Vol.6, No.4 pp.197~202 pISSN: 2287-5891 https://doi.org/10.3745/KTCCS.2017.6.4.197

A Secure Health Data Transmission Protocol Using Identity-Based Proxy Re-Encryption in Remote Healthcare Monitoring System

Si-Wan Noh† · Youngho Park†† · Kyung-Hyune Rhee†††

ABSTRACT

The remote healthcare monitoring system enables a doctor to diagnose and monitor patient's health problem from a distance. Previous researches have focused on key establishment method between a patient and a particular doctor to solve personal health information disclosure problem in data transmission process. However, when considering a misdiagnosis of doctor, the result of a diagnosis by a many doctors is more reliable. In previous work, in order to select multiple doctors, patient should generate shared key for each chosen doctor and perform many times encryptions. Therefore, in this paper, we propose a secure data transmission protocol for receiving diagnosis from multiple doctors using identity-based proxy re-encryption scheme. In proposed protocol, a patient don't need key management work for session key. Also, monitoring server performs re-encryption process on behalf of patient. So, we can reduce computational burden of patient in previous work.

Keywords : Healthcare, Monitoring System, Proxy Re-Encryption, Identity-Based Cryptography

원격건강정보 모니터링 시스템에서 신원기반 프록시 재암호화 기법을 이용한 건강정보 전송 보안 프로토콜

노 시 완† · 박 영 호†† · 이 경 현†††

요 약

원격 건강정보 모니터링 시스템에서 의사는 원격지에서 환자의 건강상태를 진단하거나 모니터링하여 적절한 의료서비스를 제공한다. 기존의 연구들은 공개된 네트워크를 통한 전송과정에서 환자의 민감한 건강정보의 노출로 인한 문제를 해결하기 위해 환자와 의사 사이에 비밀 공유키를 생성하여 메시지를 암호화하는 방법에 중점을 두고 있었다. 하지만 의사의 오진을 고려할 때 다수의 의사에게 진단을 받는 것이 좀 더 신뢰할 수 있는 진단결과를 얻을 수 있다. 하지만 기존 프로토콜에서는 환자가 여러 의사에게 메시지를 전달하기 위해서는 모든 의사와 각각 공유하는 키의 생성이 필요하고 전송과정에서 선택한 모든 의사들을 위해 여러 번의 암호문 생성과정을 필요로 하였다. 이에 본 논문에서는 신원기반 프록시 재암호화 기법을 사용한 원격건강정보 모니터링 시스템의 전송 보안 프로토콜을 제안한다. 제안 프로토콜에서 환자는 별도의 세션키 관리가 필요하지 않고 전송과정에서 환자가 비밀키로 생성한 암호문을 모니터링 서버에서 재암호화하여 선택한 의사에게 전달하므로 기존 프로토콜을 적용했을 때 환자에게 필요한 과도한 연산부담을 개선할 수 있다.

키워드 : 헬스케어, 모니터링 시스템, 프록시 재암호화, 신원기반 암호

1. 서 론

원격 건강정보 모니터링 시스템(Remote Health Monitoring System)은 환자가 직접 진료실에 방문하지 않고 가정에서도 다양한 의료용 센서(혈압, 혈당 등)들로 구성된 Wireless Body Area Network(WBAN)를 통해 수집된 개인 건강정보(Personal Health Information, PHI)를 의사에게 전송하여 의사는 진단 후, 환자의 식단이나 생활습관 개선 등을 제안하여 당뇨와 같은 만성질환을 가진 환자나 노약자에 대한 장기적이고 지속적인 건강관리 서비스를 제공할 수 있다.

시스템에서 환자의 PHI는 공개된 네트워크를 통해 원격지에 위치한 의사에게 전달된다. Raytheoon-Websense에서 2015년 발표한 보고서[1]에 따르면 개인의 의료정보는 암시장에서 금융정보보다 10배 이상 비싼 가격에 거래되며 이는 신용카드

※ 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF- 2014R1A2A1A11052981).
※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터 육성지원사업의 연구결과로 수행되었음(IITP-2017-2015-0-00403).
※ 이 논문은 2016년도 한국정보처리학회 추계학술발표대회에서 '원격건강정보 모니터링 시스템 상에서 신원기반 프록시 재암호화를 이용한 개인 건강정보 전송'의 제목으로 발표된 논문을 확장한 것임.
† 준 회 원 : 부경대학교 정보보호학(협) 석사과정
†† 정 회 원 : 부경대학교 전자정보통신연구소 전임연구원
††† 종신회원 : 부경대학교 IT융합응용공학과 교수
Manuscript Received : December 23, 2016
Accepted : January 25, 2017
* Corresponding Author : Kyung-Hyune Rhee(khrhee@pknu.ac.kr)

번호나 비밀번호 등의 금융정보는 노출되었을 경우 변경이 가능하지만 개인 의료 내역이나 연령, 성별 등의 정보는 변경이 불가능하기에 사이버 범죄 영역에서 의료정보의 가치는 매우 높게 평가되고 있기 때문이다. 개인의 건강정보를 비롯한 의료정보의 노출은 개인에게 금융정보의 노출보다 더 큰 피해를 줄 수 있고 보험 사기나 의료 사기 등의 가능성으로 인해 의료정보 유출의 위험성이 점점 부각되고 있고 때문에 PHI의 네트워크 전송과정에서의 보호[2-4]와 스마트 카드 등을 사용한 사용자 인증기법[5, 6]이 주로 연구되어 왔다.

PHI의 전송 과정 중 보호를 위해 Lin 등은 [2]에서 Boneh가 제안한 신원기반의 암호기법[7]을 사용하여 시스템에서 전송되는 환자의 건강정보를 보호하기 위해 환자와 환자가 선택한 의사 사이에 비대화식으로 공유하는 공유키를 생성하여 PHI를 보호하는 eHealth 모델을 제시하였고 Yang 등은 [3]에서 Lin 등의 eHealth 모델에서 환자의 비밀키를 저장하는 단말기의 분실 시 환자의 비밀키 분실로 인한 위협을 감소시키기 위해 키격리 기법(key-insulation technique)을 적용하여 단말의 분실 시 기존의 비밀키를 새로운 주기의 키로 갱신하여 이전 주기의, 즉 분실한 키의 사용을 막아 키의 분실로 인한 위협을 감소시키는 방법을 제안하였다. 하지만 [2, 3]의 제안 프로토콜에서 환자는 PHI를 전송할 특정한 의사를 선택하여 둘 사이에 공유하는 세션키를 생성하여 전송에 사용한다. 보다 신뢰할 수 있는 진단결과를 위해 다수의 의사가 한명의 환자의 건강정보에 대해 진단을 내리고 환자는 진단 결과를 종합적으로 수용할 수 있는 시스템 모델을 고려할 때 Lin과 Yang이 제안한 방식을 적용할 경우 환자는 선택한 모든 의사와 세션키를 생성·관리해야 하고 PHI 전송 시 선택한 의사들을 위한 여러 번의 암호문 생성과정이 필요하다. [4]에서 Thilakanathan 등은 클라우드 스토리지를 사용하여 환자가 업로드한 데이터에 액세스 권한을 부여받은 의사들이 데이터에 접근하여 진단을 수행하는 모델을 제안하였다. 제안 모델에서 환자는 액세스 권한을 부여함으로써 여러 의사에게 진단을 위한 PHI를 전달할 수 있지만 클라우드 서비스 제공자를 신뢰기관으로 설정하였고 PHI의 업로드 및 다운로드 과정에서 사용된 알고리즘으로 인해 사용자에게 연산부담이 발생하는 문제가 있었다.

이에 본 논문에서는 암호문의 복호화 권한을 프록시를 통하여 위임하는 프록시 재암호화 기법(Proxy re-encryption) [8-10]을 사용하여 환자가 자신의 비밀키로 암호화한 PHI의 복호화 권한을 사전에 선택한 의사에게 위임하여 환자와 의사들 사이에 공유하는 별도의 세션키 없이 암호문을 전달할 수 있는 프로토콜을 제안한다. 프록시 역할을 수행하는 모니터링 서버는 재암호화 과정에서 PHI의 평문을 얻을 수 없고 재암호화키를 제외한 환자의 정보가 서버에 저장되지 않음으로서 신뢰할 수 없는(semi-trusted) 서비스 제공자에 대해 환자의 프라이버시 보장이 가능하다. 또한 환자는 암호화를 위한 비밀키만을 관리하고 전송 시에 하나의 암호문만을 생성하므로 제한적인 자원을 가지는 단말기에서의 연산부담을 경감시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 연구의 배경으로 기존에 제안된 프로토콜에서 환자가 다수의 의사를 선택하고자할 때 발생하는 문제점을 지적하고 그 해결책을 제시한다. 3장에서는 제안 프로토콜의 시스템 모델과 제안 프로토콜의 설계를 서술한다. 그리고 4장에서는 제안 프로토콜의 보안요구사항에 대한 분석을 수행하고 5장에서 결론을 맺는다.

2. 연구 배경

[2]에서 환자 P는 선택한 의사 D의 신원정보를 사용하여 해당 의사와 비대화식으로 공유하는 키 K_{P-D}를 생성한 후, 이를 사용하여 암호화한 건강정보를 모니터링 서버에 전송하면 서버는 이를 해당하는 의사에게 전송, 이를 전송받은 의사는 환자의 신원정보를 사용하여 환자가 암호화에 사용한 키와 동일한 키 K'_{P-D}를 계산하여 암호문을 복호화한 뒤 건강정보를 획득한다. K_{P-D}는 다음과 같이 계산된다 (여기서 위수로 소수 q를 가지는 두개의 순환군 G, G_T에 대한 겹선형 페어링 $e: G\times G\rightarrow G_T$와 암호학적 해시함수 $H_1: G_T\rightarrow\{0,1\}^{l_1}$, $H_2: \{0,1\}^{*}\times G_T\rightarrow\{0,1\}^{l_2}$를 사용하며 s는 신뢰기관 TA의 마스터키이고 SK_X는 TA가 생성한 개체 X의 비밀키이다.).

$$\begin{aligned} K_{P-D} &= H_2(e(SK_P, H_1(ID_D))) \\ &= H_2(e(sH_1(ID_P), H_1(ID_D))) \\ &= H_2(e(H_1(ID_P), sH_1(ID_D))) \\ &= H_2(e(H_1(ID_P), SK_D) \\ &= K'_{P-D} \end{aligned} \tag{1}$$

서론에서 설명한 것과 같이 의사의 오진으로 인한 문제를 해결하기 위해 환자가 다수의 의사들을 선택하여 건강정보를 전송할 때 [2]의 프로토콜을 적용할 경우의 시나리오는 다음과 같다.

환자 P는 건강정보를 전송하여 이에 대한 진단을 받을 의사 $D_1, ..., D_n$를 선택한다. 각 의사의 신원정보를 사용하여 각 의사와의 비대화식 공유키 $K_{P-D_1}, \cdots, K_{P-D_n}$을 생성한다. 건강정보 PHI를 생성한 뒤 각 의사와 공유하는 키를 사용하여 선택한 의사들를 위한 암호문을 Equation (2)와 같이 생성한다.

$$\begin{aligned} C_1 &= Enc_{K_{P-D_1}}(PHI) \\ &\vdots \\ C_n &= Enc_{K_{P-D_n}}(PHI) \end{aligned} \tag{2}$$

환자는 선택한 의사들을 위해서 동일한 PHI에 대해 각기 다른 의사들과의 세션키를 사용한 암호화 과정을 수행하여 선택한 의사들을 위한 n개의 암호문을 생성한다. 시스템에서 환자는 스마트폰을 통해 연산을 수행한다고 가정했을 때 환자가 가지는 연산의 부담이 선택한 의사의 수에 비례하여 증가하게 된다.

Table 1. Notations

Notation	Description
G_1, G_2	Multiplicative groups of the same prime order p
g	Generator of G_1
$\hat{e}: G_1 \times G_1 \rightarrow G_2$	Admissible bilinear map
$H_1: \{0,1\}^l \rightarrow G_1$	Cryptographic hash function
$H_2: \{0,1\}^* \times G \rightarrow Z_p$	Cryptographic hash function
$H_3: \{0,1\}^* \rightarrow Z_p^*$	Keyed hash function
sk_{id}	Private key of id for re-encryption
Sgk_{id}	Private key of id for signature
$rk_{id_1 \rightarrow id_2}$	Re-encryption key to re-encrypt a ciphertext under id_1 to id_2
$Sig_{Sgk_{id}}()$	Identity-based signature under the id's private key
ts	Time stamp

제안하는 프록시 재암호화 기법을 사용하는 시나리오는 다음과 같다. 환자는 진단을 받고자하는 의사 $D_1, ..., D_n$을 선택한 후, 각 의사를 위한 재암호화키 $rk_{P \rightarrow D_1}, ..., rk_{P \rightarrow D_n}$를 계산하여 모니터링 서버에 전송, 서버는 이를 자신의 데이터베이스에 저장한다. 건강정보의 전송 시 환자는 자신의 비밀키로 암호화한 암호문을 생성한 뒤 모니터링 서버에 전송한다. 서버는 이를 해당하는 의사를 위한 재암호화키를 사용하여 재암호화한 뒤 재암호문을 의사에게 전달하고 의사는 재암호문을 자신의 비밀키로 복호화하여 건강정보를 획득한다.

제안 시나리오에서 환자는 자신의 비밀키를 사용하여 생성한 암호문만을 모니터링 서버에 전송하고 모니터링 서버는 저장된 재암호화키를 사용하여 재암호화 연산을 수행, 재암호문을 생성하여 해당하는 의사에게 전달한다. 본 논문에서는 모니터링서버를 충분한 연산 능력을 가졌다고 가정하여 환자의 과도한 연산량을 서버에서 부담하도록 하여 제한적인 자원을 가지는 환자의 단말기에서도 충분히 동작하도록 하였다.

3. 제안 프로토콜

3.1 시스템 모델

제안 기법의 시스템 참여 개체의 역할은 다음과 같다. 본 논문에서는 [2]에서 제안된 시스템 모델을 기반으로 하며 또한 참여자의 익명성 보장을 위한 익명 발급과 참여자의 키를 발급하는 비밀키 생성자(Private Key Generator, PKG)의 역할을 하는 신뢰기관(Trusted Authority, TA)을 가정한다. Fig. 1은 시스템의 구성을 간략하게 표현한 것이고 Table 1은 제안 프로토콜에서 사용하는 표기법이다.

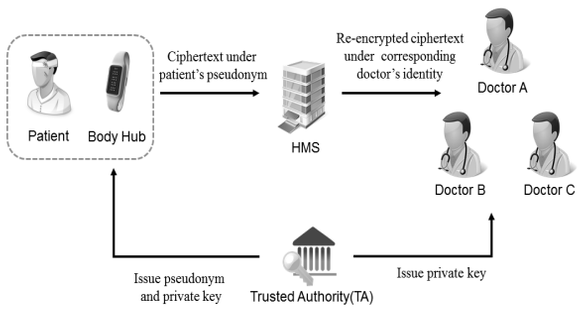

Fig. 1. System Model of the Proposed Scheme

- 환자(Patient)

생성한 건강정보(Personal Health Information, PHI)를 의사에게 전송하여 의료서비스를 제공받는다. 등록과정에서 진단을 받기를 원하는 의사를 선택한 뒤, 선택한 의사들을 위한 재암호화키를 생성한다.

- 의사(Doctor)

환자가 전송한 건강정보를 이용하여 환자에게 의료서비스를 제공한다.

- HMS(Healthcare Monitoring Server)

환자가 전송한 건강정보를 환자가 선택한 의사에게 전달하는 중개인의 역할과 환자가 선택한 의사를 위한 재암호화키(Re-encryption Key)를 데이터베이스에 저장하여 환자가 건강정보를 환자의 비밀키로 암호화하여 전송하면 환자가 선택한 의사에 해당하는 재암호화키를 사용하여 재암호화를 수행한다.

- BH(Body Hub)

의료용 센서 노드들이 측정한 환자의 건강정보를 통합하여 의사에게 전송한 메시지를 생성한다. 제안 기법에서는 개인의 스마트폰을 가정하며 센서와 BH 사이의 전송과정에서의 보안은 블루투스(Bluetooth) 등을 사용하여 도청과 같은 원격지에서의 공격에 안전하다고 가정한다.

- TA(Trusted Authority)

신뢰할 수 있는 기관을 가정하며 시스템에서 사용할 공개 파라미터의 생성과 배포 및 시스템의 참여자들을 위한 신원기반의 비밀키 발급, 그리고 환자의 익명성의 보장을 위해 환자에게 시스템에서 사용할 익명을 발급한다.

이상의 시스템 구성에 대해 본 논문에서는 다음과 같은 두 종류의 공격자를 가정한다.

- 악의적인 사용자(Malicious Users)

환자와 의사간의 PHI의 전송과정에서 환자와 환자가 선택한 의사를 제외한 제3자를 가정하며 정보에 접근할 권한이 없는 사용자가 정보에 접근하고자할 때 이를 악의적인 사용자로 정의한다.

• 신뢰할 수 없는 서비스 제공자
시스템에서 서비스 제공자인 HMS는 환자의 PHI를 환자가 선택한 의사에게 전달하는 역할을 수행하는 중개인의 역할을 수행한다. 제안하는 시스템에서 HMS는 프로토콜을 정상적으로 수행하지만 전달과정에서 환자의 PHI를 열람할 가능성이 있는 honest-but-curious한 개체를 가정한다.

위에서 가정한 공격자에 대해 본 논문에서 고려하는 보안 요구사항은 다음과 같다.

• 환자의 익명성
시스템에서 의사는 환자의 PHI에 대한 진단을 통해 환자의 건강관리를 수행한다. 많은 진단 상황에서 의사는 환자의 실제 신원정보와 관련한 정보(병력 등)를 반드시 필요로 하지 않는다. 때문에 환자는 시스템에서 익명을 사용하여 실제 신원정보와 익명의 관계를 신뢰할 수 없는 다른 개체에 노출되는 것을 방지할 수 있어야한다.

• PHI의 기밀성
시스템에서 전송되는 환자의 PHI는 환자와 환자가 선택한 의사를 제외한 누구도 접근할 수 없어야하고 외부의 제3자에 의한 도청에도 안전해야한다. 또한 암호문에 접근할 권한이 없는 대상에게 접근 권한을 비정상적으로 위임할 수 없어야 한다.

3.2 초기화

TA는 시스템에서 사용할 공개 파라미터를 다음과 같이 생성 및 배포한다.

1) 위수로 소수 p를 가지는 곱셈 군 G_1, G_2와 허용 가능한 겹선형 사상 $\hat{e} = G_1 \times G_1 \rightarrow G_2$를 정의한다.

2) $\alpha \in Z_p^*$를 선택한 뒤 $g_1 = g^{\alpha} \in G_1$를 계산하고 $g_2, \eta \in G_1$를 랜덤하게 선택한다.

3) 서명에 사용할 파라미터로 $\beta \in Z_p^*$를 선택한 뒤 $g_3 = g^{\beta}$ 를 계산한다.

4) 암호학적 해시함수인 $H_1 : \{0,1\}^l \rightarrow G_1$, $H_2 : \{0,1\}^* \times G \rightarrow Z_p$,과 키-해시함수인 $H_3 : \{0,1\}^* \rightarrow Z_p^*$를 선택한다.

5) TA의 마스터키 $msk = g_2^{\alpha}$를 계산하고 시스템에서 사용할 공개 파라미터 $params$를 다음과 같이 생성하고 시스템의 참여자들에게 배포한다.

$$params = < G_1, G_2, p, \hat{e}, g, g_1, g_2, g_3, \eta, H_1, H_2, H_3 >$$

3.3 등록

시스템에 참여하는 모든 환자와 의사는 최초 1회 TA로부터 신원기반의 비밀키를 발급받는다. 서비스 제공자 HMS는 환자의 의사선택 과정을 위해 시스템에 존재하는 의사들의 목록을 제공한다.

1) TA는 환자가 시스템에서 사용할 익명 pid_i와 서명을 위한 서명용 비밀키 $Sgk_{pid_i} = H_1(pid_i)^{\beta}$를 발급한다.

2) 재암호화에 사용할 파라미터 $u_i = H_3(msk \| pid_i)$를 계산한 뒤 발급한 익명을 사용하여 환자의 비밀키 $sk_{pid_i} = (d_0, d_1) = (g_2^{\alpha} H_1(pid_i)^{u_i}, g^{u_i})$를 계산하여 안전한 채널을 사용하여 환자에게 전송한다.

3) 환자는 비밀키 sk_{pid_i}를 자신의 BH에 저장한다.

4) 진단받을 의사를 선택한 뒤 TA로부터 선택한 의사의 재암호화키의 생성에 필요한 시드값 $\widetilde{rk_{pid_i \rightarrow D_j}} = \left(\frac{H_1(pid_i)}{H_1(D_j)} \right)^{u_j}$을 받는다($u_j = H_3(msk \| D_j)$).

5) 환자는 랜덤한 $\delta_j \in Z_p^*$를 선택한 뒤 해당하는 의사를 위한 재암호화키 $rk_{pid_i \rightarrow D_j}$를 다음과 같이 계산한다.

$$rk_{pid_i \rightarrow D_j} = (rk_{1,D_j}, rk_{2,D_j}) = (\eta^{\delta_j} \left(\frac{H_1(pid_i)}{H_1(D_j)} \right)^{u_j}, g^{\delta_j}) \quad (3)$$

6) 환자는 선택한 의사의 목록과 해당하는 재암호화키를 HMS에 전송한다.

7) HMS는 재암호화키를 자신의 데이터베이스에 저장한다.

의사도 환자와 마찬가지로 등록과정에서 TA가 재암호화 파라미터 $u_j = H_3(msk \| D_j)$를 계산한 뒤 의사의 비밀키 $sk_{D_j} = (d_{0,D_j}, d_{1,D_j}) = (g_2^{\alpha} H_1(D_j)^{u_j}, g^{u_j})$를 생성하여 전달한다.

3.4 PHI 전송

환자는 생성한 PHI를 자신의 비밀키로 암호화하여 HMS에 전송한다.

1) $r \in Z_p^*$를 선택한 뒤 암호문 C 를 다음과 같이 생성한다.

$$C = (C_1, C_2, C_3, C_4) = (PHI \bullet \hat{e}(g_1, g_2)^r, g^r, H_1(pid_i)^r, \eta^r) \quad (4)$$

2) 환자는 자신의 서명용 비밀키 Sgk_{pid_i}를 사용한 신원기반의 서명[11] $\sigma = Sig_{Sgk_{pid_i}}(C, ts)$을 생성한다.

3) $m = < pid_i, \sigma, ts >$를 HMS에 전송한다.

3.5 재암호화

HMS는 데이터베이스에 저장된 환자가 선택한 의사의 재암호화키를 사용하여 의사를 위한 재암호문을 생성한다.

1) 환자의 신원정보 pid_i를 이용하여 신원기반의 서명 $\sigma = Sig_{Sgk_{pid_i}}(C, ts)$를 검증한다.

2) C'_{1,D_j}을 다음과 같이 계산한 후 의사 D_j를 위한 재암호문 $C_{D_j} = < C'_{1,D_j}, C_2, C_3 >$를 생성한다.

$$C'_{1,D_j} = C_1 \cdot \frac{\hat{e}(C_4, rk_{2,D_j})}{\hat{e}(C_2, rk_{1,D_j})} \quad (5)$$

3) 메시지 $m = < C'_{D_j}, pid_i, D_j, \sigma, ts >$을 생성하여 해당하는 의사에게 전송한다.

3.6 복호화

의사는 자신의 비밀키 sk_{D_j}로 재암호문을 복호화하여 환자의 PHI를 획득한다.

1) 환자의 신원정보 pid_i를 사용하여 신원기반의 서명 $\sigma = Sig_{Sgk_{pid_i}}(C, ts)$를 검증한다.

2) 환자의 PHI를 다음과 같이 자신의 비밀키 $sk_{D_j} = < d_{0,D_j}, d_{1,D_j} >$를 사용하여 복호화한 뒤 PHI를 획득한다.

$$PHI = C'_{1,D_j} \cdot \frac{\hat{e}(C_3, d_{1,D_j})}{\hat{e}(C_2, d_{0,D_j})} \quad (6)$$

4. 분 석

• 환자의 익명성

등록과정에서 환자는 TA로부터 시스템에서 실제 신원정보 대신 사용할 익명 pid_i를 발급받는다. TA는 신뢰기관이라 가정하였으므로 신원이 확인된 환자에 대해서만 유효한 익명의 발급을 수행한다. 즉, TA가 안전한 채널을 통해 익명을 발급하였고 환자가 익명과 실제 신원정보의 관계정보를 고의적으로 노출하지 않았다고 가정하면 시스템의 다른 참여자(HMS, 의사, 외부 공격자)는 익명을 통해 환자의 실제 신원정보를 추적할 수 없다.

하지만 몇몇 진단상황의 경우 수집된 데이터만으로는 정확한 진단이 어렵고 개인의 병력(Medical history)이나 가족력(Family history) 등에 관한 정보가 필요한 경우가 존재한다. 즉, 필요의 경우 의사는 환자의 익명과 실제 신원정보의 관계를 확인할 수 있는 조건부 프라이버시(Conditional privacy)를 만족하여야한다. 의사는 HMS를 통해 TA에 환자의 신원정보를 요청하게 되고 TA는 요청의 타당성을 검증한 후, 요청이 타당할 경우에만 의사에게 환자의 실제 신원정보를 제공하게 된다.

• PHI의 기밀성

시스템에서 재암호화를 수행하는 HMS는 환자가 생성한 의사 D_j를 위한 재암호화키 $rk_{pid_i \to D_j}$와 환자의 비밀키로 암호화되어 전송된 암호문 C에 대한 접근이 가능하다. HMS는 앞서 가정한 것과 같이 honest-but-curious한 개체로서 프로토콜 수행 중 환자의 PHI를 열람할 가능성이 있다. HMS의 PHI의 열람을 방지하기 위해서는 재암호화 과정 수행 중 HMS가 PHI의 평문을 획득하거나 전송받은 암호문과 재암호화 과정을 거친 재암호문의 복호화를 위한 환자와 의사의 비밀키를 획득하지 못하도록 하여야한다. 또한 HMS와 특정 의사(재암호화의 대상인)가 공모(Collude)하였을 경우 HMS가 가진 재암호화키 $rk_{pid_i \to D_j}$와 공모한 의사의 비밀키 sk_{D_j}를 사용하여 환자의 비밀키 sk_{pid_i}를 알아내는 공모 공격(Collusion attack)과 환자와 환자가 선택한 의사 D_j의 재암호화키 $rk_{pid_i \to D_j}$와 의사 D_j의 비밀키 그리고 환자가 선택하지 않은 의사 D_k의 비밀키를 사용하여 의사 D_k를 위한 재암호화키 $rk_{pid_i \to D_k}$를 생성하는 위임-양도 공격(Transfer of delegation attack)에 대한 저항성(resistance)을 보장해야 한다.

제안 프로토콜에서 HMS는 위임-양도 공격을 위해서 재암호화키 $rk_{pid_i \to D_j} = (\eta^{\delta_j} \left(\frac{H_1(pid_i)}{H_1(D_j)} \right)^{u_j}, g^{\delta_j})$와 의사 D_j의 비밀키 sk_{D_j}가 필요하다. HMS가 환자가 선택하지 않은 의사 D_k를 위한 재암호화키 $rk_{pid_i \to D_k}$를 생성하기 위해서는 신뢰기관 TA가 생성한 재암호화 시드 값 $\widetilde{rk_{pid_i \to D_k}} = \left(\frac{H_1(pid_i)}{H_1(D_j)} \right)^{u_k}$가 필요하다. $H_1(pid_i), H_1(D_j), H_1(pid_i)$를 각각 g^x, g^y, g^z라고 하였을 경우 $\widetilde{rk_{pid_i \to D_k}}$를 계산하는 것은 $g, g^x, g^y, g^z, g^{(x-y)u_{D_j}}, g^{u_{D_j}}$과 $g^{u_{D_k}} \in G_1$가 주어졌을 때 $g^{(x-y)u_{D_k}} \in G_1$를 구하는 것으로 이는 CDH(Computational Diffie-Hellman) 문제로서 결국 위임-양도 공격은 실제적으로 불가능하다. 즉, 제안 프로토콜은 HMS와 의사가 공모한 경우 발생할 수 있는 위임-양도 공격에 대해 안전하다. 또한 HMS와 의사가 공모하여 해당하는 재암호화키로부터 환자의 비밀키를 계산하는 공모공격에 대해서 환자의 비밀키를 얻기 위해서는 $u_i = H_3(msk \| pid_i)$의 계산이 필요하지만 계산에는 TA의 마스터키 msk가 필요하므로 TA가 신뢰기관이라는 가정에 의해 공모공격에 대해서도 제안프로토콜은 안전하다.

5. 결 론

본 논문에서는 기존의 원격건강정보 모니터링 시스템에서 제안된 프로토콜들이 한명의 의사만 선택하여 진단을 받는 것에 비해 의사의 오진을 고려하여 환자가 다수의 의사를 선택하여 진단을 받는 모델을 설계, 이를 위해 프록시 재암호화 기법을 사용하여 환자는 한 번의 암호문 생성만으로 안전하게 원하는 의사들에게 자신의 건강정보를 전달하는 프로토콜을 제안하였다. 또한 HMS를 신뢰할 수 없는 서비스 제공자로서 honest-but-curious한 개체로 가정하였을 때 HMS와 피위임자인 의사가 공모하였을 경우 생기는 문제 등에 대해서도 안전함을 보였다. 제안 방안은 향후 고령화

사회의 도래에 따른 노년층을 위한 헬스케어 산업의 발전에 도움이 될 것으로 기대한다.

References

[1] Raytheon, Websense® Security Labs, “2015 Industry Drill-Down Report Healthcare,” 2015.

[2] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, “SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems,” *IEEE Journal on Selected Areas in Communications*, Vol.27, No.4, pp.365-378, 2009.

[3] H. Yang, H. Kim, and K. Mtonga, “An Efficient Privacy-Preserving Authentication Scheme with Adaptive Key Evolution in Remote Health Monitoring System,” *Peer-to-Peer Networking and Applications*, Vol.8, No.6, pp. 1059-1069, Springer, 2014.

[4] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, “A platform for secure monitoring and sharing of generic health data in the Cloud,” *Future Generation Computer Systems*, Vol.35, pp.102-113, 2014.

[5] A. K. Das and A. Goswami, “A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care,” *Journal of medical systems* Vol.37, No.3, pp.9948, 2013.

[6] Y. F. Chang, S. H. Yu, and D. R. Shiao, “An uniqueness-andanonymity-preserving remote user authentication scheme for connected health care,” *Journal of Medical Systems*, Vol.37, pp.9902, 2013.

[7] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Advances in Cryptology—CRYPTO 2001, LNCS 2139, pp.213-229, Springer, 2001.

[8] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” *ACM Transactions on Information and System Security (TISSEC)*, Vol.9, No.1, pp.1-30, 2006.

[9] M. Green and G. Ateniese, “Identity-based proxy re-encryption,” *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, pp.286-306, 2007.

[10] L. Wang, L. Wang, L. M. Mambo, and E. Okamoto, “New identity-based proxy re-encryption schemes to prevent collusion attacks,” *International Conference on Pairing-Based Cryptography,* Springer Berlin Heidelberg, pp.327-346, 2010.

[11] C. J. Cha and J. H. Cheon, “An identity-based signature from gap Diffie-Hellman groups,” *International Workshop on Public Key Cryptography*. Springer Berlin Heidelberg, pp.18-30, 2003.

노 시 완

e-mail : nosiwan@pukyong.ac.kr

2016년 부경대학교 IT융합응용공학과 (학사)

2016년～현 재 부경대학교 정보보호학협동과정 석사과정

관심분야 : 정보보호, 차량통신보안, 헬스케어 보안

박 영 호

e-mail : pyhoya@pknu.ac.kr

2000년 부경대학교 전자계산학과(학사)

2002년 부경대학교 전자계산학과(석사)

2006년 부경대학교 정보보호학협동과정 (박사)

2014년～현 재 부경대학교 전자정보통신연구소 전임연구원

관심분야 : 정보보호, 암호기술응용, 통신보안, 인증, 키 관리

이 경 현

e-mail : khrhee@pknu.ac.kr

1982년 경북대학교 수학교육과(학사)

1985년 한국과학기술원 응용수학과(석사)

1992년 한국과학기술원 수학과(박사)

1985년～1993년 한국전자통신연구원 연구원, 선임연구원

1993년～현 재 부경대학교 IT융합응용공학과 교수

관심분야 : 정보보호, 암호이론, 암호 프로토콜, 통신보안