불법적인 접근 제어 방지를 위한 안전한 헬스케어 시스템

논 문
59-3-27

Prevent Illegal Access Control for Secure Healthcare System

서 대 희† · 백 장 미* · 문 용 혁** · 조 동 섭***
(Dae-Hee Seo · Jang-Mi Baek · Yong-Hyuk Moon · Dong-Sub Cho)

Abstract - Today, rapid evolution of Internet makes various types of services in ubiquitous environment are intelligent and active. As a result, user's demand on high quality of life increases and health care service based on ubiquitous environment draws a lot of attention. However, user's private information used for health care service is illegally distributed and exposed, causing serious individual and social problems. Therefore, this thesis is intended to suggest a secure health care service to prevent unauthorized third party's access and to protect user's privacy in health care systems. The proposed scheme establishes a session key through communication channel between health care system and user based on explicit mutual authentication and provides secure communication and access control, improving security as one of the leading health care systems.

Key Words : Ubiquitous Computing, Healthcare System, Access Control, Mutual Authentication

1. 서 론

헬스케어 서비스는 사용자의 삶의 질에 대한 욕구가 증대되고 유비쿼터스 환경의 보편성에 기인해 다양한 연구가 진행되고 있다. 특히, 기존의 질병 발생 후에 대응하던 수동적인 페러다임에서 벗어나 환자가 의료 기기를 이용하여 일상생활 가운데에서 의료 서비스를 제공 받음으로써 신속한 의료 서비스를 제공한다.

특히, 유비쿼터스 환경에서의 헬스케어 서비스는 지능형화된 의료 센서나 기기에 대한 생체 정보의 사용이 다양해지고 건강 정보의 공유가 확대됨으로써 사용자의 정보 욕구와 삶의 질을 향상 시킬 수 있는 계기가 되고 있다.

그러나 헬스케어 서비스는 개인 정보가 유무선 네트워크에서 전송됨으로써 다양한 문제점을 내포하고 있다. 기반 기술 뿐만 아니라 헬스케어 서비스와 관계된 모든 개체들간의 보안 및 프라이버시 보호에 대한 다양한 취약성을 보완할 수 있어야 하며, 이를 위해서는 안전하고 효율적인 형태의 헬스케어 서비스를 제공하기 위한 연구는 매우 의미있다고 할 수 있다[1][6].

따라서 본 논문에서는 유비쿼터스 환경에서 헬스케어 서비스를 사용자에게 제공할 때 비인가된 제 3자에 의해 불법적으로 사용자의 프라이버시 데이터 접근을 방지하기 위한 안전한 헬스케어 시스템을 제안하기 위하여 2장에서는 헬스케어 서비스와 헬스케어 서비스에서 정보보호의 필요성을 기술하고 3장에서는 기존의 헬스케어 서비스를 분석하고 보안 요구사항을 제시하고자 한다. 4장에서는 불법적인 접근 제어 방지를 위한 안전한 헬스케어 서비스를 제안하고 5장에서는 3장에서 제시한 보안 요구사항을 기반으로 기존 연구와의 비교 분석을 수행한 뒤 마지막으로 6장에서 결론 및 향후 연구 방향을 제시하고자한다.

* 정 회 원 : 순천향대학교 강사
** 정 회 원 : 한국전자통신연구원 연구원
*** 시니어회원 : 이화여자대학교 교수
† 교신저자, 정회원 : 한국전자통신연구원 선임연구원
E-mail : dhseo@etri.re.kr
접수일자 : 2009년 7월 13일
최종완료 : 2009년 11월 18일

2. 기술 개요

다음은 헬스케어 서비스의 개요와 헬스케어 서비스에서 정보보호의 필요성에 대해서 기술하고자 한다.

2.1 헬스케어 서비스의 개요

헬스케어 서비스는 사용자 중심의 헬스케어 서비스를 제공하기 위한 정보 통신 기술과 의료 서비스의 융합 방식으로 언제 어디서나 예방, 진료, 치료 및 사후 관리 서비스를 제공한다. 이러한 서비스는 사용자의 삶의 질에 대한 욕구에 의한 것으로써 고도화된 의료 서비스의 발전을 기반으로 한다.

또한 환경적인 측면에서 유비쿼터스 컴퓨팅 기술과 더불어 기술들의 융합을 통해 사용자 중심의 헬스케어 서비스의 고도화와 자동화가 가능하도록 하였다.

헬스케어 서비스는 단순한 의료 장비에 디지털 데이터와 네트워크 기능을 추가한 기존의 시스템에서 벗어나 보다 발전된 형태의 서비스로의 진화를 가져오고 있다. 이와 관련하여 국내외적으로 많은 연구가 진행되고 있으며, 체지방 측정, 착복형 진단 셔츠, 체내 이식용 의료 기기 개발등 다양한 연구들이 추진되고 있다[2].

그러나 최근 개인 정보보호의 중요성이 증대되면서 사용자의 프라이버시 보호 의식이 확산되어 헬스케어 분야에서도 이를 중요한 문제로 제시되고 있으며 다각적인 측면에서 대응 방안이 제시되고 있다. 특히, 사용자의 단말에 대한 불법적인 접근을 비롯하여 네트워크를 통한 의료 정보 시스템의 불법적인 침해에 따라 보안 위협으로부터 안전하고 신뢰성 있는 헬스케어 서비스를 위한 보안 기술의 개발이 시급히 요구된다.

2.2 헬스케어 서비스에서 정보보호의 필요성

헬스케어 서비스는 기존의 유무선 네트워크를 기반으로 제공되는 서비스중의 하나로써 사용자의 프라이버시 정보와 밀접하게 연관되어 있다.

따라서 기존 유무선 네트워크의 취약성을 보완하기 위한 별도의 보안 서비스 뿐만 아니라 헬스케어 서비스의 특성에 따라 정확한 진료를 받기 위한 개인의 중요 정보를 제공하게 되고 여러 헬스케어 개체와 공유된다. 따라서 개인의 인증 및 식별 정보의 다양화에 따른 개인의 유일한 생체정보가 불법적으로 사용될 경우 개인적인 문제뿐만 아니라 사회적인 문제로 양산될 수 있다.

따라서 안전하고 향상된 의료 서비스를 제공하기 위해서는 개인 정보에 대한 접근의 용이성 뿐만 아니라 환경적인 측면에서 초기 설계시에 보안 기술에 대한 요구사항을 만족할 수 있어야 한다[3].

헬스케어 서비스에 대한 정보보호 기술은 기존의 정보보호 시스템 기술과 같이 독자적으로 존재하는 것이 아닌 다양한 형태로 운용이 가능해야 한다. 따라서 기본적인 인터넷 프로토콜이 의료장비에 필수적으로 지원되면서 기존의 네트워크 보안 제품을 그대로 사용할 수 있을 뿐만 아니라 추가적으로 사용자의 인증과 효율적인 관리를 위한 지속적인 연구가 반드시 요구된다.

3. 기술 개요

다음은 기존의 헬스케어 시스템에 대한 연구를 분석하고자 한다.

3.1 SHOES 방식

본 논문은 2006년 Song외 1명이 제안한 방식으로 actual 네트워크 기반의 헬스케어 서비스를 제공하기 위한 아키텍처이다. 본 방식의 경우 통신상의 안전성과 사용자 정보의 안전성 확보 및 접근 제어를 제공한다. 따라서 신뢰된 헬스케어 서비스를 규정하고 안전한 통신 방법을 제공할 수 있는 아키텍처를 제시함으로써 안전한 통신과 관리의 효율성을 제공하고자 하였다[4]. 그러나 본 방식의 경우 다음과 같은 취약성을 내포하고 있다.

- 통신상의 안전성: 본 방식은 통신상의 안전성을 위하여 인증서 기반으로 XML 서명과 암호화 방식을 이용하였다. 그러나 구체적인 통신에 대한 방식을 제시하지 않았으며, 관리적인 측면에서 미들웨어에서 제공되는 통신상의 보안을 정책적으로 규정함으로써 사용자와 시스템간의 통신상에서의 안전성을 확보할 수 없다.
- 데이터의 안전성 (저장 데이터, 전송 데이터): 저장, 전송 데이터의 안전성은 별도의 미들웨어를 정의하고 해당 미들웨어에서 이를 관리하도록 하였다. 그러나 저장 데이터 측면에서 별도의 보안 서비스를 제공하지 않아 저장 데이터에 대한 안전성을 보장할 수 없다.
- 접근제어: 모든 데이터에 대한 별도의 접근 제어 서비스를 통해 사용자의 접근 제어를 제공해야 하지만 본 방식에서는 별도의 접근 제어 방식을 제공하지 않는다.
- 관리의 효율성: 각각의 보안 서비스를 위해 해당 보안 서비스별 미들웨어를 필요로 함으로써 부가적인 미들웨어 증가로 인해 내부 통신의 증가와 이를 통합적으로 관리해야 하는 취약성을 내포하고 있다.

3.2 Ross 방식

본 논문은 2008년 Ross 외 2명이 제안한 방식으로 홈 네트워크 환경에서 안전한 통신을 통해 헬스케어 서비스를 디바이스를 통해 제공받는다. 사용자는 홈 네트워크 환경에서 사용자의 개인 디바이스의 근거리 무선 통신을 통해 헬스케어 정보를 제공받고 사용자의 헬스케어 정보는 외부 공개 네트워크를 통해 헬스케어 센터에 제공된다. 따라서 각각의 근거리 무선통신 기술에 대한 안전성과 사용자 정보의 전송시 안전한 통신 과정을 제한함으로써 홈 네트워크 환경에서의 안전하고 효율적인 헬스케어 서비스를 제공하는 방식이다[5]. 그러나 본 방식의 경우 다음과 같은 취약성이 있다.

- 통신상의 안전성: Ross방식은 근거리 무선통신을 기반으로 홈 네트워크 환경에서의 안전성을 제공하는 헬스케어 서비스를 제공하고자 하였다. 그러나 기존의 근거리 무선 통신 기술의 보완 사항 없이 그대로를 적용함으로써 기존 근거리 무선 통신의 취약성을 그대로 내포하고 있다.
- 데이터의 안전성 (저장 데이터, 전송 데이터): 전송 데이터의 경우 블루투스의 자체 보안 서비스나 WEP를 이용하였다. 그러나 블루투스 자체 보안 서비스와 WEP의 경우 전송 데이터의 안전성 및 저장 데이터에 대한 보안 취약성을 내포하고 있어 본 방식에서는 데이터의 안전성을 보장하지 못한다.
- 사용자 프라이버시 보호: Ross방식에서는 멀티레이어 보안을 제시하였다. 이는 다수의 근거리 무선 통신 보안 기술을 구조적인 측면에서 제공함으로써 사용자의 프라이버시 보호 하고자 하였다. 그러나 해당 사용자의 프라이버시 정보가 전송될 때 공격자로부터 안전성을 보장하기 위한 별도의 방식이 없어 사용자 프라이버시 보호에 대한 문제점을 내포하고 있다.
- 관리의 효율성 : Ross 방식은 내부 네트워크에 대한 안전성 확보를 통해 홈 네트워크 기반의 안전한 헬스케어 시스템을 구축하고자 하였다. 그러나 다양한 근거리 무선 통신 그룹을 멀티 레이어에 적용하기 위해서는 별도의 관리 체계가 요구됨으로서 관리의 효율성이 저하된다.

3.3 보안 요구사항

다음은 안전하고 효율적인 헬스케어 시스템을 구성하기 위한 보안 요구사항을 기술한다.

- 통신상의 안전성: 사용자 중심의 헬스케어 서비스가 제공될 경우 사용자의 프라이버시 정보에 대해서는 개체간의

안전한 상호 인증을 기반으로 전송 데이터의 기밀성과 무결성을 보장해야 한다.

- 데이터의 안전성 (저장 데이터, 전송 데이터): 데이터의 안전성은 통신상의 안전성을 기반으로 저장 데이터의 안전한 저장을 통해 신뢰된 개체에서만 접근이 가능하고 이를 확인할 수 있는 방식이 요구된다.

- 접근제어: 사용자의 프라이버시 정보와 헬스케어 정보가 불법적인 제 3자에 의해 불법적으로 사용되지 않도록 사용자에 대한 접근 제어를 제공하고 이를 통해 안전성을 유지할 수 있도록 해야 한다.

- 사용자 프라이버시 보호: 사용자의 프라이버시 정보가 헬스케어 정보에 활용될 경우 인가된 개체만이 사용자의 프라이버시 정보를 관리해야 한다. 또한 이에 대한 정보가 신뢰된 개체에 의해 안전하게 저장할 수 있는 방법을 제공해야 한다.

- 사용자 모니터링: 다양한 사용자들이 헬스케어 서비스를 이용할 경우 다수의 사용자들을 관리를 위하여 사용자들의 현재 서비스에 대한 별도의 모니터링 방식을 제공해야 한다.

- 관리의 효율성: 헬스케어 서비스는 사용자의 프라이버시 정보를 기반으로 서비스를 제공한다. 따라서 사용자들의 프라이버시 정보와 각 개체를 효율적으로 관리할 수 있는 방식이 요구된다.

4. 제안방식

제안 방식은 의료기관 내의 헬스케어 시스템에서 인가되지 않은 제 3자에 의한 불법적인 접근 제어를 방지하기 위하여 사용자간의 안전한 인증 및 관리 방식에 대해서 제안하고자 한다. (그림 1 참조)

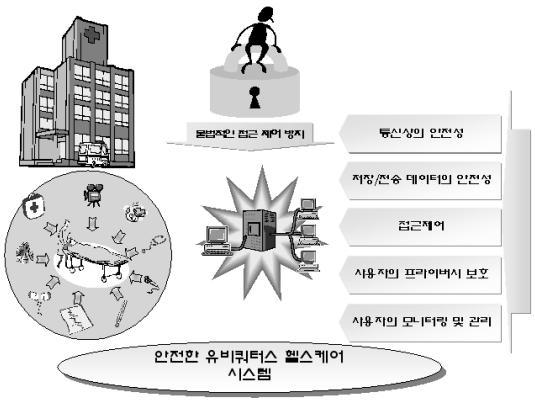

그림 1 불법적인 접근제어 방지를 위한 안전한 헬스케어 시스템

Fig. 1 Prevent Illegal Access Control for Secure Healthcare System

4.1 가정 사항

다음은 안전하고 효율적인 헬스케어 시스템을 구성하기 위한 가정 사항을 기술한다.

- 사용자는 polynomial $P(x)=\sum_{i=0}^{d} a_i x_i$ 를 계산할 수 있으며, 헬스케어 시스템은 x_*를 기반으로 $P(x_*)$를 계산할 수 있다.

- 헬스케어 서버에서 공개한 c_i에 대하여 각각의 서비스에 따라 그룹화된 형태((c_1,c_2,c_3),(c_4,c_5))로 공개된다.

- 사용자와 헬스케어 시스템은 사전에 polymomial $f()$와 차수 d를 공유한다.

4.2 시스템 계수

다음은 안전하고 효율적인 헬스케어 시스템을 구성하기 위한 시스템 계수를 기술한다.

- $r, \alpha_A \in_U Z_n$
- $E()$:안전한 암호 함수
- polymomial $f()$,차수 d
- $[n]$은 집합 $\{1,...,n\}$ 이며, $m=\log_2 |f|$
- c_i:헬스케어 서버에서 설정한 고유값으로 c_i와 m_i는 일대일 매칭된다.
- a_0, n:공개 계수
- $(r_y, v_y + r_{ij})$:세션키 설정을 위한 임의의 키쌍

4.3 기본 이론

다음은 제안방식을 기술하기 위한 기본 이론에 대해서 설명한다.

[Theory 1]

어떤 군 $<G_1,*_1>$, $<G_2,*_2>$, ..., $<G_n,*_n>$이 주어졌을 경우 임의의 두 원소 $a=(a_1,a_2,...,a_n)$, $b=b(b_1,b_2,...,b_n)\in G=\prod_{i=1}^{n} G_i$ 에 대해서, $a*b=(a_1 *_1 b_1, a_2 *_2 b_2,..., a_n *_n b_n)$ 으로써 정의된 연산 $*$은 G위에서 이항 연산이 되며 $<G,*>$은 군을 이룬다.

[Theory 2]

임의의 유한군 $G_1, G_2, ... G_n$이 주어졌을 경우 임의의 원소 $a=(a_1,a_2,...,a_n)\in G=\prod_{i=1}^{n} G_i$ 에 대해서 a의 위수 $|a|$는 각각의 원소 a_i의 위수 $|a_i|$의 최소 공배수와 같다. 따라서 $|a|=lcm\{|a_1|,|a_2|,...,|a_n|\}$이다.

4.4 프로토콜

다음은 안전하고 효율적인 헬스케어 시스템의 사용자 접근제어 시스템을 구성하기 위한 과정이다.

[Step 1] 서비스 기반의 사용자 등록 과정

헬스케어 시스템에 사용자를 안전하게 등록하기 위하여 사용자를 인증하고 사용자의 임시적인 ID를 확인하는 과정이다.

① 헬스케어 서버는 랜덤하게 선택한 $\alpha_A \in_U Z_n$을 생성하여 c_i를 계산한 뒤 사용자들에게 이를 브로드 캐스팅한다.

$$c_i = m_i^{\alpha_A} \bmod n$$

② 사용자는 헬스케어 시스템에서 브로드 캐스팅된 서비스 중에서 사용자가 제공받고자 하는 서비스(c_1을 제공받고자 할 경우)를 위하여 임의의 서비스(c_2, c_3)를 기반으로 다음을 계산하여 헬스케어 시스템에 l_1, t_{s_1}을 전송한다.

$$C_1 = c_1 \oplus m_1 \oplus ID_{s_1}, b_1 = c_2 * c_3 * r_{s_1}, l_1 = C_1^{b_1} \bmod n$$

③ 헬스케어 시스템은 사용자로부터 전송된 l_1을 임시 저장한 뒤 사용자의 임시 비밀 정보인 u_1, l_{hs}를 계산하고 랜덤 수 r_{hs}를 선택한 후 l_{hs}, l_{hs_1}, t_{ls}를 사용자에 전송한다.

$$u_1 = c_1 * c_2 * c_3, l_{hs} = l_1^{u_1^{-1}} \bmod n, l_{hs_1} = l_{hs}^{r_{hs}} \bmod n$$

④ 사용자는 헬스케어 시스템으로부터 전송된 l_{hs}에 대한 검증 과정을 수행하고 다음을 계산하여 헬스케어 서비스에 m_1, l_1'을 전송한다.

$$V_{u_1} = C_1^{(b_1^{-1} * r_{s_1})} \bmod n = C_1^{r_{s_1} * c_1^{-1}} \bmod n = l_{hs} \bmod n$$

$$l_1' = l_{hs_1}^{r_{s_1}^{-1}} \bmod n$$

⑤ 헬스케어 시스템은 사용자로부터 전송된 l_1'을 검증하고 검증이 올바른 경우 사용자가 요구하는 서비스에 대한 임시 비밀정보 y_u를 다음과 같이 계산하여 저장한다.

$$l_1'^{r_{hs}^{-1}} \bmod n = C_1^{c_1^{-1}} \bmod n$$

$$y_{u_1} = (l_1')^{\alpha_A} \bmod n$$

[Step 2] 헬스케어 시스템과의 상호 통신

헬스케어 시스템과 사용자는 Chang's OP_1^2 (1-out-2분실통신로)를 이용하여 안전한 통신 과정을 수행한다.

① 헬스케어 시스템은 사용자와의 암호 통신을 위한 세션키 쌍인 $(r_y, v_y + r_{ij})$와 랜덤하게 선택한 r_y를 전송한다.

② 사용자는 $P(x_* + r)$을 계산하여 헬스케어 시스템에 전송한 후 사용자는 $P(x)$의 계수인 a_i를 공개한 뒤 다음을 계산한다.

$$P(x) = \sum_{i=0}^{d} a_i x_i, \quad a_i = \sum_{j \in [m]} a_{ij} 2^{j-1}$$

③ 헬스케어 시스템은 $v_{ij} = 2^{j-1} x_*^i$일 때 $i \in \lceil d \rceil$이며, $j \in \lceil m \rceil$임을 확인한다.

④ 사용자는 OP_1^2를 $i * j$번을 반복 수행한 뒤 $(r_y, v_y + r_{ij})$인지 또는 $a_{ij} = 0$인지 혹은 $v_{ij} + r_{ij} = 0$인지를 확인한 뒤 사용자는 a_0와 $(r_y, v_y + r_{ij})$를 계산하여 $a_0 + \sum_{d*m} (r_{ij} \mid v_{ij} + r_{ij})$을 헬스케어 시스템에 전송한다.

⑤ 헬스케어 시스템은 $P(x_*)$를 계산하여 이를 증명한다.

$$P(x_*) = a_0 + \sum_{d*m} (r_{ij} \mid v_{ij} + r_{ij}) - \sum_{i,j} r_{ij}$$

⑥ 헬스케어 시스템과 사용자는 다음을 계산하여 세션키를 생성한다.

$$Sk_{temp} = (y_{u_1} \oplus a_0 + \sum_{d*m} (r_{ij} \mid v_{ij} + r_{ij})) \bmod n$$

[Step 3] 사용자의 권한 정보 설정

다음은 사용자가 요구하는 서비스에 따라 권한 정보를 설정하는 과정이다.

① 사용자는 c_1에 대한 서비스를 요청한다.

② 헬스케어 서버는 각각의 서비스를 일대일 매칭을 통해 $< G_1, c_1 >, < G_2, c_2 >, ..., < G_n, c_n >$으로 규정한 후 하나의 서비스($c_1$)에 대한 임의의 권한 정보 $a = (a_1, a_2, ..., a_n)$와 사용자의 권한 정보 $b = (b_1, b_2, ..., b_n) \in G = \prod_{i=1}^{n} G_i$를 생성한 뒤 사용자에 $a = (a_1, a_2, ..., a_n)$를 다음과 같이 계산하여 w, t_{hs}를 전송한다.

$$w = E_{Sk_{temp}} (a \| m_1) + h(m_1 \| t_{hs})$$

③ 사용자는 w를 [Step 2]에서 설정한 세션키로 $E_{Sk_{temp}} (a \| m_1)$를 복호화 한 뒤 $h(m_1 \| t_{hs})$를 검증하여 w에 대한 검증을 수행한다. 검증이 올바른 경우 사용자는 서비스에 대한 권한 정보에서 a의 위수 s를 선택한 뒤 다음을 계산하여 w_s, t_s를 헬스케어 서버에 전송한다.

$$w_s = E_{Sk_{temp}}(s \| c_1 \| a_1)$$

④ 헬스케어 서버는 세션키 Sk_{temp}로 w_s를 복호화한 뒤 s, c_1, a_1을 추출한 뒤 사용자가 요구하는 $s = |a| = lcm\{|a_1|, |a_2|, ..., |a_n|\}$이면 사용자가 요구하는 서비스 권한 정보 a_1과 c_1을 일대일 대응하여 저장한다.

[Step 4] 불법적인 접근 차단

다음은 사용자가 요구하는 정보가 [Step 3]에서 설정한 권한 정보와의 비교를 통해 불법적인 접근을 요구할 경우 이를 차단하는 과정이다.

① 불법적인 접근을 요구하는 사용자 u_a는 c_1에 대한 비인가된 사용을 위하여 $a = (a_1, a_2, ..., a_n)'$을 생성한 후 w_s', t_s를 헬스케어 서버에 전송한다.

$$w_s' = E_{Sk_{temp}}(s' \| c_1 \| a_1')$$

② 헬스케어 서버는 w_s'을 세션키 Sk_{temp}로 복호화한 뒤 s', c_1, a_1'을 추출한 뒤 [Step 3]에서 일대일 대응하여 저장한 a_1과 c_1와 비교한다. 비교 결과 c_1의 서비스에 대한 권한정보 $a_1 \neq a_1'$이면 $Sk_{temp} = (y_{u_a} \oplus a_0 + \sum_{d*m}(r_{ij} | v_{ij} + r_{ij})) \bmod n$에서 y_{u_a}를 기반으로 해당 사용자에 대한 정상적인 서비스인 c_i를 확인한다. 따라서 헬스케어 서비스는 c_i를 비인가된 사용자에게 전송하며, 지속적으로 불법적인 접근제어가 이루어질 경우 서비스를 요구하는 사용자의 y_{u_a}와 Sk_{temp}를 삭제하여 초기 사용자 등록 과정 [Step 1]을 재요구한다.

$$y_{u_a} = (l_1')^{\alpha_A} \bmod n$$

5. 제안 방식 분석

다음은 기존의 연구와 비교하여 3장에서 제시한 보안 요구사항을 기반으로 제안 방식을 분석하고자 한다.

5.1 안전성 분석

- 통신상의 안전성: 제안 방식은 사용자 프라이버시 보호를 위하여 불법적인 접근 제어를 제공하는 헬스케어 서비스를 제공하고자 하였다. 통신의 안전성 측면에서 이산 대수 문제를 이용한 명시적인 상호 인증 서비스를 제공하고 전송 데이터에서 안전한 해쉬 함수를 이용한 무결성을 제공한다. 또한 전송 데이터가 각 개체별로 전송되고 수신될 때 세션키를 이용한 암호화 방식과 더불어 이산 대수의 문제를 이용해 불법적인 제 3자로부터 통신의 안전성을 보장하였다.

- 데이터의 안전성 (저장 데이터, 전송 데이터): 전송 데이터의 안전성은 상호 인증을 기반으로 기밀성과 무결성을 제공하였으며, 저장 데이터의 경우 메시지에 대한 고유값 α_A로 비밀값을 생성하고 이를 기반으로 사용자의 비밀 정보 y를 안전하게 저장한다. 또한 OP_1^2 통신을 통해 안전한 상호 세션키를 생성한 후 이를 저장함으로써 저장 데이터의

- 접근제어: 제안 방식에서의 접근 제어는 각각의 서비스를 임의의 권한정보 a와 사용자의 권한 정보 b를 통해 생성하고 이를 세션키로 암호화하여 전송함으로써 사용자가 자신이 서비스 받는 서비스에 대한 권한 정보를 획득하고 이를 이용한다. 불법적인 제 3자에 의한 접근일 경우 세션키 정보에 포함된 a과 a'을 비교하여 권한 정보에 위배할 경우 세션키 Sk_{temp}에 포함된 사용자의 정보를 삭제하여 차단함으로써 불법적인 제 3자에 의한 접근을 방지한다.

- 사용자 프라이버시 보호: 사용자의 프라이버시 정보가 사용될 경우 제안 방식에서는 OP_1^2 통신을 통해 세션키를 생성하고 이를 기반으로 사용자 권한 정보와 서비스에 대한 권한 정보를 암호화하여 전송함으로써 사용자의 프라이버시 보호를 위한 서비스를 제공한다.

- 사용자 모니터링: 현재 사용하는 각각의 헬스케어 서비스에 대하여 $<G_1, c_1>, <G_2, c_2>, ..., <G_n, c_n>$를 매칭시켜 헬스케어 시스템에서 관리함으로써 사용자가 요구하는 서비스를 형태별로 관리할 수 있는 방식이다.

- 관리의 효율성: 각각의 헬스케어 서비스는 초기 상호 인증값을 기반으로 서비스한다. 따라서 헬스케어 서비스 사용자들은 각각의 초기값을 통해 상호 인증과정 이후 세션키를 설립하고 서비스를 제공받음으로써 다수의 사용자를 효율적으로 관리할 수 있는 방식이다.

5.2 효율성 분석

제안방식은 헬스케어 서버와 사용자를 위한 초기 임시 비밀값을 생성하기 위하여 이산대수 방식을 이용하였다. 이산대수 방식은 사용자에서 2회, 헬스케어 서버에서 3회를 수행함으로써 5pass의 사용자 등록 과정을 수행하였다. 따라서 기존의 SHOES 방식에서의 통신 및 프로토콜 횟수(8pass)보다 효율적이다. 또한 상호 통신 과정에서의 Chang's OP_1^2의 경우 프로토콜 계산과 통신 복잡도는 $d*m$ 반복에 기인한다. 즉, $(3*d*m+1)$의 데이터 교환이므로 전체적으로 총 $3*d*m$ Kbits와 $0.18*d*m$ msec의 통신 비용이 소모된다. 따라서 수신자는 전송자에 비해 비교과정으로 인해 $4.63*d*m$ msec의 통신 비용이 소모된다.

이에 송신자와 수신자는 $t*d*m*2*4.63$ msec와 $t*d*m*0.18$ msec가 각각 사용됨으로써 $t*(3*d*m+1)$ 메시지 교환에 따라 $t*d*m*3$ Kbps의 통신 복잡도에 따른 비용이 사용된다.

기존의 SHOES 및 ROSS 방식에서는 헬스케어 시스템에서 요구하는 서비스를 제공하기 위하여 각각의 프레임워크와 추가적인 컴포넌트를 생성하고 생성된 컴포넌트에 다양한 서비스를 제공하였다. 그러나 제안 방식에서는 추가적인 컴포넌트가 없이 안전성과 효율성을 제공함으로써 전체적인 관리의 효율성과 안전성을 제공할 수 있다.

6. 결론 및 향후 연구 방향

최근 유비쿼터스 컴퓨팅 기술을 통한 컨버전스 환경으로 진화하면서 헬스케어 서비스에 대한 연구가 활발히 진행되고 있다. 헬스케어 서비스에서는 사용자의 프라이버시 정보가 제공되고 이를 다양한 서비스 관계자간의 공유를 통해 보안의 취약성이 발생함으로써 개인적 사회적 문제로 대두되고 있다. 따라서 헬스케어 서비스에서 사용자 프라이버시 보호를 위해서는 사용자의 정보가 공유될 때 안전한 서비스를 제공하기 위한 연구가 반드시 요구된다.

따라서 본 논문에서는 기존의 연구와는 차별화된 헬스케어 서비스를 제안하였다. 제안된 방식은 추가적인 개체를 이용하지 않고 기본적인 개체를 기준으로 사용자의 프라이버시 보호 및 관리의 효율성을 갖는 헬스케어 서비스를 제공한다. 따라서 사용자 측면에서는 임시 비밀값에 기반한 사용자 등록 과정을 거쳐 OP_1^2 통신으로 통신의 효율성을 제공하였으며, 사용자와 서비스에 대하여 접근제어 방식을 제공함으로써 불법적인 제 3자에 의한 불법적인 데이터 접근을 차단하도록 하였다.

그러나 본 방식에서는 안전성 향상을 위하여 이산대수 연산을 사용함으로써 개체의 연산 효율성이 저하되며, 많은 헬스케어 서비스가 요구될 경우 헬스케어 시스템에서 정의하고 분류해야 하는 서비스의 종류의 증가함으로써 관리의 비효율성이 증대한다. 따라서 향후 연구 방향으로는 계산의 효율성과 서비스의 종류가 증가에 따른 비효율성을 보완할 수 있는 추가적인 연구가 요구된다.

참 고 문 헌

[1] Velentzas, R., Marsh, A., and Min, G. “Wireless connected home with integrated secure healthcare services for elderly people,” In Proceedings of the 1st international Conference on Pervasive Technologies Related To Assistive Environments, pp1-4, 2008.

[2] Jieun Song; Myungae Chung, "SHOES : Secure Healthcare Oriented Environment Service Model," Biomedical Circuits and Systems Conference, 2006. BioCAS 2006. IEEE , vol., no., pp.89-93, 2006.

[3] Jianguo Zhang; Stahl, J.N.; Huang, H.K.; Xiaoqiang Zhou; Lou, S.L.; Song, K.S., "Real-time teleconsultation with high-resolution and large-volume medical images for collaborative healthcare," Information Technology in Biomedicine, IEEE Transactions on , vol.4, no.2, pp.178-185, 2000.

[4] Won Jay Song; Son, S.H.; Munkee Choi; Minho Kang, "Privacy and security control architecture for ubiquitous RFID healthcare system in wireless sensor networks," Consumer Electronics, 2006. ICCE '06. 2006 Digest of Technical Papers. International Conference, vol., no., pp. 239-240, 2006.

[5] Velentzas, R., Marsh, A., and Min, G. "Wireless connected home with integrated secure healthcare services for elderly people," In Proceedings of the 1st international Conference on Pervasive Technologies Related To Assistive Environments, pp.1-4, 2008.

[6] 송지은, 김신효, 정명애, “u-헬스케어 서비스에서의 의료정보보호,” 한국정보보호학회, 정보보호학회지 제17권 제1호, pp.47~56, 2007.

감사의 글

본 연구는 2009년도 2단계 두뇌한국(BK) 21 사업에 의하여 지원되었음

저 자 소 개

서 대 희

2003년 순천향대학교 전산학과 졸업(석사)
2006년 순천향대학교 대학원 전산학과 졸업(박사)
2006년~2007년 Howard University Post-Doc
2007년 5월~2007년 12월 한국정보보호진흥원 위촉선임연구원
2008년 7월~2009년 9월 이화여자대학교 컴퓨터공학과 연구교수
2009년 10월~현재 한국전자통신연구원 SW콘텐츠단 지식정보보호부 인프라보호팀 선임연구원
관심분야 : 정보보호, 네트워크 보안, 소형 디바이스 보안, 오버레이 네트워크, 공격자 추적
E-mail : dhseo@etri.re.kr

백 장 미

2003년 순천향대학교 전산학과 졸업(석사)
2006년 순천향대학교 대학원 전산학과 졸업(박사)
2006년~2007년 Howard University Post-Doc
2007~현재 순천향대학교 컴퓨터학부 강사
관심분야 : 임베디드 시스템, 모바일 헬스케어, 지능형 소프트웨어, 지식관리 시스템
E-mail : bjm1453@sch.ac.kr

문 용 혁

2003년 8월: 단국대학교 컴퓨터공학과 공학사
2006년 2월: 한국정보통신대학교(ICU) 컴퓨터공학 석사
2006년 2월 ~ 현재: 한국과학기술원(KAIST) 정보통신공학 박사과정
2006년 4월 ~ 현재: 한국전자통신연구원 지식정보보안연구부 연구원
관심분야 : Cloud/Grid 컴퓨팅, 네트워크 융합보안
E-mail : yhmoon@etri.re.kr

조 동 섭

1981년 서울대학교 전기공학과 졸업(석사)
1986년 서울대학교 컴퓨터공학과 졸업(박사)
1985년- 현재 이화여자대학교 컴퓨터학과 교수
1996-1997년 미국 Univ.of California, Irvine Dept.of ECE Visiting Scholar
관심분야 : 임베디드 보안, 웹서비스 아키텍쳐, 휴먼컴퓨팅, 웹서버 엔지니어링
E-mail : dscho@ewha.ac.kr