symmetry

MDPI

Article

The Design and Analysis of a Secure Personal Healthcare System Based on Certificates

Jungho Kang [1], Hague Chung [1], Jeongkyu Lee [2] and Jong Hyuk Park [2,*]

[1] Department of Computer Science and Engineering, Soongsil University, 369 Sangdo-Ro, Dongjak-gu, Seoul 156-743, Korea; kjh7548@ssu.com (J.K.); standard@ssu.ac.kr (H.C.)

[2] Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), 232 Gongneung-ro, Nowon-gu, Seoul 01811, Korea; jungkyu0716@gmail.com

* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702

Academic Editor: Ka Lok Man

Received: 12 September 2016; Accepted: 4 November 2016; Published: 14 November 2016

Abstract: Due to the development of information technology (IT), it has been applied to various fields such as the smart home, medicine, healthcare, and the smart car. For these fields, IT has been providing continuous prevention and management, including health conditions beyond the mere prevention of disease, improving the quality of life. e-Healthcare is a health management and medical service to provide prevention, diagnosis, treatment, and the follow-up management of diseases at any time and place in connection with information communication technology, without requiring patients to visit hospitals. However, e-Healthcare has been exposed to eavesdropping, manipulation, and the forgery of information that is personal, biological, medical, etc., and is a security threat from malicious attackers. This study suggests a security service model to exchange personal health records (PHRs) for e-Healthcare environments. To be specific, this study suggests a scheme in which communicators are able to securely authorize and establish security channels by constituting the infrastructure each organization relies on. In addition, the possibility of establishing a security service model is indicated by suggesting an e-Healthcare system for a secure e-Healthcare environment as a secure personal health record system. This is anticipated to provide securer communication in e-Healthcare environments in the future through the scheme suggested in this study.

Keywords: e-Healthcare; authentication; security; system design; certificate

1. Introduction

Due to the recent improvement in standards of living and an increase in concern of the health conditions of contemporary people, there has been an enhancement of life quality and changes in living patterns. As such, there has been an increasing concern about healthcare, as health checkups and management have received attention. In addition, Information technology (IT) has caused a rapid increase in the demand for the development of e-Healthcare technologies and services [1–3]. e-Healthcare is a newly coined term that refers to healthcare IT services that support communication and exchanges regarding medical information over the Internet. Furthermore, the digitization of medical records at hospitals for recording health information has become widely available in order to improve the efficiency of hospital management and reinforce competitiveness in Korea and abroad [4]. Due to the digitization of medical records in the hospital, there has been an accelerated promotion of the establishment of a foundation in commonly utilizing information that includes the cooperation among hospitals and transmission of patient information, either at hospital or at home.

With the rapid development of the global e-Healthcare market, major developed countries have been strongly proceeding with nationally led projects in preparation for an aging society. According to the Knowledge Industry Information Institute, the size of the e-Healthcare market globally has

expanded from $143.1 billion in 2007 to $254 billion in 2013. It is expected to grow at an annual average rate of 15.7% up to 2018, reaching a scale of about $498.7 billion [5].

Due to the commercialization of e-Healthcare services, there have been damages, including the disclosure of users' personal and health information, unauthenticated user access, and the illegal collection of information. With this security threat, there have been secondary damages, including life threat on users, the illegal collection of information and transactions, and insurance fraud from the manipulation of biological information [6–8]. There has been an actively exerted effort to solve security issues about important information such as personal or medical information. However, providing efficient services is difficult due to insufficient security services and research. There is a need to improve e-Healthcare services by conducting research on a security service model for efficient e-Healthcare environments [9–11]. Existing e-Healthcare services are vulnerable to attacks, but the suggested method herein is secure because it generates a session key using authentication acquired from a trusted certification authority (CA). Moreover, since digitalized information increases dramatically, the suggested method does not have a single body handling both storage resources and computing resources, but instead distribute them into several bodies by the capabilities so that make it secure against the denial of service attacks. This was used as the basis for a security service model for a secure e-Healthcare environment for a secure cyber world.

This study focuses on security service models including authentication, encryption, privacy protection, and access control [12–14]. In Section 2, e-Healthcare services and security, as well as the trends and research of e-Healthcare, are explained. In Section 3, a security service model for e-Healthcare environments is suggested, discussing the configuration of the suggested model and the security service model. In Section 4, the security of the suggested model is evaluated. Section 5 is for discussion.

2. Related Works

2.1. e-Healthcare Service

In general, e-Healthcare service means to provide information or medical service fulfilling demands of users at any time and place, without restrictions by supplying medical service by utilizing IT and biometric technology (BT). Modern people have changed their focus from diagnosis to prevention, from health checkup and from disease management to health management [15,16]. Therefore, a medical service must provide user's health and medical information to not only for patients but also for others on a real-time basis in continuous connection with users, medical service providers, medical information providers, and management institutes to prevent disease and manage health conditions through diagnosis in advance [17]. e-Healthcare is integrated with more than one technology, including network technology, database technology, and sensing technology. Therefore, e-Healthcare can be served in various forms including u-Medical, u-Silver, and u-Wellness [18–20].

In general, e-Healthcare service infrastructure is comprised of communication among users, sensors, and wireless access point (APs), as shown in Figure 1. A sensor is attached to a user's body and provides e-Healthcare with sensed information through the network [21].

In addition, it communicates with wireless AP to deliver collected data to a healthcare information center. Medical service providers that are delivered user data analyze the biological and medical information through healthcare information system and transmit the results of the analysis to medical institutions or users that request medical information [22–24].

Various industries comprehensively participate in e-Healthcare including the constituting sensor, the wireless AP, and the healthcare information system [25]. e-Healthcare is comprised of sensing techniques, network techniques, and database techniques. Detailed explanations are as follows.

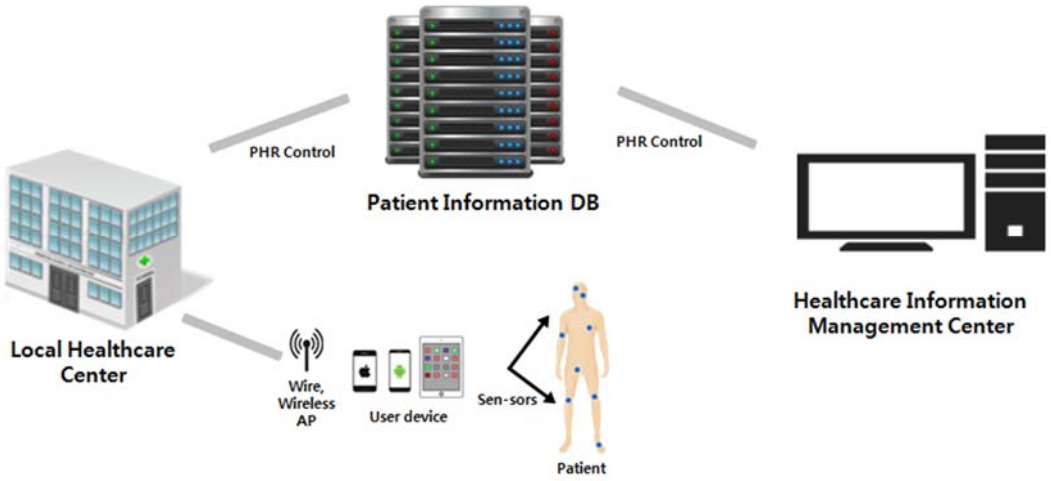

Figure 1. e-Healthcare service infrastructure.

Sensing technique: In order to use the healthcare service, users' biological information must be provided through various sensors while in use. There are many types of sensors. They have features to measure heartbeat, pulse, breathing rate, and blood pressure. Sensors have recently been internally installed in smart devices, including wearable devices still in development. It is feasible to provide various healthcare services with information from these sensors [26,27].

Network technique: In general, there are wire and wireless networks. With a wire network, it is feasible to transmit information at a high speed to a place that is physical connected to it. However, a disadvantage is that there are limited places to use such a network. On the other hand, there is no spatial limitation on wireless network [28]. However, malicious users are able to steal wireless signals; hence, there are security threats. Meanwhile, a wireless network usually transmits information in a normal sentence, and there is therefore always the security threat that a malicious attacker can steal wireless signals. A remaining disadvantage is that there is a high fluctuation in the reception rate of the network depending on the environment.

Database technique: A technique for comprehensively managing data for many users to share and utilize together, the database technique entails structuralizing, storing, and managing resources. Among them, the DW (data warehouse) is a comprehensive database for efficiently supporting required information. In the field of medicine, DW processes and produces data accumulated in the internal system of comprehensive medical information and data from the external system and provides them to organizations in need of them or manages the integrated data according to the classified definition. In addition, it is a comprehensive system established to analyze and process data on a real-time basis while pursuing various goals of medical information [29].

Due to continuous development of e-Healthcare, there has been an increasing security threat in proportion to them. Since e-Healthcare is to transmit and manage user information through wire and wireless network, they might be exposed to security threats. Due to eavesdropping and the manipulation of important information from the access of malicious attackers, there could be great damage or life threats. Besides such threats, there might be secondary damages, including illegal transactions of information or information manipulation from network attacks. For secure communication away from malicious attackers, authentication, encryption, access control, and privacy protection must be guaranteed.

2.2. e-Healthcare Security

Due to eavesdropping and the manipulation of important information from the access of malicious attackers, there could be great damage or life threats. Besides such threats, there might be secondary

damages, including illegal transactions of information or information manipulation from network attacks. The requirements for secure communication in e-Healthcare are as follows.

Authentication: In order to provide a secure e-Healthcare service, authentication is required. e-Healthcare is communicated through APs to exchange information with service providers from outside and to provide service [30,31]. Therefore, there is a possibility for it to be exposed to malicious eavesdropping or information by internal or external objects during communication or out of carelessness. Hereupon, only authenticated users are able to be provided with the e-Healthcare service and to deliver information.

Encryption: In order to use a secure e-Healthcare service, encryption is inevitable. Encryption shall be applied on personal, biological, and medical information used for authentication or service for secure transmission [31]. If providing, or provided with, information without encryption, there might be secondary damage from illegal transactions of information or manipulation of information from disclosure of information.

Access control: Although the e-Healthcare system receiver sends personal, biological, and medical user information, an authenticated user may not be allowed to access all types of information in the system.

Privacy protection: Privacy protection in a secure e-Healthcare service is the most fundamental and important element for the protection of user privacy. If privacy is not protected, personal, biological, and medical information is exposed, leading to secondary damages. As such, they might be used for crime.

2.3. Previous Research on e-Healthcare

In this section, previous research related to the e-Healthcare service is reviewed.

Yun-Young Sok [32] suggested an OCS (order communication system) and a HIS (hospital information system) as a way to establish a comprehensive medical information system in e-Healthcare service environments. The suggested comprehensive medical information system is custom-designed and optimized for mobile healthcare diagnosis environments in connection with an OCS and a HIS as a medical system for swiftly and accurately performing treatment and diagnosis for users. In addition, it suggests the establishment of a database and data mart, with an acquired consistencyHowever, the encryption of documents, the establishment of security infrastructure of security-related comprehensive medical information, and the connection methods for information produced by a user's PC, as well as the application of access control for unauthenticated users and major data, were not mentioned or addressed.

Yong Sik Jung [33] suggested an e-Healthcare comprehensive medical information system based on the establishment of a data warehouse and a network, the standardization of communication for medical information, and the formation of an e-Healthcare service component to manage information of a comprehensive medical information system and provide service in an e-Healthcare service environment. The suggested comprehensive medical information system provides general services to hospitals, such as a systematic medical decision-making process as well as information about users in combination with a previous comprehensive medical information system, such as e-Healthcare, an order communication system, a picture archiving and communication system, a laboratory information system, a nursing information system, and e-Healthcare service supporting systems. In addition, it also supports decision-making for strategic managerial activities, including a decision support system, enterprise resource planning, customer relationship management, and knowledge management system as managerial supporting system in the hospital. However, privacy and security on medical user information, which is more important than any other component in the field of health and medical treatment, have not been mentioned.

Moon Sun Shin [34] reviewed the requirements of security in relation to the protection of personal information and suggested a personalized security model based on expanded roll-based access control in an e-Healthcare service environment. The suggested u-HCSIP (u-Healthcare Service Integration

Platform) performs a function of storing or exchanging PHRs, recommending diet and exercise, trading personal medical information or experience, and managing health data in the use of smart devices. In addition, it provides information about the drugs of users and the harms or risks caused by the abuse of drugs. However, it is only possible to use it on mobile devices, without mentioning the evaluation of performance in the suggested model.

Yoon-Su Jeong [35] proposed an access model for distributing a user's biological information depending on the authority and access level of the associates in the hospital to securely approach the privacy information of patients used in e-Healthcare environments. The suggested distributed access model is to control the access of a user's biological information and to prevent a denial-of-service attack through a timestamp at the same time. In addition, the suggested model prevents privacy breaches and the disclosure of medical information of patients since the central server manages the staff of the hospital, and access is controlled by staff authorities at the same time. However, the suggested model has not objectively derived an evaluation of the performance, as it failed to apply to an actual environment, even though it prevented privacy invasion of patients from a third party in theoretical perspective.

3. Proposed Infrastructure

3.1. Proposed e-Healthcare Service Infrastructure

Figure 2 represents the infrastructure in the suggested e-Healthcare environment. In the existing e-Healthcare service, there have been issues, including threats to the protection of users and their medical information, threats to the management of said medical information, and threats to the sharing of said medical information due to the centralization of service and information by directly managing and providing information to e-Healthcare [36–38]. There is a difficulty in solving such issues in the hardware parts [39,40]. Therefore, it is required to guarantee confidentiality of encryption for users and their medical information, access control, and information dealing with the authentication center by dividing the Healthcare Information Management Center (HIMC) and the Healthcare Trusted Service Center (HTSC). As for components of the security service model for efficient e-Healthcare environments, there are Local Healthcare Centers (LHCs) providing medical services to users and delivering information to HTSC, the authenticated HTSC is producing, distributing, managing, and authorizing keys, working as an intermediary of information, and the HIMC is an authenticated organization for encrypting, storing, and providing personal and medical information. This structure allocates functions to the HIMC for providing encrypted information to medical service providers and to the HTSC in charge of authentication of information, making it feasible to encrypt and authorize personal and medical information. The role of each component for the security model of an efficient e-Healthcare environment is as follows.

LHC: A LHC is a medical service institution that provides and uploads information by consulting, diagnosing, and managing patients, such as a hospital, a health center, or a pharmacy. The LHC provides a healthcare service to users. Hereupon, the LHC can be provided with personal and medical information collected from users.

HTSC: The main role of this is to produce and manage the key. It also serves as a role of medium when transmitting information between the LHC and the HIMC. The HTSC preserves key values through mutual authentication with the LHC and with the HIMC. If the LHC requests information from the HIMC, the HTSC produces new keys. It serves as a role of authentication and information intermediary and can feasibly control the entire courses of service.

HIMC: It is feasible for one to be provided with information collected by a HTSC as an intermediary from each LHC by encrypting them to a HIMC. As a role of comprehensively managing medical information, the HIMC encrypts and manages personal and medical user information collected from the HTSC and provides information to an authenticated LHC upon the LHC's request.

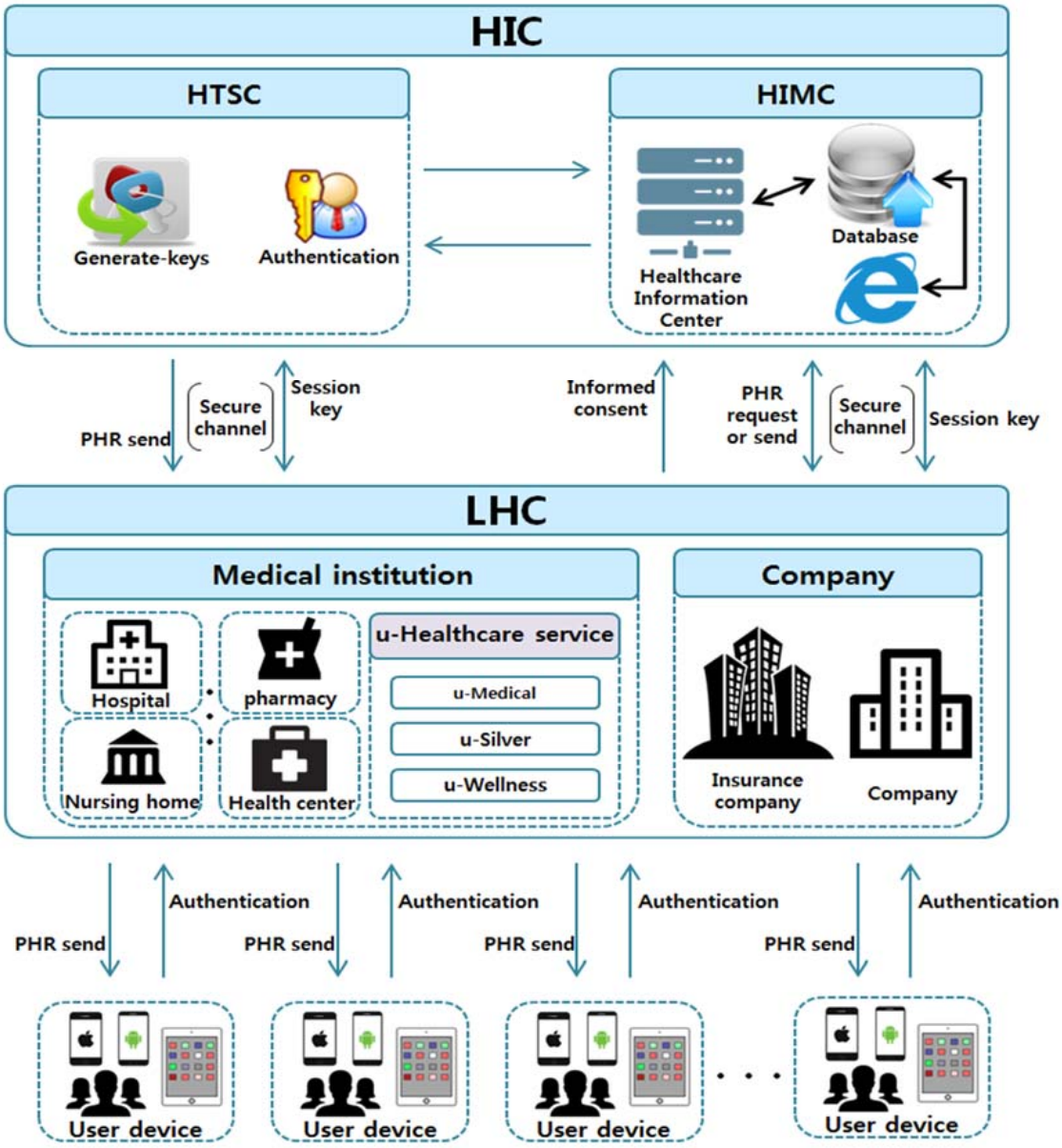

Figure 2. Proposed e-Healthcare service infrastructure.

3.2. Proposed Protocol

The suggested efficient e-Healthcare service environment is comprised of a mutual authentication protocol and an information transmission protocol. In the mutual authentication protocol, information exchanged among the local health center, the HTSC, and the HIMC is used to acquire a session key while exchanging personal health records. The HTSC delivered with PHR information transmits the delivered PHR information to the HIMC without storing it. At this time, there is no need for the HTSC to see PHR information. Therefore, it is encrypted with a random number and session key of the HTSC and the HIMC, and then sent out. An explanation of parameters of the suggested protocol is in Table 1.

Table 1. Proposed protocol parameters.

Notation	Meaning
Req	Request
Resp	Response
LHC	Local Healthcare Center
HTSC	Healthcare Trusted Service Center
HIMC	Healthcare Information Management Center
Cert	Cerificate
$R[R_1, R_2 \ldots R_6]$	Random Number
Pri	Private Key
Pub	Public Key
E()	Encryption
D()	Decryption
SK	Session Key
TS	Time Stamp
H	Hash Function
Verify()	Verification
PHR	Personal Health Record

3.2.1. Mutual Authentication Protocol

In this session, mutual authentication protocol in the service infrastructure is explained. All courses of information transmission are encrypted by using the session key after producing it. Mutual authentication protocol used for the LHC, the HTSC, and the HIMC is shown in Figure 3.

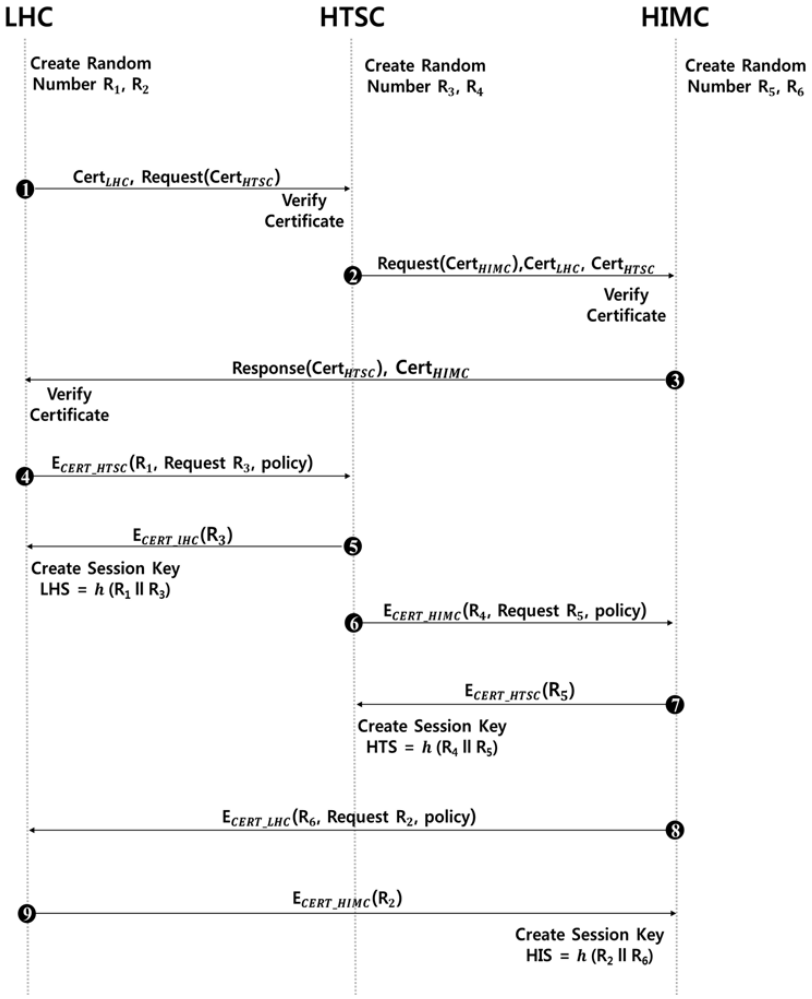

Figure 3. Proposed e-Healthcare mutual authentication protocol.

Prior to producing mutual authentication used for the LHC, the HTSC, and the HIMC, two random numbers are produced. Furthermore, the LHC and the HTSC, as well as the HIMC, receive authentication from CA, which is a secure authenticating body. Detailed procedures of producing mutual authentication are as follows.

Step 1 The LHC sends its own authentication to the HTSC and requests authentication from the HTSC.

Step 2 After receiving a certificate from the LHC, the HTSC verifies it and requests the certificate from the HIMC and sends it to the LHC and the HTSC.

Step 3 After verifying the certificate of the LHC and the HTSC, it sends the certificate of the HTSC and the HIMC to the LHC.

Step 4 After receiving certificates from the HTSC and the HIMC, the LHC verifies them and requests encrypted random number R_1 and R_3 with a certificate of HTSC and sends policies needed to establish a session key.

Step 5 After the decryption with its own certificate, HTSC acquires a random number R_1 of the LHC and encrypts its own random number R_3 with a certificate of the LHC and sends it. After receiving a random number R_3, the LHC hashes it with its own random number R_1 and produces a session key. The session key produced at this time is calculated with values that the HTSC knows. Therefore, it is possible to share the session key.

Step 6 In the same manner as Step 4, the HTSC requests random sampling numbers R_4 and R_5 encrypted with the certificate of the HIMC and sends policies together.

Step 7 R_4 requested after the decryption of random number R_4 with the certificate is sent after it is encrypted with the certificate of the HTSC. After acquiring random number R_5, the HTSC hashes its own random numbers R_4 and R_5 in connection and produces the session key. Since the HIMC knows the session key produced at this time, it is possible to share the same session key.

Step 8 In the same procedure as Step 6, the HIMC requests its own random number R_6 encrypted with the certificate of the LHC and random number R_2 of the LHC, and sends policies with them.

Step 9 After the decryption with its own certificate, the LHS is requested with random numbers R_6 and R_2 of the HIMC and sends R_2 to the HIMC. After receiving R_2, the HIMC hashes in connection with random number R_6 and produces the session key.

Each of the session keys used for transmitting information among the LHC, the HTSC, and the HIMC is produced and stored through the aforementioned mutual authentication protocol.

3.2.2. Information Transmission Phase

Utilizing the previously produced session key this phase indicates courses of information transmission and script provision among the LHC, the HTSC, and the HIMC. Detailed procedures for the information provision in Figure 4 are as follows.

Step 1 The LHC requests a personal healthcare record to the HTSC.

Step 2 After requested for information, the HTSC uses SK_LHS, a session key shared in advance with the LHC, and sends encrypted policies to be used in the future in preparation for the replay attack.

Step 3 The LHC requests the token of the HIMC from the HTSC. At this time, the value added with 1 from the time stamp is encrypted with SK_LHS and sent together to prevent a replay attack.

Step 4 The HTSC sends the token of the HIMC requested with SK_LHS that was shared in advance with the LHC. After receiving the token, the LHC decrypts and verifies it.

Step 5 The HIMC proceeds with the decryption of SK_HIS shared in advance and acquires the token from the LHC. Then, the HIMC verifies that it is an authenticated LHC.

Step 6 After receiving the token and verifying that it is a valid LHC, the HIMC grants the LHC the authority to confirm the PHR.

Step 7 After being granted with authority, the LHC confirms the personal health record.

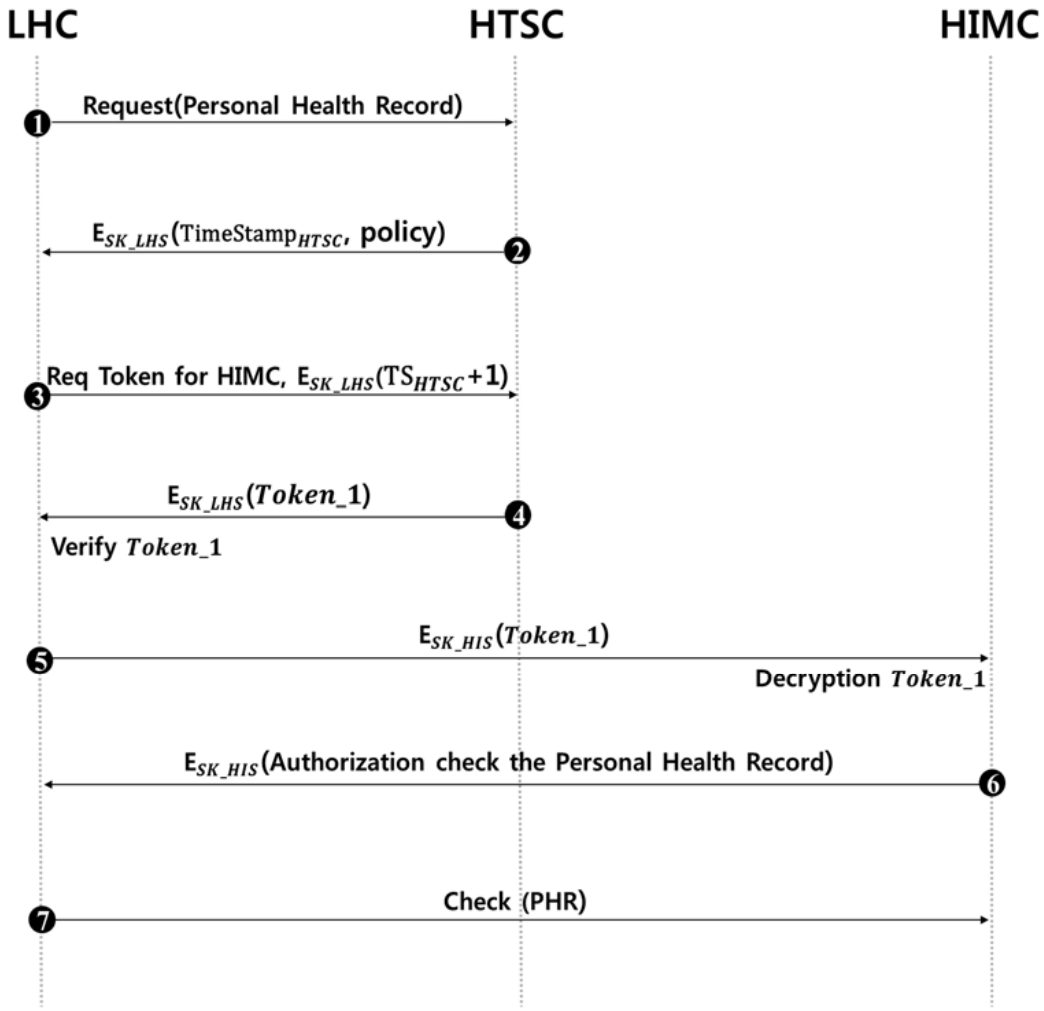

Figure 4. Proposed e-Healthcare information transmission protocol.

4. Security and Performance Analysis

4.1. Security Analysis

Table 2 shows the e-Healthcare service on the suggested protocol and the evaluation of security. The suggested protocol provides mutual authentication between the LHC and the HTSC, between the HTSC and the HIMC, and between the HIMC and the LHC. In addition, the suggested protocol is secure with relay attack, replay attack, eavesdropping, and forward security, and the HTSC plays the role of a third party so that each of them securely authenticate and share the session key. Furthermore, when comparing with previous research, proposed scheme represents a higher level of security and guarantees privacy.

Table 2. Comparative security and service analysis.

Security Requirment	Yun-Yong Sok [32]	Yong Sik Jung [33]	Moon Sun Shin [34]	Yoon-Su Jeong [35]	Proposed Scheme
Certification	X	X	X	X	O
Encryption	X	X	O	O	O
Security	X	X	Δ	O	O
Privacy	X	X	O	O	O
Eavesdropping	X	X	O	O	O
Forward Security	X	X	O	X	O
Authentication	X	X	O	O	O
Relay Attack	X	X	X	X	O
Denial-of-Service Attck	X	X	X	O	O

O: Support; Δ: not fully support; X: Not support.

Privacy: Breaches in privacy and of private information in the e-Healthcare environment is a serious issue. The suggested e-Healthcare protocol constitutes a security channel between the LHC and the HTSC, between the HTSC and the HIMC, and between the LHC and the HIMC of the users instead of a simple station-to-station security channel to solve the issue of how information is maliciously eavesdropped on or recklessly exposed, preventing privacy invasion in advance.

Relay attack: Relay attack uses a method where an attacker eavesdrops on the data transmitted by a device or server and steals the data in the network. The data and messages collected during the session are then re-used for authentication. Malicious attackers are able to attempt relay attack between the device and the HTSC or between the LHC and the HIMC of the users. However, if malicious attackers are disguised as HTSC requesting the certificate from the LHC or the HIMC, it is possible to acquire values from the LHC or the HIMC. However, all of them are random values and are hence meaningless. The random number needed to produce the session key is hashed after being connected and cannot be physically copied. Therefore, it is not feasible to establish a security channel. If malicious attackers are disguised as a LHC, making an attempt for authentication through a HTSC, the random number used for producing the session key must be produced by secure communication objects, or hash values must be restored. Therefore, it is not feasible to produce a session key.

Replay attack: Replay attack selects a valid message from the protocol and re-transmits it later to disguise itself as a legitimate user. The message sent among the LHC, the HTSC, and the HIMC might be re-used through relay attack and hence utilized by malicious users for authentication. However, the LHC requests a token to be provided with information from the HIMC with personal health records and medical information. When requesting the token, the time stamp is used to protect personal medical information that cannot be exposed to anyone except users. In addition, it prevents unauthenticated medical institutions from being disguised as authenticated LHCs and confirming the information through replay attack on the network, providing securer medical information and defending the replay attack.

Eavesdropping: Eavesdropping attack refers to eavesdropping on the exchange of packets by other people on a network. A malicious attacker acquires valid data from the wireless network to eavesdrop on the messages exchanged during a mutual authentication stage. Random users are able to eavesdrop on messages exchanged in the stages of mutual authentication. Especially, user devices and LHCs communicate with each other in wireless settings. Therefore, if wiretapped messages contain sensitive information, it might be a significant security threat. However, messages exchanged in the suggested protocol are session keys produced with a random number, securely shared in advance among the LHC, the HTSC, and the HIMC. Therefore, random numbers as sensitive data needed for producing a session key is the value sent after being encrypted with a certificate, securely produced beforehand. Therefore, it is feasible to securely protect medical information from malicious attackers.

Forward security: Even if a malicious attacker finds out the current secret key, he must be prevented from acquiring past information and using the exposed information. The past information of the objects can be used to identify the user's past location, raising concerns over privacy invasion.

In the suggested system, a malicious attacker can steal the session key between the LHC, the HTSC, and the HIMC to attempt to restore past messages. Malicious attackers might make an attempt to steal the session key among the LHC, the HTSC, and the HIMC and to restore previous messages. If the LHC, the HTSC, and the HIMC re-use the session key on a regular basis or produce the session key by using parameters that influence the past and the present, it is possible to restore the past session key. However, a random number value used for producing the session key in the suggested protocol is not re-used and removed every time it is used. Therefore, it is secure with forward security.

Denial-of service security: The malicious attacker can attempt a DoS attack between the LHC, the HTSC, and the HIMC to make the corresponding resources scarce so that they cannot be used for their original intent. However, in the suggested protocol, the LHC, the HTSC, and the HIMC received a reliable authentication from CA. By using this authentication, a random number is exchanged between the three to create a session key. This makes it secure against a DoS attack.

4.2. Computing Resource Analysis

Table 3 shows a computing resource analysis calculated when a LHC, a HTSC, and a HIMC are used when exchanging information and establishing a session key in the suggested protocol. Since the LHC, the HTSC, and the HIMC tend to have a similar value of calculation, any one particular communicator does not perform a more complicated calculation. The user device has the lowest computing power. Therefore, it requests calculation. A relatively complicated calculation is performed by communicators with similar computing power. Therefore, there are not many calculations except for two in the beginning of the random number generation. Similar computing calculations have been distributed according to the computing resource while establishing the mutual authentication and security channel with the minimum amount of calculation. In addition, although a DoS attack can be used to make resources of a given system scarce so that they cannot be used for the original intent, the suggested system will have received authentication from a trusted CA. Using that authentication for calculation, security is assured.

Table 3. Comparative computing resource analysis between communication objects.

Operation	LHC	HTSC	HIMC
Hash	1	1	1
Encryption	4	4	3
Decryption	5	3	3
Session key generation	2	2	2
Nonce generation	2	2	2
Token generation	-	1	-

4.3. Storage Resource Analysis

Table 4 shows storage resource analysis calculated when a LHC, a HTSC, and a HIMC are applied if exchanging information and establishing a session key in the suggested protocol. Storage space tends to possess a similar amount in each communicator. They also possess two random numbers, their own certificates, and certificates of other communicators while storing two session keys to establish authentication and a security channel. The LHC possesses total three certificates, including its own certificate and the ones of the HTSC and the HIMC, and two session keys for authentication. In addition, they possess one token and two time stamps for communication with the HIMC when exchanging information. The HTSC possesses certificates of each of them, two session keys, two time stamps, and a token. The LHC, the HTSC, and the HIMC are distributed with a similar storage resource depending on the capacity of the storage resource.

Table 4. Comparative storage resource analysis between communication objects.

Operation	LHC	HTSC	HIMC
Random value	2	2	2
Certificate	3	3	3
Session key	2	2	2
Timestamp	2	2	-
Token	1	1	1

5. Conclusions

Due to the progress in the field of IT, many applications have emerged in the field of medicine. Among such applications is the prevention of diseases and health management in the field of medicine. However, the paradigm has now changed to go further: to improve quality of life by providing the continuous prevention of disease and continuous health management. However, e-Healthcare services provide services with important information such as the personal, biological, and medical user information in the use of wire or wireless networks. Therefore, there have been security threats, including eavesdropping, manipulation, the forgery of important information, and the illegal utilization of information due to hacking from malicious attackers. Hereupon, there is a possibility for them to cause direct and economic damage, threatening people's lives. In addition, research on security service models for e-Healthcare services has been continuously conducted, but there has not been sufficient researches dealing with security threats for e-Healthcare services. Since the proposed secure personal e-Healthcare system is provided with authentication from a secure CA, services are provided to only authorized users. Security for the information is provided through the encryption and integrity that the process grants. In particular, proposing a secure service model for efficient e-Healthcare environments took secure cyber world into account by bringing efficiency to a security system for the services provided in e-Healthcare. Moreover, in the area combining IT and medical treatment, an e-Healthcare system can be used as SCW by providing secure e-Healthcare services. Nevertheless, there are still problems associated with the interoperability between different models as well as legal and institutional limits to important information, such as medical information. Follow-up studies are recommended to further review the issue of interoperability between different models in this kind of security system.

Acknowledgments: This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-H8601-16-1009), supervised by the IITP (Institute for Information & Communications Technology Promotion).

Author Contributions: Jong Hyuk Park performed research; Jungho Kang and Hague Chung designed the protocol; Jungho Kang and Jeongkyu Lee performed and analyzed the data; Jong Hyuk Park and Jungho Kang wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kim, J.-H.; Ahn, S.; Soh, J.; Chung, K. U-Health Platform for Health Management Service Based on Home Health Gateway. In *IT Convergence and Security 2012*; Springer: Dordrecht, The Netherlands, 2013; pp. 351–356.
2. Jung, E.-Y.; Kim, J.-H.; Chung, K. Home Health Gateway Based Healthcare Services through U-Health Platform. *Wirel. Pers. Commun.* **2013**, *73*, 207–218. [CrossRef]
3. Touati, F.; Tabish, R. U-Healthcare System: State-of-the-Art Review and Challenges. *J. Med. Syst.* **2013**, *37*, 1–20. [CrossRef] [PubMed]
4. Kang, Y.; Lee, H. A Survey of Security Threats on U-Healthcare. In Proceedings of the Korean Society of Computer Information, Wonkwang Univ.: Iksan-si, Jeollabuk-do, Korea, July 2012; Volume 20, pp. 55–58.
5. Stanford Research Institute. *A Trend and Prospect of a Sizeable Market—U-Healthcare, 2010*; Stanford Research Institute: Menlo Park, CA, USA, 2010.

6. Touati, F.; Tabish, R.; Mnaouer, A.B. Towards U-Health: An Indoor 6LoWPAN Based Platform for Real-Time Healthcare Monitoring. In Proceedings of the 2013 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), Dubai, United Arab Emirates, 23–25 April 2013.
7. Lee, Y.; Jeong, D.; Lee, H. Empirical Analysis of the Reliability of Low-Rate Wireless U-Healthcare Monitoring Applications. *Int. J. Commun. Syst.* **2013**, *26*, 505–514. [CrossRef]
8. Kim, J.; Chung, K. Ontology-Based Healthcare Context Information Model to Implement Ubiquitous Environment. *Multimed. Tools Appl.* **2014**, *71*, 873–888. [CrossRef]
9. Kelly, S.D.T.; Suryadevara, N.K.; Mukhopadhyay, S.C. Towards the Implementation of IoT for Environmental Condition Monitoring in Homes. *IEEE Sens. J.* **2013**, *13*, 3846–3853. [CrossRef]
10. Niewolny, D. *How the Internet of Things Is Revolutionizing Healthcare*; Healthcare Segment Manager, Freescale Semiconductor: Austin, TX, USA, 2013; pp. 2–6.
11. Kim, Y.J.; Kim, C.Y.; Shin, Y.J. The Effects of Ubiquitous Healthcare Service on the South Korean Economy: Using Input-Output Analysis. *Inf. Syst. Front.* **2016**, 1–12. [CrossRef]
12. Jeong, C.; Shin, C.; Joo, S. Construction of Multi-Agent-Based Distributed Framework for Application Services of u-Hospital Information Systems. *J. KIISE Comput. Pract. Lett.* **2009**, *15*, 861–865.
13. Kim, S.; Kim, S.; Jung, J. Design of Operating Room Patients Location System for u-Hospital. *J. Korea Soc. Comput. Inf.* **2013**, *18*, 103–110. [CrossRef]
14. Jang, S.H.; Kim, R.H.; Lee, C.W. Effect of U-Healthcare Service Quality on Usage Intention in A Healthcare Service. *Technol. Forecast. Soc. Chang.* **2016**. [CrossRef]
15. Lim, S.; Kang, S.M.; Kim, K.M.; Moon, J.H.; Choi, S.H.; Hwang, H.; Jung, H.S.; Park, K.S.; Ryu, J.O.; Jang, H.C. Multifactorial Intervention in Diabetes Care Using Real-Time Monitoring and Tailored Feedback in Type 2 Diabetes. *Acta Diabetol.* **2016**, *53*, 189–198. [CrossRef] [PubMed]
16. Shin, D.; Shin, D.; Shin, D. Ubiquitous Healthcare Platform for Chronic Patients. In Proceedings of the 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 15–17 February 2016.
17. Nam, I.; Kang, H.; Woo, D.H. Bio-Signal Acquisition Circuit With High Signal-to-Noise Ratio for U-Healthcare System. *Electron. Lett.* **2014**, *50*, 1671–1673. [CrossRef]
18. Fahim, M.; Lee, S.; Yoon, Y. SUPAR: Smartphone as a Ubiquitous Physical Activity Recognizer for U-Healthcare Services. In Proceedings of the 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Chicago, IL, USA, 26–30 August 2014.
19. Lee, S.-H.; Lee, D. A Study on Review and Consideration of Medical Industry Convergence Based on U-healthcare. *J. Digit. Converg.* **2013**, *11*, 193–197.
20. Hur, J.-Y.; Lee, K.Y.; Lee, D.H.; Kang, J.J. Design and Development of Smart Monitoring System for U-Healthcare. *J. Converg. Cult. Technol.* **2015**, *1*, 107–111. [CrossRef]
21. Tyagi, R.R.; Lee, K.-D.; Aurzada, F.; Kim, S.; Reisslein, M. Efficient Delivery of Frequent Small Data for U-Healthcare Applications over LTE-Advanced Networks. In Proceedings of the 2nd ACM International Workshop on Pervasive Wireless Healthcare, Hilton Head, SC, USA, 11–14 June 2012; ACM: New York, NY, USA, 2012.
22. Ryu, G.-T.; Choi, H. Implementation of U-Healthcare System for Chronic Disease Management. *J. Inst. Electron. Inf. Eng.* **2014**, *51*, 233–240. [CrossRef]
23. Lee, S.-C.; Chung, W. A Robust Wearable U-Healthcare Platform in Wireless Sensor Network. *J. Commun. Netw.* **2014**, *16*, 465–474. [CrossRef]
24. Choi, K.; Kim, J. Analysis of the Efficiency of the U-Healthcare Industry. *Indian J. Sci. Technol.* **2015**, *8*, 471–481. [CrossRef]
25. Kim, D.; Kim, S. Design of Key Tree-Based Management Scheme for Healthcare Information Exchange in Convergent U-Healthcare Service. *J. Korea Converg. Soc.* **2015**, *6*, 81–86. [CrossRef]
26. Song, C.-G.; Lee, K.; Ryu, G. Process of the Encryption Key Using a Physical Information in the U-Healthcare Service. *J. Digit. Converg.* **2014**, *12*, 573–578. [CrossRef]
27. Lee, K.-D.; Kim, S.G.; Yi, B.K. Random Access Parameter Control for Reliable U-Healthcare Services with Highly Loaded BAN Traffic. *Int. J. Auton. Adapt. Commun. Syst.* **2013**, *6*, 240–252. [CrossRef]
28. Mtonga, K.; Yang, H.; Yoon, E.; Kim, H. Identity-Based Privacy Preservation Framework over U-Healthcare System. In *Multimedia and Ubiquitous Engineering*; Springer: Dordrecht, The Netherlands, 2013; pp. 203–210.
29. Son, J.; Kim, S.; Park, G.; Cha, J.; Park, K. Security Requirements for the Medical Information Used by U-Healthcare Medical Equipment. *Int. J. Secur. Appl.* **2013**, *7*, 169–180.

30. Cho, G.-Y.; Lee, S.; Lee, T. Research on a Solution for Efficient ECG Data Transmission in U-Healthcare Environment. *J. Digit. Converg.* **2014**, *12*, 397–403. [CrossRef]
31. Kim, J.T. Authentication Process between RFID tag and Mobile Agent Under U-healthcare System. *Int. J. Bio-Sci. Bio-Technol.* **2014**, *6*, 109–116. [CrossRef]
32. Sok, Y.; Kim, S. Integrated Medical Information System Implementation for the U-Healthcare Service Environment. *J. Korea Contents Assoc.* **2014**, *14*, 1–7. [CrossRef]
33. Jung, Y.-S. Implementation Plan of Integrated Medical Information System for Ubiquitous Healthcare Service. *J. Korea Ind. Inf. Syst. Soc.* **2010**, *15*, 115–126.
34. Shin, M.S.; Jeon, H.S.; Ju, Y.W.; Lee, B.J.; Jeong, S. Constructing RBAC Based Security Model in U-Healthcare Service Platform, Hindawi Publishing Corporation. *Sci. World J.* **2015**, *2015*, 1–13. [CrossRef] [PubMed]
35. Jeong, Y.; Lee, S. A Study of Patient's Privacy Protection in U-Healthcare. *J. Korea Inst. Inf. Secur. Cryptol.* **2012**, *22*, 913–921.
36. Conejar, R.J.; Bae, J.; Kim, H. A Study of an IP-based Mobile U-Healthcare System. *Adv. Sci. Technol. Lett.* **2015**, *97*, 120–124.
37. Bang, G.H.; Lee, D.J.C.D.K. Monitoring Human Blood Pressure for U-Healthcare Using ISO/IEEE PHD Standard. In Proceedings of the Fourth International Conference on Digital Information Processing and Communications (ICDIPC2014), Kuala Lumpur, Malaysia, 18–20 March 2014.
38. Bravo Santisteban, R.D.; Youm, S.; Park, S. U-Healthcare Center Service in Busan City, South Korea: An Empirical Analysis and the Results of 1 Year of Service. *Telemed. e-Health* **2015**, *21*, 774–781. [CrossRef] [PubMed]
39. Conejar, R.J.; Kim, H. Proposed Architecture for U-Healthcare Systems. *Int. J. Softw. Eng. Appl.* **2015**, *9*, 213–218. [CrossRef]
40. Yang, Y.; Kim, M. Analysis of User Requirement on U-Healthcare System. *Int. J. Bus. Tour. Appl. Sci.* **2013**, *1*, 1–10.