유비쿼터스 헬스케어 환경에서 프라이버시 강화 및 데이터 보호를 위한 기술적 고찰

송지은*, 정명애*

*한국전자통신연구원, 정보보호연구단

Technical Guidelines for Enhancing Privacy and Data Protection in u-Healthcare Service Environment

Ji-eun Song*, Myung-ae Chung*

*Division of information security Research, Electronics and Telecommunications Research Institute.

요 약

본 논문에서는 유비쿼터스 헬스케어 서비스의 개념에 대해 간략히 소개하고 서비스를 구성하는 요소에 대해 살펴본다. 또한 유비쿼터스 헬스케어 서비스의 다양한 영역 중 Hospital Information System(HIS) 기반의 헬스케어 서비스를 위한 시스템 기술의 현황과 보안상 문제점을 살펴본다. 특히, 프라이버시 및 데이터 보호와 관련된 보안 이슈를 중점적으로 고려하여 안전한 유비쿼터스 헬스케어 서비스를 보장하기 위해 지원 가능한 기술적 방안들에 대해 기술한다.

I. 서론

유비쿼터스 헬스케어는 유비쿼터스 컴퓨팅 환경을 기반으로 언제 어디서나 의료 서비스를 제공하는 헬스케어 환경을 의미한다. 질병 발생 후에 대응하는 방식의 병원 치료적 기존 패러다임에서 탈피하여 지능적 진단 및 치료 기기를 환자가 휴대하거나 주변 환경에 설치된 의료 장치를 이용하여 일상생활 가운데서 건강을 관리 및 질병을 예방, 신속한 치료 등을 가능하게 하는 서비스이다. 특히, 본 분야는 반도체, 전자, IT, 의료 등 다양한 연구 분야의 융합 및 협력을 토대로 시장 확대 및 기술적 시너지 효과를 촉진 시킬 수 있는 분야로 기대되고 있다.

유비쿼터스 헬스케어 영역은 크게 (1)의료기관 내에서, (2)서로 다른 의료 기관 간, (3) 의료기관과 개인 사이에서 헬스케어 관련 정보 및 서비스를 제공하는 영역으로 나누어진다[1]. 유비쿼터스 기술을 헬스케어 영역에 적용하여 새로운 비즈니스 모델을 제공하는 것이 유비쿼터스 헬스케어 서비스의 기본 틀이라 할 수 있겠다. 본 논문은 의료 기관 및 의료 기관 간의 헬스케어 서비스 영역을 중점으로 의료 정보화 서비스에서 발생 가능한 보안상 취약점 및 고려사항에 대해 살펴본다. 환자 신상 정보 및 개인 진료 정보, 의료 기기 및 의료 연구 데이터 등 의료 기관은 다양한 의료정보를 보유 및 공유한다. 또한, 각 정보는 의료기관의 경제적, 기술적, 연구적 자산과 밀접한 관련이 있으며 개인 신상 정보의 경우 불법적으로 노출 및 악용될 경우 개인에게 큰 피해를 초래할 수 있다. 온라인상에서 개인 신상 정보 도용 및 매매 등으로 인해 최근 피해 사례가 급증하고 정부 차원에서 이를 범죄 행위로 간주, 법적 제제 조취를 취하는 것은 프라이버시 보호의 중요성을 잘 나타내주는 예이다. 유비쿼터스 헬스케어 분야가 안정적으로 실현 및 활발히 성장하기 위해서는 환자 개인 및 의료 기관이 이와 같은 보안적 위협으로부터 안전을 보장 받을 수 있

어야 한다. 특히, 다른 유비쿼터스 정보화 서비스 영역과 달리, 생성 및 공유되는 정보들이 환자의 질병 및 생명과 관련된 정보들이 대부분이므로 데이터의 보호 및 무결성 보장, 불법적 액세스 방지 등은 의료 서비스의 신뢰성 및 안전성(Safety) 보장을 위해 반드시 지원되어야 할 기술이다.

따라서 본 논문에서는 의료기관 중심의 유비쿼터스 헬스케어 서비스의 개념 및 구조에 대해 살펴본다. 또한 안전성을 보장하는 헬스케어 서비스를 위한 시스템 기술의 현황과 보안상 문제점을 살펴본다. 프라이버시 및 데이터 보호와 관련된 보안 이슈를 중점적으로 고려하여 안전한 유비쿼터스 헬스케어 서비스를 보장하기 위해 지원 가능한 기술적 방안들에 대해 기술한다.

II. 개인 식별자(Identity)와 프라이버시

네트워크 개인 식별(Identity)이란 사용자가 보유 및 제공한 개인과 관련된 모든 속성 정보를 의미한다. 여기서 속성 정보는 이름, 전화번호, 의료보험카드 번호, 주민번호, 주소, 보호자 정보, 지불 정보 등이 포함된다. 특히, 의료 서비스 영역에서 진료 및 처방 정보, 소속 진료부서 및 담당 의료진. 질병 군 또한 환자의 부분 식별 정보가 될 수 있다. 이와 같은 개인 식별 정보는 환자 개인 정보 데이터베이스에 저장 및 관리될 뿐 아니라 Electronic Medical Record (EMR), OCS(Oder Communication System), PACS(Picture Archiving and Communication System) 등과 같은 전자 디지털 형태로 전송 및 공유 되고 있다. 이와 같은 개인의 디지털 부분 식별자(Partial Identity) 정보는 신속하고 민감성 높은 (Sensitive) 의료 서비스를 실현하는 데 중요 기술이 되었다.

그러나 이와 같이 유비쿼터스 헬스케어 서비스 분야에서 다양한 개인 식별자 정보가 생성 및 공유됨에 따라 발생하는 문제들이 존재한다. 현재, 식별자 정보가 의료기관 별로 독자적으로 흩어져 관리되고 있는 상황에서 개인이 네트워크 식별자 정보를 관리하는 데는 어려움이 있다. 특히, 프라이버시 보호 관점에서 식별자 정보의 생성 및 등록, 관리 및 권한 위임, 폐기 등의 생명 주기를 개인이 상황에 따라 관여 및 운용할 수 있어야 한다. 이와 같은 개인 식별자 정보는 개인 인증 및 권한 관리, 더 나아가 경제적 부가가치에 까지 깊숙하게 영향을 미치기 때문이다.

공교롭게도 현 유비쿼터스 헬스케어 서비스 시스템에서는 사용자 프라이버시와 관련 민감한 정보들에 대한 보호 방법이 충분히 고려되고 있지 못하다. 최근 50억 달러를 들여 의료 정보 기술을 도입하기로 한 Health and Human Service(HHS)의 경우도 컴퓨터 암호 관리가 적절히 이루어지지 않고 있고 2중 확인 없이 직원이나 계약인이 정보 관리에 액세스 및 운영 가능 등의 보안상 취약점을 도출하고 이에 대한 피해 가능성에 대해 우려하고 있다.

개인의 프라이버시 보호를 위해 정보 노출 시, 개인 명예 및 안전에 민감한 영향을 미치는 정보 자산을 검토 및 분류하고 다양한 의료 서비스 시나리오 즉, 상황을 반영한 데이터 접근 제어가 이루어져야 한다.

III. 유비쿼터스 헬스케어 서비스

본 장에서는 유비쿼터스 헬스케어 서비스의 개념 및 구조에 대해 살펴본다. 특히, 유비쿼터스 헬스케어의 서비스 영역 중 의료 기관 내 및 의료기관 간의 환경에서의 서비스 네트워크 구조 및 구성 요소를 기술한다. 또한, 아울러 본 환경에서 발생 가능한 보안상 취약점 즉, 정보 자산에 대한 가능한 보안상 공격 등을 살펴본다.

유비쿼터스 헬스케어 서비스 네트워크의 구조 및 구성 시스템은 다음 그림 1과 같다. 유무선 의료 장비 및 센서, RFID 디바이스 등을 이용하여 생체 정보를 인식 및 측정 하는 의료 측정 장비 및 센서 단(Medical Sensor & Device Tier), 측정한 신호 정보의 노이즈 및 중복 신호를 필터링 하고 의료 정보 시스템과 호환 가능하도록 가공하는 미들웨어 단으로 구성된다. 이 때, 미들웨어는 다양한 의료 디바이스를 통합 및 이들과 상호 운용 할 수 있는 독

자적 시스템 형태로 존재 할 수 있으며, 또한 의료 디바이스 위에 탑재된 경량형 미들웨어 형태로 존재할 수도 있다.

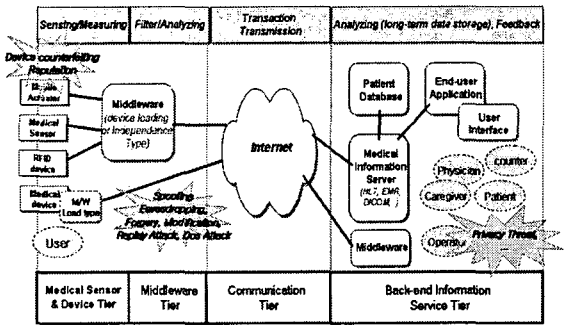

그림 1. 유비쿼터스 헬스케어 서비스 네트워크

이와 같이 측정 및 필터링 된 의료 트랜잭션 정보들은 초고속 인터넷 망, 무선 랜, 이동통신 등의 유무선 인터넷 통신 단(Communication Tier)을 이용하여 뒷단의 의료 정보 서비스 층에 전송된다. 뒷단의 의료 정보 서비스 단은 환자 정보 데이터베이스 스토리지와 EMR, Health-Level(HL7), DICOM 등을 지원하는 Medical Information Syserm (HIS), 사용자 인터페이스 및 응용 서비스 등으로 구성된다. 의료 정보 서비스의 사용자, 다른 표현으로 의료 정보 소비자(Consumer) 들은 진료 의사, 간호사 등의 해당 진료에 직접 관여하는 그룹과 피진료자인 환자 그룹, 의료 행정 서비스 담당자인 수납직원, 보험 담당자, 의료장비 자산 담당자 등으로 구성되는 행정 서비스 그룹, 의료정보 서비스 시스템 관리 및 보완 관리자 등의 관리자(administrator) 그룹, 기타 의료 진료 정보 및 DNA, 유전자, 바이러스 등의 생체 정보 등을 이용하여 임상 연구를 수행하는 의료 연구자 그룹 등으로 구성될 수 있다.

이와 같이 유비쿼터스 의료 서비스는 다양한 구성 시스템 및 시나리오에 따른 다양한 사용자가 존재한다. 그러나 각 동작 단(Tier)마다 위 그림1과 같이 발생 가능한 다양한 보안상 취약점이 산재해 있다. 따라서 원활한 의료 정보 서비스를 보장하기 위하여 각 서비스 네트워크 층에서 보호할 필요성이 있는 정보 자산을 분석하고 시나리오에 따른 적절한 권한 관리가 수행되어야 한다.

IV. 보안 정보 자산에 식별과 정보보호 대안

본 절에서는 유비쿼터스 헬스케어 서비스 환경에서 보호되어야 할 정보 자산 및 발생 가능한 보안상 위협, 이에 대한 보안적 대응을 살펴본다.

개인 프라이버시와 연관 및 안전한 의료 서비스 보장을 위해 보호되어야 할 정보 자산은 정적(Static) 정보와 동적(Dynamic) 정보로 분류될 수 있다. 동적 정보는 유무선 의료 장비를 이용해 생체 신호 및 처방 정보를 획득하는 의료 신호 측정 단과 미들웨어 단에서 주로 발생하며 통신단을 거쳐 전송되는 과정에서 스푸핑, 데이터 도청 및 불법적 변경 등의 공격이 발생할 수 있다. 동적 정보 자산으로는 앞서 언급한 실시간으로 측정된 생체 및 처방 정보, Radio Frequency Identification (RFID) 리더나 무선 액세스 포인트 주소를 이용한 환자 등의 사용자 위치정보, 사용자 개인 물리적 의료 서비스 기기 및 소유물에 관련한 식별 정보 등이 속한다. 또한 정적 정보 자산은 주로 이름, 주소, 주민번호, 의료보험 번호 등을 포함한 개인 신상 정보와 환자의 병력 및 진료 내역 정보, 각 개인의 DNA나 유전자 및 임상 정보 등을 포함한다. 이 정보들은 주로 서비스 네트워크의 뒷단 영역에 존재하며 의료 진료 추이 추적 및 질병 예측, 의학 연구 임상 실험 등에서부터 의료 보험 관리, 진료비 수납, 보험 보장 등의 경제적 비즈니스 영역에 까지 활용될 수 있다. 특히, 이 정보들은 서비스 시나리오 따라 다양한 관계자가 존재한다. 따라서 섬세한 정보 권한 관리는 개인을 프라이버시 침해로 부터 방지하기 위해 반드시 고려되어야 한다. 상황에 따라 개인의 진료 정보라 할지라도 진료자나 보호자 외에 피진료자 그룹의 당사자에겐 노출되어서는 안 되는 정보가 존재 할 수 있으며, 같은 진료자 그룹이라 할지라도 이질적 진료 담당자에게 과거 환자의 모든 질병 이력이 전달되는 것은 불필요 하거나 방지 되어야 하는 경우가 존

재한다. 더 나아가, 단순 연구 목적으로 의료 및 생체 정보가 이용되는 경우, 환자에 의해 동의를 받아야 할 뿐 아니라 즉 연구자 그룹이 데이터와 그 제공자인 환자와의 연관 정보를 절대 갖지 못하도록 해야 한다. 또한 행정 서비스 그룹이나 시스템 관리자 그룹은 최소한의 환자 정보 열람 권한만 부여 받아야 한다.

프라이버시 강화 및 데이터 보호를 위하여 보안상 민감한 정보 자산을 식별하고 발생 가능한 보안상 위협과 정보보호 대안 방법을 살펴보았다. 동적 정보 자산의 기밀성 및 무결성 보장 등은 기본적인 보안 고려사항일 뿐 아니라 위에서 살펴본 바와 같이 정보 자산 소비자 그룹 및 의료 서비스 시나리오 관점에서 권한 관리 및 데이터 접근 제어가 지원되어야 한다.

V.결론

본 논문에서는 의료기관 중심의 유비쿼터스 헬스케어 서비스의 개념 및 구조에 대해 살펴보았다. 또한 해당 서비스 영역에서 생성 및 관리되는 개인 정보와 프라이버시 보호 상충 등의 관련 보안 이슈 등도 검토해보았다. 뿐만 아니라 안전성을 보장하는 헬스케어 서비스 지원에 걸림돌로 작용하고 있는 보안 이슈와 보안상 민감성이 높은 정적, 동적 정보 자산에 대해서도 식별하고 이를 보호 할 수 있는 기술적 가이드라인을 제시하였다. 본 논문이 제안한 프라이버시 보호 및 데이터 보호에 관한 가이드라인은 안전한 의료 정보 서비스를 구축하여 현재보다 더욱 유비쿼터스 헬스케어 서비스 산업이 안정적으로 정착 및 확대 되는 데 기여할 수 있을 것으로 기대된다.

[참고문헌]

[1] 이선희 외, "노인환자를 대상으로 모바일폰을 이용한 u-health 시험 서비스 구축 연구 - 혈당 및 심전도 측정을 중심으로," 대한의료정보학회지, 제 11권, 2005.

[2] Eysenbach G., What is e-health?, Journal of Medical Internet Research, Vol3,No.2, 2001

[3] S.Grizlis, J.Iliadis,D.Spinellis, and S.Katsikas, "Developing secure web-based medical applications." Med.Inform.Internet Med., Vol.24, no.1 pp.75-99,1999.

[4] (1998) A little Net privacy please. Business Week. [online]. Available : http://www.businesswe다.com

[5] ISO/IEC JTC 1/SC27 N4721 "Information technology-security techniques - a framework for identity management. " 2005.

[6] Sebastian C., Dogan K. and Tobias K., "Privacy Enhancing Identity Management: Protection Against Re-Identification and Profiling," DIM'05, Nov., 2005.

[7] M. Bauer and M. Meints (Editors). Structured overview on prototypes and concepts of identity management systems; fidis del. 3.1. available from http: //www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.over%view_on_IMS.pdf.

[8] Gail-Joon A and John Lam, "Managing Privacy Preferences for Federated Identity Management," DIM'05, Nov,. 2005