Indian Journal of Science and Technology, *Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/105098, November 2016* *ISSN (Print) : 0974-6846*
ISSN (Online) : 0974-5645

Smart Healthcare Service Model for Efficient Management of Patient at a Hospital Outpatient Visits

Y. T. Kim[1], Y. S. Jeong[2*] and G. C. Park[1]

[1]Department of Multimedia, Hannam University, 70 Hannamro, Daedeok-Gu Daejeon 34430, Korea; ky7762@hnu.kr, gcpark@hnu.kr
[2]Department of Information Communication Engineering, Mokwon University, 88 Doanbuk-ro, Seo-gu, Daejeon 35349, Korea; bukmunro@mokwon.ac.kr

Abstract

Objectives: In the present paper, a smart healthcare service management model is proposed that will enable automatic recognition of critically ill patients attached with implantable devices in their bodies without any additional administrative process when they visit hospitals as outpatients so that the patients can be provided with medical services without inconvenience. **Methods/Statistical Analysis**: The proposed model uses biometric RFID (Radio Frequency Identification) devices so that medical staff can identify patients' disease types and conditions in advance. **Findings**: The proposed model has an advantage of shortening the time required for medical services and medical administrative work by grafting RFID technology onto biometric devices. In addition, to provide security for important information related to patient treatment, the proposed model applied probability based multiple property values to patients' medical information to improve safety. **Improvements/Applications**: The proposed model was evaluated in comparison with existing medical systems in terms of service delay time, work efficiency, and patients' satisfaction with medical services. According to the results of the performance evaluation, the proposed model improved service delay time by 16.5% on average, work efficiency by 27% on average, and patients' satisfaction with services by 22.4% on average compared to existing models.

Keywords: Healthcare Service, Hospital, Implantable Device, Medical Service, Patient, Smart Healthcare

1. Introduction

Following the development of the medical industry, enterprises have been conducting many healthcare service business related investments and studies. In particular, due to factors such as the global population aging trend, increase in adult diseases and increase in demand in emerging markets, the smart healthcare industry is in the intense limelight[1].

Due to the global population aging trend and increasing longevity, smart healthcare services have been rapidly increasing mainly in generations that are easily exposed to various diseases including elderly persons[2,3]. However, various diseases occurring due to modern people's life habits have been rapidly increasing centering on chronic diseases such as cancers, diabetes, heart disease, and obesity. In addition, as the standards of living in rising, nations such as China and India have improved. Interest in national health has been increasing, leading to increases in demand for smart healthcare services centering on relatively inexpensive ones. Table 1 shows those smart healthcare products that have been developed and

**Author for correspondence*

used thus far such as home healthcare, wearable healthcare, and bioimplant healthcare products[4].

Table 1. Initial Set of features used for the experimentation

Home healthcare (Smart Toilet)	Wearable healthcare (Band, Watch, Belt)	Bioimplant healthcare
		

As Radio Frequency Identification (RFID) technology has entered the field of healthcare, papers related to the possibility of systematic healthcare are insufficient. Meanwhile, compared to those technologies such as Personal Digital Assistant (PDA), RFID technology has not been widely applied to the field of healthcare. In[5] reviewed various methods of using RFID systems at hospitals. In[5] focuses on only the application programs of RFID systems applied to hospitals and does not discuss the strengths and weaknesses of RFID systems. Although[6] analyzed those tasks and strategies that can be potentially obtained using RFID systems, it has a drawback as it did not follow the official study framework.

Other studies[7–9] mainly studied the outlines of studies of RFID application programs being used at hospitals but did not compare existing studies with each other. Therefore, systematic studies related to RFID application programs should be conducted.

In the present paper, among smart healthcare products, a smart healthcare service management model is proposed that will enable automatic recognition of patien'ts disease conditions when patients visited hospitals as outpatients to be provided with bioimplant healthcare services so that treatment methods can be provided without causing patients to feel inconvenience. To enable automatic recognition of bioimplant healthcare devices attached to patients' bodies, the proposed model has been grafted with RFID technology. The reason why RFID technology in grafted onto the proposed model is to ensure the safety and efficiency of patients' important information. The proposed model aims to minimize the time for administrative work performed by medical staff in addition to medical services. In addition, to prevent patients' important information from being provided to any third party in relation to medical services, the proposed model applies probability based multiple property information to bioimplant healthcare devices to enhance the safety.

The present paper is composed as follows. In chapter 2, the definition of healthcare services and related works are examined. In chapter 3, a smart healthcare service model having probability based multiple property information is proposed, in chapter 4, existing models and the proposed model are compared and evaluated in terms of efficiency and stability, and finally, in chapter 5, conclusions are drawn.

2. Related Works

2.1 Smart Healthcare Service

Smart healthcare services refer to personal health devices, personal health applications, personal health information platforms, and healthcare/medical services utilizing the foregoing[10].

The Figure 1 shows the structure of smart healthcare services. As shown in Figure 1, the following two medical service scenarios are possible; first, a scenario in which manufacturers, communication companies, and medical service related institutions cooperate with each other to provide medical services and second, a scenario in which communication companies, medical device companies, and medical service providers cooperate with each other to provide medical services.

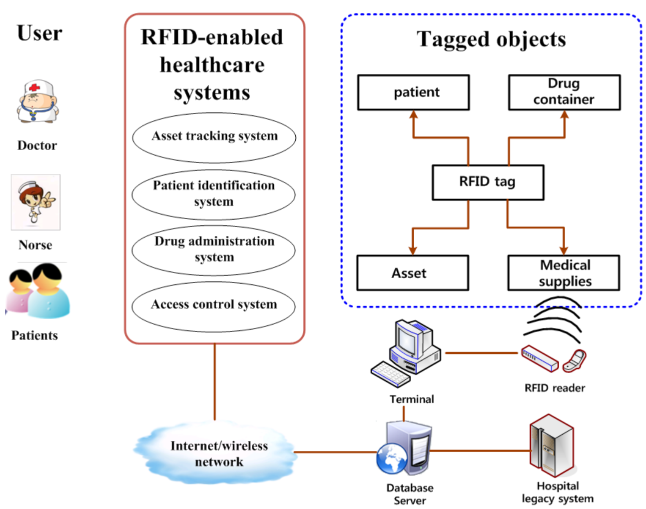

Figure 1. Design of improved decision tree algorithm for educational data mining.

As shown in Figure 1, medical systems can connect patients and medical institutions with each other through communication networks. In these medical systems, patients suffering from diabetes can measure their blood sugar and blood pressure and send the results through smartphones every week to their attending physicians, the attending physicians can inform the results of diagnosis through video telephony and transmit prescriptions through e-mail.

Recently, smart healthcare sensors have been gradually developed from the simple measuring sensors in the early stage made by adding communication functions to home/personal medical devices to wearable sensors centered on convenience and usability and 1: multiple partner complex analysis technologies. As shown in Table 2, smart healthcare services have been established as a technology necessary to sense, predict and infer patients' conditions. As shown in Table 2, smart healthcare services graft mobile devices onto medical services to monitor patients' biometric information in real time and automatically send the information to hospital staff so that patients can be provided with medical services regardless of time and space.

Smart healthcare services are quite convenient because patients are not much restrained physically or temporally. In particular, since medical services are provided and reservations for medical services are managed utilizing wire/wireless online networks, smart healthcare services have evolved more than existing healthcare services[11–14].

Smart healthcare service expanded medical information and treatment reservation related services being provided in healthcare services into wire/wireless online networks. Although smart healthcare services provide security functions centering on Public Key Infrastructire (PKI) or data encoding, security vulnerabilities occurring in wireless sections still exist.

2.2 Implantable Device

Implantable devices' medical services enable medical staff to collect, deliver, and manage patients' biometric information anytime anywhere. Here, implantable devices mean those devices that are implanted in the body in order to collect patients' life information (breathing, heart rate, temperature, blood pressure, etc.). Implantable devices are used on patients that are suffering from incurable diseases such as heart diseases and diabetes to examine patients at long distances.

The Figure 2 shows a feedback process through which the information (blood pressure, diabetes, electrocardiogram, body fat analysis, etc.) on patients attached with implantable device is delivered to smart healthcare service centers through the internet so that hospital staff (doctor) identifies the patients' conditions and treat the patients in smart healthcare environments.

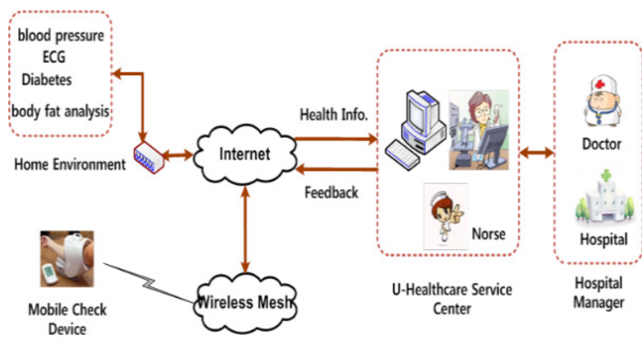

Figure 2. Overall structure of healthcare service using implantable device.

As shown in Figure 2, to check biometric information from patients' implantable devices, hospital staff should periodically request the smart healthcare service

Table 2. Direction of development of healthcare services

Division	Tele-health	e-health	u-health	Smart-health
Time	Mid 1990s	2000	2006	2010 and thereafter
Service content	Treatment in hospital	Provision of treatment and information	Treatment/prevention management	Treatment/prevention/welfare/safety
Major player	Hospital	Hospital	Hospital, ICT company	Hospital, ICT company, insurance company, service company, etc.
Major user	Medical personnel	Medical personnel, patient	Medical personnel, patient, general person	medical personnel, patient, general person
Major system	Hospital operation (HIS, PACS)	Medical record (EMR) website	Health record (HER) monitoring	Personal health record based customized service

center for patients' biometric information. To check their biometric information frequently, patients should be provided with services from the smart healthcare service center. If any patient that uses mobile measuring instruments finds any problem occurred, the patient should immediately inform the fact to the smart healthcare service center.

2.3 Exiting Studies

Recently, as the number of patients that use implantable devices has been increasing, the necessity of studies of federation ID models for implantable devices has also been increasing[15–19].

In terms of the possibility for RSA and integer factorization problem based proxy signature schemes to verify delegation, In[17] showed that certificates could first hand use proxy signature keys to generate power of attorneys and make proxy signatures using the power of attorneys. In[18] proposed a discrete algorithm problem based proxy signature scheme but this scheme has drawbacks. Dual signature algorithms should be used because RSA digital signature algorithms are used in most cases under the public key based structure and that this scheme cannot satisfy high forge impossibility that is basic stability. In[19] proposed a Rabin based proxy signature scheme in a modified form which is based on the difficulty of integer factorization problems. In this scheme, the original signer transmits a power of attorney and related signature and the proxy signer checks the validity of certificates.

In[15] presents a security model that enables the federation ID management system to safely manage federation IDs according to the types of attacks on federation IDs when adversaries attempt access to implantable devices. In[15] proposed mutual platforms for reliable establishment between clients and identifier providers based on the security model for federation ID management systems. In[16] proposed a dynamic trust model for federation ID management. In this model, to politically express dynamic trust relationships, trust relationships are expressed through dynamic trust policy languages.

3. Probability based Smart Healthcare Service Management Model Applied with RFID Technology

In this section, the types, functions, and characteristics of patient information (disease information, patients' personal information,......) are applied with RFID technology, so that when patients to be provided with bioimplant healthcare services visit hospitals, the patients' disease conditions can be automatically recognized and treated by the hospitals. A description of this process is found in this section.

3.1 Overview

In smart healthcare services, bioimplant healthcare information is diversely used depending on service environments. In the proposed model, when patients visit hospitals, the patients' bioimplant healthcare information is provided to medical staffs through smart devices so that the medical staffs can provide stable medical services and are not required to process any additional administrative work.

The proposed model aims to minimize patient treatment time by automatically figuring out patients' identities and conditions when patients have visited hospitals by obtaining patients' identity information and biometric information through biometrics RFID tags. The entire structure of the proposed model is as shown in Figure 3.

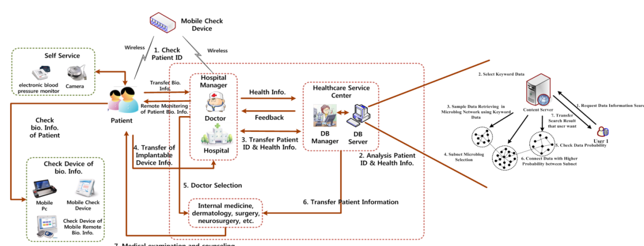

Figure 3. Overall structure of proposed model.

As shown in Figure 3, in the proposed model, if probability based smart healthcare service information is shared with medical staff, security is provided without exposing unnecessary patients' personal information. The proposed model conducts integrated management of patients' bioimplant information to enable normal authentication and identification.

The proposed model has the following characteristics. First, patients' diseases can be analyzed and treated without any additional processing of administrative work. Second, biometrics RFID tags implanted in patients' bodies are recognized by RFID readers so that patients' biometric information and patient identities can be automatically identified. Third, patients' disease conditions can be identified and treatment plans can be immediately provided to patients without any additional examination. Fourth, medical staff's burden due to administrative work can be minimized.

3.2 Definition of Terms

The terms used in the present paper are as shown in Table 3.

Table 3. Notations

Parameter	*Notation*
P	Patient
H	Hospital
ID	Implantable Device Identification
R	RFID reader
T	RFID tag
rN	Random number generated by server
OID	One-time Identification Information
DDI	Device Distribution Information

3.3 System Structure

To enable hospitals to provide smart healthcare services using RFID technology, the proposed model constructs service management structures with three components (biometrics RFID tag, RFID reader, and server) as shown in Figure 4.

Figure 4. Architecture for an RFID operation.

As shown in Figure 4, to conduct authentication between biometrics RFID tags and servers, secret data shared in advance are necessary. Communication channels between biometrics RFID tags and RFID readers are wireless sections where data are exchanged and are not safe because adversaries can easily intercept data. Communication channels between RFID readers and servers are safer than the sections between biometrics RFID tags and RFID readers because diverse security mechanisms are used.

1. Biometrics RFID tag: Biometrics RFID tags consist of microchips, antennas, and detailed hardware for cancer-specific operations. Along with RFID readers, secret data for authentication and communication are stored.

The medical service processes of the proposed model using RFID technology are largely divided into three. First, when a patient has visited the hospital for ambulatory care, the biometrics RFID tag implanted in the body of the patient is automatically recognized by the RFID reader installed at the hospital so that the patient is automatically recognized without any additional administrative processing. Second, the RFID reader transmits the information in the patients' biometrics RFID tag to the database server installed at the hospital according to disease information and analyzes the information. Third, the patients' biometric information stored in the database server is analyzed by the doctor before interviewing the patient to figure out patients' health disease conditions and treatment measures and present medical services according to diseases when the doctor treats the patient.

3.4 Probability based Bioimplant Healthcare Service Management

In this section, the process through which when a patient attached with a biometrics RFID device in the body visits a hospital, the patient's biometric information is identified in real time so that the patient is provided with relevant medical services is described. This process probabilistically processes the accuracy of patients' biometric information to improve the reliability of the results of diagnosis of patients' diseases and the results of prescription.

3.4.1 Automatic Patient Recognition Process

In this section, a description of the process through which a patient passes when visiting an hospital, the biometric RFID tag implanted in the patient's body is identified through the RFID reader installed in the hospital to identify patient information. This process consists of four stages.

Stage1: Identify biometric devices

In this stage, the patient that visited the hospital is recognized through the biometrics RFID tag implanted in the patient's body. In particular, the biometrics RFID tag implanted in the body is compared with the biometrics RFID tag information stored in the hospital database to check if the biometric device coincides with the information.

Stage 2: Identify patient information

In this stage, the patient that visited the hospital is compared with the patient information stored in the hospital server to identify the patient. The hospital recognizes the biometrics RFID tag implanted in the patient's body through the RFID reader installed at the hospital and compares and analyzes the information in the tag with the patient information stored in the hospital server. In this case, when the hospital examines the biometrics RFID tag information delivered to the hospital server, if the two sets of patients' biometric information coincide with each other, a One-time Identification Information(OID) will be issued and if not, a patient recognition process will be performed again.

Stage 3: Collect the biometric information generated in the biometrics RFID tag

In this stage, the biometric information generated in the biometrics RFID tag implanted in the patient's body is collected by the RFID reader. The biometric information $\overline{\mathbf{B}}$ generated in thebiometrics RFID tag is collected as shown by equation (9).

$$Gathering \quad \overline{\mathbf{B}} = (\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}) \tag{1}$$

Stage 4: Generate the property value of biometric information

In this stage, property values are given to the biometric information values generated in the bioimplant RFID tag. The patients' biometric information $\mathbf{b_i}$ stored in theserver generates property values as shown by equation (2).

$$\mathbf{Generate}\,\mathbf{b}_1 = (\mathbf{p_1}\ ,\mathbf{p_2}\ , \ldots, \mathbf{p_n}) \tag{2}$$

where, $\mathbf{p_n}$ refers to the characteristic value of the biometric information and $\mathbf{n}$ refers to the element ($\mathbf{n} \in \mathbb{Z}$) of set $\mathbf{Z}$.

3.4.2 Biometric Information Transmission Process

In this section, the process through which biometric information is delivered to the server using one-time identification information OID is described. In this process, the patient is assumed to have at least one biometrics RFID device implanted in the patient's body. This process consists of three stages.

Stage 1: biometric information encoding using one-time identification information and random numbers

The patient encodes patients' biometric information and biometrics RFID device information by mixing patients' one-time identification information and random numbers and delivers the encoded information to the database.

Stage 2: Identify implantable device classification information

The biometric information received from the patient is decoded by mixing patients' one-time identification information OID and random numbers. The database compares the biometric device's device classification information DDL out of the decoded information with the DDL information stored in the database. If the two pieces of DLL information coincide with each other, the patients' biometric information will be renewed and if not, the databasewill request the patient for biometric information again.

Stage 3: Deliver the biometric information to the hospital server

In this stage, classified biometric information is delivered to the database of the treatment department of the hospital. In this case, the classification information of the patients' biometrics RFID tag device is assumed to have been stored in the database in advance. The communication channel between the RFID reader and the hospital server generates and share random numbers associated with the patient identifier. The shared random numbers are generated by the hospital server in advance before being shared. The random numbers used in this stage are used to encode/decode biometric information before and after delivering the biometric information.

3.4.3 Biometric Information Analysis and Treatment Process

In the biometric information analysis and treatment process, the patients' biometric information stored in the database is analyzed before patient counseling and the doctor presents patient treatment methods and time based on the results of the analysis. This process consists of four stages.

Stage 1: Analyze the biometric information stored in the database

The patients' biometric information transmitted to the database is classified according to the classification information of the biometrics RFID tag device and analyzed using the biometric information analysis tool (ex. R) installed in the database server.

Stage 2: Receive the results of biometric information analysis

When the patients' biometric information stored in the database has been completely analyzed, the results are delivered to the attending doctor in the treatment department for patient treatment.

Stage 3: Review patient conditions

Through the results of analysis of patients' biometric information delivered from the database, the doctor reviews the patients' current conditions and treatment methods in advance.

Stage 4: Seek for patient treatment measures

Based on the results of analysis of patients' biometric information, the doctor performs ambulatory treatment while discussing with the patient regarding patients' conditions and time of treatment.

4. Evaluation

To evaluate the performance of the proposed model, the service delay time, work efficiency, communication overhead, and patient's satisfaction with services of the proposed model are evaluated in comparison with those of existing schemes.

4.1 Environment Setting

To evaluate the performance of the proposed model, an experimental environment was set as shown in Table 4. As shown in Table 4, the parameters used in the performance evaluation are the number of hospitals, the number of doctors, the number of patients, RFID devices' transmission distance, data generation intervals, and threshold. Ten hospitals were designated and experimental data were collected from 2,000 patients being treated by 100 doctors working at the 10 designated hospitals through module tests for hospital medical services. For the evaluation of the performance of the proposed model, threshold **th** was set as {1, 3, 5}.

Table 4. Parameter setup

Parameter	Setting
Number of Patients	**2,00**$_0$
Number of Doctors	**10**$_0$
Number of Hospital	**10**
Threshold	**th** = {1, 3, 5}
Transmission Distance of RFID Device	1m ~3m
Data Generation Interval	0.01 ms

4.2 Performance Analysis

4.2.1 Service Delay Time

The Figure 5 shows the results of analysis of medical service delay time spent by a patient at a hospital after the biometrics RFID device attached to the patient was automatically recognized through the RFID reader installed at the hospital due to not only the identification of the patient also the collection and analysis of the patient's biometric. According to the experimental results shown in Figure 5, the medical service delay time of the proposed model was 16.5% shorter on average than that of existing models. This result is attributable to the fact that in the proposed model, patients' biometric information was collected through the RFID reader installed at the hospital and delivered to the relevant medical department so that disease analysis and treatment measures were completed before patient treatment.

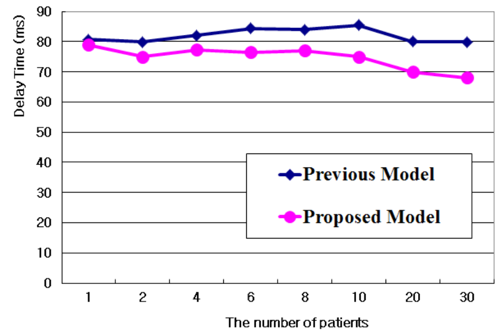

Figure 5. Delay time for medical service through patient increment.

4.2.2 Work Efficiency

The Figure 6 shows the fact that the work efficiency of the proposed model can be enhanced compared to existing schemes because the patients' biometric information transmitted/received between the biometrics RFID device and the RFID reader, and between the RFID reader and the server is analyzed in advance thereby improving the quality of treatment measures and medical services. According to the results of experiment shown in Figure 6, the proposed model showed higher work efficiency by 27% on average compared to existing models because RFID technology was grafted onto biometric devices to automatically collect and analyze patients' biometric information so that doctors can treat patients based on patients' biometric information without any additional examination.

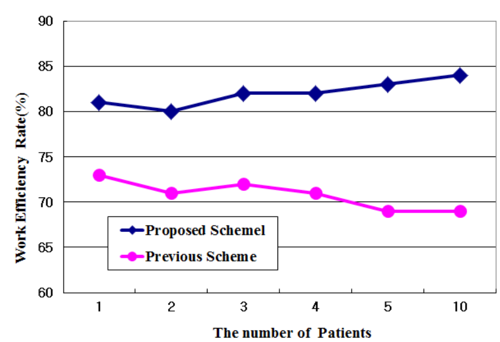

Figure 6. Work efficiency rate through the number of patients.

4.2.3 Communication Overhead

The Figure 7 shows the communication overhead occurring due to the Electro Magnetic Interference (EMI) occurring in the process of transmission/receipt of biometric information between the biometrics RFID device and the RFID reader. According to the results of experiment shown in Figure 7, the proposed model showed lower communication overhead by 7.5% on average compared to existing schemes because, in addition to the biometric information transmitted/received between the biometrics RFID device and the RFID reader, the proposed model processes biometric information using only patients' one-time identification information OID and random numbers. This result is attributable to the fact that no additional cost is incurred other than the cost to identify and process the patients' one-time identification information OID and random numbers between the RFID tag and the RFID reader in the case of the proposed model so that communication overhead is smaller when the amount of biometric information is larger.

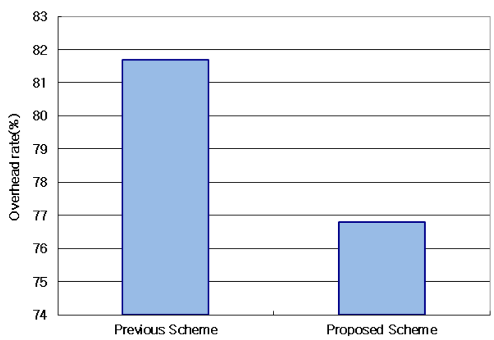

Figure 7. Communication overhead between RFID tag and RFID reader.

4.2.4 Satisfaction with Medical Services

The Figure 8 shows the results of questionnaire surveys regarding satisfaction with medical services conducted with hospitals that implanted biometric devices into patients and the relevant patients. According to the results of experiment shown in Figure 8, whereas satisfaction with medical services steadily increased over time in the case of the proposed model, it did not changes over time in the case of existing model. The results indicated that patients' satisfaction with medical services improved by 22.4% over time in the case of the proposed model compared to existing models. This result is attributable to the fact that not only users were provided with medical services without any additional examination of patients but also the quality of medical services provided by medical staff was improved in the case of the proposed model and, that in addition, treatment appropriate to patients were performed through analyzed patients' biometric information without any additional examination of patients.

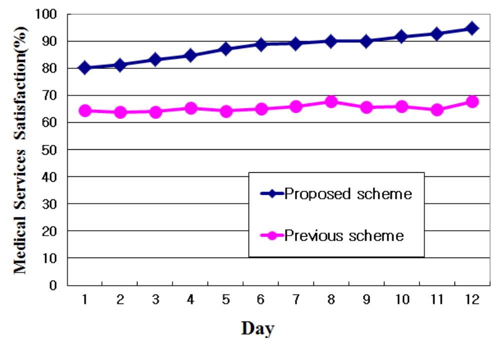

Figure 8. Satisfaction with medical service.

5. Conclusion

Recently, as dietary life has been westernized, the number of patients implanted with medical devices in their bodies to be provided with medical services has been increasing. However, many patients are dissatisfied with those medical services due to the complicatedness of hospitals' administrative work. In the present paper, a smart healthcare service management model is proposed in which patients attached with biometrics RFID devices in their bodies are recognized when they visit a hospital as outpatients and their biometric information is automatically identified through the RFID reader installed at the hospital so that the patients' disease conditions are automatically recognized without any additional hospital administrative work processing or examination and patients are not inconvenient. The proposed model minimized the waiting time to receive medical services because patients were treated through the results of analysis of disease information stored in the server conducted before patients' interviews with medical staff. In addition, the proposed model was examined through questionnaire surveys conducted with those hospitals and medical staff that were using biometric RFID device and was experimented through module tests to evaluate the medical service delay time, work efficiency, and satisfaction with medical services. According to the results of the performance evaluation, the proposed model improved service delay time by 16.5% on average, work efficiency by 27% on average, and patients' satisfaction with services by 22.4% on average compared to existing models. In future studies, the proposed model will be expanded and applied to hospital systems so that the studies are conducted at more hospitals with diverse patients through discussion with hospitals.

6. Acknowledgement

This work was supported by 2016 Hannam University Research Fund.

This work was supported by the Security Engineering Research Center, granted by the Ministry of Trade, Industry and Energy.

7. References

1. Weinstein R. RFID: A technical overview and its application to the enterprise. IEEE Journals and Managines: IT Professional. 2015 May/Jun; 7(3):27–33.
2. Jeong YS. Parallel Processing Scheme for Minimizing Computational and Communication Cost of Bioinformatics Data. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–8.
3. Moon WH, Park HS.Reuse Intention Associated with the Selection Factors and Satisfaction: Focused on Spine Specialty Hospitals in Korea. Indian Journal of Science and Technology. 2015 Oct; 8(26):1–7.
4. Yao W, Chu C, Li Z. The adoption and implementation of RFID technologies in healthcare: A literature review. Journal of Medical System. 2012 Dec; 36(6):3507–25.
5. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. ELSEVIER: Computer Networks. 2010 May; 54(15):2787–805.
6. Yu HY, Chen JJ. An intelligent space location identification system based on passive RFID tags. Proceedings of International Conference on Machine Learning and Cybernetics, China. 2014.428–33.
7. Fazlagic S. Delegating signing capability in workflow systems. Proceedings of 2nd International Conference on Computer Engineering and Technology, China.IEEE; 2010.324 –27.
8. Penttila K, Sydanheimo L, Kivikoski M. Performance development of a high-speed automatic object identification using passive RFID technology. Proceedings of IEEE International Conference on Robotics and Automation, USA. 2004.4864–8.
9. Katz J, Rice R.Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology. International Journal of Medical Information. 2009 Feb; 78(2)104–14.
10. Choi JS, Lee H, Elmasri R, Engels DW. Localization Systems Using Passive UHF RFID. Proceedings of 5th International Joint Conference on INC, IMS and IDC, Korea. 2009.1727–32.
11. Liao Y, Hsiao C. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad Hoc Networks. 2014 Jul; 18:133–46.
12. Chou JS.An efficient mutual authentication RFID scheme based on elliptic curve cryptography. The Journal of Super Computing. 2014 Oct; 70(1):75–94.
13. Zhao Z. A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. Journal of Medical Systems. 2014 May; 38(5):46.
14. Zhang Z, Qi Q. An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. Journal of Medical Systems. 2014 May; 38(5):47.
15. Khattak ZA, Sulaiman S, Manan JA. A study on threat model for federated identities in federated identity management system. Proceedings of International Symposium in Information Technology (ITSim), Malaysia. 2010.618–23.
16. Gao H, Yan J, Mu Y. Dynamic Trust Model for Federated Identity Management. Proceedings of 4th International Conference on Network and System Security, Australia. 2010.55–61.
17. Zhou Y, Cao Z, Lu R. Provably secure proxy-protected signature schemes based on factoring. Applied Mathematics and Computation. 2005 May; 164(1):83–98.
18. Saraswat V, Sahu RA. A secure anonymous proxy multi-signature scheme. Proceedings of 11th International Conference on Security and Cryptography, Austria. 2014.1–12.
19. Junru H, Yi D. An efficient signcryption scheme with shortened ciphertext. Proceedings of International Conference on Computer Application and System, Taiyuan. 2010.12:404–07.