원격건강정보 모니터링 시스템 상에서 신원기반 프록시 재암호화를 이용한 개인 건강정보 전송

노시완*, 박영호**,이경현**
*부경대학교 정보보호학협동과정
**부경대학교 IT융합응용공학과
e-mail : nosiwan@pukyong.ac.kr, pyhoya@pknu.ac.kr, khrhee.pknu.ac.kr

Personal Health Information Transmission using Identity-Based Proxy Re-Encryption in Remote Health Monitoring System

Si-Wan Noh*, Youngho Park**, Kyung-Hyune Rhee**
*Interdisciplinary Program of Information Security, Graduate School, Pukyong National University
**Department of IT Convergence and Application Engineering, Pukyong National University

요 약

환자가 가정에서 네트워크를 통해 자신의 건강정보를 원격지에 위치한 의사에게 전송하여 이에 대한 진단을 받는 원격건강정보 모니터링 시스템에서 환자의 개인건강정보의 보호는 매우 중요한 과제이다. 본 논문에서는 신원기반 프록시 재암호화 기법을 사용하여 환자가 다수의 의사를 선택하여 각 의사들에게 개인건강정보를 전송하여 진단을 받는 환경을 가정하여 환자가 가지는 연산부담을 줄이기 위해 환자의 비밀키로 생성한 암호문을 프록시가 재암호화하여 의사가 가진 비밀키로 복호화 할 수 있도록 하는 기법을 제안한다.

1. 서론

의료 기술의 발전으로 인간의 평균 기대 수명이 점점 증가함에 따라 고령 인구가 세계적으로 증가하는 추세이다. 이에 따라 고령 인구를 대상으로 하는 다양한 건강관련 서비스들이 주목받고 있다. 특히 원격 건강정보 모니터링 시스템은 거동이 불편한 고령 인구뿐 아니라 병원을 방문할 시간적 여유가 없는 젊은 층을 비롯한 전 연령대를 대상으로 가정에서 다양한 센서를 통해 수집한 개인건강정보(Personal Health Information, PHI)를 취합하여 원격지에 위치한 의사에게 전송하여 진단을 받는 시스템으로 병원을 방문하지 않아도 진단을 받을 수 있고 시간적인 부담도 적기에 크게 각광받고 있다.

하지만 이는 개인의 민감한 정보를 다루고 있는 만큼 개인건강정보가 외부에 노출되는 문제를 고려하지 않을 수 없다. 이에 대한 연구로 원격지에 위치한 환자를 스마트카드와 패스워드를 사용하여 인증하는 방법과 신원기반 암호 기법(Identity-Based Encryption)을 사용하여 환자와 의사 사이에 비대화식(Non-Interactive)으로 생성한 키를 PHI의 암호화에 사용하는 방법이 제안되었다. 하지만 제안 기법에서는 환자는 자신의 PHI를 전송할 의사를 단 한 명 선택하여 선택한 의사와의 사이에 비밀 세션키를 생성하는데. 의사의 오진을 고려한다면 환자의 입장에서는 다수의 의사를 선택하여 각 의사들의 종합적인 진단결과를 받고 판단하는 것이 더 효율적이고 신뢰할 수 있다. 하지만 제안 기법에서 환자가 다수의 의사를 선택하기 위해서는 선택한 모든 의사와의 사이에 비밀 세션키를 생성하고 관리하여야한다.

Yang은 [6]에서 환자와 의사 사이에 신원기반의 비밀키를 생성하여 PHI를 암호화하여 전송하는 기법을 제안하였다. 하지만 여기서 환자는 PHI를 전송할 의사를 단 1명 선택할 수 있었다. 제안기법에서 Yang은 환자가 의사와 비대화식으로 공유하는 키 K_{P-D}를 통해 PHI를 암호화하고 다시 HMS와 사이에 비대화식으로 공유하는 키 K_{P-H}를 사용하여 다시 암호화하는 형태를 제안하였다. 하지만 이 기법에서 다수의 의사에게 진단을 받기위해서는 전송하고자하는 의사 n명에 대해 각각의 비대화식 공유 비밀키를 이용한 암호화를 수행 후 HMS와 공유 비밀키를 이용해 다시 암호화를 수행해야한다. 해당 기법은 선택한 의

이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF- 2014R1A2A1A11052981)

사가 증가할수록 환자의 연산부담이 증가하는 문제점이 있었다. 또한 제안 기법에서 HMS는 PKG로서 시스템 파라미터를 생성하고 시스템의 사용자들에게 키를 생성하여 분배하는 역할을 한다. HMS는 환자와 의사에게 키를 분배하였기에 둘 사이에 비대화식으로 공유하는 비밀키를 계산할 수 있다. 즉, 중개자 역할을 하는 HMS가 PHI에 대한 복호화 능력을 가지는 문제점이 있다. 이는 환자에게 익명을 부여하여 HMS가 환자의 PHI를 식별하지 못하게 하는 것으로 해결이 가능하다.

본 논문에서는 신원기반 프록시 재암호화 기법(Identity-Based Proxy Re-Encryption, IB-PRE)를 사용하여 원격 건강정보 모니터링 시스템 상에서 환자가 자신의 신원기반의 공개키로 암호화한 PHI를 프록시를 통해 선택한 의사의 개인키로 복호화 할 수 있도록 재암호화하는 기법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서 제안기법의 시스템 모델 및 보안 요구사항과 프로토콜의 소개를 하고 3장에서 보안요구사항의 분석을 한다. 그리고 4장에서 결론을 짓는다.

2. 제안기법

본 장에서는 제안 기법의 보인요구사항과 제안기법의 구성을 기술한다. <표 1>은 제안기법의 기술에 사용되는 표기법이며 <그림 1>은 제안기법의 개괄적인 단계이다.

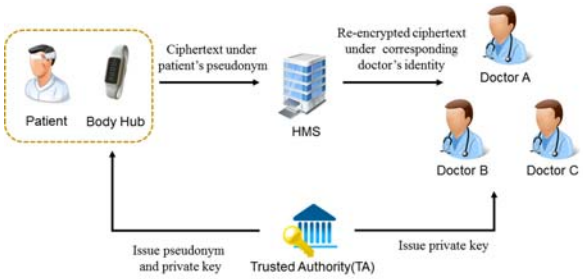
Notation	Meaning
G, G_T	Groups of the same prime order q
g	Generator of G
$e : G \times G \rightarrow G_T$	Bilinear map
PT_i, PID_i	Identify and pseudonym of patient i
sk_{id}, Q_{id}	Private key and public key of id
$rk_{id_1 \rightarrow id_2}$	Re-encryption key for re-encrypt ciphertext from id_1 to id_2
c_{id}	Ciphertext under identity id
PHI_i	Personal health information of patient i
$n()$	Polynomial function of the security parameter k
Sig_{id}	Identity-based signature under the id's private key
ts	Time stamp

<표 1> Notations

2.1 시스템 모델

제안기법에서 참여 개체의 각 역할은 다음과 같다.

- **HMS(Health Monitoring Server)** : 환자의 키로 암호화된 암호문을 환자가 선택한 의사의 키로 복호화 할 수 있도록 재암호화하는 프록시(Proxy)의 역할을 수행한다.
- **BH(Body Hub)** : 다양한 센서로부터 전달받은 정보를 종합하여 의사에게 전달한다. 개인의 스마트폰이나 가정의 데스크톱 컴퓨터를 가정한다.
- **환자(Patient)** : BH를 통해 수집한 PHI를 자신의 비밀키로 암호화하여 HMS에게 진단을 받길 원하는 의사를 위한 재암호화키와 함께 전달한다.
- **의사(Doctor)** : HMS로부터 환자의 PHI의 재암호문을 전달받아 자신의 키로 복호화하여 환자의 PHI를 얻어 진단을 한다.
- **TA(Trusted Authority)** : 신뢰기관으로 가정하며 환자의 익명발급과 키 발급을 수행한다.



<그림 1> System model of the proposed scheme

Green이 [2]에서 제안한 IB-PRE 기법을 사용함으로써 제안기법은 기본적으로 다음과 같은 보안요구사항을 만족한다.

- **재암호화 과정에서 평문 노출 방지** : 재암호화를 수행하는 프록시는 수행 과정에서 평문을 획득할 수 없다.
- **기존 재암호화키에서 새로운 재암호화키 생성 불가** : 재암호화키가 노출되더라도 여기서 새로운 재암호화키를 만들기 위한 유효한 정보를 획득할 수 없다.

이를 통해서 시스템에서 프록시 역할을 하는 HMS가 재암호화 과정에서 환자의 PHI의 평문을 획득할 수 없고 또한 재암호화키가 공격자에 노출되더라도 공격자는 키에서 공격을 위한 새로운 재암호화키를 생성하거나 정보를 얻을 수 없다는 사실을 보장할 수 있다. 우리의 제안 기법에서는 이를 제외한 다음과 같은 보안 요구사항을 고려한다.

- **HMS와 의사에 대한 환자의 익명성 보장** : 환자는 시스템에서 HMS와 의사에게 익명으로 서비스를 제공받고 제3자에게 환자의 익명과 실제 신원정보의 관계가 노출되어서는 안 된다.

- **사용자 인증** : HMS와 의사는 환자의 PHI를 받았을 때 시스템에 등록된 환자에게서 전송된 것인지 환자로 위장한 공격자에게서 온 것인지 확인할 수 있어야한다.

- **메시지 무결성** : HMS와 의사는 암호문의 재암호화나 복호화 전에 암호문의 무결성을 확인할 수 있어야한다.

2.2 제안기법

▪ **초기화**

1) TA는 페어링 연산 $e : G \times G \rightarrow G_T$를 정의한다.
2) 자신의 마스터키로 사용할 $s \in Z_q^*$를 랜덤하게 선택, 파라미터 $params = < H_1, H_2, H_3, H_4, H_5, g, g^s, e >$를 생성한 뒤 시스템의 참여자들에게 배포한다. 사용된 해시 함수는 다음과 같이 정의한다.

$$H_1 : \{0,1\}^* \rightarrow G, H_2 : \{0,1\}^* \rightarrow G$$
$$H_3 : \{0,1\}^* \rightarrow G, H_4 : G_T \times \{0,1\}^n \rightarrow Z_q^*$$
$$H_5 : G_T \rightarrow \{0,1\}^n$$

▪ **등록**

시스템에 참여하는 모든 환자와 의사는 오프라인으로 TA에게서 신원기반의 비밀키를 발급받는다.

1) TA는 환자 PT_i에게 익명 PID_i와 익명을 사용하여 생성한 비밀키 $sk_{PID_i} = H_1(PID_i)^s$를 전달한다. 의사의 경우는 의사의 신원 D_j를 이용한 $sk_{D_j} = H_1(D_j)^s$를 전달한다.
2) 환자는 전달받은 비밀키 sk_{PID_i}를 자신의 BH에 저장한다.
3) 환자는 랜덤한 $N \in \{0,1\}^{n(k)}$를 선택한 뒤 $K = e(sk_{PID_i}, H_1(D_j))$를 계산한다.
4) 환자는 다음과 같이 선택한 의사 D_j를 위한 재암호화키를 계산한다.
$$rk_{PID_i \rightarrow D_j} = < N, H_2(K \| PID_i \| D_j \| N) \cdot sk_{PID_i} >$$
5) 환자는 선택 의사 목록 DL_{PID_i}를 HMS에 전송한다. 목록의 구성은 진단을 받길 원하는 의사와 의사를 위한 재암호화키로 구성된다.
$$DL_{PID_i} = < (rk_{PID_i \rightarrow D_1}, D_1), \ldots, (rk_{PID_i \rightarrow D_n}, D_n) >$$
6) HMS는 $< PID_i, DL_{PID_i} >$를 데이터베이스에 저장한다.

▪ **PHI 전송**

환자는 전송하고자하는 $PHI_i \in \{0,1\}^n$을 자신의 익명 PID_i를 사용하여 다음과 같이 암호화를 수행한다.

1) 랜덤한 $\sigma \in G_T$를 선택한 뒤 $r = H_4(\sigma, PHI_i, ts)$를 계산한다.
2) $< A, B, C > = < g^r, \sigma \cdot e(g^s, H_1(PID_i)^r), PHI_i \oplus H_5(\sigma) >$를 계산한다.
3) $S = H_3(PID_i \| < A, B, C >)^r$를 계산한 뒤 암호문 $c_{PID_i} = < S, A, B, C >$를 생성한다.
4) 환자는 자신의 비밀키 sk_{PID_i}를 사용한 신원기반의 서명 $Sig_{PID_i} = IBS_{sk_{PID_i}}(C, ts)$을 생성한다.
5) $m = < PID_i, c_{PID_i}, Sig_{PID_i}, ts >$를 HMS에 전송한다.

▪ **재암호화**

HMS는 Sig_{PID_i}를 $Q_{PID_i} = H_1(PID_i)$를 사용하여 검증한다. 검증 후 환자로부터 받은 c_{PID_i}를 데이터베이스에 저장하고 있던 환자의 재암호화키를 사용하여 환자가 선택한 의사들이 복호화 할 수 있는 재암호문을 생성한다.

1) $c_{PID_i} = < S, A, B, C >, rk_{PID_i \rightarrow D_j} = < N, R >$로 분해한다.
2) $h = H_3(PID_i \| < A, B, C >)$를 계산한다.
3) $e(g, S) = e(h, A)$를 확인한 후 일치하면 과정을 계속 진행하고, 불일치할 경우 메시지를 폐기한다.
4) 랜덤한 $t \in Z_q^*$를 선택한 뒤 $B' = B / \frac{e(A, R \cdot h^t)}{e(g^t, S)}$를 계산한다.
5) 의사 D_j를 위한 재암호문 $c_{D_j} = < A, B', C, PID_i, N >$를 생성하고 전송할 메시지 $m_{D_j} = < c_{D_j}, PID_i, D_j, ts, Sig_{PID_i} >$를 구성한 후 이를 해당하는 의사들에게 전송한다.

▪ **복호화 및 PHI 획득**

HMS와 마찬가지로 Sig_{PID_i}를 Q_{PID_i}를 사용하여 검증한다. 이후 자신의 비밀키 sk_{D_j}를 사용하여 복호화한다.

1) $c_{D_j} = < A, B', C, PID_i, N >$로 분해한다.
2) $K = e(H_1(PID_i), sk_{D_j})$를 계산한다.
3) $\sigma' = B' \cdot e(A, H_2(K \| PID_i \| D_j \| N))$를 계산한다.
4) $PHI_i' = C \oplus H_5(\sigma')$와 $r' = H_4(\sigma', PHI_i', ts)$를 계산한다.
5) $A = g^{r'}$를 확인하여 유효할 경우 PHI_i'를 얻는다.

3. 분석

이 장에서는 앞서 기술한 보안요구사항을 제안기법에서 어떻게 만족하는지를 설명한다.

- **환자의 익명성** : 환자 PT_i의 익명성은 TA로부터 발급받는 익명 PID_i를 통해 보장받을 수 있다. 신뢰기관 TA는 사용자 인증을 통해 정당한 사용자에게만 익명을 발급하고 안전한 채널을 통해 익명을 전달한다고 가정할 때 익명을 발급받는 환자 PT_i를 제외한 다른 개체(HMS, 의사, 다른 환자)는 환자의 익명에서 실제 신원정보를 추적할 수 없다.

- **사용자 인증** : 환자의 PHI 전송 메시지 생성과정에서 신원기반의 서명[7]을 생성한다. 서명의 생성에는 TA로부터 받은 sk_{PID_i}를 사용하는데 TA가 인증된 사용자에게만 익명을 발급하고 비밀키의 전달에서 외부에 키가 노출되지 않았다는 가정 하에 서명의 생성은 TA로부터 익명과 비밀키를 발급받은 인증 받은 사용자만이 서명을 생성할 수 있다. 메시지를 전달받는 HMS나 의사들은 환자의 공개키 $Q_{PID_i} = H_1(PID_i)$를 사용하여 서명을 검증할 수 있다. 또한 서명에는 암호문 생성의 시간 ts를 포함하여 제 3자에 의한 서명의 재사용을 방지한다. 제3자가 서명을 획득하여 다른 메시지의 전송에 사용하려 하더라도 서명에 포함된 시간과 암호문 C가 일치하지 않으므로 서명 검증과정에서 확인이 가능하다.

- **메시지 무결성** : 환자가 생성한 암호문의 구성은 다음과 같다.

$$
\begin{aligned}
S &= H_3(PID_i \| < A, B, C >)^r \\
A &= g^r \\
B &= \sigma \cdot e(g^s, H_1(\Pi D_i)^r) \\
C &= PHI_i \oplus H_5(\sigma)
\end{aligned}
$$

환자는 랜덤한 $\sigma \in G_T$를 선택하여 $r = H_4(\sigma, PHI_i)$을 계산하여 암호문의 생성에 사용한다. 즉 σ과 이를 사용하여 계산한 r은 환자만이 알고 있는 암호문 생성시의 비밀 값이다. HMS와 의사는 암호문을 수신했을 때 이 값을 확인하는 것으로 메시지의 무결성을 확인한다.

HMS는 아래의 계산식을 통해 비밀 값을 직접적으로 확인하지 않고도 값의 검증이 가능하다. 만약 암호문의 전송과정에서 변경이 있었다면 $e(g, S) \neq e(h, A)$이므로 이 경우 HMS는 해당 재암호화 과정을 실행하지 않는다.

$$
\begin{aligned}
e(g, S) &= e(g, H_3(PID_i \| < A, B, C >)^r) \\
&= e(g, H_3(PID_i \| < A, B, C >))^r \\
&= e(g^r, H_3(PID_i \| < A, B, C >)) \\
&= e(g^r, h) \\
&= e(h, A)
\end{aligned}
$$

HMS로부터 재암호문을 전달받은 의사는 $K = e(H_1(PID_i), sk_{D_j})$와 $\sigma' = B \cdot e(A, H_2(K \| PID_i \| D_j \| N))$를 계산한 후 $PHI_i' = C \oplus H_5(\sigma')$를 계산한다. 이후 $r' = H_4(\sigma', PHI_i')$를 계산, $A = g^{r'}$의 일치여부를 확인하여 일치하면 환자의 PHI를 얻는다. 앞서 환자가 계산한 암호문에서 $A = g^r$이므로 $g^r \neq g^{r'}$라면 암호문에 어떠한 변경(재암호화 과정이나 전송 과정)이 생겨 환자가 암호화에 계산한 $r = H_4(\sigma, PHI_i)$과 의사가 전송받은 재암호문을 사용하여 계산한 $r' = H_4(\sigma', PHI_i')$이 일치하지 않으므로 의사는 메시지의 무결성을 확인할 수 있다.

4. 결론

본 논문에서는 원격건강정보 모니터링 시스템 상에서 효율적인 PHI의 전송과 진단을 위해 환자가 다수의 의사를 선택하는 환경에서 IB-PRE를 사용하여 환자의 PHI의 복호화 권한을 재암호화를 통해서 환자가 선택한 의사에게 전달하는 기법을 제안하였다. 제안 기법은 단방향의 특성을 가지므로 환자에서 의사로의 재암호화만 가능하지만 필요에 따라 의사에서 환자로의 재암호화를 가능하도록 하는 단방향의 프록시 재암호화 기법을 두 번 사용하는 것만으로 양방향의 프록시 재암호화 기법을 사용한 것과 같은 기능을 제공할 수 있다. 또한 HMS가 PHI의 내용을 확인할 수 없고 환자는 선택한 의사의 수에 상관없이 자신의 비밀키로 암호화를 한번만 수행하면 되므로 상대적으로 낮은 성능을 가지는 환자 측면에서 연산적인 부담이 보다 효율적이다.

참고문헌

[1] Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage." ACM Transactions on Information and System Security (TISSEC) 9.1 (2006): 1-30.

[2] Green, Matthew, and Giuseppe Ateniese. "Identity-based proxy re-encryption." Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2007.

[3] Dan Boneh, Matthew Franklin, Identity-Based Encryption from the Weil Pairing, Advances in Cryptology – CRYPTO 2001, LNCS 2139, pp.213-229, Springer, 2001.

[4] Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47 - 53. Springer, Heidelberg (1984)

[5] Blaze, Matt, Gerrit Bleumer, and Martin Strauss. "Divertible protocols and atomic proxy cryptography." International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 1998.

[6] H Yang, H Kim, 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.

[7] Zhang, Fangguo, Reihaneh Safavi-Naini, and Willy Susilo. "An efficient signature scheme from bilinear pairings and its applications." International Workshop on Public Key Cryptography. Springer Berlin Heidelberg, 2004.