An Efficient Patient Information Transmission and Receiving Scheme using Cloud H-IoT System

Yoon-Su Jeong, Dong-Ryool Kim, Seung-Soo Shin

Abstract: ***The medical environment, combined with IT technology, is changing the paradigm for medical services from treatment to prevention. In particular infrastructure technologies such as big data and internet of things are being used in conjunction with the cloud as ICT convergence digital healthcare technology is applied to hospital medical systems. In particular, as medical services are used with IT devices, the quality of medical services is increasingly improving to make them easier for users to access. Medical institutions seeking to incorporate IoT services into cloud health care environment services are trying to reduce hospital operating costs and improve service quality, but have not yet been fully supported. In this paper, a patient information collection model from H-IoT(Hospital IoT)_system, which has established a cloud environment, is proposed. The proposed model prevents third parties from illegally eavesdropping and interfering with patients' biometric information through IoT devices attached to the patient's body at hospitals in cloud environments that have established H-IoT systems. In the proposed model, patients are now eligible for medical service by installing an IoT device, and medical staff can analyze patient disease information so that patients who visit the hospital can collect and receive treatment for diseases related to their eating habits. The disease information analyzed in the proposed model minimizes hospital work to facilitate the treatment and management of prescriptions according to the degree of disease in patients. On average, the time required for medical staff to collect and analyze IoT patient information was 7.8 percent lower than previous techniques. The results of 11.1% improvement in server efficiency for processing IoT patient information were obtained. The IoT medical information transmitted from IoT devices was 16.3% lower than the traditional technology, using diffusion band technology.***

Keywords : H-IoT, Cloud service, User privacy, Information analysis, eavesdropping, Biometric information.

I. INTRODUCTION

Recently, IoT technology is actively being studied in medical and electronic fields. As Internet of Things technology is applied to medical services, a number of different elemental technologies are integrated to effectively deliver medical services to users [1-3]. As IoT technology is applied to medical services, it is now possible to create new markets for medical services in hospitals. The Internet of Things in the medical service sector is being used as a means to strengthen the competitiveness of medical services such as the prevention and management of patient diseases.

The medical use of Internet of Things technology is different from other areas, such as reducing the time and cost of analyzing genetic information of users who receive medical services and checking health conditions as they are provided through genetic information analysis [4,5].

The medical sector uses IoT services to store and process large amounts of data around mobile phones to support seamless medical services. Because most IoT services used in the health care sector must provide users with a large number of medical data across a variety of networks, data management for IoT services is essential [6].

In this paper, an efficient information transmission receiving model is proposed to prevent third parties from illegally eavesdropping and interfering with patients' biometric information through IoT devices attached to patients' bodies in hospitals that have established H-IoT systems. The proposed model allows clinicians to analyze the user's disease information so that they can collect and treat diseases associated with the eating habits of patients visiting the hospital through IoT devices. The analyzed disease information minimizes hospital tasks to facilitate the handling of prescriptions and care according to the degree of illness of the user. The proposed model processes patient disease information based on the assumptions of two environments: First, they share a code in advance for encoding users' information. Second, the synchronization process for the user's disease information should take place in the patient's IoT device. The proposed model improved safety by adding user information collected through IoT devices to the code to encode the total probability component values of health information linked to a combination of different medical information so as not to be exploited illegally by third parties.

The composition of this paper is as follows. Chapter 2 explores IoT healthcare services and IoT medical research. Chapter 3 proposes a user information collection model for H-IoT systems that have built up a cloud environment, and Chapter 4 evaluates the proposed model in terms of performance and safety, and finally concludes in Chapter 5.

Revised Manuscript Received on July 22, 2019.

***** Correspondence Author

Yoon-Su Jeong, Department of Information and Communication Convergence Engineering, Mokwon University, Daejeon, Korea

Dong-Ryool Kim, School of Mechatronics Engineering, Tongmyong University, Busan, Korea

Seung-Soo Shin, Department of Information Security, Tongmyong University, Busan, Korea

II. PROCEDURE FOR PAPER SUBMISSION

A. H-IoT

IoT has increased equipment associated with smart sensors to ensure convergence and connectivity between devices while increasing interest in the field of wireless communications [1,6]. In an IoT environment, home automation and security systems should be controlled through a wireless network or smart city services managed. Various health care technologies are being commercialized through various wireless network equipment. IoT health care service equipment is applied to bracelets, cell phones, glasses and clothes using web-based application protocol to provide IoT health care service to users [2,5,7]. One of the essential principles for protecting privacy in an IoT environment is to minimize data [4].

B. Previous Research

A variety of studies have recently been proposed to provide medical services by applying IoT technology in the cloud environment. X. Cui et. al proposed a K-average-based medical information optimization technique using MapReduce to quickly analyze medical information used in medical services [8]. This technique used MapReduce(MR) to map data sets to the centroid using sampling techniques at the beginning and the end of the MR so that medical information is K-average. The W. Zhao et. al technique proposed an MR-based K-Means algorithm that could distribute medical information in parallel [9]. However, this technique randomly selected the initial seed to be multiple iterations in order to process medical information in large quantities. The Bahmani et. al technique proposed an algorithm that could be processed after equal clustering of medical information data [10]. The Cai et. al technique proposed a technique to modify the K-Means algorithm to classify large amounts of medical information into data sets of different sizes. This technique is characterized by multiple clustering without specifying the number of data sets in advance [11-13]. These techniques suggested techniques using the DBSCAN algorithm in MR. Some researchers have proposed techniques that have expanded the size of data sets to improve the performance of this technique [14,15].

III. PATIENT INFORMATION MANAGEMENT TECHNIQUES USING H-IOT SYSTEM BASED ON CLOUD ENVIRONMENT

Various ways to reduce the workload of hospital officials have been studied at hospitals recently by using the biometric information of patients visiting hospitals. Most patients who visit hospitals often visit hospitals to get treatment for illnesses caused by eating problems. To minimize hospital work, hospitals are currently using the IoT system to collect and analyze patients' biometric information without any sanctions. However, it is not easy to analyze accurate patient's disease information because such methods include and analyze noise generated by the patient's IoT devices. This section proposes patient information transmission techniques to prevent third parties from illegally eavesdropping and interfering with patients' biometric information through IoT devices attached to the patient's body at hospitals that have established cloud environment-based H-IoT systems. The proposed technique treats patient disease information based on the assumptions of two environments: First, codes for encoding patients' biometric information are shared in advance. Second, the synchronisation process for patient's disease information should be done on the patient's IoT device.

A. Overview

Recently, hospitals are changing their environment to check the health of patients visiting hospitals through sensors. The reason why the hospital environment has changed is because the number of patients visiting hospitals has increased compared to hospital staff, improving the efficiency of hospitals and the quality of medical services. In this paper, even if a third party wants to leak the patient's health status information, it is not possible to safely check the information of the partitioned code if the value of the total probability element of the personal information is unknown. In the proposed model, patients' health status information is sent and received with the following objectives: First, the proposed model performs synchronization using pre-shared codes between IoT devices and hospitals to encode medical information generated by patients' IoT devices. Second, the overhead is minimized so that the patient's biometric information can be minimized in order to minimize the noise generated by the medical team's.

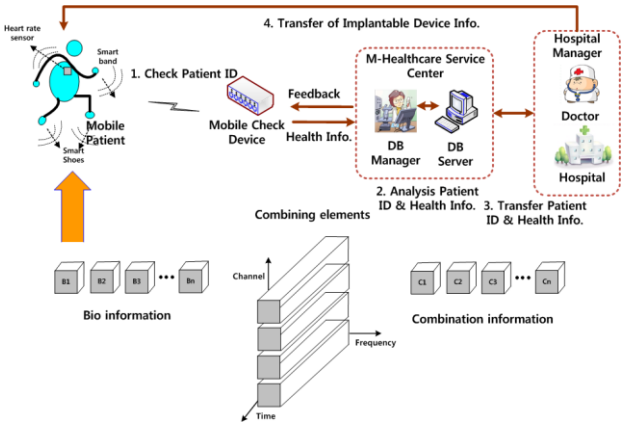

Fig 1. Overall Process of Proposed Model

Fig. 1 shows the process of encoding/decoding codes that occur when patient's disease information is collected and analyzed through IoT devices in the proposed model. Fig. 1 consists largely of four stages of detailed operation.

· Step 1: Patient disease information is collected through IoT devices attached to the body and communicated to the IoT gateway.

· Step 2: A number of patient information collected through the IoT gateway is transferred to the service center and stored in the database.

· Step 3: Information stored in the database is transferred to the clinical workforce or the clinical workforce accesses the patient's database.

· Step 4: The medical team analyzes the patient's information and feedback the analyzed information to the patient.

As with Fig. 1, the proposed model uses a combination of patient's medical information collected through IoT devices to link patient's medical information with different combinations of medical information. The link values added to a patient's medical information have the effect of not illegally exploiting the patient's medical information from a third party.

- Generate code for IoT medical information

IoT patient information process that is collected through IoT device in proposed technique is same as Fig. 2. To generate different signals, such as Fig. 2, the IoT patient information is generated by dividing it statistically into interleaved parts in time units.

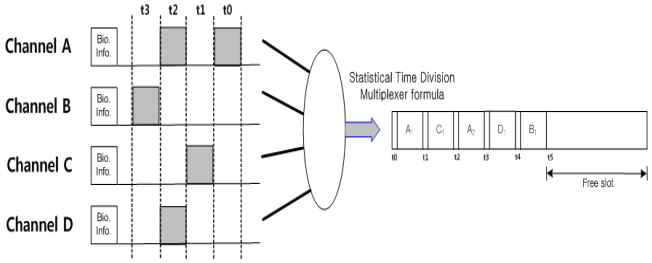

Fig 2. Code generation process for IoT medical information

As Fig. 2, when IoT patient information is generated from each IoT device, IoT patient information is collected by a designated frame size and stored in a temporary buffer along with one frame address area. The most recent IoT patient information frame stored in the buffer is allocated to and transmitted in a time slot. The server recognises IoT patient information by separating frames according to the address area of the received IoT patient information.

- Encoding/decoding of IoT medical information through code division

Proposed techniques use large bandwidth using IoT medical information that is transmitted from IoT devices. Proposed techniques generate code so that the server can receive and recognize IoT patient information generated from IoT devices. Code of IoT patient information generated performs modulation process such as encoding and decoding of IoT patient information signals so that the server can recognize them. In the proposed technique, the process of transmitting and receiving IoT patient information signals consists of five stages. The proposed technique does not allow the malicious use of patients' information signals alone, even if third parties illegally eavesdrop on patient information collected from IoT devices.

·Step 1: Modulation of IoT patient information signal

In the devices attached to the patient's body, IoT patient information signals are modulated first by using phase modulation and frequency modulation.

· Step 2: Modulation of the spread of IoT patient information

Signals with primary modulated IoT patient information perform modulation operation once more to increase bandwidth.

·Step 3: Transfer through a secure channel

Modulated signals of IoT patient information are passed to the server through a secure channel.

· Step 4: Perform secondary demodulation or reverse diffusion of IoT patient information

The server performs demodulation or reverse diffusion to encode signals from patients with widely modified IoT.

·Step 5: Information on IoT patients in primary order

Because secondary or reverse diffused signals are almost equivalent to primary spread IoT patient signals in IoT devices, they are output after primary demodulation.

IV. EVALUATION

A. Environment Settings

The data used in Table 1 were evaluated based on the results of the survey conducted on the medical staff (doctors and nurses) and staff in charge of administrative affairs at the medical institution using IoT devices from July 1, 2018 to August 31, 2018.

Table- I: Notations

Parameter	Setting
Period	July 1, 2018 to August 31, 2018.
Survey method	Wired Telephone and Visiting
Medical staff (doctor)	15
Medical staff (career)	20
Staff	25

B. Performance Analysis

Performance evaluation uses existing medical service techniques that provide medical services to patients without using IoT devices and proposed techniques that provide medical services to patients using IoT devices to conduct comparative assessments in three aspects: medical service care time, efficiency and overhead.

- Medical Service Hours

Fig. 3 is a result of the medical team analyzing patient information collected through IoT devices and evaluating the time needed to provide medical services to patients according to the number of medical staff. As with the results of Fig. 3, the amount of time it takes for medical staff to collect and analyze IoT patient information was 7.8% lower on average than previous techniques. These results are the result of analyzing information of IoT devices through codes given to IoT patient information.

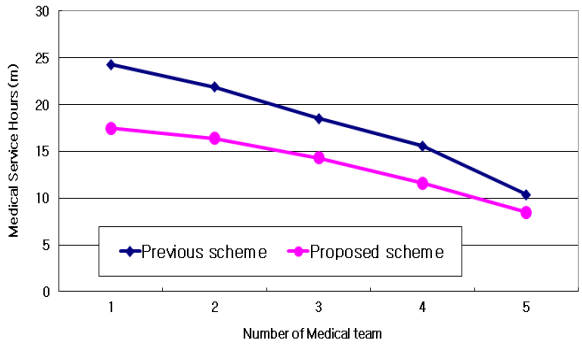

Fig 3. Medical Service Care Time to Analyze IoT Patient Information

- Efficiency

Fig. 4 is a result of comparing efficiency in the process of collecting and analyzing IoT patient information by the server with existing techniques when information collected through IoT device is delivered to the server. As a result of Fig. 4, the proposed technique resulted in an 11.1% improvement in the efficiency of the server for processing IoT patient information over existing technologies, as it was linked by generating a bit column of probability element values for different personal information by dividing and receiving patient health status information based on code division of various heterogeneous IoT devices. Such results prevent third parties from illegally eavesdropping on patient information collected from IoT devices in the course of sending and receiving IoT patient information signals, so the IoT patient information signals alone cannot be used maliciously. In addition, the proposed technique provides various IoT patient information of heterogeneous species with probability variables based on the joint probabilities, thus processing IoT patient information more efficiently than existing techniques.

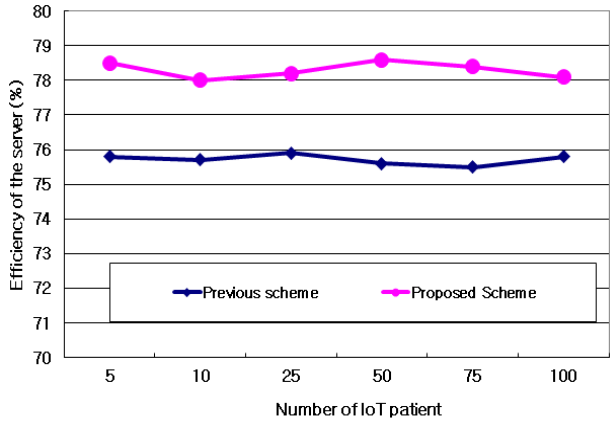

Fig 4. Server efficiency in collecting and processing IoT patient information

- Overhead

Fig. 5 is a result of comparing overhead that is handled by servers when IoT patient information is sent and received by servers. An experiment by Fig. 5 showed that IoT medical information sent from IoT devices utilizes diffusion band technology, showing that the overhead of the server was 16.3% lower than that of conventional technology. These results are the result of the modulating process of encoding and decoding by generating code so that the server can receive and recognize IoT patient information generated by IoT devices.

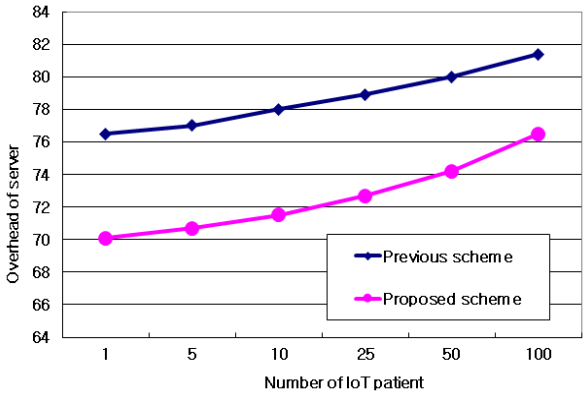

Fig 5. Overhead of server according to number of IoT patient information

V. CONCLUSION

The role of IoT technology in the medical service sector is very important, and it is used as a means to strengthen the competitiveness of medical services. In this paper, an efficient information transmission model was proposed to prevent third parties from illegally eavesdropping and interfering with patient's biometric information through IoT devices attached to the patient's body in hospital where H-IoT system was established. The proposed model minimized hospital work so that medical staff could analyze the user's disease information so that they could be collected and treated through IoT devices, and that prescribing and managing them easily according to the degree of the user's illness. The proposed model has enhanced the load reduction and throughput that can occur when decoding by adding to the code the overall probability element value of medical information linked to the combination of different medical information that divides users' IoT medical information into different codes of different sizes. According to the results of the experiment, the amount of time it takes for medical staff to collect and analyze IoT patient information was 7.8% lower on average than previous technologies. The proposed technique resulted in an 11.1 percent improvement in the efficiency of the server because it divided and received patient health status information based on code division and linked the probability element values for different personal information on the patient's health status information to each code. In addition, the proposed technology showed that the overhead of the server was 16.3% lower than that of the existing technology, using IoT medical information sent from IoT devices. In future research, the company plans to evaluate performance by applying it to the IoT system of other hospitals currently in operation based on the proposed technique.

ACKNOWLEDGMENT

This work was supported by the BB21+ Project in 2019

REFERENCES

1. G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
2. W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
3. H. Poor, An Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, ch. 4.
4. B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
5. E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.
6. J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," IEEE J. Quantum Electron., submitted for publication.
7. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
8. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 1987, pp. 740–741 [Dig. 9th Annu. Conf. Magnetics Japan, 1982,
9. T. H. Park. and B. N. Noh, "Survey and Prospective on Privacy Protection Methods on Cloud Platform Environment," Korea Institute Of Information Security And Cryptology, vol. 27, no. 5, Oct. 2017, pp. 1149-1155.
10. Y. S. Jeong, "An Efficiency Management Scheme using Big Data of Healthcare Patients using Puzzy AHP," Journal of Digital Convergence, vol. 13, no. 4, Apr. 2015, pp. 227-233.
11. Y. S. Jeong, "An Efficient IoT Healthcare Service Management Model of Location Tracking Sensor," Journal of Digital Convergence, vol. 14, no. 3, Mar. 2016, pp. 261-267.
12. Y. S. Jeong, "Measuring and Analyzing WiMAX Security adopt to Wireless Environment of U-Healthcare," Journal of Digital Convergence, vol. 11, no. 3, Mar 2016, pp.279-284.
13. A. Singh, and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, no. 1, Feb. 2017, pp. 88-115.
14. H. Bao, and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," IEEE Internet of Things Journal, vol. 2, no. 3, Mar. 2015, pp. 248–258.
15. J. Qian, F. Qiu, F. Wu, N. Ruan, G. Chen, and S. Tang, "Privacy-Preserving Selective Aggregation of Online User Behavior Data," IEEE Transactions on Computers, vol. 66, no. 2, Jul. 2017, pp. 326–338.
16. X. Cui, P. Zhu, X. Yang, K. Li, and C. Ji, "Optimized big data K-means clustering using MapReduce," Journal of Supercomputing, vol. 70, no. 3, Dec. 2014, pp. 1249-1259.
17. W. Zhao, H. Ma, and Q. He, "Parallel k-means clustering based on mapreduce," Proceedings of the 1st International Conference on Cloud Computing, Dec, 2009, pp 674-679.
18. B. Bahmani, B. Moseley, A. Vattani, R. Kumar, and S. Vassivitskii, "Scalable k-means++," Proceedings of the VLDB Endowment, vol. 5, no. 7, Mar. 2012, pp. 622-633.
19. X. Cai, F. Nie, and H. Huang, "Multi-view k-means clustering on big data," Proceedings of the Twenty-Third international joint conference on Artificial Intelligence, AAAI Press., Aug. 2013, pp. 2598-2604.
20. H. Karau, A. Konwinski, P. Wendell, and M. Zaharia, "Learning Spark: Lightning-Fast Big Data Analysis," O'Reilly Media, Inc., Jan. 2015, pp. 1-276.
21. Y. H. Kim, K. S. Shim, M. S. Kim, and J. S. Lee, "DBCURE-MR: an efficient density-based clustering algorithm for large data using MapReduce," Journal of Information Systems, vol. 42, Jun. 2014, pp. 15-35.
22. X. Cui, J. S. Charles, T. Potok, "GPU enhanced parallel computing for large scale data clustering," Journal of Future Generation Computer Systems, vol. 29, no. 7, Sep. 2013, pp. 1736-1741.
23. G. Andrade, G. Ramos, D. Madeira, R. Sachetto, R. Ferreira, and L. Rocha "G-dbscan: A gpu accelerated algorithm for density based clustering," Journal of Procedia Computer Science, vol. 18, Dec. 2013, pp. 369-378.

AUTHORS PROFILE

Yoon-Su Jeong is received the B.S. degree in the department of computer science, Cheongju National University in February 1998. He received the M.S. degree and Ph.D in the department of computer science, Chungbuk National University in February 2000 and 2008. He is currently working professor in the department of Information and Communication Convergence Engineering, Mokwon University. His research interests also include cryptography, network security, information security, healthcare service, bioinformatic, cloud service, wire/wireless communication security, Privacy, Big data.

Dong-Ryool Kim was born in Busan, Korea in 1967. He received a bachelor's degree in mathematics at Ulsan University. He received his master's degree in mathematics at Ulsan University in February 2001 and his doctorate at College of Education Kyung-nam University in 2005. He has been working in the Department of Engineering at the University of Tongmyong since 2005. His interest in research is also. Includes cryptographic technology, network security, information security and mathematics education.

Seung-Soo Shin is received the B.S. degree in the department of mathematic, Chungbuk National University in February 1988. He received the M.S. degree and Ph.D in the department of mathematic, Chungbuk National University in February 1993 and 2001. And He received the Ph.D in the department of computer engineering, Chungbuk National University in February 2004. He is currently working professor in the department of Information Security, Tongmyong University. His research interests also include cryptography, network security, information security