u-헬스케어(Healthcare) 환경에 따른 의료 정보 보안 이슈

정준호* · 김정숙**

1. 서 론

수년간 이어져온 ICT 기술의 발전은 전통적으로 이를 적극 활용해 온 금융뿐만 아니라 의료영역에서도 큰 영향을 미치고 있다. 각각의 병원들은 종이에 수기로 관리하던 의료관련정보를 디지털화하여 전자의무기록(EMR, Electronic Medical Records)으로 구축하였다. 그리고 더 나아가서 의료정보의 공유 및 활용을 통해 의료 활동을 지원할 수 있도록 도와줄 수 있는 전자건강기록(EHR, Electronic Heath Records)을 기반으로 하는 정보 시스템의 구축 또한 진행하였다.

최근에 이르러서는 인터넷과, 스마트 기기, 그리고 클라우드 서비스의 발전은 언제 어디서나 이용 가능한 예방, 진단, 치료 및 사후관리 등이 가능한 u-헬스케어 환경을 더 이상 SF영화에서나 볼 수 있었던 삶이 아닌 현실의 삶에서 이루어질 수 있도록 도와주고 있다.

삶의 질이 향상됨에 따라 보건의료 서비스가 공급자 중심, 치료 중심의 서비스에서 예방 및 건강증진에 중점을 두는 수요자 중심의 서비스로 변화되고 있다. 이에 다수의 국가에서는 사회경제적 비용감소, 시장규모 증가 등의 경제·산업적 파급효과, 공공의료서비스와 예방 보건 등에 관한 사회·정책적 효과를 기대할 수 있는 효과적인 대안으로써 u-헬스케어에 관한 서비스를 지원할 수 있도록 추진되고 있다.

하지만 이러한 삶의 질적 편의를 도와줄 수 있는 장점에도 불구하고 이와 같은 의료행위를 지원하는데 있어서 발생하는 다양한 의료정보는 개인정보와 병력정보와 같이 프라이버시를 침해할 수 있는 민감한 정보들을 포함하여 보안의 위협으로 다가 올 수 있다.

그러므로, 본 원고는 u-헬스케어 환경에서 발생할 수 있는 의료정보에 관한 보안 요구사항을 살펴보고 이를 해결 할 수 있는 방안에 대해서 논의를 진행하고자 한다.

2. u-헬스케어 의료정보시스템

2.1 의료정보시스템

많은 연구자와 기관에 의해서 u-헬스케어는 다양하게 정의되어 왔다. ICT 기술과 선진의료기술이 결합된 고부가가치 융·복합 산업으로 환자의 생체신호 및 건강정보를 측정하고 유무선 네트워크를 통하여 데이터를 의료기간에 전송한 후 분석

※ 교신저자(Corresponding Author) : 김정숙, 주소 : 경기도 김포시 월곶면 김포대학로 97 김포대학교 본관 210호, 전화: 031-999-4659, FAX: 031-999-4775, E-mail : kimjs@kimpo.ac.kr
* 동국대학교 경주캠퍼스 전자상거래연구소 (E-mail : yanyenli@dongguk.edu)
** 김포대학교 스마트IT학부 스마트콘텐츠과

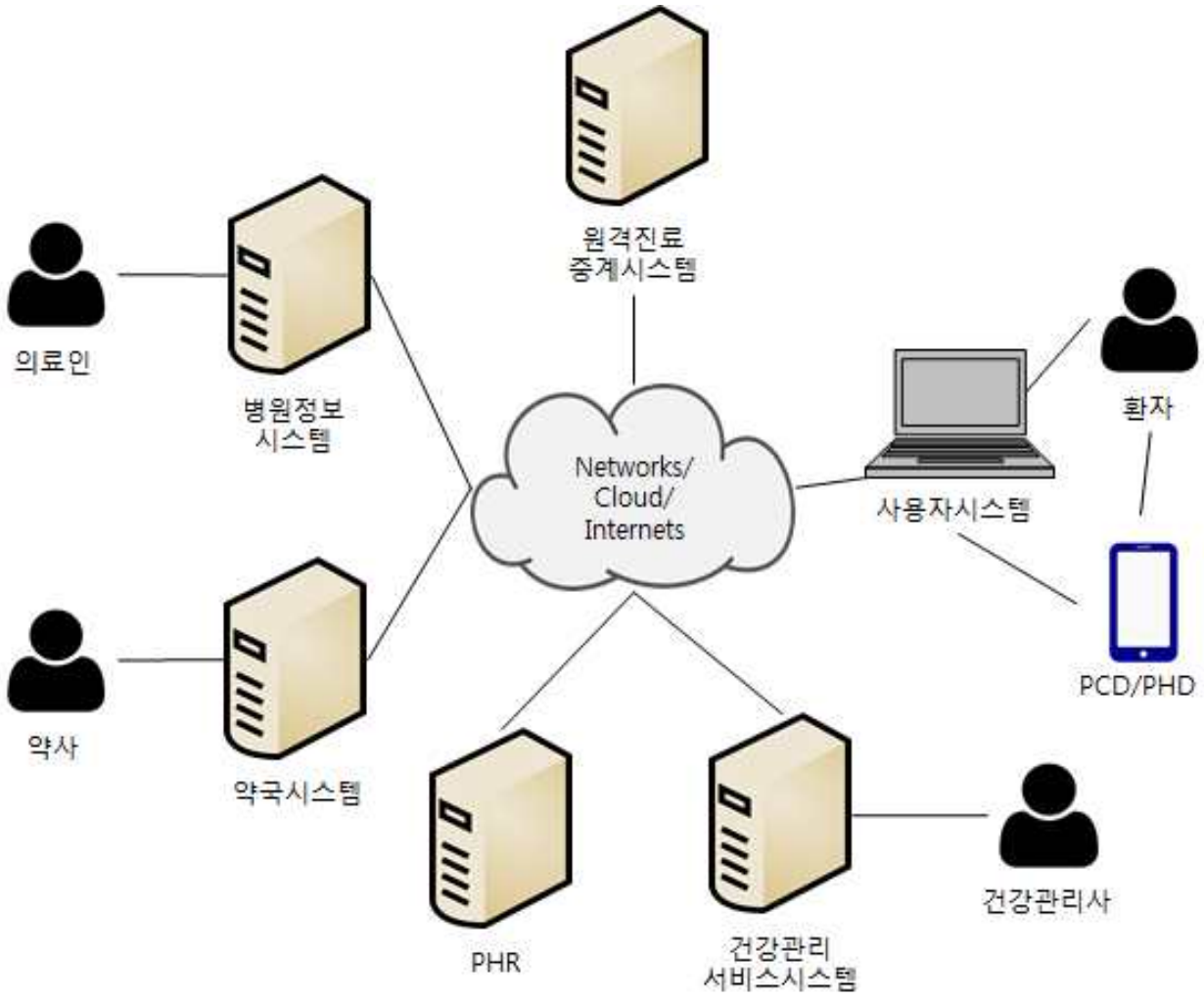

그림 1. 표준기반 R&D 로드맵 스마트의료정보

하고 다시 피드백 해 줌으로써 환자의 질병에 대해서 원격 관리뿐만 아니라 일반인의 건강관리가 가능할 수 있는 서비스로 정의하고 있다[1].

또한, 보건의료 자원 및 서비스 전달과정에 ubiquitous computing의 언제, 어디서나 접속할 수 있고, 언제나 상황을 인식하여, 그에 따른 항시 능동적인 서비스를 제공 가능한 속성이 추가되어 새로이 창출된 예방, 진단, 치료, 사후관리 등의 보건의료서비스를 제공하며 자신의 건강상태가 의료진에게 필요할 때 모니터링 될 수 있어 건강관리의 편의를 제공할 수 있는 의료서비스의 개념이라 할 수 있다.

그림 1은 국가기술 표준원에서 작성한 헬스케어 시스템의 하나인 스마트의료정보에 대한 관계도이다. 병원정보시스템, 약국시스템, 원격진료 중계시스템, 건강관리서비스시스템, 사용자시스템, PHR관리시스템 등이 클라우드 컴퓨팅 서비스와 연동되어 동작할 수 있도록 하고 있다. 각각의 서비스에서 발생하는 대용량 데이터들은 클라우드 스토리지에 저장이 될 것이고, 향후 필요한 정보가 다양한 시스템에 저장이 될 것이다.

이러한 서비스 시스템의 핵심은 대량으로 발생하는 의료정보의 데이터베이스화이다. 이를 통해 체계적인 환자와 질병에 관한 분석 등이 가능해

진 것이다. 하지만 의료업계종사자와 환자들이 의료정보를 바라보는 관점은 상이하다.

의사와 같은 의료업계종사자들의 관점에서 u-헬스케어 환경에서 고려해야할 중요한 사항의 첫 번째는 다른 의료기관들 간의 환자정보 및 의료기술 데이터 통합화를 통한 정보공유 및 협력 방안이다. 즉, 의료정보에 대한 접근권한을 어떻게 처리할 것인가에 대한 것이다. 두 번째는 생체계측 데이터와 같이 대량으로 발생하는 데이터에 대한 효율적인 관리를 위한 정책 및 이를 지원할 수 있는 기술이다. 다른 말로 해서, 클라우드 컴퓨팅을 활용한 빅 데이터를 저장하고 관리하고 분석할 수 있는 방안에 대한 것이라 할 수 있다.

그에 반해서 환자의 관점에서는 본인의 건강기록(PHR, Personal Health Records)을 언제, 어디서든 본인이 확인하고 싶을 때 확인할 수 있어야 하며, 자신의 건강상태를 측정하고 이를 활용할 수 있는 서비스가 제공되길 바라고 있다. 또한 궁극적으로 원격진료를 이용하여 의료서비스 사용의 편리를 도모하고자하는 것이다.

2.2 보안위협

헬스케어 시스템과 같이 의료정보를 공유하고 활용하는 시스템에서 존재할 수 있는 보안위협에 대해서 다양한 연구가 진행되었다[2-3]. 그 중에서도 그림 2와 같이 공격당할 수 있는 희생 대상을 중심으로 보는 방법과 위협의 목적에 따른 방법으로 구분하여 분석할 수 있다[3].

그림 2에서 보듯이 헬스케어 시스템에서의 가장 중대한 보안 위협은 정보 유출과 기기 오작동이다. 정보 유출의 경우 u-헬스케어 환경에서 존재할 수 있는 환자의 건강 정보를 수집하는 각종 센서로부터 직접 유출이 되는 경우, 스마트폰이나 웨어러블 장치와 같이 각종 의료용 기기로부

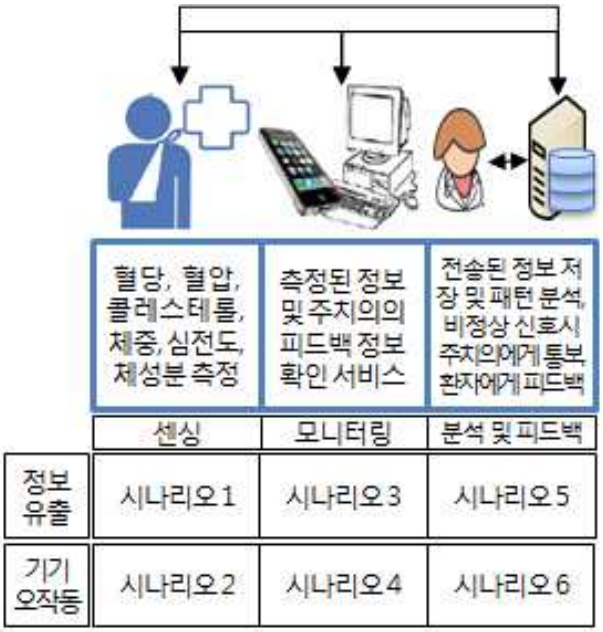

그림 2 헬스케어 시스템의 보안위협에 대한 분류

터 공격을 통해 정보가 유출될 수도 있다. 마지막으로 가장 심각한 사항 중 하나는 의료정보시스템을 공격하여 이로부터 의료정보를 획득하는 경우이며, 대단위의 피해를 발생시킬 수 있는 위험이 있다. 기기 오작동의 경우에 의해서 센싱 장치나 기존 기록된 정보 등을 삭제하거나 잘못된 정보가 기록되는 문제가 생길 수 있다. 각각의 사항이 모두 치명적이지만 u-헬스케어환경에서는 다수의 센싱 장치에서 수집된 정보를 바탕으로 의료가 진행될 수 있는데 센싱 장치가 잘못된 정보를 전달하도록 하여 환자에게 오판된 의료행위를 유도하여 환자의 생명에 치명적인 결과를 초래할 수 있는 위험이 존재한다.

표 1은 국내외 주요 헬스케어 시스템의 보안침해 사례이며 보안 위협에 따른 분류를 수행하였다[3]. 표 1의 결과를 통해 과거에 많이 발생한 의료 정보 보안 위협 사건은 의료정보시스템의 공격이 많음을 알 수 있다. u-헬스케어 환경이 도래함에 따라 더욱 더 많은 정보를 가지고 있는 시스템에 대해서 공격이 예상됨으로 공격에 대응

표 1. 국내외 헬스케어 시스템들의 보안 침해 사고들, S: 위협 시나리오($S \in \{1,2,3,4,5,6\}$)

사건	일시	이유	상세	S
인공 심장박동기/인공심장 해킹 취약성	2008.05.	해킹에 의한 인공심작 오작동	인공심박동기/인공심장을 해킹하여 기기 오작동 가능하다는 연구발표	2
보스턴 BIDMC병원 데이터 유출 - 1	2011.07.	악성코드 감염	2,021명의 환자기록(이름, 성별, 생년월일, 의료기록번호, 방사선 치료 날짜)이 인터넷으로 유출	3/5
The Surgeons of Lake Country 해킹 및 데이터 인질극	2012.06	해커 침입 후 Data Ransom	일리노이 주 의료기관 시스템에 해커 침입 후 데이터를 암호화한 후 패스워드에 대한 대가 요구	6
보스턴 BIDMC병원 데이터 유출 - 2	2012.07	전문의 Laptop 도난	Laptop내 데이터 암호화 부재와 도난으로 인해 3,900명의 환자 기록 탈취	5
생화확 자동분석장치 소프트웨어	2013.01	생화학 자동 분석 장치에 연결된 DB해킹	COBAS ITEGRA 400 plus 분석기에서 사용하는 오라클의 데이터베이스 취약점을 이용하여 원격으로 잘못된 정보를 DB 저장	4
미국 Froedtert 병원 환자 개인정보 유출	2013.02.	바이러스 감염	43,000명의 환자 중 일부의 사회보장번호가 유출	5
네트워크 접속형 의료기기, 모바일기기	2013.06	악성코드 감염	낡은 의료기기의 취약성으로 모니터링 시스템 내 악성코드감염	5
국내 의료뉴스 웹사이트를 통한 악성코드 우포	2013.08.	악성코드 유포	의료용 인증서, 개인용 인증서, EMR인증서 유출	5
대형병원 임상실험센터 웹사이트	2014.04.	해킹 및 악성코드 유포	국내 대형병원 임상실험센터의 웹사이트가 해킹되어 악성코드 유포지로 악용됨	5

할 수 있는 방안에 대한 보안 기술이 필요할 것이다. 또한 과거에는 자주 발생하지는 않았지만 개개인을 위한 다양한 의료지원 기기들이 등장하기에 기기의 잘못된 정보의 전달을 통한 환자의 생명을 위협하는 일이 없도록 하는 기술에 대해서도 고민이 필요할 것이다.

3. u-헬스케어 의료 정보 보안 연구

과거의 사고들을 바탕으로 의료정보의 유출은 의료종사자와 환자 모두에게 치명적인 결과를 초래하므로 수집 및 기록되는 의료 정보를 암호화하는 것은 기본적인 보안 방법이라 할 수 있다.

이렇게 기본적인 암호화를 통해 정보를 관리할 경우 정보의 소유자만 암호화된 정보를 복호화할 수 있게 된다. 이는 의료 행위를 수행하는데 있어서 큰 장애로 나타나게 된다. 왜냐하면 의료행위는 의사 한 사람에 의해서만 행해지는 것이 아니라 의사와 환자뿐만 아니라 제3자, 보험단체, 행정 등 다양한 사람들이 의료 정보에 접근을 필요하기 때문이다. 또한 환자의 주치의가 바뀌는 경우도 존재할 수 있다. 따라서 암호화된 의료정보는 공유되어 활용될 수 있어야 한다.

즉, 암호화된 데이터에 접근할 수 있는 권한의 조정이 쉬운 방법이 있어야 한다는 것이다. 따라서 이와 같이 암호화된 정보에 권한을 조정하기 위한 다양한 연구들이 진행되었다[4-6]. 그 중 Yang 등의 연구는 다중 클라우드 환경에서 CP-ABE(Ciphertext-Policy Attributed-based Encryption)을 활용하여 저장된 데이터의 효과적인 접근권한 부여 및 권한의 폐기에 대해서 다루

었다[6]. 데이터의 접근권한을 부여도 중요하지만 권한이 폐기되었을 때의 효과적인 처리도 매우 중요하다. 데이터에 접근할 수 있는 사람은 항상 올바른 대상이어야 되기 때문이다.

암호화된 의료정보는 안전하고 효과적으로 검색하기 위한 방법이 필요하다. 데이터를 암호화하여 저장하더라도 데이터를 검색하는 키워드가 공격자에게 노출이 된다면 공격자는 유출된 키워드를 바탕으로 환자의 프라이버시를 침해할 수가 있다. 이와 같이 검색하는 키워드가 시스템 내외부에서도 안전하게 검색 가능하도록 하는 검색가능 암호화(Searchable Encryption) 기법에 대해서 다양한 연구가 진행되었다[7-9]. N. Cao 등은 클라우드 환경에서 프라이이버시 침해를 방지하면서 다중 키워드에 대해서 검색할 수 있는 기법에 대해서 연구하였다[9]. 다른 정보와는 다르게 의료정보의 경우 일부의 키워드의 노출만으로도 환자의 프라이버시를 침해할 여지가 많음으로 반드시 키워드 검색에서 부터의 보안도 필요하다.

마지막 의료정보는 공유되고 활용됨으로 악의적인 공격자에 의해서 위·변조 및 훼손이 될 위험이 따른다. 따라서 저장된 데이터에 대해서 주기적인 감사를 시행하여 데이터가 안전하다고 할 수 있다. 따라서 데이터소유입증(Provable Data Possession)과 같이 저장된 데이터의 무결성을 검증하는 다양한 기법에 대해서도 연구가 진행되었다[10-13].

위의 세 가지 보안요소는 의료정보 유출에 대비하는 최소한의 안전장치라 할 수 있으며 이 이외에도 다양한 정책적, 기술적인 보안요소들을 고려하여야만 편의를 위해 사용되는 u-헬스케어가 환자들에게 프라이버시의 노출로 인한 불편을 막아줄 것이다.

4. 결 론

본 원고에서는 u-헬스케어에 대한 정의와 보안 위협을 살펴보고 이를 해결하기 위한 주요 보안 연구 동향에 대해서 살펴보았다. 법과 윤리, 그리고 보안문제를 해결하여 의료종사자와 사용자들 모두에게 편의를 가져다 줄 수 있는 u-헬스케어 시스템이 구축 되어 더욱 건강한 삶을 살 수 있는 환경이 되길 기대해본다.

참 고 문 헌

[1] U. Varshney, “Pervasive Healthcare,“ IEEE Computer, Vol. 36, No. 12, pp.138-140, 2003.

[2] 송유진, 박광용, “의료데이터 공유 및 활용 서비스를 위한 보안/프라이버시 요구사항,” 정보보호학회지, Vol. 20, No. 3, pp. 90-96, 2010.

[3] 이혜림, 조재연, 윤지원, “클라우드 환경에서의 사이버물리시스템관점에서 본 헬스 케어 보안 관련 이슈들,” 한국정보보호학회지, Vol.24, No.6, pp.7-13, 2014.

[4] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems,“ IEEE Transactions on Infromation Forensics and Security, Vol 8, No. 11, 2013.

[5] M. Sharma, Y. Bai, S. Chung, and L. Dai, “Using Risk in Access Control for Cloud-Assisted eHealth,“ IEEE International Conference on High Performance Computing and Communications, pp. 1047-1052, 2012.

[6] K. Yang, X. Jia, “Expressive, Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage,“ IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 7, pp. 1735-1744, 2014.

[7] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, “Public Key Encryption with Keyword Search,” Eurocrypt'04, 2004.

[8]정준호, 홍영식, “클라우드 컴퓨팅 환경에서 검색 가능 암호화 시스템을 위한 전사적 공격에 효과적인 다중 색인 기법,” 정보과학회논문지: 정보통신 Vol.40, No.5, pp.286-293, 2013.

[9] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," IEEE transactions on parallel and distributed systems, Vol.25, No.1, 2014.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” In Proceedings of the 14th ACM conference on Computer and communications security, ACM, pp. 598-609. 2007.

[11] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Transactions on Parallel and Distrubuted Systems, Vol. 22, No. 5, 2011.

[12] S. Tan, Z. Chen and J. Zhang, “Data Blocks’ signature in Cloud Computing,” International Symposium on Computational and Business Intelligence (ISCBI), pp.49-55, 2013.

[13] S. Tan, L. Tan, X. Li, Y. Jia, "An Efficient Method for Checking the Integrity of Data in the Cloud," Journal of China, Vol. 11, No. 9, pp.68-81, 2014.

정 준 호

• 2009년 동국대학교, 컴퓨터공학과, 공학석사
• 2015년 동국대학교, 컴퓨터공학과, 공학박사
• 현 재 동국대학교 경주캠퍼스 전자상거래 연구소, 연구초빙교수
• 관심분야: 핀테크 보안, 클라우드 및 네트워크 보안

김 정 숙

• 1993년 : 동국대학교 컴퓨터공학과 공학사
• 1995년 : 동국대학교 대학원 컴퓨터공학과 공학석사
• 1999년 : 동국대학교 대학원 컴퓨터공학과 공학박사
• 2000년～현재 : 김포대학교 스마트IT학부 교수
• 2005년～현재 : 한국멀티미디어학회 이사

• 관심분야 : IT융합, 상황인지, 인공지능, 유전 및 분산 알고리즘

Phone : +82-31-999-4659
E-mail : kimjs@kimpo.ac.kr