PAPER Special Section on Information and Communication System Security

A Healthcare Information System for Secure Delivery and Remote Management of Medical Records

Hyoung-Kee CHOI[†], ***Member***, **Ki-Eun SHIN**[†], ***Nonmember***, ***and*** **Hyoungshick KIM**[†a)], ***Member***

SUMMARY With the rapid merger of healthcare business and information technology, more healthcare institutions and medical practices are sharing information. Since these records often contain patients' sensitive personal information, Healthcare Information Systems (HISs) should be properly designed to manage these records in a secure manner. We propose a novel security design for the HIS complying with the security and privacy rules. The proposed system defines protocols to ensure secure delivery of medical records over insecure public networks and reliable management of medical record in the remote server without incurring excessive costs to implement services for security. We demonstrate the practicality of the proposed system through a security analysis and performance evaluation.

key words: *Healthcare Information System (HIS), privacy, Elliptic Curve Cryptography (ECC), Protected Health Information (PHI)*

1. Introduction

Large-scale deployment of information and network technologies will improve communication among patients, physicians, and insurers as well as permit the delivery of accurate health information anytime, anywhere. Many healthcare providers such as clinics, pharmacies, and hospitals have deployed an online healthcare information system (HIS) as a way to reduce costs and improve the quality of their services.

An HIS can collect, transfer, and exchange health information in the form of an Electronic Health Record (EHR). This health information is shared and accessed by various stakeholders such as healthcare staff, healthcare clearinghouses, government agencies, and insurance companies. This diffusion of access while maintaining strict security will facilitate and expedite every aspect of healthcare delivery. Moreover, as patients become aware of the benefits of EHRs, they are likely to take a more active role in their own health management and consequently be more involved in keeping, managing, and sharing important and very sensitive health information.

Security, however, is an indispensable element in planning a successful HIS that will deliver these benefits. The security design for such a system poses tough choices in achieving a balance between access control, privacy, and practicality. We want health information to be available under precise conditions and circumstances to legitimate personnel only; also, we do not want any civilians with malicious intent to be able to eavesdrop health information at any cases even if the shared nature of wireless devices, public-domain networks and the mobility of the patients may interfere with security.

A strict sense of conventional security is not always well suited for certain situations in the medical work flow. Too strict and inflexible access control may prevent health information from being retrieved promptly by legitimate medical personnel, especially in emergency situations in which a patient may be unconscious and unable to respond. Further, the anonymity of healthcare information is meaningless when a patient must provide his or her health information to a healthcare provider during a consultation. This uniqueness of the medical work flow has led organizations and governments to reexamine the security issues posed in the delivery of healthcare and to subsequently declare their own interpretations of security design. One example of the promulgation of such rules and regulations are Health Insurance Portability and Accountability Act (HIPAA) [1] in the United States. Any HIS should comply with the rules and regulations enacted by the government of the country in which it operates.

We initiated research into the question of whether one can develop a security suite of elaborate and carefully designed elements for an HIS. First, we established an architectural model of the HIS that is composed of three planes; those are acquisition, delivery, and management planes. Specifically we tackle research issues on secure delivery of the EHR over public networks and reliable management of the EHR at remote servers. We specify not only the practical entities and security requirements but also the four-phased procedure for secure transactions within an HIS. Along with an efficient cryptographic algorithm this design makes it possible to assure the privacy and security of health information and at the same time deliver the efficient and effective practicality necessary for deployment of a system in a real-world healthcare environment. To prove our design's feasibility, we evaluated the performance of the proposed system in terms of service delay and storage overhead.

2. System Model

2.1 Architectural Model

Figure 1 illustrates an HIS architectural model composed

Manuscript received May 21, 2015.
Manuscript revised October 10, 2015.
Manuscript publicized January 13, 2016.

[†]The authors are with the School of Information and Communication Engineering, Sungkyunkwan University, Suwon, 16419 Korea.
a) E-mail: hyoung@skku.edu (Corresponding author)

DOI: 10.1587/transinf.2015ICP0007

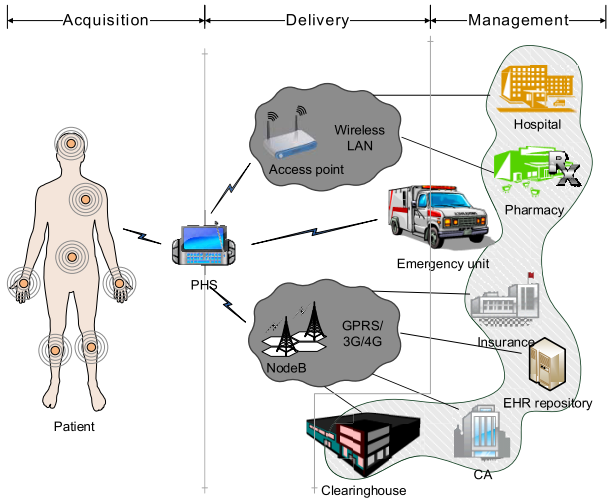

Fig. 1 Healthcare Information System (HIS)

of three distinct planes: (1) acquisition, (2) delivery, and (3) management planes. The health information on a patient's physical condition is collected in the acquisition plane and transmitted over the delivery plane to entities in the management plane.

In the acquisition plane, a set of biomedical sensors monitors a patient's vital signs, forming a wireless body area network (WBAN). A patient possesses a Personal Healthcare Server (PHS) capable of collecting personal healthcare information from these sensors and communicating this information to other entities in the management plane over public networks. A PHS can store personal healthcare information in its smart card with other data such as emergency data, metadata for health information, the patient's private-public key pair, and an insurance contract signed by the insurer.

The delivery plane serves mainly to distribute patients' health information securely and safely over these open-to-the-public networks. When telemedicine and a transaction involving an EHR on remote servers on the Internet are occurred, a 3G/4G wireless network is used to first connect a PHS to an access network and then to the Internet.

Each patient's medical records are created, stored, and managed by entities in the management plane. Each clinic, pharmacy, and hospital is a Healthcare Provider (HP) and creates health information when a patient visits the HP for consultation. An Emergency Unit (EU) is a special HP. An EU is the only HP that creates a health information in an emergency situation and differs from general practitioners in how it interacts with a patient. The Healthcare Clearinghouse (HCH) is in charge of managing patients' accounts for billing. The EHR repository is a remote server that stores patients' health information and collectively supplies a patient's comprehensive health history.

This paper will concentrate, with only a few exceptions, on the delivery plane because we are interested in handling the transmission of health information over insecure public networks rather than over private or closed networks.

2.2 Technical Challenges

Patient-centric healthcare is an emerging model that optimizes the healthcare system's focus on patients' experiences and outcomes toward achieving better health and well-being. According to this concept, covered entities in the system are digitally restricted to access any health information without a patient's explicit consent when the health information is being accessed.

For operational simplicity and backward compatibility with incumbent clinical workflow, human involvement in the processing of healthcare information should be minimized. Human intervention in an automatic procedure sometimes errs and brings unexpected outcomes. This burden, though small, will encourage some patients to disable or work around the mechanism, nullifying its security protection.

A HIS must operate within the guidelines established by a well-known regulation, HIPPA. This regulation governs the privacy and security of medical records and any personal information they contain. HIPAA further specifies delegation of the patient's authority to release information in emergencies in which a patient is unconscious.

All operating intelligence resides in the PHS, which is operated with covered entities on behalf of patients. The PHS is powered by a battery. In an effort to extend a battery lifetime the PHS has stringent computational limitations. Besides, storage limitations is also applicable because the storage size is proportional to a cost of the PHS. These two limitations render us to rule out numerous available protocols and instead require design of one highly efficient and compact in terms of its computational and storage requirements.

2.3 Security Requirements

The basic design model shares the general security requirements of data in an insecure wireless communication. Those requirements are the *confidentiality* and *integrity* of medical data and *mutual authentication* of entities in the HIS. In what might be called "*availability*" and "*accountability*," respectively, we require that medical records are available to all legitimate entities at the location of the caregiver, and any form of manipulation of medical records must be monitored so as to trace and determine responsibility for any improper and/or illegal access.

The concept of privacy differs somewhat from the conventional concept. Although conventional privacy is aligned with the anonymity of users, privacy as defined in this paper is quite close to confidentiality and availability granted under precise conditions with a patient's knowledge. The revised concept is that a patient's privacy is preserved as long as his or her healthcare information is confidential, accessible by legitimate covered entities, and disclosed only according to the law and/or the patient's explicit consent.

Some security requirements unique to the healthcare

deserve to be mentioned in the manuscript. A patient's unique identification is useful for auditing and tracking. The biometric of a patient $h(bio)$ is such identification used for auditing and authenticating an emergency unit on behalf of an unconscious patient.

An emergency unit (EU) must have ways to authenticate a patient even if a patient is unconscious. A great care need to be taken not to release healthcare information before the EU is authenticated in the system.

Any new security procedures must not interfere with incumbent clinical workflow. The proposed system is designed after considering interactions and workflows among six covered entities. Furthermore, we conceived the security procedure to minimize involvement of human actions. These two concepts renders the new security procedure to be transparent to clinical personnel and covered entities.

3. Proposed Secure Protocol for an HIS

3.1 Healthcare Service Registration Phase

A patient contracts for healthcare insurance. These two entities, a potential patient and an insurer, should meet in person to agree on a contract and for the patient to give biometric information (bio). Patients under age 18 may share a PHS with their parent or guardian. As for sharing information, medical information needs to be managed separately in the PHS as well as in the HIS.

As preparation for registration, the insurer selects an elliptic curve E defined over $GF(p)$ or $GF(2^m)$ and generates a random integer $K_{pr,I} \in [1, n-1]$ as the insurer's private key and derives its public key by computing $K_{pu,I} = K_{pr,I} \cdot G$ where G is a base point of the elliptic curve E. Cryptographic computation for the patient takes place in the PHS.

A.1: The insurer selects a random integer $k \in [1, n-1]$ and computes Eq. (1) to Eq. (3) to execute the signature on contract $CTRT$. The signature for the contract is (r, s) generated based on the ECDSA [2]. Only the insurer can generate the signature because of the insurer's private key, $K_{pr,I}$ in the signature. Equation (4) shows the computation of K_m, a patient's master key. $h(\cdot)$ represents a SHA-256 hash operation and prime number n is the order of G.

$$k \cdot G = (x_I, y_I) \tag{1}$$

$$r = x_I \bmod n \tag{2}$$

$$s = k^{-1}(h(CTRT) + K_{pr,I} \cdot r) \bmod n \tag{3}$$

$$K_m = h(k \oplus (h(bio) \parallel CTRT)) \tag{4}$$

A.2: The insurer forwards $\{r, s, CTRT, K_m, h(bio)\}$ to the patient.

A.3: The patient computes Eq. (5) to Eq. (7) to verify the signature. The signature is valid if $x_I = r \bmod n$.

$$u_1 = h(CTRT) \cdot s^{-1} \bmod n \tag{5}$$

$$u_2 = r \cdot s^{-1} \bmod n \tag{6}$$

$$(x_I, y_I) = u_1 \cdot G + u_2 \cdot K_{pu,I} \tag{7}$$

A.4: The patient stores important data in the PHS; this data consists of the patient's public-private key pairs, elliptic curve E's parameters, and healthcare data such as the $CTRT$, K_m, $K_{PI} = h(h(K_m))$ and data for emergency use in a protected form, $h(bio) \oplus (K_{PI} \parallel eData)$.

This set of sequential operations can be thought of as offline operations that need to be performed before any other phases.

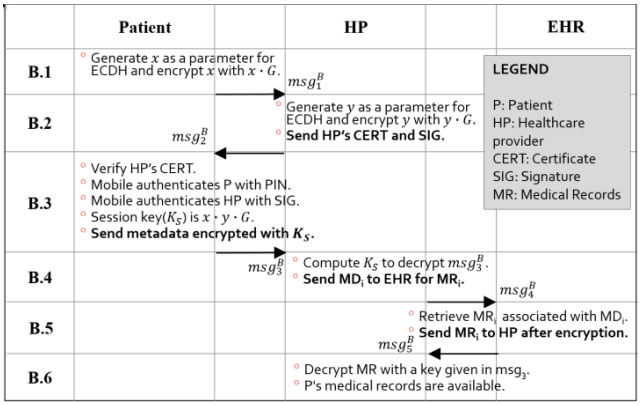

Fig. 2 Medical record retrieval phase

3.2 Medical Record Retrieval Phase

When a patient visits an HP, both parties mutually authenticate in a challenge-response fashion. An HP consulting with a patient retrieves the patient's medical records from the EHR repository as shown in Fig. 2.

B.1: The patient generates a random number, x, and sends $R_1 = x \cdot G$ to the HP.

B.2: The HP generates another random number, y, and computes $R_2 = y \cdot G$. The HP forms msg_2^B, as shown in Eq. (8), to send it to the patient. hid is an identification of the HP. A certificate of the HP's public key and a signature on $R_1 \parallel R_2 \parallel hid$ are included in msg_2^B with other parameters.

$$msg_2^B := \{hid, R_2, cert(K_{pu,H}), sig_H(R_1 \parallel R_2 \parallel hid)\} \tag{8}$$

B.3: Resource constraints make it almost impossible to maintain the CRLs in the PHS. Alternatively, the PHS on behalf of the patient performs verification by forwarding the HP's certificate $cert(K_{pu,H})$ to the Certificate Authority (CA). Once the patient confirms that the certificate of the HP is valid, he or she checks the signature in msg_2^B with $K_{pu,H}$. If the signature is valid, the mobile phone requests the input of a personal identification number (PIN). The patient authenticates the HP with a valid signature in msg_2^B, and the patient is authenticated by supplying the correct PIN. Once mutual authentication is completed, the patient derives a session key, K_s, as shown in Eq. (9), based on the ECDH. K_s is used to protect messages in an insecure channel between the patient and an HP. Then, the PHS searches the metadata of the medical records in association with hid and derives $K_{md_i} = h(h(K_m) \parallel MD_i)$ from both the patient's master key K_m and the metadata MD_i. This K_{md_i} is used to encrypt and decrypt the patient's medical records. Finally, the

PHS constructs msg_3^B as shown in Eq. (10). This message is encrypted with the session key K_s to protect it from being intercepted.

$$K_s = x \cdot R_2 = y \cdot R_1 \tag{9}$$

$$msg_3^B := E_{K_s}\Big(PI \parallel MD_i \parallel K_{md_i}(h(PI \parallel MD_i \parallel K_{md_i}))\Big) \tag{10}$$

B.4: The HP also derives session key K_s to decrypt msg_3^B. Once the integrity of msg_3^B is ensured, the HP requests the patient's medical record by forwarding $msg_4^B = PI \parallel MD_i$ to the EHR repository. Confidentiality is unnecessary in this case because the links between the HP and the EHR repository are secure.

B.5: The EHR repository searches for a medical record in association with PI and MD_i and forwards to the HP the encrypted medical records $E_{K_{md_i}}(MR_i)$.

B.6: The HP decrypts the medical record with K_{md_i} and is now able to access the patient's medical history.

The essence of this phase is to define the way that an HP acquires a patient's symmetric key K_{md_i} in order to decrypt his or her encrypted medical data. In providing secure transmission of the decryption key, this phase also provides mutual authentication, integrity, and confidentiality.

3.3 Medical Record Update Phase

This phase comes after completion of any form of healthcare transaction between an HP and a patient. Figure 3 illustrates the updating of medical records and the billing for services.

C.1: After a healthcare transaction, an HP sends to a patient a new medical record MR_j, a new emergency record $eData$, and a bill for medical services $bData$. For authentication, the HP's signature is included in both the medical record and the billing data. Any particularly critical information about a patient's ailments should be added to $eData$ in the smart card for emergency use. The communication link between a patient and an HP is securely protected by encryption.

C.2: A patient updates $eData$, if it is available in the message, and adds the metadata of the new medical record, MD_j, into the list. A patient derives encryption key $K_{md_j} = h(h(K_m) \parallel MD_j)$ for the medical record and forms the second message shown in Eq. (11). msg_2^C is composed of four components: the patient's signature on the medical record, the patient's signature for medical expenses, an encrypted medical record, and encrypted emergency data. The first signature is used to simultaneously check the integrity of the medical record and authenticate its source. The second patient signature acknowledges the medical expenses incurred.

$$msg_2^C := \Big\{sig_P(PI \parallel E_{K_{md_j}}(MR_j) \parallel eData \parallel MD_j), \; sig_P(PI \parallel bData), E_{K_{md_j}}(MR_j), E_{h(bio)}(eData)\Big\} \tag{11}$$

C.3: The HP generates and transmits msg_3^C to the EHR repository to update the medical record of this patient. The fourth message msg_4^C is sent to the HCH to claim medical expenses. msg_3^C and msg_4^C are shown in Eq. (12) and Eq. (13), respectively. Emergency medical data $eData$ is copied to the EHR repository as well.

$$msg_3^C = \Big\{sig_P(PI \parallel E_{K_{md_j}}(MR_j) \parallel eData \parallel MD_j), \; PI, E_{K_{md_j}}(MR_j), E_{h(bio)}(eData), MD_j\Big\} \tag{12}$$

$$msg_4^C := \{sig_P(PI \parallel bData), PI, bData\} \tag{13}$$

C.4: The EHR repository verifies the signature contained in msg_3^C and keeps MD_j, $E_{h(bio)}(eData)$, and $E_{K_{md_j}}(MR_j)$ in the database indexed by the PI. The HCH also verifies the signature contained in msg_4^C and stores the PI and $bData$ in its local database. The EHR repository sends the fifth message msg_5^C to the patient to confirm to him or her that $E_{K_{md_j}}(MR_j)$ is properly stored. The HCH also forwards a text message (msg_6^C) to the patient to acknowledge billing.

The HP claims payment for medical services from the HCH after an acknowledgement by the patient. Along with a delivery path from a patient to the EHR repository via an HP, a medical record is securely protected by encryption with K_{md_j}.

3.4 Emergency Phase

In a situation in which a patient is unconscious, emergency care may be delayed because medical records are not available immediately to the EU or HP. A patient's biometrics can be used as an alternative to the PIN. Figure 4 shows the

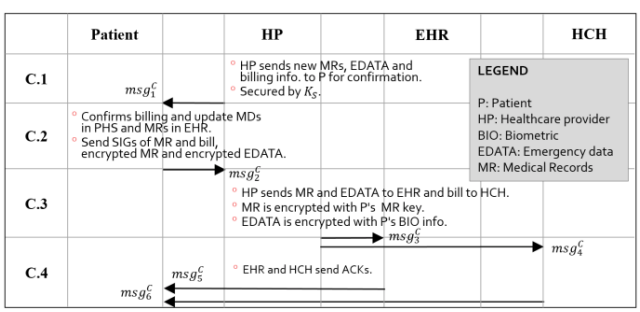

Fig. 3 Procedures in the medical record update phase

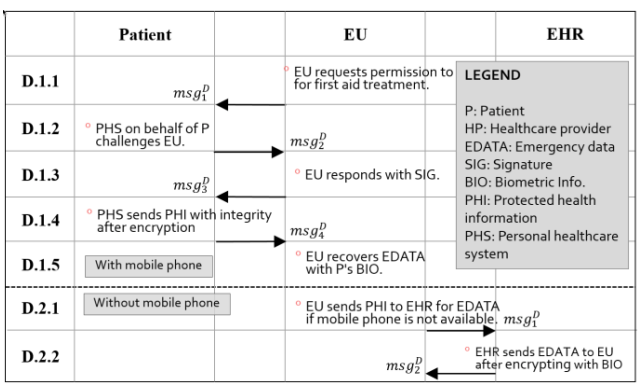

Fig. 4 Emergency phase

procedure in the emergency phase. In an emergency, medical records are available to the EU immediately if a patient has his or her mobile phone at the scene. Otherwise, the EU must contact the EHR repository to retrieve a patient's *eData*. Consider these two cases:

D.1.1: An EU arrives at the scene and requests permission for instant treat of an unconscious patient.

D.1.2: The PHS, on behalf of the patient, sends a challenge in order to authenticate the EU. The challenge is a random number, *pNonce*.

D.1.3: The EU signs *pNonce* with its private key and sends the signature, $sig_E(pNonce)$, along with the certificate $cert(K_{pu,E})$.

D.1.4: The PHS forwards the fourth message msg_4^D shown in Eq. (14) to the EU. This message is protected from eavesdropping by encrypting *eData* with K_{PI} and XORing it using $h(bio)$. K_{PI} is an encryption key for the patient's identification (PI) and can be recovered from the first term in Eq. (14) by using $h(bio)$. The concatenation of $h(bio) \oplus (K_{PI} \parallel eData)$ in the second term is for an integrity check to detect changes to any one of the values $h(bio)$, K_{PI}, or *eData*.

$$msg_4^D := \Big\{h(bio) \oplus (K_{PI} \parallel eData), E_{K_{PI}}\big(PI \parallel (h(bio) \oplus (K_{PI} \parallel eData))\big)\Big\} \quad (14)$$

D.1.5: The EU reads the patient's biometric information to get $h(bio)$. From the derived $h(bio)$, the EU can obtain *eData* and give first-aid treatment.

The following two steps explain how the EU acquires *eData* when a patient does not have his or her mobile phone.

D.2.1: The PI is derived from the patient's biometrics. The PI is sent to the EHR repository to request emergency medical records.

D.2.2: The EHR repository searches $E_{h(bio)}(eData)$ associated with the received PI and sends the appropriate records to the EU. The EU decrypts the message with $h(bio)$.

Because we value a prompt response of the EU, we have designed the PHS to carry emergency medical data (*eData*). Our design, which permits the PI to be obtained directly from the PHS, allows faster access to emergency medical data than if the EHR repository were used. In those instances in which a patient might be unconscious and his or her source of biometrics damaged, the EU has an option of first contacting a governmental organization and then having the insurer send the PI to the EU.

4. Security Analysis

Confidentiality In the proposed system, encryption provides confidentiality of personal medical records. The encryption key K_{md_j} is generated by an individual patient. Before medical record MR_j is stored in the EHR repository, this medical record is encrypted with $K_{md_j} = h(h(K_m) \parallel MD_j)$. For secure communication between a patient and an HP, messages are encrypted with a session key K_s. Moreover, to ensure a non-linkability between encrypted data, a patient with multiple medical records may have several encryption keys. These encryption keys would all be derived from the patient's secret master key, K_m, and the metadata of the medical records. The same mechanism can be applied to an emergency medical record. This record is saved in the EHR repository after being encrypted with the patient's biometrics: $E_{h(bio)}(eData)$.

Integrity Message modification is impossible in the medical record retrieval phase because of the signature included in $msg_2^B := \{hid, R_2, cert(K_{pu,H}), sig_H(R_1 \parallel R_2 \parallel hid)\}$ (see Fig. 2). A valid certificate and the signature together ensure that msg_2^B has not been modified. Furthermore, the signature in msg_2^B includes R_1 sent from the patient so that the patient also can confirm that msg_1^B has not been modified. The integrity of the health information is guaranteed because of the MAC included in $msg_3^B := E_{K_s}(PI \parallel MD_i \parallel K_{md_i} \parallel MAC)$. The HP is able to ensure the integrity of information by comparing the received MAC with derived $MAC' = h(PI \parallel MD_i \parallel K_{md_i})$.

Availability In our protocol, availability is considered in two situations. After authenticating the EU (**D.1.2** and **D.1.3**), the PHS promptly forwards msg_4^D in Eq. (14) to the EU. Hence, the EU can acquire the medical data of an emergency patient and provide optimal care by recovering *eData* and K_{PHI}. If the patient does not carry a mobile phone so that *eData* is available, the EU should nevertheless be able to retrieve his or her emergency medical record from the EHR repository by using the patient's PI. Also, in the exceptional cases, legal units such as governmental entities can access medical data without the explicit permission of a patient. In the proposed system, an insurer can access the encrypted medical data for payment or for public health and safety. Furthermore, governmental organizations can access medical data, if the law allows it.

Accountability In the medical record update phase (see Fig. 3), an HP sends signed billing data ($bData$ in msg_1^C) and a patient signs for receipt of the billing data ($sig_P(h(PI \parallel bData))$ in msg_2^C). Because both parties sign for the billing data in msg_1^C and msg_2^C, neither can dispute it. These two messages also prevent either a patient or an HP from denying responsibility for updating the medical record as a way to avoid accountability for medical accidents and disputes. In our system, both a patient and an HP sign for medical data MR_j in msg_1^C and msg_2^C. These signatures on the two messages represent confirmation by both entities that the medical record has been updated.

Mutual Authentication To access a patient's medical records, entities in our HIS must acquire K_{md_j} from a patient. Before sending a decryption key, a patient and an HP should mutually authenticate each other to avoid fraud. A patient uses a secret PIN for his or her authentication. An HP uses a challenge-response and a certificate-based signature for authentication. If the validity of the PIN and certificate are both verified, the PHS forwards K_{md_j} to the HP for decryption of medical record MR_j.

Privacy According to the definitions contained within the security and privacy rules of the HIPAA, patient privacy in an HIS as well as in a conventional healthcare system is

preserved if the system can ensure the confidentiality and the availability of medical records and the disclosure of medical records under the patient's explicit consent. Confidentiality and availability have already been explained. The patient acknowledges permission to access his or her medical records by releasing K_{md_i} to a legitimate HP. The patient's explicit consent is expressed by releasing the encryption key.

5. Performance Analysis

5.1 Storage Overhead

We have used a smart phone with a USIM card as storage to measure the delay and overhead. In this evaluation, we assumed that a USIM has a 64-kilobyte memory. Because of the efficient design of its storage, the short key size used in the ECC can save space in a USIM. A USIM stores the following components: a certificate, a private key, a contract, a signature for the contract, PHI, K_m, $E_{K_{ph}}(PHI \parallel h(bio) \oplus (K_{ph} \parallel eData))$, and metadata md_i. The size of the public key certificate and the corresponding private key are 1,064 and 40 bytes, respectively. As evidence of subscription, the 1,024-byte contract and the 40-byte signature on the contract are saved in the USIM. The 128-byte PI and 20-byte K_m are also saved in the USIM. Note that other secret keys such as K_{ph} and K_{md_i} need not be stored in the USIM because they can be derived from K_m. An encrypted form of $eData$, $E_{K_{ph}}(PI \parallel h(bio) \oplus (K_{ph} \parallel eData))$, is 148 bytes long and should be stored in the USIM. These components occupy 2,464 bytes of the 64-kilobyte USIM, as shown in Fig. 5. The rest of the storage is reserved for medical metadata. The size of each metadata is 11 bytes long. Because this amount is only 3.76% of the total space, we can store about 5,730 metadata, which means that we are able to access and control 5,730 medical records with an USIM.

5.2 Computational Delay

We evaluated the computational delay both at the patient's side (USIM) and at the HP side in the three phases. We did not consider the healthcare service registration phase because it occurs off-line. The calculation also excludes transmission and processing delays and the user's response time in entering the PIN.

As a way to measure the computational delays in the HP and in the EHR repository, we also measured the computational delays of the cryptographic operations on a Linux server running on Intel Xeon 3.06GHz and 1GB RAM. We used cryptography module *Crypto++ 5.4* to implement the cryptography of interest [15]. Table 1 lists the estimated computational delay for cryptographic operation. Further, we defined the size of each message in each phase as shown in Table 2.

Figure 6 shows the computational delays of the three phases with respect to the patient. ECDSA-G and ECDSA-V refer, respectively, to the generation and verification of the signature. It takes 189ms, 194ms and 114ms, respectively, to complete each of the three phases. We also emulated the three phases to measure computational delays in the HP.

Figure 7 illustrates the computation delays in the HP. It takes about 36ms, 58ms and 1.6ms, respectively, to complete the three phases. The long delay in the medical records update phase is because of operations such as the two ECDSA signature generations and two SHA-1 operations. The shortest delay in the emergency phases on the patient's side was possible by storing $E_{K_{PI}}(PI \parallel (h(bio) \oplus (K_{PI} \parallel eData)))$ in the USIM in advance. This pre-calculation saves a delay up to 44ms.

5.3 Comparison with Other Studies

Lee *et al.* [3] proposed key management as a way to com-

Table 1 Computational delay of cryptographic operations

Operation	Patient (USIM)	HP/EHR repository
SHA-1 (th)	1 ms	0.69 ms
AES-128 (te)	4 ms	0.92 ms
ECDSA-160 signing (ts)	30 ms	27.4 ms
ECDSA-160 verification (tv)	70 ms	57 ms
ECDH (td)	15 ms	7.1 ms

Table 2 Message sizes in each phase

Message	Record retrieval	Record update	Emergency
msg_1	40	25+MS	10
msg_2	10+40+1,064+40=1,154	40+40+MS=80+MS	40
msg_3	192	40+128+MS+10+11=189+MS	1,064+40=1,104
msg_4	128+11=139	40+128+15=183	20+148=168
msg_5	MS	80	
msg_6		80	

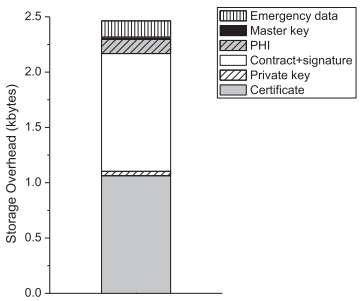

Fig. 5 Storage overhead. These six default components occupy 2,464 bytes in an USIM

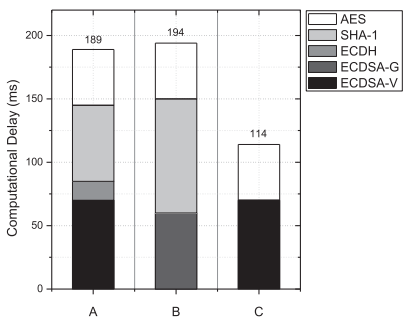

Fig. 6 Comparison of computational delay on the patient's side

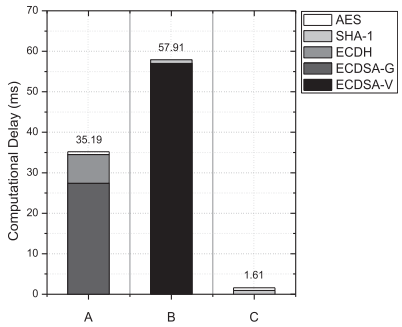

Fig. 7 Comparison of computational delay on the HP's side

Table 3 Comparisons with other two studies

Schemes	Lee et al. [4]	Lin et al. [5]	Ours
Typical healthcare process	Not considered	Partially	Fully
Storage for medical record	EHR + smart card	EHR	EHR + USIM
Emergency data acquisition	Possible	Not considered	Yes
Patient control of medical data	Only for PHI	No	All data
Privacy	Only for PHI	Yes	Yes
Mutual authentication	No	Yes	Yes

ply with the HIPAA privacy and security regulations. In their system, the privacy of the patient and the integrity of the medical record are preserved by well-established cryptographic mechanisms and the reliability of a smart card. However, this approach makes no provision for mutual authentication and key management between a patient and an HP. Lin *et al.* [4] proposed a privacy-preserving scheme for an HIS. They divided the privacy issues in an HIS into two categories: content-oriented privacy and contextual privacy. They argued that simply providing content-oriented privacy was insufficient, and contextual privacy also should be considered and preserved for an HIS to be considered secure. Contextual privacy means an adversary is unable to link the source and the destination of a message.

Table 3 presents a comparison of both the earlier studies and the proposed system. Unlike the earlier studies, our proposed system fully considers typical healthcare processes in the real world, including medical record management and emergency treatment.

In Lee *et al.*'s approach, a patient's PHI and medical records are saved in a smart card and the EHR repository, respectively. In Lin *et al.*'s work (i.e., SAGE), medical data are stored in a remote database server. On the other hand, our protocol maintains both the metadata of medical history and emergency data in a USIM. A copy of the emergency data is also saved in the EHR repository so that it can be accessed in case a mobile phone is not available at the scene of an emergency.

Emergency patients face life-threatening situations, so an emergency procedure should be defined explicitly as part of any HIS. SAGE does not consider an emergency situation in its protocol. Lee *et al.*'s work does not explicitly suggest a way to retrieve emergency data. Instead, an HP can request medical data without a patient's consent when the patient is unconscious. However, additional overhead is introduced because an HP must first query the database for emergency data and then ask the insurer to decrypt these records. In the proposed protocol, because a patient's emergency data is held in the USIM, these data are available immediately to an authorized EU.

Preserving the privacy of patients is achieved by encrypting the PHI and the medical records. The privacy of the PHI, medical records, and emergency data) are preserved in the proposed system, respectively, by encryption with a session key (K_s), individual medical record keys (K_{md_j}) and a patient's fingerprint. On the other hand, Lee *et al.*'s proposal fails in certain situations to guarantee the privacy of a patient's medical records. For instance, once a PHI is given to an HP, the patient is unable to control his medical data. In other words, thereafter the HP can access medical data beyond what a patient intended to authorize.

Mutual authentication between the patient and the HP is quite important in the preservation of privacy. Lee *et al.*'s proposal does not provide mutual authentication but Lin *et al.*'s work and ours do.

6. Literature Survey

The challenge in the *acquisition plane* is mainly twofold: protection of sensitive data by encryption and identification of individuals. Biometrics excels as a tool for establishment of a secure channel in the WBAN. In cases in which the body parts used in biometrics vary slightly, a fuzzy commitment compensates for the variation (see [5] and the references therein). One risk of his approach is that communications between the WBANs of different individuals could easily intermingle and cause significant problems. However, a carefully chosen biometric avoids this potential situation [6]. The author of [7] presented a secure mobile hotspot which can support multiple heterogeneous networking technologies.

One of the most critical security issues in the *management plane* is to control medical records while also preserving patient privacy. The best practice described in much of the recent research is access control by the HP and encryption of the records. A valuable survey paper [8] introduced state-of-the-art work on access control to the EHR. Cryptography-based confidentiality and authentication in the EHR have been popular in much research work [9]–[11] because they are proven concepts, and this software protocol is easy to apply to any system. Lounis et al. [12] proposed a cloud-based architecture for healthcare system to provide high scalability.

The authors of [13] valued patient privacy and proposed access control that supports patient consent while making medical records available. So-called rendezvous-based access control requires the physical co-locality of the HP and the patient to access that patient's medical records. At the heart of this protocol lies the protection of the token carried by the patient and the encrypted data carried by the HP.

The main issue in the *delivery plane* is to ensure the se-

curity of data transmissions in the HIS. Much of the recent research [9]–[11] is aligned with resilient key management and authentication. The authors of [9] proposed key generation as the way to secure communication. The unique aspect of this study was the generation of a random key from physiological data instead of from a pseudo-random generator. IBE-Lite, developed by [10], is lightweight identity-based encryption suitable for sensors with limited computation capability.

Because medical records are stored in remote servers, the availability of the records hinges on network availability. To boost the availability of medical records, the concept of portability has been introduced into the HIS and involves a patient carrying his or her own records on portable devices. A scheme in [14] proposed storage of personal medical records on a smart phone to keep them close at hand in case of emergencies. A software prototype for a portable personal health record was presented in [11]. This software system allows patients to collect their health records from cooperative doctors and safely and accurately maintain them.

7. Conclusion

The proposed system is composed of four phases and designed as to provide a secure channel between a patient and healthcare providers. Analysis and evaluation show that the proposal supports the five security requirements essential for healthcare systems. Furthermore, the various types of operational overhead — service delay and storage — are within reasonable limits. We believe that based on our analysis, our proposed system is quite practical and sufficiently secure to be deployed in a real-world healthcare environment.

Acknowledgments

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (No. NRF-2014M3C4A7030648).

References

[1] HIPAA privacy rules [Online]. Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding.
[2] C. Paar and J. Pelzl, "Elliptic Curve Cryptography and Digital Signature," in Understanding Cryptography: A Textbook for Students and Practitioners, pp.239–288, Springer, 2009.
[3] W.B. Lee and C.D. Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations," IEEE Trans. Inf. Technol. Biomed., pp.34–41, Jan. 2008.
[4] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems," IEEE J. Sel. Areas. Commun., vol.27, no.4, pp.365–378, May 2009.
[5] S.D. Bao, et al., "Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network," IEEE Trans. Inf. Technol. Biomed., pp.772–779, Nov. 2008.
[6] C.C.Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health," IEEE Commun. Mag., vol.44, no.4, pp.73–81, April 2006.
[7] Z. Ahmed, H. Jamal, R. Mehboob, S. Khan, and M. Shahbaz, "Secure cognitive mobile hotspot," IEEE Trans. Consum. Electron., vol.56, no 2, pp.606–612, May 2010.
[8] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Commun., vol.17, no.1, pp.51–58, Feb. 2010.
[9] G.H. Zhang, C.C.Y. Poon, Y. Li, and Y.T. Zhang, "A Biometric Method to Secure Telemedicine Systems," Proc. 31st IEEE Engineering in Medicine and Biology Society '09, pp.701–704, Sept. 2009.
[10] C.C. Tan, et al., "IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks," IEEE Trans. Inf. Technol. Biomed., pp.926–932, Nov. 2009.
[11] W.G. Yee and B. Trockman, "Bridging a Gap in the Proposed Personal Health Record," Proc. ACM Healthcare Information and Knowledge Management (HIKM) '06, pp.49–56, Nov. 2006.
[12] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and Scalable Cloud-Based Architecture for e-Health Wireless Sensor Networks," Proc. IEEE ICCCN, July 2012.
[13] F.W. Dillema and S. Lupetti, "Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment," Proc. ACM SNSHALE '07, pp.1–6, June 2007.
[14] R.W. Gardner, S. Garera, M.W. Pagano, M. Green, and A.D. Rubin, "Securing Medical Records on Smart Phones," Proc. ACM Security and Privacy in Medical and Home-Care Systems '09, pp.31–39, Nov. 2009.
[15] Crypto++ Library [Online]. Available at http://www.cryptopp.com/

Hyoung-Kee Choi received a Ph.D. degree in electrical and computer engineering from Georgia Institute of Technology in 2001. He is an associate professor in Sungkyunkwan University, Korea. He joined Lancope in 2001 and remained until 2004, where he guided and contributed to research in Internet security. His research interests span network security and Internet traffic modeling.

Ki-Eun Shin received a master degree in Mobile Systems Engineering from Sungkyunkwan University in 2010. He is a software engineer at Samsung Electronics. His research interests include security and privacy in mobile communications.

Hyoungshick Kim is an assistant professor at the Sungkyunkwan University. His research interests include security engineering and usable security. He has a PhD in computer security from the University of Cambridge. After completing his PhD, he worked as a post-doctoral fellow at the University of British Columbia. He also worked on Samsung Electronics for trustworthy home networks.