http://dx.doi.org/10.3745/KIPSTC.2012.19C.1.063

속성기반 암호화를 이용한 원격 헬스케어 모니터링 시스템

송 유 진[†] · 도 정 민[††]

요 약

원격 헬스케어(e-Healthcare) 서비스에서 취급되는 의료정보는 개인의 프라이버시를 침해할 수 있으므로 암호화 등의 보안기술 도입이 필수적이다. 민감한 의료정보를 보호하기 위해서 접근 권한을 위임받은 사용자만 데이터에 접근 가능하며 또한, 위임된 접근 권한을 철회하는 기능이 필요하다. 이러한 요구사항에 근거하여 속성기반 암호화가 제안되었다.

본 논문에서는 안전한 원격 헬스케어 서비스를 위해서 의료데이터의 접근 권한에 대한 위임 및 철회기능을 수행할 수 있는 속성기반 암호화를 원격 헬스케어 모니터링 시스템에 적용한다. 그리고 속성기반 암호화를 이용하여 원격 헬스케어 모니터링 시스템을 구성한다. 마지막으로 시스템 이용에 장애가 될 수 있는 사용자간의 공모 공격에 대해서 분석한다.

키워드 : 원격 헬스케어, 속성기반 암호화, 위임, 철회, 접근권한 관리, 공모 공격

Remote Healthcare Monitoring System Using Attribute based Encryption

You-Jin, Song[†] · Jeong-Min, Do[††]

ABSTRACT

To ensure privacy of individual information in remote healthcare service, health data should be protected through a secure technology such as encryption scheme. Only user who delegated decryption right can access to sensitive health data and delegator needs capability for revocating access privilege. Recently, in ubiquitous environment, CP-ABTD(Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes) which extends CP-ABE(Ciphertext-Policy Attribute-Based Encryption) has been proposed for these requirements. In this paper, we construct remote healthcare monitoring system with delegation and revocation capability for attribute in CP-ABTD. Finally, we analyze collusion attack between users in our system.

Keywords : Remote Healthcare, Attribute Based Encryption, Delegation, Revocation, Access Privilege Management, Collusion Attack

1. 서 론

최근 정보기술(IT)의 발달과 더불어 유비쿼터스 컴퓨팅의 개념이 등장했다. IT와 의료산업을 융합하는 현재의 추세에 따라 유비쿼터스 컴퓨팅의 개념을 도입하여 원격의료기술을 활용한 건강관리 서비스 즉, 원격 헬스케어 서비스 모델이 제시되고 있다[1][2][3]. 원격 헬스케어 서비스는 의료정보화를 통한 의료서비스 질의 향상, 생산성과 작업의 효율화, 의료사고의 감소 등을 목표로 하고 있다[1][2][3][10]. 의료정보화의 의의는 '정보기술과 전자기술 응용기기 등을 이용하여 환자, 의료진을 포함한 모든 사람들에게 의료 및 진료서비스 등을 제공하는 것'이며 전자의무기록시스템(EMRS, Electronic Medical Record System), 처방정보전달시스템(OCS, Ordering Communication System), 의료영상저장통신시스템(PACS, Picture Archiving and Communication System), 원격의료 서비스 등과 같은 의료 종합 시스템들로 구성된다[1].

원격 헬스케어 산업이 활성화되기 위해서 개인의 진료정보 보관 및 관리가 중요하다. 현재 의료기관에서 진료기록을 관리하는 방법에 문제점이 많다. 의료기관별로 정보가 분산되어 있고, 환자가 아닌 의료기관 중심으로 관리되고 있으며, 환자가 필요할 때 접근이 불가능하고 현행법상 정보에 대한 소유권이 의료기관에 있다. 또한, 표준화작업이 필요한 시점으로 의료기관 중심이 아닌 환자 중심의 표준화 작업이 시급하다. 따라서 언제, 어디서나 대인 진료기록에 접근할 수 있고 중복검사를 방지하며 환자의 평생건강기록(PHR, Personal Health Record)을 보호하고, 개인의 진료정

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2011-0027333).
† 정 회 원 : 동국대학교 정보경영학과 교수
†† 준 회 원 : 동국대학교 전자상거래협동과정 석사과정
논문접수 : 2011년 10월 26일
수 정 일 : 1차 2011년 12월 19일
심사완료 : 2011년 12월 26일

보를 의료기관이 공동으로 활용할 수 있도록 개선이 필요한 시점이다[11].

원격 헬스케어 서비스는 기존 유비쿼터스 컴퓨팅 서비스와는 다른 보안 요구사항들이 존재한다. 개인 의료정보가 여러 사용자 그룹에 의해 공유되어야 하며 정확한 진료를 위해서는 정보의 공유 및 2차 활용(Primary care, Secondary use)이 필수적이다. 이러한 정보의 공유 때문에 보안 취약사항이 노출되고 원격 헬스케어 서비스에 대한 보안 이슈가 제기되고 있다[4][5][8][10]. 현재 진료목적으로 제공하는 정보가 모든 사용자 그룹(의사뿐만아니라 간호사나 물리치료실 관계자, 약사, 행정직원 등 병원에 종사하는 모든 사람들)이 열람가능하며 정부기관을 비롯 보험회사, 제약회사, 해커 등 제 3자도 충분히 침입가능한 문제가 발생되고 있다[11].

서비스 대상자(환자)의 입장에서 자신의 의료정보가 정당한 사용자에 의해 의료 서비스 목적에 맞게 최소한의 공유가 이루어지고, 상황에 따라서 데이터에 대한 접근 권한을 제어할 수 있는 기능이 필요할 것이다. 즉, 환자의 동의에 따른 의료정보의 안전한 공유 및 활용을 요구하고 있으며 이를 만족시키기 위해서 암호방식의 도입이 필수적이다[7]. 이러한 서비스 대상자의 요구사항을 고려하여 서비스 대상자가 자신의 속성을 기반으로 암호화된 건강기록정보를 정당한 사용자가 열람 가능하도록 복호 권한을 위임 및 철회가 가능한 암호방식이 요구된다[9].

본 논문에서는 이러한 문제에 대한 기술적인 대책으로서 정당한 속성을 갖는 사용자만이 진료정보에 접근이 가능하도록 의료정보를 암호화하는 방법을 제안한다. 그리고 원격 헬스케어 모니터링 시스템[4]에서 사용자 속성을 위임, 철회 가능한 속성기반 암호방식을 검토하고 속성기반 암호화를 이용하여 원격 헬스케어 모니터링 서비스 시스템 구조를 제안한다. 또한, 사용자간의 공모 공격에 대한 안전성에 대해서 분석한다.

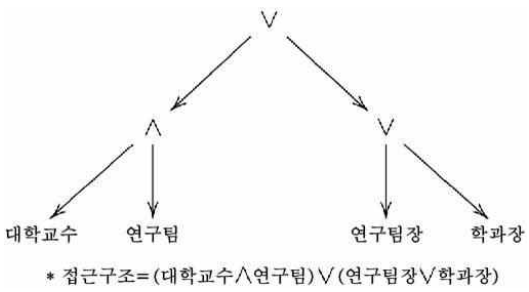
2. 관련 연구

2.1 사용자 속성의 위임 및 철회 가능한 속성기반 암호방식

1) 접근구조

속성기반 암호화 CP-ABPRE(Ciphertext Policy Attribute Based Proxy Re-Encryption)[12]에서 사용자 비밀키는 속성집합과 관련되며 암호문은 속성 접근구조와 관련이 있다[7]. 암호문 내의 특정 복호정책에 대해서 사용자의 비밀키 속성집합이 만족되면 암호문은 복호된다.

예를 들어, 의과대학에서 신종플루에 대한 연구를 수행하고 있다. 의과대학의 연구자가 그동안 연구해 왔던 데이터에 대한 접근을 원한다면 비밀키는 대학교수이고 연구팀 또는 연구팀장이나 학과장의 속성을 기반으로 만들어져야 하며 접근구조(대학교수∧연구팀)∨(연구팀장∨학과장)는 (그림 1)과 같이 만들어져야 한다. 비밀키가 이러한 접근구조를 만족하면 연구자는 데이터를 복호할 수 있다.



(그림 1) 접근구조

기존 CP-ABE 방식은 철회(Revocation)와 위임(Delegation)에 대한 문제를 고려하고 있지 않다. 사용자 속성의 위임 및 철회 가능한 속성기반 암호화(CP-ABTD, Ciphertext Policy Attribute Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes)[9]는 속성기반 암호화의 확장된 형태로서 유연한 속성 위임과 동시에 속성 철회 기능을 수행할 수 있다. 이러한 CP-ABTD는 3가지 특징을 가지고 있다. 첫째, 속성집합과 관련된 비밀키를 가지는 위임자는 피위임자에게 자신의 권한을 위임할 수 있다. 둘째, 위임자는 피위임자에게 자신의 권한을 위임할 수 있도록 결정할 수 있다. 셋째, 제안된 방식은 속성철회가 가능하다.

2) 알고리즘 상세

PRE는 프록시 서버가 평문에 대한 어떠한 정보의 습득없이 A의 암호문을 B가 복호 가능하도록 재암호화하는 방식이다[12]. 즉, A는 B에게 자신의 암호문에 대한 복호 권한을 위임하는 재암호화키(Re-encryption key)를 생성한 후, 프록시 서버에 송신한다. 그리고 프록시 서버는 재암호화키를 통해서 A의 암호문을 B의 비밀키로 복호 가능한 암호문으로 변환하여 B에게 전달한다. B는 자신의 비밀키로 암호문을 복호한다. PRE는 Key Generation, Encryption, Re-encryption, Decryption의 4가지 알고리즘으로 구성된다.

사용자 속성의 위임 및 철회 가능한 속성기반 암호화 CP-ABTD는 Setup, KeyGen, Encrypt, Delegate, m-Delegate, m-Decrypt, Decrypt로 총 7개의 알고리즘으로 구성되고 참가자는 위임자, 피위임자, 인증기관(TA, Trusted Authority), 프록시이다. 여기서, Setup과 KeyGen은 TA, Encrypt와 Delegate는 위임자, m-Delegate와 m-Decrypt는 프록시, Decrypt는 피위임자에 의해서 수행된다.

① Setup(k) : 보안파라메터 k를 입력받아서 생성자 g, 소수 위수 p인 G_0를 생성한다. bilinear map은 $\hat{e}: G_0 \times G_0 \rightarrow G_1$이고 시스템 속성 집합 $\Omega = (a_1, a_2, \ldots a_n)$ (n은 정수)이며 $a_j \in \Omega$는 임의의 요소 $t_j \in Z_p^*$를 선택한다. $y = \hat{e}(g,g)^{\alpha}$ ($\alpha \in_R Z_p^*$, $T_j = g^{t_j} (1 \le j \le n)$), 공개키 $pk = \left(\hat{e}, g, y, T_j (1 \le j \le n)\right)$, 마스터키 $mk = \left(\hat{e}, g, y, T_j (1 \le j \le n)\right)$가 생성된다.

② KeyGen(mk, w, I_u) : 속성 집합 w와 위임자의 식별자 I_u로 비밀키를 생성한다.

(a) 비밀키의 베이스 콤포넌트를 계산 : $d_0 = g^{\alpha - u_{id}}$ ($u_{id} \in {}_R Z_p^*$)를 계산.

(b) 비밀키의 속성 콤포넌트를 계산 : 속성 $a_j \in w$, $u_j \in {}_R Z_p$를 선택하고 $d_{j,1} = g^{u_j t_j^{-1}}$와 $d_{j,2} = g^{(u_{id} - u_j) t_j^{-1}}$를 계산. 첫 번째 비밀키 쉐어 $sk_{wI_w,1} = (\forall a_j \in w : d_{j,1})$를 프록시에게 전송하고, 두 번째 비밀키 쉐어 $sk_{wI_w,2} = (d_0, \forall a_j \in w : d_{j,2})$를 위임자에게 전송한다.

③ Encrypt(m, τ, pk)($m \in G_1$) : $s \in Z_p^*$를 임의로 선택하고 $c_0 = g^s, c_1 = m \cdot y^s = m \cdot \hat{e}(g,g)^{\alpha s}$를 계산한다. 최종 사용자 속성(leaf attribute) $a_{j,i} \in \tau$, $c_{j,i} = T_j^{s_i}$를 계산한다. 위임자의 암호문 $c_\tau = (\tau, c_0, c_1, \forall a_{j,i} \in \tau : c_{j,i})$를 만들어낸다.

④ Delegate($sk_{wI_w,2}, \hat{w}, I_j$) : $r' \in Z_p$를 임의로 선택하고 $a_j \in \hat{w}$로 $g^{t_j r'} = g^{r_j''}$을 설정한다. 속성 전환키 $sk_{w \to \hat{w}} = g^{r'}$을 설정하고 $a_j \in \hat{w}$로 $\widehat{d_{j,2}}$을 계산한다.

$$\widehat{d_{j,2}} = g^{(u_{id} - u_j) t_j^{-1} - r'} = g^{(u_{id} - u_j) t_j^{-1} - r_j'' t_j^{-1}}$$
$$= g^{(u_{id} - \hat{u_j}) t_j^{-1}} (\hat{u_j} = u_j + r_j'')$$

비밀키 쉐어 $sk_{\hat{w}I_j,2} = (d_0, \forall a_j \in \hat{w} : \widehat{d_{j,2}})$를 피위임자에게 전송하고 $\hat{w}$와 $sk_{w \to \hat{w}}$를 프록시에게 전송한다.

⑤ m-Delegate($sk_{wI_w,1}, \hat{w}, sk_{w \to \hat{w}}$) : 속성 위임 리스트(Attribute Delegation List)를 체크하고 속성 위임대상이라면 $a_j \in \hat{w}$로 $sk_{\hat{w}I_j,1}$을 계산한다. 속성 위임 리스트에 확인되지 않으면 계산은 진행되지 않는다.

$$\widehat{d_{j,1}} = g^{u_j t_j^{-1} + r'} = g^{\hat{u_j} t_j^{-1}}$$

비밀키 쉐어 $sk_{\hat{w}I_j,1} = (\forall a_j \in \hat{w} : \widehat{d_{j,1}})$를 피위임자에게 전송한다.

⑥ m-Decrypt($c_\tau, sk_{\hat{w}I_j,1}, I_j$) : 속성 철회 리스트(Attribute Revocation List)를 체크하고 속성 철회대상이 아니라면 $\hat{c_\tau}$를 계산한다. 철회대상이라면 계산이 진행되지 않는다. 모든 속성 $a_j \in w'$로 계산한다.

$$\hat{c_\tau} = \prod_{a_j \in w'} \hat{e}\left(T_j^{s_i}, g^{u_j t_j^{-1}}\right) = \hat{e}(g,g)^{\sum_{a_j \in w'} u_j s_i}$$

⑦ Decrypt($\hat{c_\tau}, sk_{\hat{w}I_j,2}$) :

(a) 모든 속성 $a_j \in w'$로 계산:

$$c_\tau'' = \prod_{a_j \in w'} \hat{e}\left(T_j^{s_i}, g^{(u_{id} - u_j) t_j^{-1}}\right)$$
$$= \prod_{a_j \in w'} \hat{e}\left(g^{t_j s_i}, g^{(u_{id} - u_j) t_j^{-1}}\right)$$
$$= \hat{e}(g,g)^{\sum_{a_j \in w'} (u_{id} - u_j) s_i}$$

(b) 계산:

$$\hat{e}(c_0, d_0) \cdot \hat{c_\tau} \cdot c_\tau''$$
$$= \hat{e}\left(g^s, g^{\alpha - u_{id}}\right) \cdot \hat{e}(g,g)^{\sum_{a_j \in w'} u_j s_i} \cdot \hat{e}(g,g)^{\sum_{a_j \in w'} (u_{id} - u_j) s}$$
$$= \hat{e}\left(g^s, g^{\alpha - u_{id}}\right) \cdot \hat{e}(g,g)^{u_{id} s} = \hat{e}\left(g^s, g^\alpha\right)$$

(c) m의 반환

$$m = \frac{c_1}{\hat{e}\left(g^s, g^\alpha\right)} = \frac{m \cdot \hat{e}(g,g)^{\alpha s}}{\hat{e}\left(g^s, g^\alpha\right)}$$

2.2 원격 헬스케어 모니터링 시스템

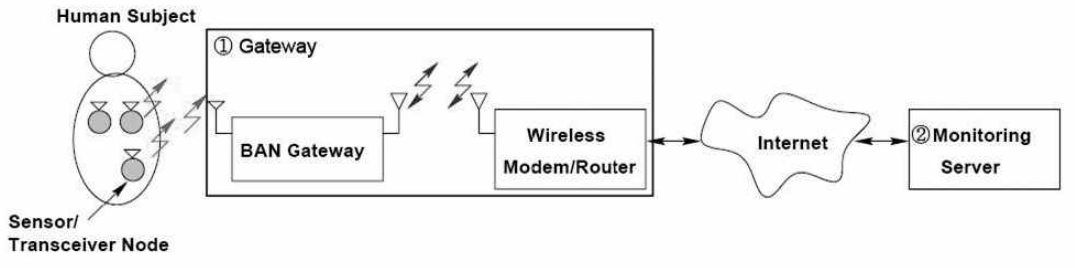
최근 RFID, 바이오센서, 무선 네트워크 분야의 기술적 성장은 원격 헬스케어 서비스의 발전을 촉진하고 있다. 아울러 삶의 질 향상과 의료 비용 감소의 잠재적 가능성을 위한 서비스 모델이 제시되고 있다[4][5]. 원격 헬스케어 모니터링은 무선 BAN(Body Area Network)에서 서비스 사용자가 자신의 건강과 관련된 데이터를 모니터링 서버에 전송하고 모니터링 서버는 이러한 데이터를 수집·분석하여 개인화된 의료 서비스를 제공하는 것이다. 원격 헬스케어 모니터링은 개인에게 민감할 수 있는 생체정보를 다루기 때문에 데이터 암호화가 필수적이다. 기본적으로 서비스 사용자(환자)의 데이터는 암호화되어야 하고 유연하고 안전한(flexible and secure) 의료 서비스를 받기 위해서 자신의 건강기록에 대한 접근권한을 위임하고 상황에 따라서 권한을 철회하는 기능이 필요하다. 이러한 기능을 위해 사용자의 속성을 위임, 철회 가능한 암호방식이 요구된다.

1) 시스템 구성

시스템의 구성요소는 다음과 같다.

① 게이트웨이 : 게이트웨이는 센서에서 전송된 데이터 수집, 처리, 전반적인 BAN 네트워크 관리를 수행하게 되며 충분한 메모리와 처리능력을 보유해야 한다. 시스템 모듈 중 Setup, Registration의 기능을 수행한다.

② 모니터링 서버 : 모니터링 서버는 게이트웨이로부터 받은 데이터를 수집, 분석하여 의사결정하는 강력한 백엔드 소프트웨어를 가동한다. 개인의 데이터를 이해하고 효율적으로 처리하기 위해서는 의료와 관련된 것이 미리 학습되어 있어야 한다. 즉, 모니터링 서버는 실시간으로 업로드되는 서비스 사용자의 데이터를 수집·분석하여 분석된 결과를 보고하



(그림 2) 원격 헬스케어 모니터링 시스템 구성[4]

는 역할을 한다. 시스템 모듈 중 Monitoring & Reasoning, Value Added Services, Report의 기능을 수행한다.

2) 시스템 모듈 구성

① Setup : 초기 신호 설정 인터페이스는 무선 신호, 네트워크 설정의 수신상태를 체크하고 발생할 수 있는 여러 가지 문제를 해결한다. 추가적으로, 이 모듈은 BAN과 무선 네트워크를 확실하게 존속시키고 협약을 만든다.

② Registration : 이 모듈은 데이터 검색을 단순화하는 GUI를 포함한다. 이 모듈은 환자의 바이오센서 데이터를 유지하고 필요한 모든 정보를 기록한다.

③ Monitoring & Reasoning : 건강기록을 참고하여 환자의 건강상태를 유지한다. 환자의 치료를 위한 의사결정을 만들어낸다. 학습/추론 알고리즘을 사용하고 모든 중요한 변화를 관리한다.

④ Value Added Services : 환자의 지리학적인 위치, 가까운 병원, 지방 의사의 가용성, 날씨 등과 같은 정보를 제공한다.

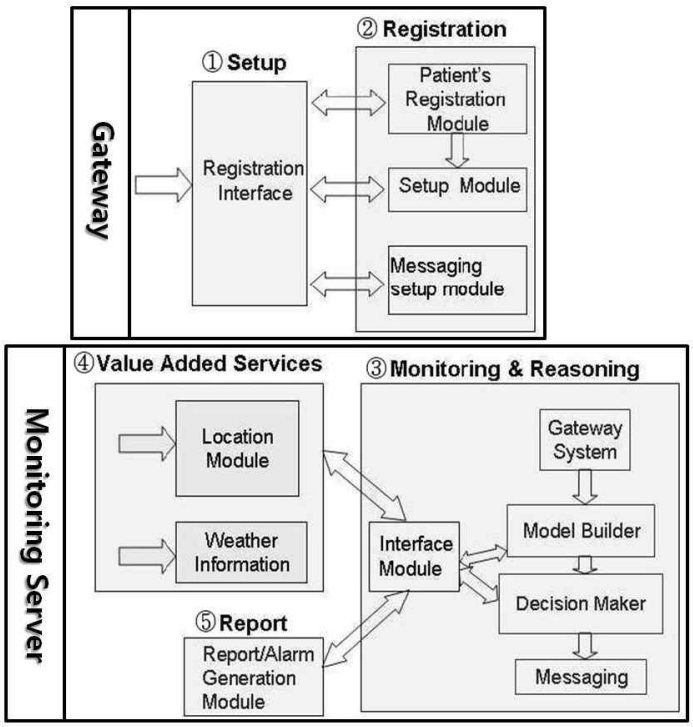
⑤ Report : 외부 모듈과 통신하는 것을 책임진다. 예를 들어, 경고를 산출하여 이러한 내용을 담당자에게 전달한다.

5가지 시스템 모듈 중 Setup, Registration은 시스템 구성 요소의 게이트웨이에서, Monitoring & Reasoning, Value Added Services, Report는 모니터링 서버에서 작동된다.

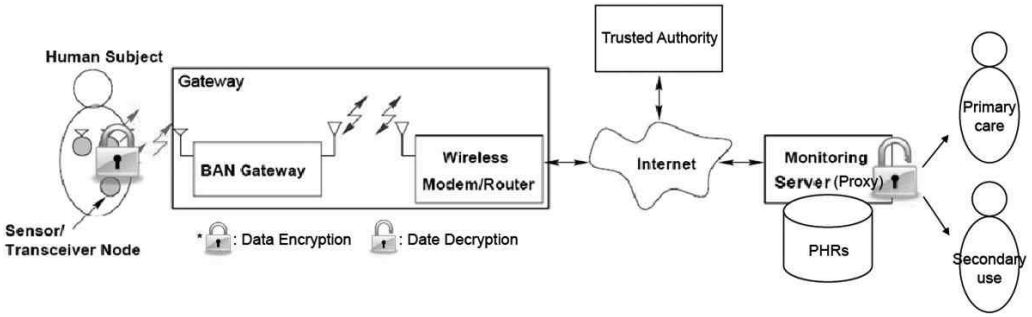
3. 속성기반 암호화를 이용한 시스템 구성

3.1 시스템 개요

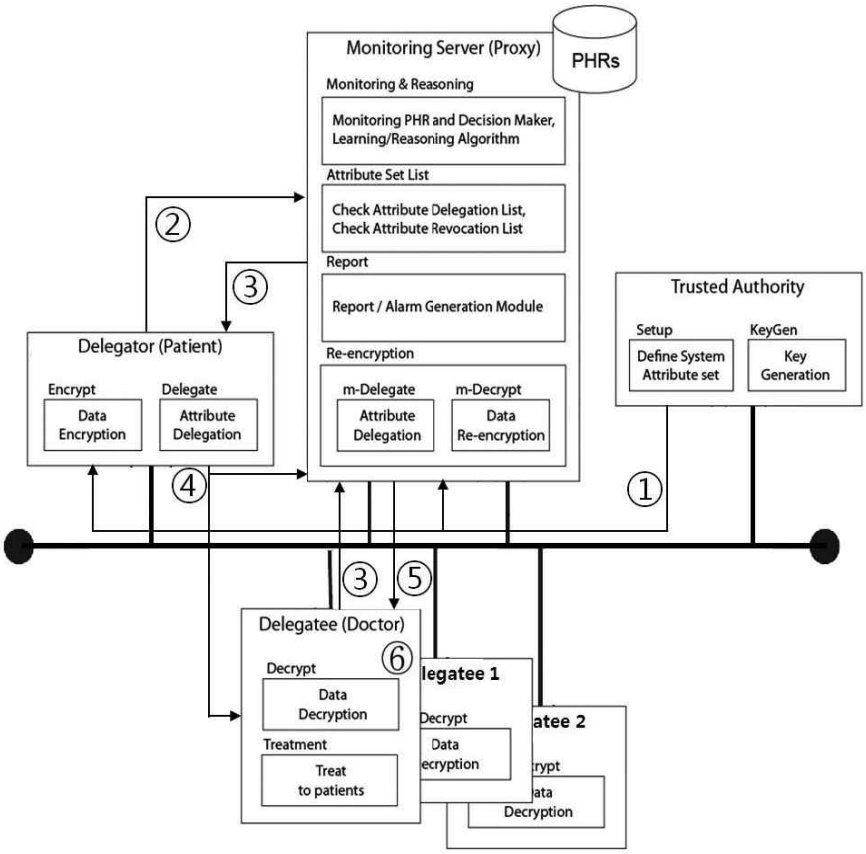
기존의 원격 헬스케어 시스템은 환자에 대한 데이터가 평문 형태로 저장되어 모니터링 서버에 전송되고 의사가 접근하여 사용했다. 진정한 원격 헬스케어 서비스가 이루어지려



(그림 3) 원격 헬스케어 모니터링 시스템의 모듈[4]



(그림 4) 속성기반 암호화를 적용한 원격 헬스케어 모니터링 시스템 개요



(그림 5) 속성기반 암호화를 적용한 원격 헬스케어 모니터링 시스템 구성

면 데이터의 공유 및 활용은 필수적이다. 이때 사용되는 데이터는 개인에게 있어 치명적일 수 있는 정보다. 그러므로 환자의 데이터가 안전하게 공유 및 활용되기 위해서 정당한 사용자에게 데이터 접근 권한을 부여하는 위임기능과 경우에 따라서 접근 권한이 부여된 사용자의 권한을 박탈하는 철회기능이 요구된다. 이러한 요구사항을 감안하여 접근 권한을 위임, 철회할 수 있는 사용자 속성기반 암호화를 이용한 원격 헬스케어 모니터링 시스템을 소개한다(그림 4).

우선, 속성기반 암호화를 이용한 원격 헬스케어 모니터링 시스템은 환자의 속성을 기반으로 한 접근구조로 데이터를 암호화하여 모니터링 서버에 전송한다. 환자의 암호화된 데이터를 공유 및 활용하고자 하는 의사는 모니터링 서버에 복호권한을 요구한다. 환자는 복호권한을 요구한 의사가 자신의 데이터를 이용할 수 있는 정당한 사용자임을 판단한 후에 속성을 위임하는 키를 만들어 모니터링 서버에게 보내준다. 이 시스템 상에서 모니터링 서버는 속성위임 리스트와 속성철회 리스트를 보유하고 있어야 한다. 모니터링 서버는 속성위임 리스트를 체크하고 속성을 위임하는 키로 데이터를 재암호화한 후 의사에게 제공한다.

3.2 시스템 구성

속성기반 암호화를 이용한 시스템 구성의 목적은 센서로부터 수집된 생체데이터를 CP-ABTD 알고리즘으로 암복호화하여 안전하게 공유 및 활용하는 것이다. CP-ABTD에서

m은 생체데이터이며 CP-ABTD 알고리즘상의 모든 파라미터가 그대로 사용된다. 시스템의 구성원은 Trusted Authority, 모니터링 서버, 환자, 의사이다. Trusted Authority는 Setup(k), KeyGen(mk, w, I_u) 알고리즘을 이용하여 사전에 필요한 설정을 구성한다. 모니터링 서버는 원격 헬스케어 모니터링 시스템의 기능과 프록시로서의 역할인 Re-encryption 기능(m-Delegate, m-Decrypt 알고리즘)을 수행한다. 환자는 자신의 생체데이터에 대한 암호화(Encrypt (m, τ, pk) 알고리즘)와 접근권한을 위임하는 의미의 속성위임(Delegate 알고리즘) 기능을 수행한다. 의사는 생체데이터에 대한 복호(Decrypt 알고리즘) 기능을 수행한다.

속성기반 암호화를 이용한 원격 헬스케어 모니터링 시스템 구성은 다음과 같다(그림 5).

속성기반 암호화를 적용한 원격 헬스케어 모니터링 시스템이 실제로 활용되는 시나리오를 아래와 같이 제시한다.

① Trusted Authority(TA)가 Setup(k) 알고리즘을 이용해서 시스템 파라메터을 정의하고 공개키 pk와 마스터키 mk를 생성한다. 그리고 KeyGen(mk, w, I_u) 알고리즘을 이용하여 환자의 속성 w과 공개키 I_u와 연관된 두 개의 비밀키 쉐어 sk_{wI_w1}와 sk_{wI_w2}를 생성하여 모니터링 서버에게 sk_{wI_w1}와 환자에게 sk_{wI_w2}를 분산한다.

② 환자는 Encrypt(m, τ, pk) 알고리즘으로 데이터 m를 암호화한 암호문 c_τ를 모니터링 서버의 데이터베이스로 전송한다. 여기서, 데이터는 일반적으로 PHR(Personal Health Record) 데이터를 말한다.

③ 의사는 환자의 데이터 m에 접근하기 위해서 모니터링 서버에 복호 토큰(속성집합과 암호문)을 요구한다. 모니터링 서버는 의사의 요구사항을 환자에게 전달한다.

④ 환자는 의사에게 암호문 c_τ에 대한 복호 권한을 위임하기 위해서 자신의 속성집합 w를 기초로 $\hat{w}$를 정의한다. 자신의 비밀키 쉐어 sk_{wI_w2}와 $\hat{w}$, 의사의 공개키 I_j로 의사를 위한 비밀키 쉐어 $sk_{\hat{w}I_j2}$와 속성을 위임하는 프록시키 $sk_{w\to\hat{w}}$를 생성하여 각각 의사($\hat{w}$, $sk_{\hat{w}I_j2}$)와 모니터링 서버($sk_{w\to\hat{w}}$)에게 보낸다.

⑤ 모니터링 서버는 자신의 비밀키 쉐어 sk_{wI_w1}, 프록시키 $sk_{w\to\hat{w}}$와 환자가 정의한 속성집합 $\hat{w}$로 의사를 위한 비밀키 쉐어 $sk_{\hat{w}I_j1}$을 생성한다. 암호문 c_τ를 의사의 공개키 I_j, $sk_{\hat{w}I_j1}$로 재암호화한 $\hat{c_\tau}$를 의사에게 보낸다.

⑥ 의사는 모니터링 서버와 환자로부터 받은 키 $sk_{\hat{w}I_j2}$와 암호문 $\hat{c_\tau}$으로 복호하여 데이터 m을 획득한다.

3.3 시스템 특징

제안 시스템은 사용자의 속성을 위임, 철회 가능한 암호방식의 알고리즘을 활용하여 다음과 같은 특징이 있다. 이러한 특징을 통해서 제안 시스템은 복호권한에 대한 효과적인 관리가 가능하다.

- 복호권한 위임 후 환자는 반드시 온라인 상태가 아니더라도 상관없음 : 제안 시스템에서 복호권한 위임은 의사가 최초 데이터에 접근하려고 할 때 한번만 수행하면 된다. 즉, 모니터링 서버는 복호권한을 위임받은 사용자의 속성을 속성 집합 리스트(Attribute Set List)에 저장하고 데이터를 요구할 때 복호기능만 수행한다.

- 위임한 복호권한에 대해서 철회가 가능함 : 환자의 요구에 따라 위임한 복호권한을 빼앗는 기능을 수행할 수 있다. 환자가 특정의사에게 위임한 속성 집합에 대해서 복호 서비스를 제공하지 않을 것을 모니터링 서버로 통보하면 모니터링 서버는 속성 집합 리스트에 저장한다. 복호권한이 철회된 사용자가 모니터링 서버에 접근하면 서비스가 불가하다는 것을 통보한다.

4. 분 석

4.1 속성기반 암호화를 이용한 시스템의 특징

CP-ABE는 기존 암호방식(공개키기반 암호화, ID기반 암호화 등)과 비교해서 악의적인 사용자간의 공모공격에 안전하다는 특징을 부각시키며 제안되었다[12]. 하지만 최근 제안된 CP-ABTD와 비교해서 CP-ABE는 사용자 속성의 위임과 철회기능이 없으며 권한관리나 위임에 대한 어떠한 내용도 다루고 있지 않다.

CP-ABTD는 기존의 CP-ABE에 속성을 위임하거나 철회하는 기능을 제공하고 있다. 이러한 CP-ABTD의 사용자 속성을 위임하고 철회하는 기능은 원격 헬스케어 환경에 적합하다. 또한, 권한위임에 대한 내용을 언급하고는 있으나 명확한 모델을 제시하지 못하고 있다. 본 논문에서는 권한위임에 대한 모델과 시나리오를 제공한다. 권한위임은 위임자가 자신의 데이터 제공에 대한 권한을 프록시에게 위임하는 것이다. 위임받은 권한으로서 프록시는 위임자의 데이터에 대한 피위임자의 접근이 정당한지 판별할 수 있다.

4.2 속성위임과 철회

CP-ABE에 속성 위임의 적용은 프록시 재암호화 방식을 통해서 지속적으로 연구되어 왔다. CP-ABTD도 그러한 연구 중 하나이다. 속성위임은 위임자을 위한 암호문의 복호권한을 피위임자에게 위임하는 기능이다. 즉, A(위임자)와 B(피위임자)라는 사용자가 있을 때 A의 암호문을 B가 복호할 수 있도록 권한을 양도하는 것이다.

속성철회는 위임했던 속성을 제거하거나 사용 불가하게 하는 것이다. 예를 들어 속성값 a_j의 철회 이벤트 발생시 인증기관(TA)이 프록시에게 a_j와 관련된 어떠한 연산도 할 수 없도록 통보한다. 그리고 모든 속성이 통합된 시스템 속성 집합에서 a_j를 제거하고 a_j와 관련된 비밀키를 소지하고 있는 모든 사용자에게 비밀키를 새로 발급하여 전송한다. 또한 재암호화키도 재생성한다.

CP-ABE와 CP-ABTD의 특징을 비교한 표는 다음과 같다.

〈표 1〉 CP-ABE와 CP-ABTD의 특징 비교표

특징	CP-ABE	CP-ABTD
속성위임	위임에 대한 개념을 제시하고 있지만 구체적인 측면에서 다루고 있지 않음	복호권한을 부여하기 위해서 속성을 위임하는 구체적인 알고리즘 제시
속성철회	속성철회의 필요성과 개념에 대한 언급이 없음	위임했던 속성을 제거하거나 사용 불가하게 만드는 알고리즘 제시
공모 공격에 대한 안전성	비밀키 생성시 선택하는 난수를 통하여 사용자간의 공모 공격에 안전함	선택된 난수와 비밀키의 분리로 사용자간의 공모 공격에 대해서 안전함

4.3. 공모 공격에 대한 안전성

속성기반 암호화 방식의 중요한 보안 특징은 공모 공격에 대한 안전성이다. 공모 공격이란 둘이상의 사용자들이 그들의 복호 권한을 확장하기 위해서 그들의 속성집합을 조합하는 것이다. 예를 들면 접근구조 $\tau = (a_1 \wedge a_2)$로 구성된 암호문이 있다. 사용자 A의 비밀키는 속성집합 $w_A = (a_1, a_3)$로 구성되어 있고 사용자 B의 비밀키는 속성집합 $w_B = (a_2, a_4)$로 구성되어 있다. 여기서, 공모 공격이란 사용자 A와 사용자 B의 비밀키를 조합하므로서 $w_A \cup w_B = (a_1, a_2, a_3, a_4)$와 관련된 비밀키를 생성하여 접근구조 $\tau = (a_1 \wedge a_2)$로 구성된 암호문을 열람하는 것이다. 의미론적으로 안전하다(semantically secure)는 것은 공격자가 암호문과 공개키를 사용해서 주어진 암호문을 만들때 평문에 대한 어떠한 것도 습득해서는 안되는 것을 뜻한다[9]. 이러한 공모 공격에 대한 안전성의 개념은 다음과 같이 3가지로 정의한다[9].

- 사용자들간의 공모 공격을 방지해야 한다; 2명 이상의 사용자가 그들의 복호권한을 확장하기 위해서 각자의 속성집합을 조합할 수 없어야 한다.
- 프록시와 사용자의 공모 공격을 방지하여야 한다; 접근정책에 만족하는 비밀키를 가지고 있지 않은 사용자와 프록시간의 악의적인 협력에 의해서 암호문을 복호할 수 없어야 한다.
- 위임된 비밀키(위임자가 피위임자를 위해 생성한 비밀키 쉐어)가 안전성을 위태롭게 해서는 안된다; 위임된 비밀키를 이용한 인증기관의 마스터키 도출 등 위임된 비밀키에 의해서 안전성이 저해되어서는 안된다.

CP-ABTD는 속성집합과 관련된 비밀키를 조합하는 공모 공격에 안전하다. 그 이유는 KeyGen 알고리즘에서 각 사용자의 고유 식별자 u_{id}가 임의의 난수로 생성되어 비밀키에 내재되기 때문이다(e.g 사용자의 비밀키 쉐어 $sk_{wI_w,2} = (d_0, \forall a_j \in w : d_{j,2}), (d_0 = g^{\alpha - u_{id}}, d_{j,2} = g^{(u_{id} - u_j)t_j^{-1}})$). 즉, 인증기관이 임의의 난수로 결정한 u_{id}를 각 사용자가 알 수 없으므로 공모 공격을 위한 비밀키를 조합시킬 수 없다.

여기서, CP-ABTD에서 마스터키를 안전하게 저장하는 인증기관은 전적으로 신뢰(fully trusted)하고 프록시는 어느 정도 신뢰(semi-trusted)할 수 있는 기관이다. 즉, 피위임자의 비밀키 쉐어를 만들고 재암호문을 생성하여 사용자들에게 정직하게 분배해야 한다. 이와 같이 본 논문에서 제안하는 시스템의 보안 특성은 CP-ABTD의 공모 공격에 대한 안전성과 관련된 의미론적 안전성에 근거를 두게 된다.

5. 결 론

정보기술의 발전으로 원격 헬스케어 서비스에 대한 모델이 제안되었다. 하지만 의료환경에서 안전한 정보의 공유를 위해서 암호방식의 도입이 필수적이다. 이러한 요구사항을 만족하는 사용자 속성 위임 및 철회 가능한 속성기반 암호화가 제안되었지만 의료환경에서의 서비스 모델을 구체화하지 못했다. 이에 본 논문은 원격 헬스케어 모니터링 시스템에 사용자 속성 위임 및 철회 가능한 속성기반 암호화의 적용 가능성과 공모 공격에 대한 안전성에 대해서 검토하였다. 속성기반 암호화가 위임과 철회기능을 갖추고 있어 원격 헬스케어 서비스에의 활발한 응용이 예상된다. 향후 과제로는 서로 다른 도메인 상에 있는 사용자 그룹의 속성을 고려한 도메인간의 데이터 공유가 가능한 속성기반 암호방식[6]을 분석하여 본 논문의 시스템 구조를 확장할 것이다. 예를 들면 2개의 기관이 존재할 때 각 기관마다 데이터에 대한 서로 다른 접근구조가 존재할 것이다. 이 경우 접근구조를 변환하여 접근을 허가하는 방식을 사용하여야 하는데 이때 속성에 대한 정의, 속성집합의 구성을 검토할 것이다. 또한, 환자의 데이터 중 일부분 혹은 전체를 위임할 수 있는 방식[13]에 대하여 연구하여 제안 시스템의 구조를 확장한다. 즉, 환자가 피위임자의 보안등급에 따라 데이터를 위임할 범위를 설정하여 부분적인 복호권한을 위임하는 기능에 대해서 검토할 것이다.

참 고 문 헌

[1] 오정연, “의료정보화 현황 및 과제,” NCA CIO REPORT, 05-11호, 한국전산원, 2006.
[2] 박건희, “보건의료정보화와 개인정보보호,” 서울대의대 2006년 상반기 토픽 리뷰, 2006.
[3] 송지은, 김신효, 정명애, 정교일, “u-헬스케어 보안 이슈 및 기술동향,” 전자통신동향분석, 제 22권 제 1호, 한국전자통신연구원, 2007.
[4] S. Y. Lim, T. H. Oh, Y. B. Choi and T. Lakshman, “Security Issues on Wireless Body Area Network for Remote Healthcare

Monitoring," Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference, pp.327-332, 2010.

[5] M. Tentori, J. Favela and M. D. Rodriguez, "Privacy-Aware Autonomous Agents for Pervasive Healthcare," IEEE Intelligent Systems, pp.55-62, 2006.

[6] J. Sun and Y. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record System," IEEE Transactions on Parallel and Distributed Systems, pp.754-764, 2010.

[7] 박광용, 송유진, "속성기반 암호기술," 한국정보보호학회, 정보보호학회지, 제20권 제2호, pp.85-92, 2010.

[8] P. Robinson, H. Vogt and W. Wagealla, "Privacy, Security, and Trust Within the Context of Pervasive Computing," The Springer International Series in Engineering and Computer Science, Vol.780, 2005.

[9] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009 University of Twente, Centre for Telematics and Information Technology, Internal Report, 2009.

[10] EHR핵심연구개발사업단, "건강정보보호 및 보안 체계 개발," 5세부, 2009.

[11] 김주한, "개인정보 암호화 한 평생기록 추진," 메디칼 업저버, 창간 5주년 기념 정책토론회, 2006.

[12] X. Liang, Z. Cao, H. Lin and J. Shao, "Attribute Based Proxy Re-encryption with Delegating Capabilities," ASIACCS 2009, ACM, pp.276-286, 2009.

[13] L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, "A Type-and-Identity-based Proxy Re-Encryption Scheme and its Application in Healthcare," 5th VLDB Workshop on Secure Data Management, SDM, pp.185-198, 2008.

송 유 진

e-mail : song@dongguk.ac.kr

1982년 한국항공대학교 전자공학과(학사)

1987년 경북대학교(공학석사)

1995년 일본 Tokyo Institute of Technology (공학박사)

1988년～1996년 한국전자통신연구원 선임연구원

2003년～2005년 미국 University of North Carolina at Charlotte 연구교수

2006년～2006년 일본 정보보호대학원대학 객원교수

1996년～현 재 동국대학교 정보경영학과 교수

2005년～현 재 동국대학교 부설 전자상거래연구소장

1998년～현 재 한국정보보호학회 부회장(영남지부장)

2006년～현 재 국제 e-비즈니스학회 이사

2006년～현 재 한국사이버테러정보전학회 이사

2001년 ICISC2001 운영위원장

2003년 하계CISC2003 프로그램위원장

2006년 CISC-S2006 공동프로그램위원장

2007년 한국정보시스템학회 추계학술발표대회 공동 조직위원장

관심분야 : Privacy Protection, Secret Sharing, 전자상거래응용 보안(Location Privacy, 디지털컨텐츠 보호, SCM/ CRM 보안 등), Context Aware Application Security 등

도 정 민

e-mail : havdrim@hotmail.com

2009년 동국대학교 정보경영학과(학사)

2010년～현 재 동국대학교 전자상거래 협동과정 석사과정

관심분야 : 정보보호, 암호이론(Secret Sharing, Attribute-Based Encryption), Context Aware Application Security 등