http://dx.doi.org/10.14400/JDC.2014.12.7.279

응급 상황에서 환자의 프라이버시를 보장하는 속성기반 접근 제어 프로토콜

정윤수*, 한군희**, 이상호***
목원대학교 정보통신공학과*, 백석대학교 정보통신공학과**, 충북대학교 소프트웨어학과***

Access Control Protocol for Privacy Guarantee of Patient in Emergency Environment

Yoon-Su Jeong*, Kun-Hee Han, Sang-Ho Lee*****
Dept. of Information Communication & Engineeringe, Mokwon University*
Dept. of Information Communication & Engineeringe, Baeseok University**
Dept. of Software, Chungbuk National University***

요 약 최근 m-헬스케어는 응급상황이 발생할 경우, 환자의 정보가 제 3자에게 쉽게 노출되어 악용될 수 있는 문제가 있다. 본 논문에서는 m-헬스케어의 응급상황 환경에서 환자의 정보를 이용하여 환자의 프라이버시 노출을 최소화하기 위한 속성 기반의 환자 접근 제어 프로토콜을 제안한다. 제안 프로토콜은 환자의 민감한 정보를 제 3자에게 노출시키지 않도록 환자의 민감한 정보를 개인 건강 정보에 포함하여 병원관계자와 환자가 생성한 랜덤수로 해쉬한 서명키로 암호화한다. 또한 제 3자로부터 환자 정보가 불법적으로 악용되는 것을 예방하기 위해서 환자와 병원관계자 사이의 동기화를 유지함으로써 개인 건강 정보의 유출을 예방한다.

주제어 : 접근 제어, 프라이버시, 프로토콜, 속성기반, 응급상황

Abstract Recently, m-health care is be a problem that the patient's information is easily exposed to third parties in case of emergency situation. This paper propose an attribute-based access control protocol to minimize the exposure to patient privacy using patient information in the emergency environment. Proposed protocol, the patient's sensitive information to a third party do not expose sensitive information to the patient's personal health information, including hospital staff and patients on a random number to generate cryptographic keys to sign hash. In addition, patient information from a third party that is in order to prevent the illegal exploitation of the patient and the hospital staff to maintain synchronization between to prevent the leakage of personal health information.

Key Words : Access Control, Privacy, Protocol, Property based, Emergency Environment

1. 서론

최근 의료 서비스 분야에서는 다양한 종류의 소형 체내삽입장치를 휴대 가능한 스마트폰에 접목하여 원거리에 있는 환자의 건강상태를 모니터링하는 m-헬스케어(m-Healthcare, Mobile Healthcare) 서비스가 각광을 받

* 이 논문은 2013년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음
Received 18 May 2014, Revised 16 June 2014
Accepted 20 July 2014
Corresponding Author: Sang-Ho Lee (Dept. of Software, Chungbuk National University)
Email: shlee@cbnu.ac.kr

ISSN: 1738-1916

고 있다[1]. 비록 m-헬스케어가 기존 의료서비스 기술에 접목하여 언제, 어디서나, 보건의료 서비스를 제공하더라도 m-헬스케어는 바이오정보를 포함한 개인정보와 의료정보를 다루기 때문에 해킹으로 인한 정보유출 사고발생 시 국가적인 혼란과 사회적인 불신을 야기할 수 있는 문제점이 있다[2].

m-헬스케어는 기회 컴퓨팅 파라다임을 개인 건강 정보(PHI, Personal Health Information) 처리에 적용할 수 있다. 그러나 개인 건강 정보는 개인정보이고 환자에게 매우 민감하기 때문에 조심스럽게 다루어야져야 한다[3,4]. raw 개인 건강 정보가 기회 컴퓨팅에서 처리된다면 개인 건강 정보의 프라이버시는 제 3자에게 쉽게 노출될 수 있다. 따라서, 기회 컴퓨팅이 개인 건강 정보의 프라이버시 노출을 최소화하도록 하기 위해서는 환자와 병원관계자 사이에서 스마트폰내에 저장되어 있는 개인 건강 정보의 의존도를 높게 유지하면서 m-헬스케어 응급상황에 적용할 기술이 필요하다.

본 논문에서는 기회 컴퓨팅 환경에서 사용할 수 있는 헬스케어 장비(ex. 체내삽입장치)로 스마트폰과 연결하여 응급상황 환경에서 환자의 개인 건강 정보에 대한 프라이버시 노출을 최소화하기 위한 속성 기반의 환자 접근 제어 프로토콜을 제안한다. 제안 프로토콜은 환자의 민감한 정보를 제 3자에게 노출시키지 않도록 환자의 민감한 정보들을 개인 건강 정보에 포함하여 병원에서 다양한 형태로 존재하는 환자의 정보를 환자가 기억하지 않아도 인증되도록 중앙 서버가 집중관리 할 수 있도록 유헬스케어 서비스 센터와 환자가 생성한 랜덤수로 해쉬한 서명키를 사용한다. 또한 제 3자로부터 환자 정보가 불법적으로 악용되는 것을 예방하기 위해서 환자와 병원관계자 사이의 동기화를 유지함으로써 개인 건강 정보의 유출을 예방할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 m-헬스케어 서비스 개념과 보안 문제에 대해서 알아본다. 3장에서는 m-헬스케어의 응급상황 환경에서 환자의 정보를 이용하여 환자의 프라이버시 노출을 최소화하기 위한 속성 기반의 환자 접근 제어 프로토콜을 제안하고, 4장에서는 제안 모델의 성능 및 보안 평가를 분석하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

m-헬스케어 서비스는 홈네트워크 상의 장치나 휴대용 장치 등의 정보통신기술이 의료와 접목되어 생체 정보를 실시간으로 모니터링하고 자동으로 병원 및 의사와 연결되어 시간과 공간에 구애 받지 않고 언제 어디서나 건강을 관리하고 증진시키며 질병을 예방하고 관리하는 새로운 형태의 의료 서비스를 의미한다[2,3]. m-헬스케어는 과거 전통적인 헬스케어의 영역에서 물리적, 시간적으로 제약되어 있던 서비스의 편리성을 높이기 위해 유·무선 온라인 네트워크를 활용하여 전자적 의료정보 및 진료 예약관리 등을 제공하던 e-헬스케어 단계에서 한단계 더 진화된 서비스이다[5,6].

의료 서비스 기술이 발달함에 따라 m-헬스케어의 의료정보 보안에 대한 요구가 급증하고 있으며, PKI 또는 데이터 암호화 등을 중심으로 보안 기술들을 제품에 적용하고 있다[8]. m-헬스케어 환경에서 데이터 보호 및 프라이버시 보호 문제와 관련된 다양한 보안 취약점과 위협 요소들은 유·무선 네트워크 기반 서비스에서 발생 가능한 보안상 취약점과 유사하다. 그러나 m-헬스케어 서비스는 기존 유·무선 네트워크 기반 서비스와는 다른 보안 요구사항들이 존재한다[7,8]. m-헬스케어에 사용되는 새로운 장비들과 네트워크상에서 존재하는 신규 취약점에는 첫째, 서비스를 지원하는 서버를 공격하는 DoS 공격 유형, 둘째, 바이러스/웜 해킹 공격 유형, 셋째, 의료정보 도청/위변조 공격 유형, 넷째, 유·무선 인프라에서 가능한 여러 불법 접근 공격 유형, 다섯째, 오프라인을 통한 방범 시스템 고장 및 인위적인 기기 마비, 방해전파, 화재와 같은 인재 또는 악의적인 행위를 통한 공격유형 등이 있다.

3. 속성기반 접근 제어 프로토콜

이 절에서는 다양한 의료 서비스 환경에서 환자의 상태에 따라 환자의 프라이버시 접근을 제어하는 프로토콜을 제안한다.

3.1 개요

제안 프로토콜에서는 속성 기반의 환자 접근 제어 프

로토콜을 사용한다. 제안 프로토콜에서는 병원간 건강/의료 정보 공유 시, 환자를 포함한 인가 받은 정보 소비 주체들이 불필요한 개인 정보 노출 없이 익명성을 보장 받는다. 제안 프로토콜은 인증 및 관리 효율성을 위해서 정상적인 인증 및 식별이 가능하도록 환장의 통합 ID 관리 정보를 관리한다.

환자의 프라이버시 위협이 증가하는 환경에서 병원이나 약국이 환자의 기록을 이용할 경우, 제안 프로토콜에서는 병원이나 약국에서 제한된 권한을 부여하여 환자의 동의에 따라 진찰 및 치료 내역을 이용할 수 있도록 접근 권한을 부여한다.

3.2 용어 정의

<Table 1>은 제안된 프로토콜에서 사용하는 용어에 대한 설명이다.

〈Table 1〉 Notation

Notation	Definition
SC	Service Center
U_i	i^{th} patient
$\vec{p}$	Personal Information of Patient
P_i	i^{th} Hospital Manager
ID_i, ID_j	Unique Identifier of U_i and P_i
$E_K(M)$	Symmetric key Encryption of the plain text M using the key K
$D_K(C)$	Symmetric key Encryption of the plain text C using the key K
SK_i	Signature key of i
$h(\bullet)$	One-way Hash Fucntion
$\|\|$	Concatenation operation

3.3 환자 속성 정보 보호 프로토콜

이 절에서는 응급상황에서 환자의 프라이버시를 보호하기 위하여 환자의 프라이버시 속성정보(데이터 소비자, 시간, 센서, 목적, 의무, 위임 그리고 상황 등)을 부여하고, 제3자에게 환자의 프라이버시 접근을 제어하는 프로토콜을 제안한다.

3.3.1 환자 프라이버시 규칙

환자의 프라이버시 규칙들은 조건(Condition)과 동작(Action)으로 구분되며, 환자의 프라이버시에 대한 접근 제어를 수행하기 위해 <Table 2>와 같은 정보를 포함한다. 데이터 제공자들은 자신들의 프라이버시 규칙을 <Table 2>를 참조하여 정의한 후 데이터베이스에 저장한다.

〈Table 2〉 Status and Action Rule of patient

Option		Property
Status	Data sharer	User name, group name etc.
	Purpose	Use purpose
	Obligation	Obligations
	Mandate	Delegator
	Location	Predefined tables, local coordinates
	Time	Time range, repetition time
	Sensor	Sensor channel name
	Status	situation which can be be used in sensor
Action		Action, activity

3.3.2 초기화 과정

이 과정은 환자가 응급상황이 발생하기 전 환자의 프라이버시 정보를 보호하기 위한 키 정보를 초기화하는 과정이다. 이 과정은 크게 6단계로 구성된다.

- 단계 1 : 환자 U_i는 응급상황이 발생하기 전 환자의 속성 정보를 이용하여 환자의 프라이버시 정보 $\vec{p}$를 식 (1)처럼 생성한다. 여기서, n은 환자의 체내삽입 장치 수를 의미한다.

$$\vec{p} = (a_1, a_2, ..., a_n) \quad (1)$$

- 단계 2 : 환자의 프라이버시 정보 $\vec{p}$이 생성되면 환자는 환자 U_i의 인식자 정보 UI_i를 공유키 K_i로 암호화하여 병원관계자 P_i에게 전달한다. 여기서, 공유키 K_i는 안전한 경로를 통해 환자 U_i와 병원관계자 P_i 사이에 사전에 공유한 키를 의미한다.

$$Transfer\ E_K(\vec{p},\ UI_i) \quad (2)$$

- 단계 3 : 병원관계자 P_i는 환자로부터 전달받은 정

보를 공유키 K_i로 복호화한 후 환자 U_i의 개인정보 $\vec{p}$에 접근하기 위한 키를 식 3처럼 생성한다. 식 3처럼 생성된 키는 2개로써 랜덤하게 생성한다.

$$Generate \quad (t_1,\ t_2) \in Z_q^* \tag{3}$$

- 단계 4 : 병원관계자 P_i는 환자 U_i의 접근제어 키 ak_i와 비밀키sk_i를 식 (4)와 식 (5)처럼 생성하여 환자 U_i에게 식 (6)을 전달한다.

$$ak_i = (q^{x+at_1},\ q^{t_1},\ q^{t_2}) \tag{4}$$
$$sk_i = H(UI_i \| \vec{p} \| ak_i) \tag{5}$$
$$Transfer \ E_K(ak_i,\ sk_i) \tag{6}$$

- 단계 5 : 환자 U_i는 병원관계자 P_i로부터 전달받은 정보를 공유키 K_i를 사용하여 복호화한 후 자신의 상태를 $State$ 정보에 저장한다. $State$는 0과 1의 값에 따라 정보의 갱신 유·무를 판별한다.

- 단계 6 : 환자는 프라이버시 정보 $\vec{p}$ 와 체내삽입장치로부터 수집된 환자의 개인 건강 정보 PHI_i(= $(phi_1,\ phi_2,\ ...,\ phi_n)$)의 쌍을 세션키 sk_i로 암호화하여 병원 관계자와 데이터베이스에 전송한다.

$$Transfer \ E_{sk_i}((\vec{p},\ PHI_i) \| State) \tag{7}$$

응급상황이 발생할 경우 병원관계자 P_i는 데이터베이스에 저장되어 있는 $E_{sk_i}((\vec{p},\ PHI_i) \| State)$ 정보를 수신받아 세션키 sk_i로 복호화한 후 환자의 상태 정보 $State$를 점검한다. 만일 상태 정보 $State$가 정상이면 환자의 개인정보를 모니터링하고 그렇지 않으면 종료한다.

3.3.2 접근제어 과정

이 과정은 환자 U_i에게 응급상황이 발생하였을 경우 환자 U_i 자신의 개인 건강 정보 PHI_i에 대한 프라이버시 노출을 최소화하기 위한 접근제어 과정이다.

- 단계 1 : 병원관계자 P_i는 체내삽입장치를 구성하는 환자 U_i의 프라이버시 정보 $\vec{p}$를 체내삽입장치를 통해 수집한다.

$$Gathering \ \vec{p} = (a_1,\ a_2,\ ...,\ a_n) \tag{8}$$

- 단계 2 : 병원관계자 P_i는 환자 U_i의 개인 건강 정보 PHI_i에 대한 자세한 정보를 복구 및 조회하기 위해서 데이터베이스에 저장되어 있는 $E_{sk_i}((\vec{p},\ PHI_i) \| State)$를 검색하여 비밀키 sk_i로 복호화한 후 환자 U_i의 프로파일 정보 $\vec{p}'$, 개인정보 정보 PHI_i', 환자의 상태 정보 $State'$ 등을 비교한다.

$$Compare \ \vec{p} \equiv \vec{p}' \text{ and } PHI_i \equiv PHI_i' \text{ and } State \equiv State' \tag{9}$$

- 단계 3 : 병원관계자 P_i는 환자의 인식자 정보 UI_i를 이용하여 비밀키 sk_i를 계산한 후 환자에게 비밀키 sk_i를 전달한다.

$$sk_i = H(UI_i \| \sum_{i=1}^{n} x_i H(a) \| ak_i) \tag{10}$$

- 단계 4 : 병원관계자 P_i는 환자 U_i의 개인 건강 정보 PHI_i를 실시간으로 모니터링하면서 환자 U_i의 이전 개인 건강 정보 PHI_i를 레벨 속성값 PN_i과 함께 해쉬함수 $H()$에 적용하여 환자 U_i의 개인 건강 정보 PHI_i를 새로 갱신한다.

$$PHI_i' = \sum_{i=1}^{n} H(PN_i \bullet PHI_i) \tag{11}$$

4. 성능 평가

이 절에서는 스마트폰과 병원관계자 P_i 구간, 환자 U_i와 병원관계자 P_i 구간사이의 통신 범위에서 안전한 통신이 이루어진다는 가정한다. 제안 프로토콜의 성능평가는 처리율과 복잡도(통신 복잡도와 계산 복잡도) 등으로 평가한다.

4.1 환경설정

제안 프로토콜의 성능 평가를 위해 각각의 환자 U_i는 체내삽입장치를 부착하고 스마트폰은 전송범위를 20m롤 정의한다. 환자 U_i는 $v \in [0.5, 1.2]$m/s로 개별적으로 움직이며, 응급상황이 발생하는 환자 U_i가 발생하면 시간 t는 0으로 설정하고 threshold th는 {1, 3, 5}로 설정한다. 응급상황을 고려하여 환자 U_i의 개인 건강 정보 PHI_i는 20분 이내에 각 구성요소별 처리가 완료된다고 가정한다.

〈Table 3〉 Simulation Setting

Parameter	Setting
Simulation area	500m × 500m
Number, velocity of users	l = {20, 40, 60}, v =0.5-1.2m/s
Simularity threshold	th = {1, 3, 5}
Transmission of smartphone	20m
PHI data generation interval	envery 10 seconds

4.2 성능분석

4.2.1 처리율

환자 U_i와 병원관계자 P_i 사이에서 요구되는 처리 비용은 다음과 같이 계산한다. n은 환자 U_i내 부착된 체내삽입장치의 수이고 r은 체내삽입장치의 센서 범위를 의미한다. 체내삽입장치의 개인 건강 정보 PHI_i는 환자 U_i당 $n \times r = \log_2\frac{N}{M}+\log_2 M = \log_2 N$이다. 병원관계자 P_i는 $n \times r = (2*\frac{N}{M})+\frac{N}{M}*(2*\log_2 M)=2*\frac{N}{M}(\log_2 m+1)-1$이다. 통신 비용은 $2*\log_2\frac{N}{M}+\log_2 M =2*\log_2 N-\log_2 M$이다. 여기서 M과 N은 통신범위내 환자 U_i와 병원관계자 P_i이 환자 U_i의 개인 건강 정보 PHI_i를 처리하는 수이고 통신범위 내의 장치들은 개인 건강 정보 PHI_i를 모두 공유되는 것으로 나타낸다.

4.2.2 복잡도

제안된 프로토콜에서는 환자 U_i의 개인 건강 정보 PHI_i과 관련하여 프라이버 정보 $\vec{p}$, 랜덤 수 $(a, x) \in Z_q^*$와 $(t_1, t_2) \in Z_q^*$, 비밀키 sk_i, 키 material (ak_i, sk_i), 상태값 $State$, 세션키 $k_i(=H(sk_i||State))$ 등의 메시지들이 교환된다. 시뮬레이션에서 랜덤 수가 64비트일 경우, 제안 프로토콜의 통신 비용은 [8,10]에서 요구된 180 바이트와 거의 동일한 1453비트나 183 바이트의 통신 복잡도를 가진다.

4.3 보안분석

제안 프로토콜에서 새로 생성된 키들은 동일 서비스 범위내에 있는 공유키 K_i로 암호화된다. 범위내에서 공유키 K_i가 동의되면 이전에 요청된 환자 U_i의 개인 건강 정보 PHI_i는 액세스 할 수 없다. 제 3자가 환자 U_i의 개인 건강 정보 PHI_i를 추출하려고 시도하더라도 프라이버 정보 $\vec{p}$ 부족과 접근제어 키 $ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2})$를 생성하기 위한 랜덤 수 t_1, t_2를 제3자가 모르기 때문에 비밀키 sk_i 및 공유키 K_i를 액세스 할 수 없다. 제안 프로토콜에서 범위내에 위조된 환자 U_i의 개인 건강 정보 PHI_i를 삽입하려고 하는 침입 노드를 예방하기 위한 방법은 간단하며 지연없이 수행될 수 있다. 병원관계자 P_i는 모든 전송된 데이터를 조사하여 접근제어 키 $ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2})$가 누설될 경우 위조 전송을 탐지한다.

5. 결론

본 논문에서는 m-헬스케어의 응급상황 환경에서 데이터베이스에 저장되어 있는 환자의 프라이버시를 보호하기 위한 속성 기반의 환자 접근 제어 프로토콜을 제안하였다. 제안 프로토콜은 환자의 민감한 정보를 제 3자에게 노출시키지 않도록 환자의 민감한 정보들을 병원관계자와 환자가 생성한 랜덤수로 해쉬한 서명키로 암호화하였다. 또한 제 3자로부터 환자 정보가 불법적으로 악용되는 것을 예방하기 위해서 환자 U_i와 병원관계자 P_i사이에서 생성된 접근제어 키 $ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2})$, 비밀키 $sk_i(=H(U_i||\vec{p}||ak_i))$ 등을 동기화하여 개인 건강 정보의 유출을 예방하였다. 향후 연구에서는 병원과 환자 사이에서 안전한 환자의 개인 건강 정보를 확장하여 다수의 병원에서 환자의 개인 건강 정보를 통합운영 관리할 수 있도록 실제 환경에 적용할 예정이다.

ACKNOWLEDGMENTS

This work was supported by the research grant of Chungbuk National University in 2013

REFERENCES

[1] Y. Y. Shieh, F. Y. Tsai, Arash, M. D. Wang, C.-M.C.Lin(2007), "Mobile Healthcare: Opportunities and Challenges", International conference on the Management of Mobile Business(ICMB 2007), pp. 50.

[2] J. Zhou, Z. Cao, X. L. Dong, X. D. Lin(2013), "Securing m-healthcare social networks: challenges, countermeasures and future directions", IEEE Wireless Communications, Vol. 20, No. 4, pp. 12-21.

[3] R. X. Lu, X. D. Lin, X. M. Shen(2013), "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE Transaction on Parallel and Distributed Systems, Vol. 24, No. 3, pp. 614-624.

[4] F. Miao, L. Jiang, Y. Li, Y. T. Zhang(2009), "Biometrics based novel key distribution solution for body sensor networks", 2009. Annual International Conference of the IEEE Engineering in Medicine and Biology Society(2009 EMBC), pp. 2458-2461.

[5] F. Miao, L. Jiang, Y. Li, Y. T. Zhang(2009), "A Novel Biometrics Based Security Solution for Body Sensor Networks", 2nd International conference on biuomedical Engineering and Informatics 2009(BMEI '09), pp. 1-5.

[6] G. Sudha, R. Ganesan(2013), "Secure transmission medical data for pervasive healthcare system using android", 2013 International Conference on Communications and Signal Processing(ICCSP), pp. 433-436

[7] U. Harish, R. Ganesan(2012), "Design and development of secured m-healthcare system", 2012 International conference on Advances in Engineering, Science and Management(ICAESM), pp. 470-473.

[8] M. Y. Hwang, C. H. Jin, U. Yun, K. D. Kim and K. H. Ryu(2012), "Building of prediction model of wind power generation using power ramp rate", Journal of the Korea Society of Computer and Information, vol. 17, pp. 211-218.

정 윤 수(Jeong, Yoon Su)

- 2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월 : 충북대학교 대학원 전자계산학 박사
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
- 관심분야: 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail: bukmunro@gmail.com

한 군 희(Han, Kun Hee)

- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 멀티미디어, 정보보호
- E-Mail : hankh@bu.ac.kr

이 상 호(Lee, Sang Ho)

- 1976년 2월 : 숭실대학교 전자계산학과 학사
- 1981년 2월 : 숭실대학교 대학원 전자계산학과 석사
- 1989년 2월 : 숭실대학교 대학원 전자계산학과 박사
- 1981년 3월 ~ 현재 : 충북대학교 전자정보대학 소프트웨어학과 교수
- 관심분야 : 네트워크보안, Protocol Engineering, Network Management
- E-Mail: shlee@chungbuk.ac.kr