Comparision & Analysis of HIGHT and SEED for the Protection of Biometric Information at U-Wellness Healthcare System

Jae-Pil Lee, Young-Hyuk Kim, Il-Kwon Lim, Jae-Gwang Lee, Hyun-Namgung, Jae-Kwang Lee
Department of Computer Engineering
Hannam University
Daejeon, Korea
{jplee, yhkim, iklim, leejk, ghnam, jklee}@newk.hnu.kr

***Abstract*- This paper is for patients with chronic conditions who use a patient monitoring service with a smart mobile at the U-WHS(Ubiquitous-Wellness Healthcare System). This system is for collecting and transmitting of biometric information in a wireless environment. Also, in order to protect biometric information at the U-WHS in a safe manner, a model applied with SEED algorithm including HIGHT, which has been designed based on previous studies [3] applying of the existing HIGHT algorithm, has been compared and analyzed.**

Keywords—Acceleration; wellness, HIGHT, SEED

I. INTRODUCTION

It is a global trend that rates of an aged population and of patients with chronic conditions and this trend is followed by the increase in social costs related with national health. In South Korea, the size of a Wellness industry is about 75.982 trillion won and it has a high growth rate of 7% comparing to GDP in 2009. The size of a global wellness market is estimated to be about $ $1.9 trillion, and the top 3 upper areas (aesthetics and anti-aging, fitness, nutrition and diet) are taking about 70% of the overall industry [1]. Currently, a paradigm of customer's health management has been changed to be prevention-oriented. Especially, a rate of patients with chronic conditions who require of continuance health monitoring is expanded throughout age groups. In order to resolve this situation, a Ubiquitous-Wellness Healthcare System has been studied.

U-Wellness Healthcare System is a system which can measure and manage biometric information of patients without any limitation on time and space, and it also pursues the optimum conditions in terms of physical, mental, sensual, social and intellectual areas [2]. U-WHS is a remote controlled health care system which integrates modern technologies onto wellbeing and fitness for supporting of individuals to reach or maintain to be active and pleasant mentally and physically.

Along the increase in needs of individuals to achieve of higher life quality, people tend to pay more attention on wellness. This concept of wellness is continuously expanded to an area of social responsibility and the expectation and importance of a wellness industry are getting higher as well.

In this paper, a health care service based on biometric information should be developed to be used at home, fitness center, and medical institute in the U-WHS environment, and this service model should be applied with HIGHT and SEED algorithms in order to protect individuals' biometric information in a safe manner and then compared and analyzed.

The previous study [3] applied HIGHT algorithm only to protect and transmit personal health information in a mobile environment for a medical service and patients monitoring service which uses a smart phone to transmit biometric information to the HIS(Hospital information system) based on u-RMPS (USN Remote Patient Monitoring System).

Just like the previous study, most of studies on a u-RPM model employ of HIGHT, focusing on security. Therefore, this study aims to analyze a service model employed with both HIGHT algorithm and SEED algorithm in the U-WHS environment for the comparison of HIGHT and SEED based on the previous study [3]. In the chapter 2, encryption algorithms are reviewed upon the corresponding studies, and in the next chapter, an overall system design and a model applied with encryption are reviewed and a conclusion and future study tasks are suggested.

II. RELATED STUDIES

A. *Comparison of HIGHTand SEED algorithm*

The overall structure of HIGHT and SEED is a Feistel transformation structure, and for HIGHT algorithm, a 64-bit encryption is outputted through 32 rounds by using a 64-bit plain text, 8 of a 8-bit whitening key and 128 of a 8-bit serve key. In case of SEED algorithm, it outputs a 128-bit encryption block through 16 rounds with a 128-bit plain text block and a 128- bit key("Fig. 1,2."). [7][8].

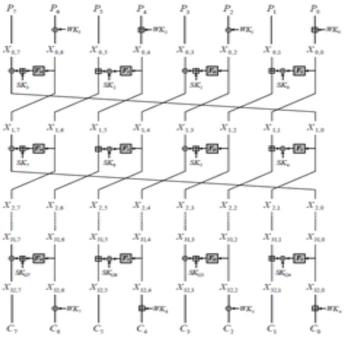


Figure 1 Structure of HIGHT

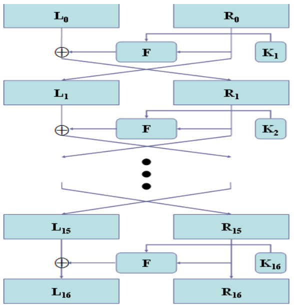


Figure 2 Structure of SEED

B. *Design of a DEB-based Real Time Biometric Signal Encryption Module*

"Fig. 2" is a scenario of a wearable PHD(Personal Healthcare Device)-based health care service in which an encryption module is applied..

When a PHD USER sets a password on his/her terminal, assessed biometric signals and PHI generated upon the assessed biometric signals are encrypted and transmitted to HSP(Healthcare Service Provider)의 HCRC(Health Care Repository and Clearinghouse) through a WPAN(Wireless Personal Area Network) and gateway, and saved there. As for the realization of algorithm, DES which can process with a bit operator is embedded in consideration ultra low power 16-bit micro controller to encrypt biometric signals in real time [5].

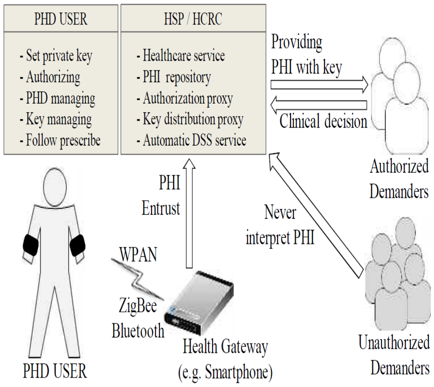


Figure 3 The wearable PHD based healthcare service scenario applied with proposed encryption module

C. *Attribute based Encryption*

A remote controlled health care monitoring is to provide a personalized medical service in which a service user transmits health-related data to a monitoring server and the monitoring service collects and analyzes these data to prepare a proper medical service in a wireless BAN (Body Area Network). The figure 3 shows a remote healthcare monitoring system employed with attribute based encryption. In order to share and use patients' data in a safe manner, it requires an authorization function which authorizes a proper user to get accessed to data and a withdrawal function which withdraws the authorization for accessing to data. This is a remote healthcare monitoring system which utilizes user attribute based encryption and have the aforementioned two features.

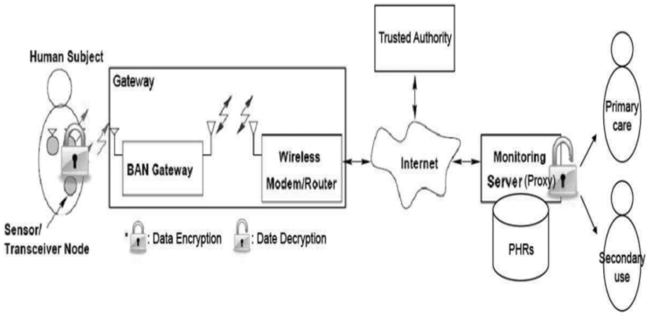


Figure 4 Healthcare Monitoring System Employed with Attribute Based Encryption

The remote healthcare monitoring system, employed with attribute based encryption, encrypts patients' data in a patients' attribute based access structure and then transmits the encrypted data to a monitoring server. Any doctor who is trying to share and utilize the encrypted data requests of decryption authorization to a monitoring server. A patient checks whether the doctor requesting of decryption authorization is a proper user who can use his/her personal data and then creates a delegation key and send to a monitoring server [6].

III. Design and Realization of U-WHS

u-Wellness Healthcare System of this study is composed as shown in the fig.4. This system has been designed for patients with chronic disease and use of a smart mobile. This system suggests the scope as a format of collection and transmission of biometric information of patients with chronic conditions. Types of biometric information are as follows- PID (patient identity), Breath, Heartbeat, Temperature, Pulse, and Momentum. Formats of data are varied. Therefore, the system transforms these variously formatted data into single format of 'string'. In order to collect randomly distributed biometric information, a SGM (Security Gateway Manager) is placed and biometric information sent by randomly placed sensor nodes are separated as an individual data with a separator of '_' and saved. Therefore, it is creased as a single frame and then divided into two models and applied with both HIGHT and SEED algorithm.

Through this, these two types of a model are encrypted and transmitted to a server of U-WHS and then again transmitted to a fitness center, home, and medical institutes[3].

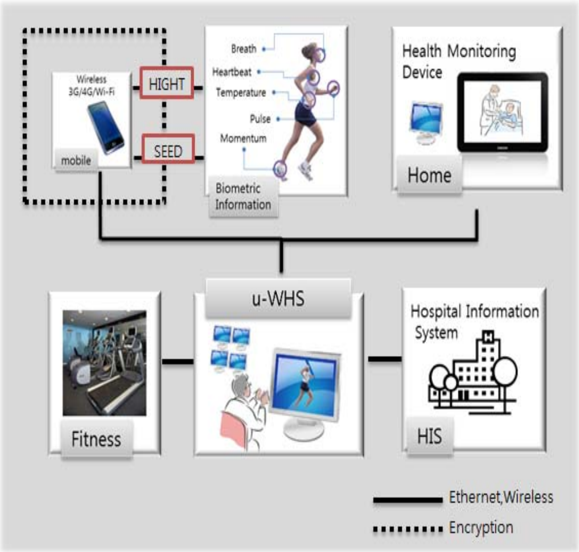


Figure 5 U-WHS configuration

A. *Design Model of HIGHT& SEED*

"Fig. 7" shows a model designed for the comparison and analysis of HIGHT and SEED algorithms, which are symmetric signal algorithms in a smart mobile environment, based on the previous study [3]. Therefore, HIGHT and SEED are applied to the same U-WHS design model in the HU-WHS environment. The overall scenario is as follows. Biometric information of patients with chronic conditions are collected through either SGM1 or SGM2. The SGM1 collects information on the PID and the SGM2 collects information on Breath, Heartbeat, Temperature, Pulse, and Momentum. Then, data format of both SGM1 and SGM2 changed to 'string'. It complies with a human body wireless network standard data frame size of South Korea [9][10], and each data is separated as an individual data with a separator of '_' and saved as the data payload format, and encrypted through a HIGHT and SEED algorithm process at a mobile and transmitted to the U-WHS or a medical institute.

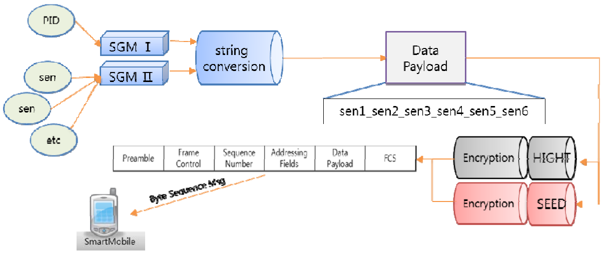
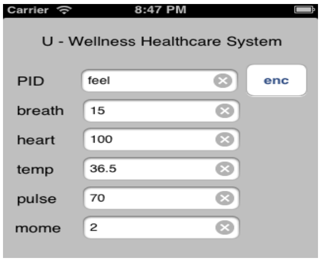


Figure 6 Model Applied with HIGTH & SEED in the Whole

B. *Realization*

As shown in the "Fig. 7", this study is for the comparison and analysis of HIGHT and SEED algorithms in the U-WHS environment. In case of biometric information collected at SGM, it requires of a patient with chronic conditions to wear sensor equipment. Therefore, in this study, virtual biometric data is created and based on this input value, mobile-based biometric information is inputted as the "Fig 7 & 8" and encrypted. For a development environment, a MAC OS X-based Xcode tool is used, and objective-C is used as a development language. This model is realized by applying HIGHT and SEED algorithms in the iOS simulation environment.



U - Wellness Healthcare System

PID feel
breath 15
heart 100
temp 36.5
pulse 70
mome 2

Figure 7 Mobile-Based Biometric Information System

Moreover, biometric information is converted in a string format and expresses mobile-based HIGHT & SEED encryption speed as the "Fig. 7." In case of HIGHT, the key length is 128 bits and input/output length is 64 bits and the number of rounds is 32. On the other hand, the key length and input/output length of SEED are 128 bits and 128 bits, respectively, and it has 16 rounds. HIGHT & SEED both use the same key length of 128bit. However, input/output key length of HIGHT is 64 bits, only half of SEED. Therefore, it was confirmed that HIGHT algorithm encryption speed was fast when it was applied onto encryption.

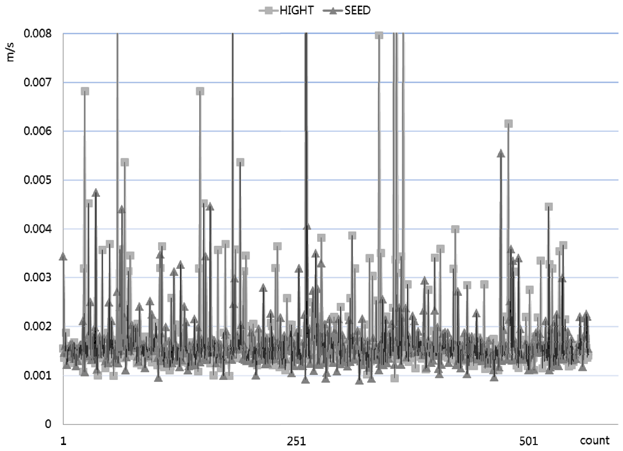


Figure 8 Expression of Encryption Speed of Mobile-Based HIGHT & SEED

IV. Conclusion

In this paper, the U-WHS service has been studied as a measure for resolving issues of patients with chronic conditions who require continuous health monitoring. Till now, studies on u-RPM service models have applied of only HIGHT, a mobile security standard. Therefore, based on the previous study [3], a model has been designed and realized for the comparison and analysis of HIGHT and SEED algorithms.

Results of the realization showed that HIGHT has faster encryption speed than SEED as shown in the "Fig. 10". Amid fast development of smart devices, a level of performance of these devices is increased at unprecedented speed as well.

Therefore, it is reasonable to expect that the scope of the application of encryption algorithm suitable for a smart mobile device would be increased in order to increase the security strength. It would be necessary to conduct a study on encryption performance tests for various mobile devices for protection of biometric information of patients with chronic conditions as well as the application of multiple algorithms.

Acknowledgment *(Heading 5)*

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0013029)

References

[1] National IT Industry Promotion Agency, "The industry development plan research through the business model analysis of the wellness industry", 2012.

[2] S.H. Park, D.G. Jang, "The IT Convergence tendency of the field of the wellness", 2013.

[3] Y.H. Kim, I.K Lim, J.K. Lee, "Mobile based HIGHT encryption for secure biometric information transfer of USN remote patient monitoring system, 2011

[4] Korea Internet & Security Agency, "HIGHT Algorithm Specification", 2009.

[5] Korea Internet & Security Agency, "SEED 128 Algorithm Specification", 2009.

[6] J.C. KIM, S.K. Yoo, "Design of Real-time Vital-Sign Encryption Module for Wearable Personal Healthcare Device", 2013.

[7] Y.J. Song, J.M. Do, "Remote Healthcare Monitoring System Using Attribute based Encryption", 2012

[8] TTAK.KO-10.0227: A method of transmitting PHY and Packet with an Interior of Human Body WBAN block base

[9] TTAK.KO-10.0301: A structure of network physical stages of human communication network physical structure