted and "Pih" was obtained. "ba85989bcbe6c9ab2dc1190755a9baa9" was obtained by converting "Pih" using MD5 hash code. If the encrypted weigh or hash code was neither spoofed nor falsified, the server receives identical values and the hash values obtained by "Pih" are identical to the received hash code value, indicating that there was no spoofing. However, as shown in Table 1, different code values are obtained in the event of spoofing. This implies that the security check was carried out successfully (1).

Table 1. Experiment Results with Weight Data

Num-ber	Weig ht	Encryp ted	Hash code from encrypted data (A)	(Fake) weight	Hash code from fake data (B)	Security chk
1	67	MFb	badaf1ade62de9f69fdbbbc16da5141c	bbbb	b9e5933f6c59b88f24e8a9cd94a8a548	1
2	60	Mdb	7ea6ef7997367bf55ca44b607ed9425d	abc	29531e4a89997b85b8ba73833d7ecb68	1
3	67	MFb	945952b661ff991d2e32241bb1e0e64e	123	b9e5933f6c59b88f24e8a9cd94a8a548	1
4	45	Kxb	4a5e45423c2adeecd4504581a9d7554c	pbr	fbde317e5d66e651f96ab0030e820180	1
5	98	PJb	ba85989bcbe6c9ab2dc1190755a9baa9	hjs	069f89bff3aa69bd06b1ad177b0b8ffa	1
6	66	MBb	f8c6f7f3ad1aca08ba042296cc20c944	sns	d34f5710ac312d1ed41d1906a1e8527e	1
7	58	LJb	bb5f5f8362282241c4acb7d1bae96f3a	5284	592cdcda3e1c41b84369527ea7a9d666	1
8	102	Hdbo	87e33fa26968cbed200492ec1456efed	EfGh	6f0204db1358b85b20923dc62e14ed79	1
9	58	LJb	39987678122bd7e26873fa5268b22aaa	DDDD	592cdcda3e1c41b84369527ea7a9d666	1
10	63	Mpb	6a6bba40c5b1059e038a42b8dcb43d35	FFFF	d71292a817ef443517a2ca2184dff1ee	1

Table 2 shows the results of security check using the systolic blood pressure values. 10 tests were performed and the values were obtained using the same method and procedures as those used for weight. In this case, both integrity and confidentiality were confirmed.

Table 2. Experiment Results with Systolic Blood Pressure

Num-ber	SBP	Encryp ted	Hash code from encrypted data (A)	(Fake) SBP	Hash code from fake data (B)	Security chk
1	136	Hpbp	e3da11462ed3b780c1c1e6a9ab10bba4	4321	e9dd929741582d52acbd9b5879318f8d	1
2	145	HtXp	048fb55bffb2e0a4e530be5086d18983	BPBP	b693cea68a050d89a00c376652df1c5e	1
3	137	Hprp	8f70a73c991914f3246555691ac6182a	AAAA	9b1e4feab0b4222046ccb488a7ce32df	1
4	155	HxXp	a31b2c4f9e22b3be44746dddfd7ef85c	EPL	1668e583107c664bf32a20ccc3802559	1
5	160	HBHo	7ea6ef7997367bf55ca44b607ed9425d	9999	4eb9a6cd815cb899e5b76e64852856f6	1
6	157	Hxrp	0eb6a050f76fadfb6610e07ac3128fbc	InS	83d1cbedd19c8cc3f4a518249764cead	1

 Copyright ⓒ 2015 SERSC

7	141	HtXo	23d8966d6c7e594d8be22c78943ec81a	YYYY	b0d132d17cb258aeeb1acb274a5b8288	1
8	171	HFXo	bb5f5f8362282241c4acb7d1bae96f3a	GA	bc621a477ef52fae7d345b61a791ad91	1
9	140	HtHo	4cc041b629459f0f6cbb365ff43263cd	8888	2ce455af71c7451052ce599c82a3f8e1	1
10	150	HxHo	240362c958c158365623a88aef252ea1	GGGG	b693cea68a050d89a00c376652df1c5e	1

Table 3 shows the results of the test using the blood glucose values measured before breakfast. The test was performed a total of 10 times to obtain blood glucose values and they were transmitted and measured using the same methods and procedures as those for the other tests. In this case as well, the results met the criteria for integrity and confidentiality.

Table 3. Experiment Results with Glucose before Breakfast Meal

Num-ber	Gluc ose	Encryp ted	Hash code from encrypted data (A)	(Fake) Glucose	Hash code from fake data (B)	Security chk
1	180	HJHo	15671aefd2e80a8367608cb410a3d677	BBc	880a1393b95efcf50d7896f3e398983c	1
2	199	HNXm	57717d5dc056325f9a38001a3582b60d	AaAa	5548f6b3b896d214889d6be66ad190f1	1
3	108	HdHm	4a0e326aaf553aa68ba39951d24608ca	bbCC	e9457a22d1427d66dd555128395033d2	1
4	85	Oxb	a964391735f27fcbfb2fd15aa8ad7d0b	Vga	f93978a3e627da4338437943cea728f0	1
5	205	IdXp	56bc9c39f80900dfa8984be60ab75bc3	MsP	a8e7f818cfe29124069d216b3d36609e	1
6	130	HpHo	96b9eaa243819eb52cca4a67d89629ac	CNs	9dad08af4e26845ac3840ee51936917e	1
7	178	HFHm	badaf1ade62de9f69fdbbbc16da5141c	3690	781397bc0630d47ab531ea850bddcf63	1
8	266	IBbp	9376689e5fda8e5d00cbd69fadb9b804	3B9c	0666c3e88e0d888b6e85258d73dd8781	1
9	136	Hpbp	e3da11462ed3b780c1c1e6a9ab10bba4	HHcp	614dc2f560df54fb304df7921fbfdbbf	1
10	102	Hdbo	6f0204db1358b85b20923dc62e14ed79	AAAA	098890dde069e9abad63f19a0d9e1f32	1

5. Conclusion

With an increase in the use of mobile health applications and services, there is a greater risk of intrusion upon personal bio data, previously used only in hospitals. When personal and medical information are transmitted through mobile devices, they can be conveniently viewed anywhere at any time; however, there is a much greater risk of leakage or spoofing, and thus, a better security method is needed.

Thus in this paper, the authors suggested a secure transmission method to protect the personal bio data transmitted by mobile health systems. We suggested a method integrating user authentication and device authentication in this paper. To prove the validity of the suggested system, this paper performed tests by transmitting the data with MD5 and Spritz encryption algorithms applied with the aim of ensuring the confidentiality and integrity of data.

Weight, blood pressure and blood glucose were measured, encrypted and transmitted. During transmission, the authors performed hacking tests intentionally using Burp Suite and the results of the server security check if met the criteria for this study. This suggests countermeasures to be taken for the storage of personal bio data in mobile devices and against man-in-the-middle attacks during the transmission of personal bio data to the server.

However, the authors focused primarily on the security of data transmission between mobile devices and the server, which requires expansion in a more secure manner than saving the personal bio data in the mobile devices. Thus, there is a need for further studies of secure local storage management.

Copyright ⓒ 2015 SERSC

Acknowledgements

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

Korea Association of Universities, Research Institutes and Industry (AURI), Gachon University Industrial-Academic Cooperation Group.

References

[1] DigiEco, Tap On The Door of Mobile First World, Trend Spectrum**, (2015)**
[2] Zhihan Lv: Wearable Smartphone: Wearable Hybrid Framework for Hand and Foot Gesture Interaction on Smartphone. Proc. of International Conference on Computer Vision Workshops (ICCVW), 2013 IEEE International Conference , **(2013).** 436--443
[3] G. Bailly, J. Müller, M. Rohs, D. Wigdor and S. Kratz.: Shoe-sense: a new perspective on gestural interaction and wearable applications. Proc. of the SIGCHI Conference on Human Factors in Computing Systems, **(2012)** 1239--1248,
[4] Silva, Bruno M.; Lopes, Ivo M.; Rodrigues, Joel J. P. C.; Ray, Pradeep Sapo Fitness: A mobile health application for dietary evaluation. Proc. of International Conference on e-Health Networking Applications and Services (Healthcom), , **(2011)** 375--380
[5] B.M. Lee, Editor. Requirements for a Mobile Service Model on a Personal Bio Record System for the elderly, Advanced Science and Technology Letter, (2015), Vol 86. pp. 81-84.
[6] Google fitness platform service web, https://developers.google.com/fit/
[7] W.D. Yu, L. Davuluri, M. Radhakrishnan, M. Runiassy: A Security Oriented Design (SOD) Framework for eHealth Systems. Proc. of international workshop on Computer Software and Applications Conference. **(2014)** 122--127
[8] K. Knorr, D. Aspinall : Security testing for Android mHealth apps. Proc. of IEEE 8th International Conference on Software Testing, Verification and Validation Workshops, **(2015)** 322--325
[9] M.J. Su, H.W. Zhang. Y.J. Lin, Y.H. Su, S.J. Chen, H.S. Chen, Editors. Pilot Study on a Community-Based Ubiquitous Healthcare System for Current and Retired University Employees. IEEE International Conference on Communications Workshops, 2009, **(2009)** June 14-18; Dresen
[10] T. Cohen, Medical and Information Technologies Converge. IEEE Engineering Medicine and Biology Magazine, **(2004)**, Vol. 23, No. 3, pp. 59-65.
[11] Richard K., Ele F., John B., Michael S. The Metabolic Syndrome Time: for a Critical Appraisal. Diabetes Care, (**2005)** , 28(9), pp. 2289-2304.
[12] American Diabetes Association, Standards of Medical Care in Diabetes. Diabetes Care, (**2010)**
[13] C. Thoma and R. H.R. Kelman, Unreimbursed expenses for medical care among urban elderly people. Journal of Community Health, **(1990)**
[14] C. Su and W. Yude, Editors. The care of the elderly with chronic disease based on electronic health records. International Symposium of ITME, **(2012)** August 3-5; Hokkaido, Japan
[15] J.T. Kim, H. J. Pan, Y. H. Lee, U.G. Kang, and B.M. Lee, Scenario for Secure Transmission of Bio-information between Mobile application and Health Server, Proceeding of International Conferences, CAN and ITCS 2015, **(2015),** Vol 99. pp. 176-179.
[16] B.M. Lee, Editor. Requirements for a Mobile Service Model on a Personal Bio Record System for the elderly, Advanced Science and Technology Letter, **(2015)**, Vol 86. pp. 81-84.
[17] B.M. Lee, Editor. Authorization Protocol using a NFC P2P mode between IoT device and Mobile phone, Advanced Science and Technology Letter, **(2015)**, Vol 94. pp. 85-88.
[18] P. Chen, Y. Liang and T. Lin, Editors. Using E-Plate to Implement a Custom Dietary Management System. IEEE International Symposium on Computer, Consumer and Control, **(2014)** June 10-12; Taichung
[19] N. Ukita and M. Kidode: Wearable virtual tablet: fingertip drawing on a portable plane-object using an active-infrared camera. Proc. of the 9th international conference on intelligent user interfaces, IUI '04, **(2004)** 169—176
[20] A. Depari, A. Flammini, E. Sisinni and A. Vezzoli, Editors. A wearable smartphone-based system for electrocardiogram acquisition. IEEE International Symposium on MeMeA, **(2014)** June 11-12; Lisboa

 Copyright ⓒ 2015 SERSC

Authors

Jong Tak Kim, He received B.S., M.S and Ph.D. degree in Computer Engineering, Incheon National University, Korea, in 1996, 2001 and 2008. He has worked Manager of U-Healthcare Department, BIT Computer Co., Ltd. He is currently Director of R&D Center, MSP C&S, INC, Korea. He research interests include u-healthcare, Context Awareness, Health IT, and Mobile Health Gateway.

Un Gu Kang, He received a received a M.S. and Ph.D. degree from Inha University, Korea, in 1998 and 2002. He is currently a professor in the School of Computer Science, Gachon University, Korea. His research interests include Software Engineering and mobile healthcare.

Youngho Lee, He received M.S. degrees from Hankuk University of Foreign Studies and a Ph.D. degree from Ajou University, Korea, in 1995 and 2007. He has worked for IBM Korea and was a research scholar at Arlington Innovation Center: Health Research Virginia Tech - National Capital Region. He is currently a professor in the School of Computer Information Engineering, Gachon University of medicine and science, Korea. His research interests include data mining and mobile healthcare.

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 Incheon National University, in 1990 and 2007. He had worked for LG Electronics for 7 years and was a visiting scholar professor at California State University Sacramento, USA. He is currently a professor in the department of Computer Engineering, Gachon University, South Korea. His research interests are pervasive healthcare, its network protocol, IoT for healthcare, wireless sensor networks, operating system, etc.

Copyright ⓒ 2015 SERSC

Copyright ⓒ 2015 SERSC