35th Annual International Conference of the IEEE EMBS
Osaka, Japan, 3 - 7 July, 2013

Design of Real-time Encryption Module for Secure Data Protection of Wearable Healthcare Devices

Jungchae Kim, Byuck jin Lee, and Sun K. Yoo*

Abstract— **Wearable devices for biomedical instrumentation could generate the medical data and transmit to a repository on cloud service through wireless networks. In this process, the private medical data will be disclosed by man in the middle attack. Thus, the archived data for healthcare services would be protected by non-standardized security policy by healthcare service provider (HSP) because HIPAA only defines the security rules. In this paper, we adopted the Advanced Encryption Standard (AES) for security framework on wearable devices, so healthcare applications using this framework could support the confidentiality easily. The framework developed as dynamic loadable module targeted for lightweight microcontroller such as msp430 within embedded operating system. The performance was shown that the module can support the real-time encryption using electrocardiogram and photoplethysmogram. In this regard, the processing load for enabling security is distributed to wearable devices, and the customized data protection method could be composed by HSP for a trusted healthcare service.**

I. Introduction

Recently, wearable devices were developed for healthcare services based on Wireless Sensor Network (WSN). They had a personal area network subsystem such as Bluetooth, Zigbee, and Infrared Data Association [1]. Also, they were combined with biosensor subsystem that measures the condition of a patient. Such wearable devices could generate the clinical data and transmit to a repository on could service for healthcare via wireless network infrastructure [2].

For examples, wireless sensor network based wearable smart shirt measures electrocardiogram (ECG) and acceleration signals for continuous and real time health monitoring, so the wearable sensor device could get clear ECG signal even though during running or physical exercise of a person[3]. And wearable pulse diagnosis system using exerting appropriate pressure on human radial artery was developed for non-invasive treatment and disease prevention by remote monitoring [4]. In addition, the wearable systems facilitate the management of chronic disease patient by monitoring daily behavioral activities, so it is possible to promote independent living [5-8]. Most of healthcare application using wearable device as shown in above studies had adopted the method that the collected medical data was transmitted to remote server or saved to a local memory.

In this process, the medical data will be disclosed by man in the middle attack. This problem causes a serious legal responsibility to stakeholders adopting healthcare service. Because Health Insurance Portability and Accountability Act (HIPAA) provides rights and protections for the personal healthcare record and states the obligation to protect the healthcare information [9][10]. However, the specific method for the data protection with wearable device has not been established yet. Furthermore, it is difficult to relevant level of security and privacy features in the wearable device for healthcare purposes [11]. Earlier studies have considered that their security policy was implemented in a gateway which communicates between wearable devices and remote server [11-12]. The methods with gateway including security policy are unsuitable for someone who wanders from place to place, because a gateway doesn't cover anywhere. Even though a gateway can be movable with someone, he must always possess a portable device for performing the security policy and communicating with remote server. That is, if a gateway doesn't support security policy, the medical data transmitted to the gateway may not be protected anymore.

In this paper, we proposed an encryption module to enhance secure transmission of wearable device. The encryption module is positioned between application layer and transmission layer, so any types of healthcare applications can use the data encryption service before transmitting to wireless medium. Our technical aspect focused on wearable device with 16 bit microcontroller because it has limited processing power to perform bio-signal acquisition, encryption, and data communication at the same time. So the Advanced Encryption Standard (AES) was implemented for encryption procedure considered optimal code size, and was compiled using "msp-gcc" for MSP430 chipset. Our main goal is that a wearable device can perform encryption in real-time without hardware accelerator. Our criteria are best effort to satisfy the needs of wearable device such as a small size, low energy consumption, and reliable performance.

The rest of this paper is organized as follow: Section II introduces about applicable healthcare scenario at first. Next, describes about hardware platform and software framework. In Section III, we evaluate the performance of our encryption module, and compared with other encryption algorithms. Section IV concludes this study.

*This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2010-0026833), and this work was supported by The Ministry of Knowledge Economy (MKE) grant funded by The Korea government(10031993).

Jungchae Kim is with the Graduate Programs of Biomedical Engineering, Yonsei University, Seoul, South Korea (e-mail: jungchkim@gmail.com).

Byuck jin Lee is with the Graduate Programs of Biomedical Engineering, Yonsei University, Seoul, South Korea (e-mail: bjlee1397@gmail.com).

*Sun K. Yoo is a professor at the Dept. of Medical Engineering, Yonsei University, Seoul, South Korea (corresponding author to provide phone: 82-2-2228-1919; fax: 82-2-363-9923; e-mail: sunkyoo@yuhs.ac).

978-1-4577-0216-7/13/$26.00 ©2013 IEEE

II. Methods

In our proposed method, the secret key is able to be managed by wearable devices' owner. So even if the medical data is assessed to illegal users, they cannot interpret the encrypted data. The applicable healthcare scenario was described in Fig. 1.

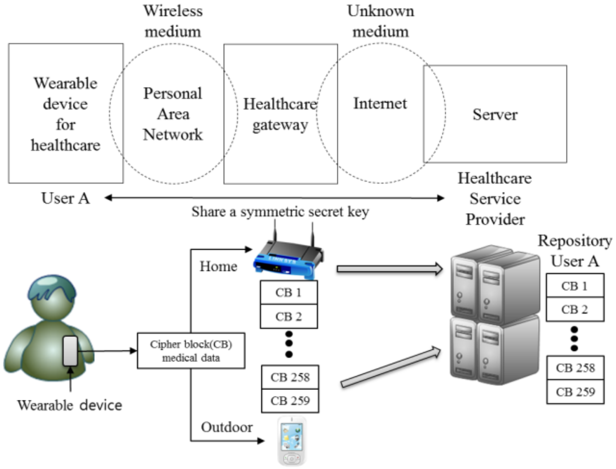

Figure 1. Applicable healthcare scenario using proposed encryption module.

A. Applicable healthcare scenario

A healthcare service provider (HSP) provides healthcare service to User A. The HSP can monitor the condition of client by collecting bio-signal from Users' wearable device. Before collecting the medical data, the HSP request a symmetric secret key to User A for decrypting the cipher block. User A has an authority to decide whether distributing the key or not. In this regard, the possibility of medical data disclosure is reduced because the medical data is encrypted in the wearable device. In this scenario, the healthcare gateway is mainly in charge of data communication between User A and HSP. It is possible that our data protection policy is preserved in case of the changing main gateway from home to outdoor because the encryption module is implemented in wearable device independently.

B. Hardware platform

We adopted Telos Rev. B for wearable device platform. It is an ultra-low power consumption wireless sensor module developed by UC Berkely, and mostly used to wireless sensor network researches. It has TI MSP430 microcontroller embedding12 bit analog to digital converter. Also, it supports 48 KB size of program memory and 10 KB size of RAM and IEEE 802.15.4 for wireless subsystem using Chipcon CC2420. It is designed to operate at a minimum voltage of 1.8v as ultra-low power module, and to communicate with workstation using universal serial bus interface [13]. In this paper, we combined Telos Rev. B and biosensor subsystem using electrocardiogram (ECG) and photoplethysmogram (PPG). The identical biosensor subsystem in our previous research paper was used as shown in Table 1 [14].

TABLE I. THE SPECIFICATIONS OF BIOSIGNAL SUBSYSTEM

Bio-Signal	Specifications		
	Bandwidth	***Gain***	***Sensor interface***
ECG	0.01-250Hz	1000	Ag-AgCl
PPG	0.05-16 Hz	4	TDS2000 (BIOPAC co.)

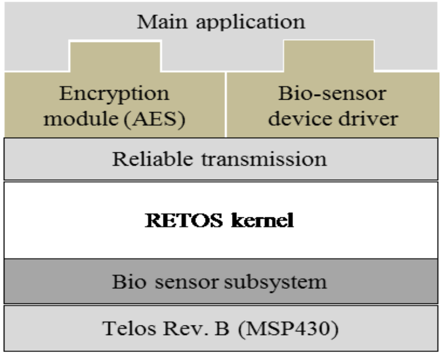

Figure 2. The system artitecture of designed wearable device

C. Software framework

Our software framework, as shown in Fig. 2, It was designed as well-structured stack with operating system, reliable transmission system call and two dynamic loadable modules.

1) Operating system

RETOS (Resilient, Expandable, and Threaded Operating System for Wireless Sensor Network) supports multi-threaded programming interface. It separates kernel and application for reliable operation and supports dynamic loadable kernel module programming for expandable system. It provides some system calls, so we include the reliable transmission system call for wireless communication [15]. RETOS is a closed source project but the kernel image and its tutorial are available in their website [19].

2) Encryption module

Advanced Encryption Standard (AES) is the currently adopted encryption standard to be recommended by National Institute of Standards and Technology to replace DES [16]. It was originally called Rijndael that was proposed by Vincent Rijmen and Joan Daemen [17]. AES is a block cipher based on symmetric encryption. That is, 128-bits size of block can be encrypted at once. We implemented AES for MSP430 chipset and complied with "msp-gcc". To use the encryption module, there are two interfaces for setting secret key and encrypting a cipher block.

3) Bio-sensor device driver

Bio-sensor subsystem is an extension hardware distinguished with WSN platform. To interface this external device, main application has to access WSN hardware address directly. But operating system doesn't allow this illegal access. Thus, we made device drivers to interface main application and WSN platform. To use the bio-sensor subsystem, there are two interfaces for initializing the subsystem and acquiring the result of analog-to-digital conversion.

4) Main application

The main application based on multi-threaded programming is composed with three multithreads and a main function. This application calls quantized bio-signal to fill the 128-bti block continuously. When the block is filled with bio-signal data, it encrypts the block and transmits the block to receiver [14].

5) Real-time monitoring server

Fig. 3 is the real-time monitoring server. This application was developed by Microsoft Visual Studio 2010 with National Instrument Measurement Studio 2010 on .Net framework 4.0. The cipher block is transmitted from a wearable device in real-time, and the cipher block is decrypted to plain block at the same time.

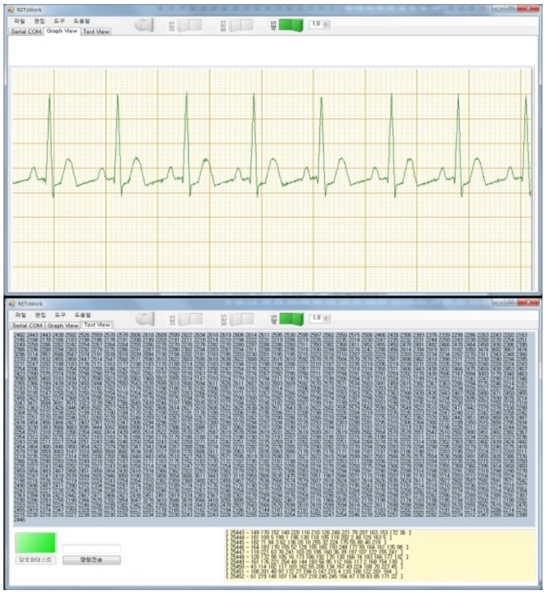

Figure 3. The real-time monitoring server

III. RESULTS AND DISCUSSION

In previous study [14], we developed DES and 3DES for encryption algorithms. At first, we compared the code size among encryption algorithms because the wearable device has limited resources. And next, we measured the performance of real-time encryption module. NETECH MiniSim 1000 Patient Simulator was used for generating simulated ECG.

A. Code size and encryption time

The result of code size is described in Table II. AES demands the largest code size but AES are more powerful algorithm than DES and 3DES [18]. As shown in Table III, AES have the double size of cipher block, and it is faster than DES and 3DES. Through the experimental results, we confirmed that the performance of real-time bio-signal encryption was improved by using AES.

TABLE II. THE SPECIFICATIONS OF BIOSIGNAL SUBSYSTEM

(byte)	DES		3DES		AES	
	ROM	RAM	ROM	RAM	ROM	RAM
Code	8358	2176	8854	2176	9800	6094

TABLE III. A BLOCK ENCRYPTION TIME COMPARED WITH [14]

	DES	3DES	AES
Block size	64 bit	64 bit	128 bit
Encryption time avg.	1.802 ms	6.683 ms	2.295 ms

B. Evaluate module performance

The cipher block was displayed as a chaotic waveform both Fig.4 and Fig.5. When the cipher block is decrypted to the plain block in real-time, the waveform is displayed as a readable ECG waveform. Through the performance evaluation, we confirmed that the encryption module can operate in real-time encryption and support the interoperability between wearable device and workstation.

C. Discussion

Both Fig. 4 and Fig. 5 represent abnormal heart rhythms. These waveforms include the condition of someone, so the medical data from wearable device must protect from the man of in the middle attack. We designed the encryption module for wearable devices to reduce unexpected disclosure.

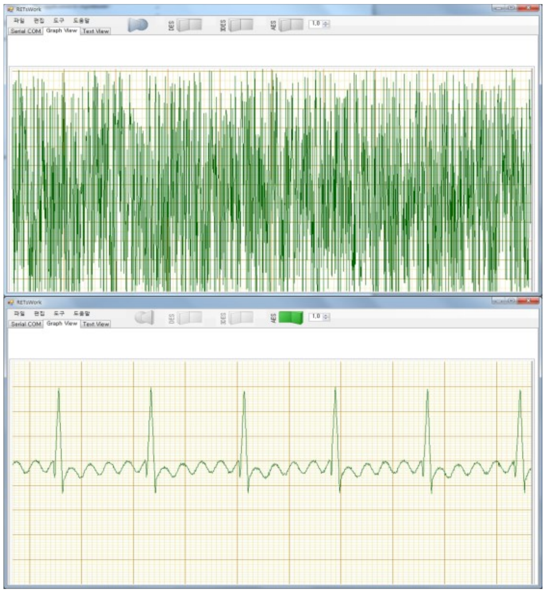

Figure 4. The result of arterial flutter wave: the above noisy waveforms describes the cyphered ECG, and the bottom shows a decrypted ECG waveforms.

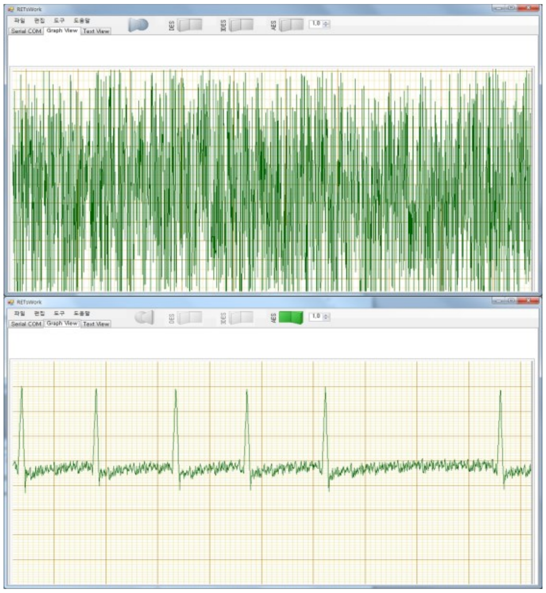

Figure 5. The result of arterial fibrillation wave: the above noisy waveforms describes the cyphered ECG, and the bottom shows a decrypted ECG waveforms.

IV. CONCLUSION

It will be more important that the healthcare service using wearable device in the future. The development of communication technology is accelerating this trend. The risk of leakage of data that is transmitted over the network fundamentally cannot be ruled out. We proposed the method that protects the private medical data from wearable device without gateway. Even though proposed method does not solve all of the security issues, it can support strong confidentiality. By implementing AES, the encryption module can comply with international standard and the performance was improved from our previous research [14]. This study is the one of method about the security policies in wearable healthcare device. In future work, we will study how to apply for proposed method in the actual healthcare services.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2010-0026833), and this work was supported by The Ministry of Knowledge Economy (MKE) grant funded by The Korea government(10031993).

REFERENCES

[1] H. Alemdar, C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Computer Networks*, 54(15): pp.2688-2710, May 2010.

[2] K. JeongGil, L. Chenyang, M. B. Srivastava, J. A. Stankovic, A. Terzis, M. Welsh, "Wireless Sensor Networks for Healthcare," *Proceedings of the IEEE*, 98(11): pp.1947-1960, November 2010.

[3] Y. D. Lee, W. Y. Chung, "Wireless sensor network based wearable smart shirt for ubiquitous health and activity monitoring," *Sensors and Actuators B: Chemical*, 140(2): pp.390-395, May 2009.

[4] G. Jibing, L. Shilong, W. Rui, C. Li, "PDhms: Pulse Diagnosis via Wearable Healthcare Sensor Network," *Communications (ICC), 2011 IEEE International Conference on*, pp.5-9 June 2011, 1-5.

[5] A. K. Bourke, S. Prescher, F. Koehler, V. Cionca, C. Tavares, S. Gomis, V. Garcia, J. Nelson, "Embedded fall and activity monitoring for a wearable ambient assisted living solution for older adults," *Engineering in Medicine and Biology Society (EMBC), 2012 Annual International Conference of the IEEE*, Aug. 28 2012-Sept. 1 2012, pp.248-251.

[6] A. G. Bonomi, K. R. Westerterp, "Advances in physical activity monitoring and lifestyle interventions in obesity: a review," Int J Obes, 36(2): pp.167-177, May 2012.

[7] L. Atallah, B. Lo, R. King, Y. Guang-Zhong, "Sensor Positioning for Activity Recognition Using Wearable Accelerometers," *Biomedical Circuits and Systems, IEEE Transactions on*, 5(4): pp.320-329, August 2011.

[8] C. Bellos, A. Papadopoulos, R. Rosso, D. I. Fotiadis, "CHRONIOUS: A wearable platform for monitoring and management of patients with chronic disease," *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE*, Aug. 30 2011-Sept. 3 2011, pp.864-867.

[9] HIPAA, “Summary of the HIPAA Privacy Rule,” http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last accessed Feb. 2013.)

[10] M. Ameen, J. Liu, K. Kwak, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications". Journal of Medical Systems, 36(1): pp.93-101, February 2012.

[11] L. Shinyoung, O. Tae Hwan, Y. B. Choi, T. Lakshman, "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring," *Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on*, 7-9 June 2010, pp.327-332.

[12] L. Xiaohui, M. Barua, C. Le, L. Rongxing, S. Xuemin, L. Xu, H. Y. Luo, "Enabling pervasive healthcare through continuous remote health monitoring," *Wireless Communications, IEEE*, 19(6): pp.10-18, December 2012.

[13] J. Polastre, R. Szewczyk, D. Culler, "Telos: Enabling Ultra-Low Power Wireless Research," *Information Processing in Sensor Networks 4th International Symposium on*, pp. 364-369, Los Angeles, USA, April 2005.

[14] Jungchae Kim, Sun K. Yoo, “Design of Reai-time Vital-Sign Encryption Module for Wearable Personal Healthcare Device,” *Journal of The Institute of Electronics Engineers of Korea*, 50(2):pp.193-203, February 2013.

[15] H. Cha, S. Choi, I. Jung, H. Kim, H.Shin, J. Yoo, C. Yoon, "RETOS: resilient, expandable, and threaded operating system for wireless sensor networks," *In Proc. of IPSN’07*, New York, USA, 2007.

[16] S. P. Singh, R. Maini, "Comparison of Data Encryption Algorithms," *International Journal of Computer Science and Communication*, 2(1): pp.125-127, June 2011.

[17] J. Daemen, V. Rijmen, “AES Proposal: Rijndael,” Banksys/Katholieke Universiteit LeuvzXen, Belgium, AES submission, June 1998.

[18] A. Nadeem, M. Y. Javed, "A performance comparison of data encryption algorithms," *Information and communication technologies, 2005. ICICT 2005. First international conference on*, pp.84-89, 2005.

[19] RETOS tutorials. [Online]. Available: *http://retos.yonsei.ac.kr/quick.htm*.