https://doi.org/10.33778/kcsa.2019.19.3.029

의료 ICT융합 환경에서 안전한 사용자 관리를 위한 인증시스템 설계 및 구현: 중소형 의료기관을 중심으로★

김 양 훈*, 최 연 정**

요 약

전통적인 산업과 ICT의 융합은 ICT에서 나타나는 보안 위협 및 취약점과 기존 산업의 특수한 산업 종속적인 문제점이 혼합되어 새로운 보안위협 및 취약점이 나타나고 있다. 특히, 의료ICT융합산업에서는 의료정보시스템을 중심으로 사용자 인증에 대한 다양한 문제가 파생되어, 오남용, 보안취약점에 악용되고 있는 실정이다. 이에 따라, 본 연구에서는 의료 ICT 융합환경에서 안전한 사용자 관리를 위한 사용자 인증시스템을 설계하고 프로토타입을 구현하였다. 구체적으로, 의료정보시스템을 중심으로 개인화 기기를 활용하여 사용자 인증을 수행함으로써 ID 공유로 나타나는 오남용과 보안 취약점을 해결하고, 개별 ID/PW 방식 인증의 불편함을 해소하기 위한 방안을 설계 및 프로타입을 구현하였다.

Design and Implement of Authentication System for Secure User Management for Secure on Medical ICT Convergence Environment

Yanghoon Kim*, Yean Jung Choi**

ABSTRACT

The convergence of traditional industry and ICT is a combination of security threats and vulnerabilities in ICT and specific industry-specific problems of existing industries, and new security threats and vulnerabilities are emerging. In particular, in the medical ICT convergence industry, various problems regarding user authentication are derived from the medical information system, which is being used for abuse and security weaknesses. According, this study designed and implemented a user authentication system for secure user management in medical ICT convergence environment. Specifically, we design and implement measures to solve the abuse and security weaknesses of ID sharing and to solve the inconvenience of individual ID / PW authentication by performing user authentication using personalized devices based on medical information systems.

Key words : Convergence Security, ICT Convergence Environment, Hospital Security, Fast IDentity Online System, User Authentication System

접수일(2019년 8월 26일), 수정일(1차: 2019년 9월 21일), 게재확정일(2019년 9월 26일)

★이 성과는 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (No. NRF-2018R1C1B5046760).

* 극동대학교 산업보안학과, 제1저자
** 극동대학교 식품영양학과, 교신저자

1. 서 론

사물인터넷, 빅데이터, 인공지능 등의 신기술을 기반으로 4차 산업혁명이 진행됨에 따라 개별적으로 ICT를 활용하는 각종 산업들은 ICT 융합 생태계로 확장되고 있다. 이러한 4차 산업혁명은 실시간으로 저장되는 대량의 데이터를 응용하고 분석하여 가치창출을 이뤄내고 있다[11].

이와 같은 환경의 변화와 함께 의료산업의 ICT 활용에 대한 수요가 높아지고 있다. 이로인한 의료 ICT융합 기술은 빠르게 고령화되고 있는 국내의 실정에서 다양한 문제해결에 응용될 수 있을것으로 기대되고 있다. 특히, 고령화에 따른 급격한 의료서비스의 수요 증가와 이로 인한 의료비용의 급증, 환자의 삶의 질 저하, 전문 의료진의 부족현상 심화 등 다양한 문제에 대하여 의료 ICT융합 기술은 효율적인 의료서비스를 제공하여 이러한 문제들을 해결할 수 있다[3].

한편, 전통적으로 의료정보의 기록은 ICT 활용에 따라 EMR(Electronic Medical Record)과 같은 시스템으로 전환되었다. 이러한 ICT 시스템 중심의 환경의 변화로 이용자는 원격 진료나 웨어러블 디바이스를 활용한 헬스케어와 같은 환자들의 진료 편의성을 높이는 서비스를 제공받을 수 있게 되었으며 의료기관 중심이었던 보건의료의 패러다임이 이용자 중심으로 바뀌게 되었다[5].

의료 ICT융합 환경에서 디지털화된 의료정보는 환자의 개인정보, 민감정보를 의료기관 뿐만 아니라 공공기관 및 보험회사와 네트워크를 통하여 공유하고 있으며, 일부 진료협진을 위한 정보공유도 이루어지고 있는 상황이다. 이에 따라, 의료정보의 유출은 환자의 일반 정보, 신체/건강 정보, 금융정보 등의 조합을 통하여 새로운 추가 피해로 이루어질 수 있다. 그러나, 의료기관, 특히 중소 의료기관에서는 ICT 시스템은 단순 활용의 대상으로 간주하는 성격이 있기 때문에 개인정보보호에 대한 관심 외에 보안 수준은 미흡한 상황이다[4,5,12]. 이에 따라, 의료인들의 로그인 등 관리정보 공유를 통한 환자정보의 유출의 인증 문제, 외부 정보의 오남용으로 인한 랜섬웨어 감염의 외부 네트워크 연결문제, 개인정보 관리 미흡으로 인한 유출의 관리적 문제 등으로 다양한 보안사고가 일어나고 있다.

공공웹사이트 등에서는 공인인증서 등을 활용한 다양한 인증방법을 이미 활용하고 있으며, 의료서비스환경에서 사용자의 인증을 강화하기 위한 다양한 방법에 대한 연구가 꾸준히 진행중에 있다. 특히, 전통적인 ID/PW 방식에서부터 PW 기반의 사설인증서, 공인인증서를 활용한 공개키 기반 인증방식 등을 활용중에 있다. 또한, 사용자의 인증 뿐만아니라 권한관리까지 통합적으로 수행할 수 있는 기술과 이에 동반되는 인증 기술의 신뢰성 향상과 속도를 담보할 수 있는 기술에 대한 연구가 꾸준이 진행중에 있다.

그럼에도 불구하고, 중소형 의료기관에서는 초기에 도입한 ICT 시스템을 기반으로 구성되어 있으며, 다양한 의료ICT 시스템에서 활용되는 ID/PW 방식 인증 시스템은 단순 공유로 인한 유출 가능성이 있으며, 중소규모 의료기관에서 인증서 등으로 대체하기에는 불편함이 있는 상황이다. 이러한 보안사고는 중소형 의료기관의 물적, 인적자원의 한계에 기인한다.

이에 따라, 본 연구에서는 의료 ICT융합 환경에서 중소형 의료기관을 중심으로 안전한 사용자 관리를 위한 인증시스템을 설계하고 프로토타입을 구현하고자 한다. 구체적으로 기존의 ID/PW 방식에서 개인화 기기를 활용한 인증방식을 설계하고 구현하고자 한다.

2. 선행 연구

2.1 중소형 의료기관 및 정보시스템 현황

통계청에 따르면, 소규모 병의원, 중규모 병원, 상급종합병원을 포함하여 치과, 한의원, 약국 등 국내의 의료기관은 고시 최종년도인 2017년 현재 91,545개로 나타났다. 그중 1차기관으로 분류되는 의원, 치과의원, 보건진료소 등의 중소형 의료기관

은 65,926개로 약 72%에 해당하는 것으로 나타났다.

대표적인 의료기관의 정보시스템은 표 1과 같으며, 중소형 의료기관일수록 정보시스템에 대한 활용성이 최소화되고 EMR을 중심으로 기능이 재편된다. 이러한 데이터 저장, 유통, 관리의 핵심이라 할 수 있는 EMR의 도입률은 상급종합병원의 경우에는 90%를 초과하고 있으며, 소규모 의원은 67.8%에 그쳐 중소형 의료기관의 ICT 활용이 아직도 미흡한 형태로 나타났다[7].

이러한 현황을 기반으로 의료융합환경에서 의료서비스의 패러다임이 진료 중심에서 질병의 사전예방 및 관리체계로 변화하고 있으며, 이에 따라 개인의 효율적인 건강관리를 위한 의료정보 활용의 중요성이 증가하고 있다[2]. 일부 도서 산간 지역 등 의료접근성이 어려운 곳을 포함하여 국민의 만성질환 및 건강관리를 위하여 병원 외부에서 혈압계, 체중계, 혈당계, 체성분계 등의 개인건강정보기기(PHD, Personal Health Device)를 활용한 정보수집체계를 갖추고 있다[4].

2.2 의료 ICT 보안기술

의료기관의 ICT 환경은 외부와 연결된 일부 개방형 구조를 갖고 있기 때문에 개방형 및 폐쇠형 구조를 함께 갖추고 있다. 의료기관에서 활용되는 대다수의 데이터는 개인정보보호법 및 의료법으로 인하여 개인정보와 민감정보로 분류되어 외부로 공개되지 않는다. 반면에 외부로는 개인의 의료수가 산정에 따른 다양한 진료비 청구심사 절차를 진행하기 위하여 건강보험심사평가원과 정보를 공유하며, 필요에 의해 내부 실험을 위한 식별 데이터 삭제 후 정보활용을 진행하고 있다. 또한, 진료용 PC가 외부 네트워크와 연결되어 진료의 참고자료 검색 등에 활용되고 있다. 이러한 내부, 공공기관·보험사를 포함한 정당한 제3자들의 의료정보 활용은 의료 ICT 보안에 다양한 취약점을 제공한다.

전통적인 기술적 방식으로는 기본적인 의료환경에 대한 보안위협을 의료기기 하드웨어, 상용 OS, 의료기기 관리 및 제어, 의료 게이트웨이, 의료기관 네트워크에 대한 보안 위협으로 나누고, 의료정보시스템에 대한 보안 위협은 계정 및 패스워드, 접근통제, 취약한 설정 및 비인가 프로그램 사용, 취약한 소프트웨어 사용으로 구분하였다.

<표 1> 의료기관 정보시스템 종류와 개념정리

병원 정보시스템	개념
전자의무기록시스템EMR(Electronic Medical Record)	기존에 종이차트에 기록했던 인적사항 ,병력, 건강상태, 진찰, 입/퇴원기록 등 환자의 모든 정보를 전산화하여 입력, 관리, 저장하는 정보시스템
처방전달시스템(OCS: Order Communication System)	의사의 처방을 인력이나 수동적인 방법에 의존하지 않고 컴퓨터를 이용해 신속, 정확하게 진료 지원부서에게 전달하는 시스템
의료영상 저장전송시스템(PACS : Picture Archiving and Communication System)	디지털 의료영상이미지를 DICOM(Digital Imaging and Communications in Medicine)이라는 국제표준규약에 맞게 저장·가공·전송하는 시스템. CT,MRI 같은 디지털의료영상 장비를 사용하여 획득된 의료영상이미지는 DICOM형식으로 저장되게 되며 판독결과와 진료기록이 추가될 수 있음. 또한 네트워크를 통해서 병원내,외의 단말로 전송이 가능하다.
임상병리정보시스템(LIS : Laboratory Information System)	병원에서 진단 후 처방된 자료가 검사 장비와 연동되어, 자동으로 검사항목 및 결과와 문제 상황이 입력되고 통보되는 시스템을 말함. 이는 병원 각 검사실과 진료과에 구축되어 있는 네트워크가 핵심인데, 환자의 문제를 직접 진단하거나 검사하지는 않지만 치료에 참여하는 진료과들에 유용한 시스템

이에 따라, 전통적인 기술적 보안요구사항을 사용자 접근 통제 및 인증, 패스워트 및 암호화키 관리 등을 포함하여 14가지로 도출하고 의료환경에 적합하게 표 2의 우측과 같이 대응방안을 설계하였다[13]

한편 프로세스 중심으로 재분석한 연구에서는 의료정보의 생애주기를 중심으로 융합환경을 분석하여 취약점과 보안 요구사항을 도출하였다. 구체적으로 의료기관에서 활용하는 의료정보의 의료정보의 생성(수집), 저장, 활용(내부유통과 외부제공)~폐기과정에 따른 융합보안 취약점을 분석하여 구체적인 5대 대응기술을 표 2의 우측과 같이 설계하였다[5, 12].

2.3 인증

인증이란, 참이라는 근거가 있는 무언가를 확인하거나 확증하는 행위로써, 인증대상이 사람인 경우 사용자 인증, 디바이스와 같은 경우 기기인증이라고 한다. 인증은 지식 기반 인증, 소유 기반 인증, 생체 기반 인증으로 분류되며, 이와같은 개념을 기반으로 현대에는 Usable Security 인증 기술, 행위 기반 인증 기술, FIDO(Fast IDentity Online) 기술 등이 활용되고 있다[1].

FIDO 기술 규격은 온라인 환경에서 생체인식 기술을 활용한 인증방식에 대한 개방형 기술표준으로서, 안전한 사용자 인증을 위해 사용자의 디바이스에서 제공하는 보안 기능을 활용하고, 사용자가 암호, 인증서 등을 생성하고 외우는데서 발생하는 불편함을 해소하고자 FIDO Alliance에서 개발하였다. FIDO 기술 규격은 크게 두 가지 방식으로 나뉘는데, 지문 및 음성, 얼굴인식 등 생체정보에 기반한 사용자 인증 과정에 활용되는 표준인 UAF(Universal Authentication Framework) 방식과, 기존 ID/Password 인증 방식 및 추가의 보안 정보를 보관하는 USB(Universal Serial Bus) 방식, 스마트카드 등 별도의 인증 장치를 사용하는 U2F(Universal Second Factor) 방식으로 구분된다[9].

<표 2> 선행 의료 ICT 보안기술 정리

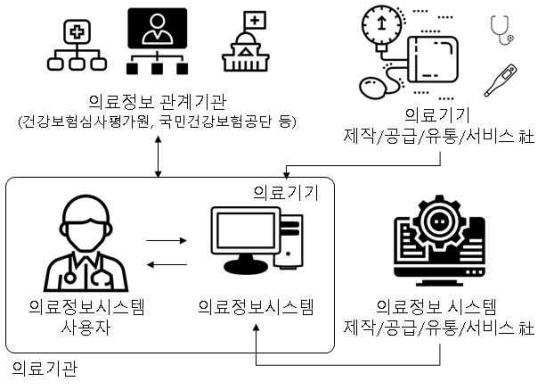
구성 단계	보안위협	보안 요구사항	의료정보 생애주기	보안취약점	보안 요구사항
의료기기	데이터 유출 악성코드 감염 기기오작동 비인가 접근	사용자 접근 통제 및 인증 패스워드 및 암호화 키 관리 의료기기 임베디드 보안 데이터 보호 게이트웨이 보안 악성코드 감염방지 이동식 저장매체 보안 소프트웨어 보안패치 시큐어 코딩 네트워크 보안 무선 네트워크 보안 망분리 의료기기 보안성 검토 감사로그 기록 및 관리	생성	의료정보 활용동의 고의누락 시스템 해킹 용도 외 사용	통합보안기술 -사용자인증 -계정 및 권한 관리 -의료기기 인증 -개인정보 보호 비식별화 기술 -의료정보 상호 호환성 및 보호 -의료정보 무결성 보장 보안게이트웨이 -다양한 통신보안 의료기기 악성코드 방역
게이트웨이	악성코드 감염 서비스 마비 데이터 유출 중간자 공격		저장	로그기록 누락 암호화 누락	
네트워크	데이터 유출 서비스 마비 비인가 접근 데이터 무단조작		활용	의료정보 불법제공 의료정보 위변조 인가된 제3자 유출 접근 모니터링 미흡 과도한 접근권한 부여	
의료 정보시스템	데이터 유출 취약한 설정/패스워드 관리 악성코드 감염 취약한 버전의 SW 사용		폐기	외부기관/개인 의료정보 임의제공 의료정보 미파기	

3. 의료ICT융합환경 안전한 인증방법

3.1 의료 ICT융합환경 안전한 인증방법 설계

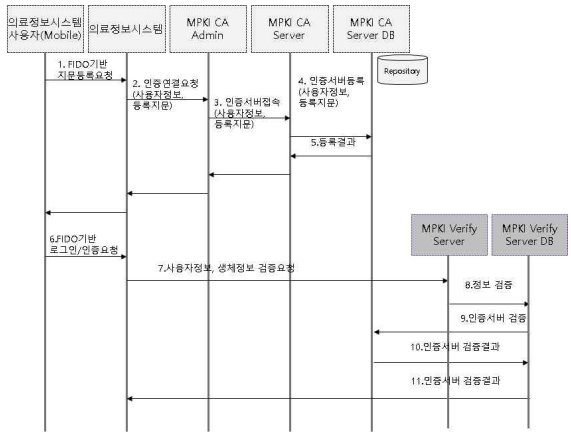
본 연구의 목적은 의료 ICT 융합환경에서 중소형 규모의 의료기관이 자원적 한계로 인하여 의료정보관리의 시작이 되는 인증시스템에 대한 구축이 어렵기 때문에 한정적인 환경에서 관련 시스템을 설계하고 프로토타입을 구현하여 소규모 시스템의 즉시도입과 연계의 가능성을 확인하는데 있다.

의료 ICT 융합환경에서 중소형 의료기관 의료정보시스템의 보안성 향상을 위한 안전한 인증방법을 설계하기 위하여 대상 식별을 위한 기본적인 의료기관의 구조를 선행연구를 기반으로 추상화시키면 그림 1과 같다. 그림 1의 구조는 본 연구를 위하여 기본적으로 ICT와 연계되는 구조만으로 한정지었기 때문에, 제약과 관련되거나 외부 처방전달과 관련된 많은 부분은 생략하였다.



(그림 1) 의료정보시스템 중심 의료기관 구조도

의료정보시스템을 중심으로 의사, 간호사 등의 의료인은 사용자 및 관리자로 구분된다. 의료기관의 정보는 외부 의료정보 관계기관에 정보를 공유한다. 그리고, 의료정보시스템에 대한 기본적인 구조, 정보, 내용을 제작·공급·유통·서비스를 수행하는 의료정보시스템 제작사가 있다. 마지막으로 ICT와 융합된 건강관리 및 진료에 활용되는 의료기기 제작사가 식별된다. 이와 같은 관계자들은 의료정보시스템을 중심으로 정보를 입력·저장하고, 관리하는 등의 구조를 갖는다.



(그림 2) 안전한 인증 시퀀스 다이어그램

이러한 의료정보시스템 중심 의료기관 구조도를 기반으로 한단계 상세하게 들어가 의료정보시스템 사용자와 의료정보시스템, 그리고 외부관계사를 핵심 식별자로 하여 본 연구에서 제안하는 의료 ICT 융합환경에서 안전한 인증을 위한 방법의 시퀀스 다이어그램을 설계하면 그림 2와 같다.

스마트 폰 등의 모바일로 간주될 수 있는 개인화기기가 있고, 인증서버와 외부연결 또는 자체 서버운영에 따른 연결을 전제로 구성하였다.

개인에게 보급되어있는 스마트폰을 FIDO를 활용한 의료정보시스템 인증의 기본 단말로 설정하고, 해당 의료정보시스템과 인증을 하기 위한 인증서버 관리자 MPKI Admin, 인증서버 MPKI CA Server, 실제 인증코드 관리를 위한 MPKI CA Server DB의 형태로 논리적 분할 설계를 하였다.

각 대표번호에서 상세하게 발생하는 데이터 전이의 내용은 다음 표3과 같다. 상세하게는 의료정보시스템 사용자가 모바일을 위한 인증정보 등록과정과 의료정보시스템을 활용시에 인증하는 과정에 대한 시퀀스이다. 기본적으로 FIDO 기반의 인증 프로세스를 갖추고, 개인화기기(Mobile)의 지문인식 기능과 모바일 인증서를 활용하여 최초 사용자 정보를 등록한다. 의료정보시스템에서 정보에 대한 확인, 진료정보 저장 등의 로그인 및 인증 행위가 필요할 시, 의료정보시스템에 지문인식을 통한 로그인/인증을 요청하면, 인증서버를 통하여 검증하고 결과를 회신한다.

<표 3> 시퀀스 다이어그램 상세과정

[Registration Sequence]
1.1 Mobile(ID, FPKey)
1.2 Req(Registration)
2.1 login(MpkiID)
2.2 Trans(ID, FPKey)
3.1 Select(ID)
4.1 Insert(ID, FPKey)
5. CallBack(oCert)
[Certification Sequence]
6. Input(FPKey)
7. Sdata(ID, FP)
8. MpkiVerify(ID, FP)
9. MpkiCA(Cert)
10. CallBack(MpkiCACert)
11. CallBack(oCert)

3.2 의료 ICT융합환경 안전한 인증방법 프로토타입 구현

본 연구의 타당성, 실현 가능성을 검증하기 위하여 프로토타입을 구현하였다. 프로토타입 구현을 위한 Spec 정보는 다음 표 4와 같다.

<표 4> 프로토타입 구현 PC, Mobile Spec

● 대상 의료정보시스템 PC
- CPU: I5-6500
- RAM: 16GB
- SSD: 512GB
- 운영체제: Windows 10,
● 안전한 인증 기기
- 삼성 갤럭시 노트9
- 안드로이드 9.0 파이

의료정보시스템에 대한 일부 기능을 구현하여 대상 의료정보시스템 PC를 개발하였으며, 안전한 인증기기의 검토를 위하여 Mobile 기기에 앱을 통하여 시스템을 작성하였다. 그 결과, 화면을 기반으로 한 프로토타입과 프로세스는 그림 3과 같이 나타난다. 의료정부시스템을 실행 후, 인증서를 기반으로 로그인을 요청하고, 개인화 기기에서 FIDO기반 지문인식을 수행하여 결과의 전달을 요청하면, 검증결과를 의료정보시스템에 보내주고, 결과에 따라 로그인이 결정된다. 이를 통하여 로그인/인증 뿐만 아니라 권한관리 등에 편리한 활용이 가능할 것으로 예상된다.

3.3 프로토타입 시스템 기능성 FGI 검증

본 연구의 타당성, 실현 가능성을 검증하기 위하여

(그림 3) 의료정보시스템 인증방법 설계에 대한 프로토타입 구현화면

프로토타입을 구현하였으며, 실제 현장에 적용하기 위한 정성적, 정량적 검증을 위하여 FGI(Focus Group Interview)를 수행하였다. 대상은 의료정보시스템 관계자 2인, 정보보안 시스템 개발자 2인, 의료기관 관계자 2인의 6인으로 구성하였으며, 30분간 본 설계내용에 대한 상세한 설명과 활용방안, 프로토타입 결과의 테스트를 통하여 진행하였다. 그리고, 본 연구내용이 현장에 활용되기 위한 타당성을 리커드 5점 척도로 조사한 결과 4.3점으로 우수한 것으로 나타나 활용성에 있어서 타당한 것으로 나타났다.

그리고 정보보안 시스템 개발자와 의료정보시스템 관계자들의 별도 인터뷰를 통하여 개발 및 활용가능성을 확인한 결과 매우 타당하며, 빠른 활용역시 가능한 것으로 나타났다.

4. 결론 및 향후연구

기존의 전통적인 의료산업이 ICT에 대한 활용을 넘어 의료 ICT 융합환경으로 전환됨에 따라, 디지털화된 의료정보는 다양한 보안위협 및 취약점에 노출되고 있다.

특히, 중소형 의료기관은 EMR을 중심으로 핵심적인 정보시스템을 기반으로 의료서비스를 영위하기 때문에, 의료정보시스템의 보안 위협 및 취약은 의료서비스의 중단으로 연결될 수 있는 문제점을 지닌다.

그럼에도 불구하고, 중소형 의료기관에서는 초기에 도입한 ICT 시스템을 기반으로 구성되어 있으며, 다양한 의료ICT 시스템에서 활용되는 ID/PW 방식 인증 시스템은 단순 공유로 인한 유출 가능성이 있으며, 중소규모 의료기관에서 인증서 등으로 대체하기에는 불편함이 있는 상황이다. 이러한 보안사고는 중소형 의료기관의 물적, 인적자원의 한계에 기인한다.

이에 따라, 중소형 의료기관을 중심으로 의료정보시스템에서 안전한 사용자 관리를 위한 인증시스템을 설계하고 프로토타입을 구현하였다. 본 연구는 다음과 같이 세가지 의미를 가진다.

- 첫째, 중소형 의료기관에 대한 현황을 분석하여 보안위협과 취약점을 해결하기 위한 동인을 제안하였다.
- 둘째, 중소형 의료기관에 대한 명확한 권한관리와 접근제어, 인증에 대한 신뢰성을 향상시키고 절차적 속도를 담보할 수 있는 방향성을 제시하였다.
- 셋째, FIDO 기술의 응용으로 인하여 비용효율적으로 빠르게 적용할 수 있는 보안성 향상 방안을 제시하였다.

향후 연구로는 내부의 의료정보시스템과 연계되는 외부 헬스케어 시스템의 안전한 활용을 위한 다양한 방안에 대하여 연구하고자 한다.

참고문헌

[1] 기주희, “인증 기술의 과거와 현재”, 정보통신기획평가원, 주간기술동향, 1814호, pp. 13-22, 2017

[2] 김미화, “우리나라 보건의료 정보화 현황”, 보험연구원 고령화리뷰, 제10호, pp. 19-21, 2017.

[3] 김승환, “의료IT융합 기술 연구 동향”. 전자공학회지, 제43권, 제2호, pp. 18-24, 2016.

[4] 김양훈, 안병구, “의료융합 환경에서 수용성을 고려한 비용 효율적 보안체계구축 방안 연구: 중소의료기관을 중심으로”, 융합보안논문지, 제18권, 제5호, pp. 75-81, 2018.

[5] 김자원, 장항배, “ 중소형 의료기관 보안관리 평가모델 설계 연구”, 한국전자거래학회지, 제23권, 제1호, pp. 89-102., 2018.

[6] 김진묵, 홍성식, “다중 인증 기술을 이용한 의료정보 보호시스템”, 융합보안논문지, 제14권 제7호, pp.3-8., 2014.

[7] 박영택, “국내의료기관의 전자의무기록시스템 현황 및 발전방향”, HIRA 정책동향, 제11권, 제2호, pp. 52-61, 2017.

[8] 송용택, 이재우, “사물인터넷 기기의 안전한 사용자 인증 방안에 관한 프레임워크”, 한국전자거래학회지, 제24권, 제2호, pp. 217-228, 2019.

[9] 송재헌, 김인석, “전자금융 거래 시 생체인증을 전자서명에 활용하기 위한 기술 및 법률에 관한 연구”, 한국전자거래학회지, 제21권, 제4호, pp. 41-53, 2016.
[10] 윤은준, 유기영, “의료정보보호를 위한 RFID를 이용한 환자 인증 시스템”, 한국통신학회논문지, 제35권 제6호, pp.962-969, 2010.
[11] 이희주,. “4차 산업 혁명시대의 의료 환경 변화와 웰니스의 전망”, 한국웰니스학회지, 제12권, 제4호, pp. 215-223, 2017.
[12] 장항배, 김양훈, “미래 환경변화와 의료보안 과제”, S&TR Journal, 제31권, 제2호, pp. 4-9, 2018.
[13] IoT보안얼라이언스, “의료 분야 ICT 융합 제품 서비스의 보안 내재화를 위한 스마트의료 사이버보안 가이드”, 한국인터넷진흥원, 2018.
[14] Kumar, P. and Lee, H. J., “Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey,” Sensors, Vol. 12, No. 1, pp. 55-91, 2012.
[15] Williams, P., “A Practical Application of CMM to Medical Security Capability,” Information Management & Computer Security, Vol. 16, No. 1, pp. 58-73, 2008.

〔저자소개〕

김 양 훈 (Yanghoon Kim)
2005년 2월 대진대학교 컴퓨터공학 학사
2007년 2월 대진대학교 컴퓨터공학 석사
2011년 2월 대진대학교 소프트웨어공학 박사
2014년 2월 - 현재 극동대학교 산업보안학과 교수
email : yhkim@kdu.ac.kr

최 연 정 (Yean Jung Choi)
2004년 2월 한림대학교 식품영양학과(이학석사)
2007년 8월 한림대학교 식품영양학과(이학박사)
2018년 3월 - 현재 극동대학교 식품영양학과 교수
email: yeanjungchoi.2016@gmail.com