J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

의료정보 접근을 위한 동적상황인증시스템의 구현☆

Implementation of Dynamic Situation Authentication System for Accessing Medical Information

함 규 성[1] 서 원 정[2] 정 호 일[2] 주 수 종[2*]
Gyu-Sung Ham Own-jeong Seo Hoill Jung Su-Chong Joo

요 약

최근 IT 기술의 발전과 함께 클라우드 서비스, IoT 기술 및 모바일 애플리케이션을 통해 통합적인 u-헬스케어 환경기반의 의료정보 시스템이 구축되고 있다. 이러한 의료정보시스템에서는 응급 처치나 치료를 목적으로 의료진에게 환자의 의료정보를 접근할 권한이 제공되어야 한다. 따라서 의료정보시스템에서 의료진이 담당하는 환자의 생체정보 및 개인 의료정보에 접근하기 위해서는 신뢰적이고 신속한 인증과정이 필요하다. 그러나 현재 시스템 환경에서는 의료진의 ID/PWD만을 이용하는 단순하고 정적인 사용자 인증기법으로 의료정보시스템을 접근하고 있다. 이러한 이유에서 본 논문에서는 환자가 응급상태조건을 고려한 다양한 인증 요소를 포함한 의료정보접근의 투명성을 제공하는 동적상황인증기법과 이를 지원하는 동적상황인증시스템을 제안하였다. 본 동적상황인증은 사용자 인증과 이동 단말기 인증을 결합한 인증으로, 기존의 사용자 인증 뿐 아니라 의료진이 사용하는 이동 단말기의 인증을 위해 환자의 응급상태, 의료진의 역할, 근무시간, 근무위치 등과 같은 다양한 인증요소 속성들을 사용하였다. 우리는 응급상태판별, 동적상황인증, 인증지원 DB 구축을 포함한 동적상황인증시스템을 설계 및 구현하였다. 마지막으로 제안한 동적상황인증시스템의 서비스 수행성 검증을 위해, 의료진으로 하여금 동적상황인증과정과 그 이후 담당환자에 대한 의료정보접근 허가와 함께 의료정보서버로부터 의료진 자신의 이동 단말기에 모바일 애플리케이션을 내려 받아 실행함으로써 의료정보의 인증 및 접근과정을 보였다.

☞ 주제어 : 동적상황인증기법 및 인증시스템, 응급상태조건, 의료정보 및 접근서비스, u-의료정보시스템 환경

ABSTRACT

With the development of IT technology recently, medical information systems are being constructed in an integrated u-health environment through cloud services, IoT technologies, and mobile applications. These kinds of medical information systems should provide the medical staff with authorities to access patients' medical information for emergency status treatments or therapeutic purposes. Therefore, in the medical information systems, the reliable and prompt authentication processes are necessary to access the biometric information and the medical information of the patients in charge of the medical staff. However, medical information systems are accessing with simple and static user authentication mechanism using only medical ID / PWD in the present system environment. For this reason, in this paper, we suggest a dynamic situation authentication mechanism that provides transparency of medical information access including various authentication factors considering patient's emergency status condition and dynamic situation authentication system supporting it. Our dynamic Situation Authentication is a combination of user authentication and mobile device authentication, which includes various authentication factor attributes such as emergency status, role of medical staff, their working hours, and their working positions and so forth. We designed and implemented a dynamic situation authentication system including emergency status decision, dynamic situation authentication, and authentication support DB construction. Finally, in order to verify the serviceability of the suggested dynamic situation authentication system, the medical staffs download the mobile application from the medical information server to the medical staff's own mobile device together with the dynamic situation authentication process and the permission to access medical information to the patient and showed access to medical information.

☞ keyword : Dynamic Situation Authentication Mechanism and Authentication System, Emergency Status Condition, Medical Information and Access Service, u-Medical Information System Environment

1. Department of Computer Engineering, Wonkwang University, 460 Iksandaero Iksan, 54538, South Korea
2. Department of Computer · Software Engineering, Wonkwang University, 460 Iksandaero Iksan, 54538, South Korea
* Corresponding author (scjoo@wku.ac.kr)
[Received 3 August 2018, Reviewed 21 August 2018(R2 4 October 2018), Accepted 10 October 2018]
☆ 이 논문은 2018년도 교육부 재원 한국연구재단의 기초연구사업의 지원을 받아 수행된 연구임 (NRF-2017R1D1A1B03029210)
☆ 본 논문은 2018년도 한국인터넷정보학회 춘계학술발표대회 우수 논문 추천에 따라 확장 및 수정된 논문임.

1. 서 론

IT 기술의 발전과 정보처리 기술의 발달로 다양한 분야에서 IT 융합을 통한 많은 정보서비스가 이뤄지고 있다. 보건의료분야에서도 IT-BT-NT 융합을 통해 의료정보 및 사용자 정보를 활용한 건강관리 및 헬스케어 서비스 연구가 활발히 진행되고 있다[1]. 더 나아가 병원 내 병동 및 병실에 있는 IoT 센서 및 의료 기기로 구축된 IoT 환경과 더불어 클라우드 및 클라이언트/서버 애플리케이션을 접목시킨 u-의료정보시스템 환경기반의 의료서비스들이 증가하고 있다[2]. 그러나 이러한 IoT 환경에서 수집된 환자의 의료정보는 클라우드 또는 데이터베이스 서버를 통한 데이터 공유 시, 데이터 접근에 대한 사용자 인증이 요구된다[3]. 특히 사용자 인증의 신뢰성 및 편리성의 요청에 따라 의료산업에서의 정보보안에 대한 인증이 절대적으로 필요하며, 의료정보접근허가를 받기 위해 다 단계 및 다중요소를 채택한 인증에 대한 연구들이 진행되고 있다[4-5]. 이에 맞도록, 우리의 연구[6-8]에서도 동적상황인증기법을 통해 의료정보의 투명한 접근에 대한 인증연구들을 진행하여 왔다.

본 논문에서는 기존 연구를 기반으로 확장된 의료정보 접근을 위한 동적상황인증시스템을 제안하였다. 환자의 생체상황 정보를 정상상태와 응급(위급)상태로 구분하였고, 환자 응급상태에 따라 의료진의 접근권한을 조정이 가능하도록 한다. 또한 기존의 ID/PWD만을 이용하는 인증방법과는 달리 응급상태, 의료진의 역할, 근무시간, 근무위치 등과 같은 다양한 인증 구성 요소들을 포함하여 의료정보의 투명한 접근을 위한 동적상황인증기법을 제공하는 시스템을 설계 및 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서는 u-헬스케어 및 인증관련 연구들을 정리하고, 3장에서는 u-의료정보시스템에서 동적상황인증기법의 설계, 인증지원 DB 구축 그리고 이를 기반으로 한 인증과정의 전반에 대하여 기술한다. 4장은 의료상황정보의 취득 및 저장, 응급상태 판별 과정, 그리고 동적상황인증의 설계 및 구현을 보였으며, 마지막으로 결론에서 앞으로 본 연구의 확장 방안을 제시하였다.

2. 관련연구

2.1 u-헬스케어

u-헬스케어(Ubiquitous-Healthcare)는 생체 신호 및 건강정보를 유비쿼터스 네트워크를 통해 의료 기관에 전송하고 실시간 관리가 가능한 효율적 건강관리 서비스이다[9]. 현재는 이러한 u-헬스케어 환경에서 IoT(Internet of Things)를 구성하는 센서들이나 의료 디바이스들을 통해 더욱 손쉽게 사용자 데이터를 전송하거나 관리할 수 있는 서비스가 연구되고 있다[10]. 대표적인 IoT와 u-헬스케어를 결합한 응용서비스에는 IoT 헬스케어, 스마트 메디컬 홈 프로젝트, 모바일 헬스케어 시스템, 헬스케어 웨어러블 등이 있다[11-12].

모바일 헬스케어 시스템은 병원 내에서만 가능하던 의료서비스를 시간과 장소에 구애받지 않고 모바일 기기를 통하여 원격 의료정보 접속 및 모니터링 할 수 있는 시스템이다. 서울대학교 바이오의료기술개발 사업단에서는 실시간 생체 신호 모니터링 서비스와 생체 신호 기록 및 전송 서비스, 운동 모드에 따른 건강관리 시스템을 서비스하고 있다[13]. 헬스케어 디바이스는 신체에 부착하거나 일부분으로 결합시켜 사용자의 건강관리 능력을 향상할 수 있는 모든 기기를 의미한다[14]. 스마트 홈 통신망과 웨어러블 기기를 이용하여 실시간으로 생체정보를 확인하고, 문제발생 의심 시 병원 시스템에 전송하는 원격의료시스템을 제안한 연구가 있다[15]. 본 시스템은 웨어러블 디바이스와 홈 게이트웨이 그리고 주치시스템을 구성하여 문제 발생 이후에도 지속적으로 관리해 주는 시스템이다. 또한 웨어러블 디바이스를 통하여 데이터를 지속적으로 획득할 수 있는 연구가 진행되고 있다[16].

2.2 u-헬스케어의 의료정보접근과 인증 요구사항

u-헬스케어 정보는 유무선 네트워크를 통해 개인정보와 의료정보를 나눌 수 있다. 따라서 제 3자에 의한 의도적인 정보 유출이 생기거나 의료정보의 거래, 부정한 열람 및 복제의 위험에 항상 노출되어 있다. 이를 위해 의료정보를 공유하고 활용하는 시스템에서는 보안에 주안점을 둔 의료정보 접근방법에 대한 다양한 인증기법들이 제공될 필요성이 크다. 헬스케어 보안 요구사항을 수립하기 위해서는 CIA(Confidentiality, Integrity, Availability)가 보장되어야 한다. 또한 사용자의 개인정보 보호를 위한 익명성 보장, 연결 불가능성 보장, 식별 불가능성 보장, 세밀한 접근제어 기능이 보장되어야 한다[17-18]. 또한 의료정보는 사용자 접근에 따라 추적성이 확보되어야 하며, 의료정보의 암호화하는 기법의 방법, 접근의 불법 방지, 신뢰적인 데이터가 유지관리 되도록 하여야 한다[18].

2.3 의료정보 접근에 대한 권한별 인증 기법

u-의료정보시스템은 병원관계자, 즉, 의료진으로 하여금 담당 환자의 의료정보의 접근 권한 및 의료정보의 중

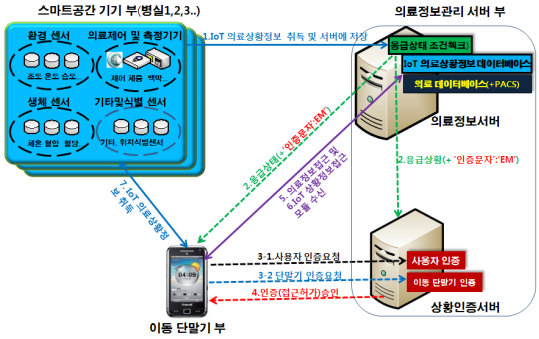
요 등급별 레벨에 합당한 접근제어를 통해 환자의 개인정보 침해 및 의료정보 유출을 방지하고, 엄격한 인증을 통해 환자의 의료정보를 접근 허가 하도록 해야 한다[5]. 관련 연구들로서 u-헬스케어의 인증 요구사항 중 환자의 의료정보 접근에 투명성을 제공하기 위한 연구들이 있다[17-19]. 현재 병원필드에서 활용되는 의료정보 접근허가를 받기 위한 사용자 인증기법들은 다음과 같다. 병원에서 의료서버 관리자는 사용자를 관리하기 위해 초기화 단계에서 사용자의 모든 속성 정보(해당 부서, 직급, 역할)를 확인하고 권한 속성을 결정한다. 사용자는 서비스를 이용하기 위해 등록단계와 상호 인증단계를 거친다. 등록단계에서 사용자의 속성 정보를 인증서버에 보낸 이후 속성에 따라 속성 값과 비밀 값으로 이뤄진 인증서를 할당한다. 또한 인증서버는 할당된 비밀키와 인증서를 서버에 저장한다. 상호인증단계에서 의료진이 특정 환자의 생체정보에 접근하고자 할 때 인증서버에 저장된 인증서를 바탕으로 의료진의 환자데이터 접근레벨이 결정된다. 이를 바탕으로 권한에 따른 접근인증방법을 통해 환자의 의료정보 접근에 대한 투명성을 제공하고 있다[17-19]. 본 논문에서 우리가 제안한 동적상황인증기법의 연구는 앞서 기술한 인증기법에 환자의 응급상태 취득 및 응급조건 판별, 응급상태알림 인증문자 그리고 사용자 소유의 이동 단말기 인증과정을 추가시켰으며, 제안한 인증기법을 적용하여 동적상황인증시스템을 설계 및 구현한다.

3. 의료정보 접근을 위한 동적상황인증기법의 설계

3.1 u-의료정보시스템 환경과 인증절차

본 절에서는 u-의료정보시스템 환경에서 의료정보 접근의 투명성을 위한 동적상황인증을 설계한다. 동적상황인증시스템 환경은 IoT 기반의 의료 센서와 의료디바이스들을 이용하여 환자의 생체의료정보 취득을 위한 스마트 공간 기기 부, 생체의료정보 및 의료정보 저장관리 서비스 모듈을 제공하기 위한 의료정보관리 서버와 사용자 및 이동 단말기 인증지원 상황인증 서버를 통합한 의료정보관리 서버 부로 그림 1과 같이 구성하였다[7]. 본 논문에서 구현 편의를 위해 상황인증서버와 의료정보서버를 의료정보관리 서버 부내에 통합하여 설치하였다. 스마트 공간 기기 부는 환경 센서, 의료제어 및 측정기기 등을 통하여 환자의 실시간 의료상황정보를 제공한다. 의료정보관리 서버 부는 의료정보서버와 인증서버로 통합 구성하였다.

이동 단말기 부는 사용자 인증과 이동 단말기 인증절차 통해 동적상황인증의 허가를 받은 의료진에게 모바일 애플리케이션을 제공함으로 써 해당 의료정보를 접근 할 수 있도록 한다. 그림 1은 u-의료정보시스템 환경에서 응급상태를 고려한 제안한 동적상황인증의 수행 절차를 보인다.



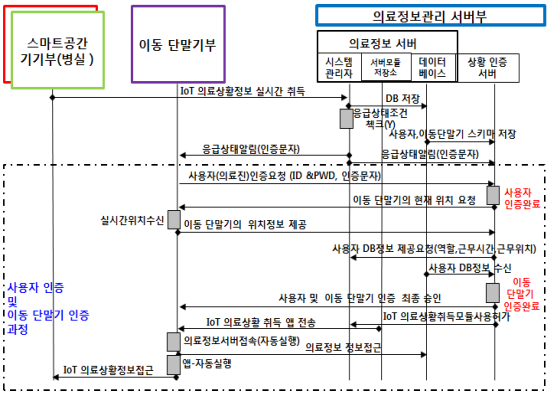
(그림 1) u-의료정보시스템 환경에서 인증절차
(Figure 1) Authentication Procedures in u-Medical Information System Environment

1) 스마트 공간 기기 부에서는 각 환자의 IoT 의료상황정보(생체정보)를 실시간 취득한다. 취득된 실시간 생체정보는 의료정보서버에 저장함과 동시에 응급상태 조건에 해당되는지를 체크한다. 2) 환자의 의료상황이 응급상태에 해당하는 경우, 환자의 담당 의료진의 이동 단말기와 인증서버에 인증문자를 포함한 응급상태 알림메시지(EM)을 각각 전송한다. 3,4) 응급상태 알림을 받은 담당 의료진은 사용자 인증과 이동 단말기인증 절차를 차례로 거친다. 5,6,7) 마지막으로 인증된 사용자는 인증된 이동 단말기를 통하여 환자의 의료정보, 스마트 공간 기기 부에서 취득된 실시간 생체정보 등 의료진 역할에 맞는 응급환자의 상위 급 중요 정보 및 실시간 IoT 의료상황정보를 접근 및 검색한다. 그림 2는 그림 1의 동적상황인증 절차를 ETD(Event Tracing Diagram)으로 상세하게 보인다.

3.2 동적상황인증 지원 의료정보 DB 구축

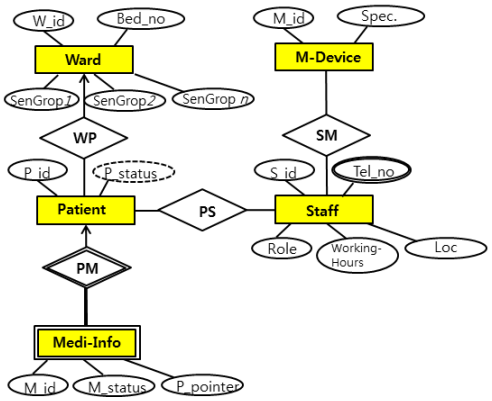
본 절에서는 의료정보관리 서버부의 의료정보서버 DB를 설계한다. 동적상황인증 지원을 위한 의료정보 DB의 구성요소인 엔티티 셑(Entity Set)[병동, 환자, 의료진, 이동 단말기]과 이들 간의 관계 셑(Relationship Set)[병동과 환자관계, 환자와 담당 의료진과의 관계, 의료진이 소유

한 이동 단말기와의 관계, 환자와 환자에 관련된 의료정보와의 관계]들에 대한 논리적 설계를 그림 3과 같이 ERD(Entity-Relationship Diagram)로 보인다[7]. 각 엔티티 셀 내 구성된 필드의 속성(Attribute)들은 제안 시스템 구현에 필요한 속성만 기술하고 나머지 속성들은 생략한다.



(그림 2) 응급상태를 고려한 동적상황인증의 세부절차 ETD

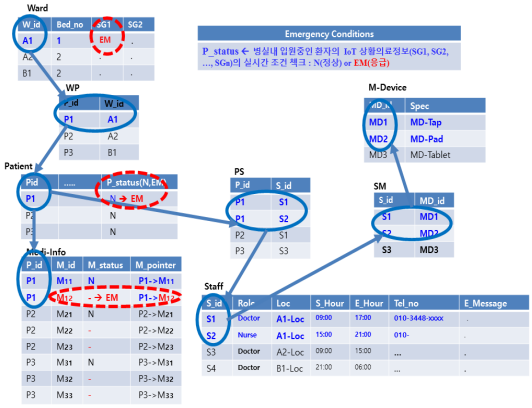
(Figure 2) ETD for showing Detailed Procedures of Dynamic Context Authentication Based on Emergency Status



(그림 3) 동적상황인증과 의료정보접근 지원 ERD 논리적 설계

(Figure 3) Logical Design ERD for Supporting Dynamic Context Authentication and Accessing of Medical Information

그림 4는 설계한 ERD를 기반으로 관계형 데이터베이스를 구축하였다. 그림 3의 ERD로부터는 8개의 관계형 DB 테이블들로 구성되는 의료정보 데이터베이스를 구축하였다. Patient 테이블은 환자 고유의 ID(P_id)와 환자상태(P_status)의 속성들을 갖는다. P_status에는 정상('N') 또는 응급('EM')상태로 환자의 상태가 저장된다. 'N'과 'EM'상태의 결정은 Ward 테이블의 속성인 센서그룹 SG(SenserGrop)1, 2, ... , n 들로부터 취득된 생체정보의 응급상태 조건에 의해 결정된다. SG 속성 값은 IoT 의료상황정보(환자의 생체정보)를 참조하여 응급상태 판별이 이루어지며, 응급상태이면 환자 상태(P_status) 속성이 'N'에서 'EM'으로 트리거된다. Patient 와 Medi-Info 테이블들 간의 관계에서는 환자의 의료상황에 따라 등급별 의료정보들의 접근허가가 지정된다. WP 관계 테이블을 통해 환자가 입원해 있는 Ward 테이블의 병실과 침대번호 및 그곳에 설치·부착된 센서그룹(센서, 의료측정기기)들이 기술된다. patient 테이블과 Staff 테이블은 PS 관계 테이블을 통해 의료진의 고유 아이디인 S_id와 의료진 역할, 근무시간, 실시간 근무위치 등과 같은 이동 단말기 인증의 속성들이 존재하며, 응급상태를 알리는 연락 번호 속성을 가진다. SM 관계 테이블을 통해 의료진 소유의 사용 가능한 M-Device의 속성들은 이동 단말기의 고유 값인 M_id와 제품사양들이 기술된다.



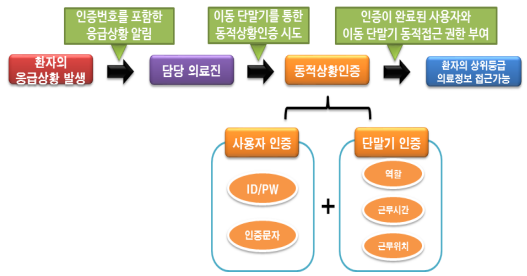
(그림 4) 동적 상황 인증 및 의료 정보 접근 지원 의료정보 DB 테이블

(Figure 4) DB Tables Supporting Dynamic Context Authentication and Accessing of Medical Information

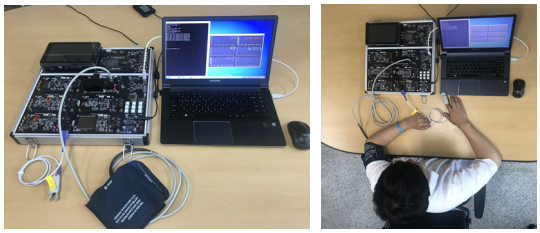
3.3 의료정보 DB기반의 동적상황인증과정

본 연구에서 제안한 의료정보의 접근 허가 및 지원을 위한 동적상황인증은 사용자 인증과 이동 단말기 인증을 결합한 통합 인증기법이다. 앞 3.2절에서 언급한바와 같

이, 사용자인증과정은 정상상태와 응급상태로 구분된다. 정상상태에서 담당 의료진의 사용자 인증으로는 평상시 M_status가 'N'에 해당하는 의료정보만 접근가능하다(예, p->M11 :환자 P1의 의료정보 등급 1을 접근). 환자 P1이 응급상태조건이 되면, Staff 테이블의 의료진 S1, S2의 연락 번호를 통해 인증문자와 함께 응급 호출을 받게 된다. 담당 의료진은 'EM'에 해당하는 의료정보를 인증서버로부터 투명접근권한을 받아 M11은 물론 상위등급의 의료정보(예, p->M12: 환자 P1의 의료정보 상위 등급 2를 접근)까지 접근할 수 있다. 이동 단말기 인증과정은 사용자 인증을 마친 이후 접근 허가된 의료정보 및 IoT 의료상황정보인 생체정보를 접근 수행하게 된다. 응급호출을 받은 의료진은 SM관계 테이블을 통해 M-Device테이블에 S_id로 등록된 사용자 소유의 이동 단말기의 사용인증이 진행된다. 의료진의 기본 사용자 인증요소를 포함해서 이동 단말기 의료진의 역할, 근무시간, 현재위치, 환자상태(응급) 등을 통해 인증서버로부터 이동 단말기의 사용인증을 받는다. 이동 단말기 인증에서 인증요소의 속성값에 대한 조건을 하나라도 만족하지 않는 경우, 기존 인증방법의 절차에 따라 수동절차를 거쳐 인증을 받게 된다. 즉, 인증된 사용자만이 인증된 이동 단말기를 사용하여 의료정보를 접근이 가능하다. 인증된 이동 단말기를 사용하여 의료관리서버에 저장된 의료정보와 스마트 공간 기기부에서 생성된 IoT 의료상황정보까지 등급별 의료정보의 동적접근권한을 부여 받는다. 응급상태 조치 후, 환자의 의료상황이 정상상태이면 허가된 동적상황인증(사용자 인증, 이동 단말기 인증)의 권한이 모두 해제되며, 담당 의료진은 해당 환자의 상위 등급(예, M12)의 의료정보 접근이 불가능하게 된다. 그림 5는 동적상황인증기법에서 담당 의료진인 사용자 인증과 자신이 소유한 이동 단말기 인증과정을 나타낸다.



(그림 5) 동적상황인증 기법에서 사용자 및 이동 단말기 인증과정
(Figure 5) Procedures of User and Mobile Device Authentication in Dynamic Context Authentication Mechanism



(그림 6) BMS를 이용한 환자의 생체정보수집 환경
(Figure 6) Environment of Patient's Biometric Information Collection Using BMS

4. 의료정보 접근을 위한 동적상황인증시스템 구현

4.1 동적상황인증시스템의 구현 환경

u-의료정보시스템 환경 내 의료정보관리 서버 부는 Window8 IIS와 리눅스(CentOS)기반의 2개의 서버를 두어 분산 처리 환경에서 동적상황인증 및 의료정보제공 서비스를 수행하도록 하였다. 데이터베이스 관리 시스템은 Mysql을 사용하고 이동 단말기를 위한 소프트웨어는 Android Studio3.1.0을 사용한다. 응급상태 시 담당 의료진에게 전송하는 인증문자를 구현하기 위해 Google사의 FCM(Firebase Cloud Massaging)을 PHP와 안드로이드 스튜디오와 연동하여 사용한다. 스마트 공간 기기 부로부터 IoT 의료상황정보(생체정보)를 받기 위해 BMS-AE-DK[1] (Bio Medical System-Analog & Embedded Development Kit)인 생체 신호모듈시스템을 사용한다. BMS는 임베디드 시스템으로 써 C 언어를 기반으로 제작된 생체 정보를 측정할 수 있는 시스템이다. BMS로부터 Spo2Module과 혈압 측정 NIBP(Non Invasive Blood Pressure) Module을 이용한 산소포화도, 혈압, 맥박, 체온 등의 생체정보를 얻는다. 그림 6은 스마트 공간 기기 부에서 환자의 생체정보 수집을 위한 환경을 나타낸다.

4.2 응급상태 인증문자 알림

본 논문에서 응급상태를 판별하기 위해 BMS로부터 얻을 수 있는 생체정보 중에서 산소 포화도와 혈압 생체

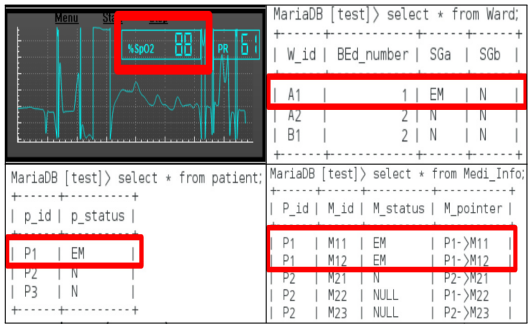
[1] HyBus, 임베디드 시스템모듈 BMS-AE-DK http://www.hybus.net

신호만을 사용하였다. 산소 포화도는 체내 산소수치를 나타낸다. 산소 포화도의 수치가 95% 이상일 경우 정상상태로 판별한다[20]. 혈압의 정상수치는 120/80mmHg이다[21]. 환자의 개인의 상태에 따라 고혈압 환자, 저혈압 환자로서 환자에 따른 기준이 달라질 수 있다. 일반적인 환자를 기준으로 수축기가 140mmHg이상일 경우 또는 이완기가 110mmHg이상일 경우 환자의 상태가 고혈압성 위기가 발생한다. 따라서 응급상태 시 인증문자 알림을 위해 환자의 생체정보에 대한 응급상태 판별 기준으로써 표 1과 같이 정의하였다.

(표 1) 환자의 생체정보에 대한 응급상태 판별 기준
(Table 1) Emergency Status Criterion for Patient's Biometric Information

구 분		상 태	기 준
산소포화도(Spo2)		저산소 혈증(%)	〈 90
혈 압	수축기	고혈합성 위기(mmHg)	〉 140
	이완기		〉 110

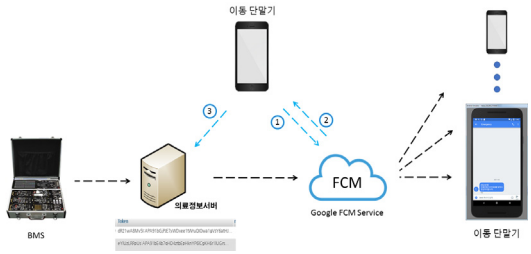
환자로부터 생체정보의 범위가 응급상태 조건에 해당하는 경우, 그림 7과 같이 Ward 테이블의 속성인 해당 센서그룹 필드에 'EM'으로 표시된다.



(그림 7) 응급상태에서의 Patient와 Medi_Info 테이블내 응급상태 표시 및 환자의 상위등급 의료정보 접근
(Figure 7) Accessing The Higher Leveled-Patient's Medical Information and Emergency Status Notice in Patient and Medi_Info Tables in Emergency Status

응급상태 발생과 동시에 트리거링을 통해 WP 관계 테이블을 참조하여 Patient 테이블의 P_status 속성의 값이 'N'에서 'EM'으로, Medi-Info 테이블의 M_Status에서 '-'는 'EM'으로 변경된다. Medi-Info는 환자의 상태가 'EM'이 될 경우 환자의 담당 의료진이 상위등급 의료정보를 확인할 수 있도록 환자의 의료정보의 접근권한이 변경된다[7].

또한 응급상태발생 이후 담당의사에 전달할 응급상태 알림 메시지를 구현하기 위해 Google의 FCM(Firebase Cloud Massaging)서비스를 이용하여 그림 8과 같이 구현하였다. 이동 단말기 등록과정은 다음과 같다. ①이동 단말기의 서비스 수행 모바일 애플리케이션은 FCM으로부터 토근 발급을 요청한다. ②FCM에서 생성된 토큰을 모바일 애플리케이션에 전달한다. ③FCM으로부터 받은 토큰을 의료정보서버의 M-Device 테이블의 MD_id 속성에 저장한다.



(그림 8) 인증문자 전송 구조 및 응급 메시지 알림
(Figure 8) Authentication Character Transmission Structure and Notification of Emergency Message Notification

환자 P1이 응급상태인 경우 의료정보서버의 PS 관계 테이블을 통하여 담당 의료진 S-id를 확인하고, SM 관계 테이블을 이용하여 담당 의료진의 이동 단말기 MD-id를 확인한다. 확인된 MD-id는 FCM에 인증문자와 함께 전송된다. 인증문자는 의료정보서버에서 임의의 숫자 6개로 생성하여 각각 인증서버와 FCM으로 전송한다. FCM은 서버로부터 받은 토큰을 식별하여 해당 의료진의 전화번호를 이용하여 이동 단말기에 인증문자와 함께 전송한다.

4.3 동적상황인증(사용자 및 이동 단말기)의 구현

환자의 의료 상황이 정상상태('N')인 경우, 해당 수행 모바일 애플리케이션에서 ID/PWD만을 입력하여 인증을 시도한다. 정상상태에서 접속한 환자를 담당하는 의료진은 예로서 담당 환자의 이름, 나이, 성별, 혈액형, 병실 위치, 기본 병명 등과 같은 기본정보만 확인할 수 있다.

응급상태('EM')인 경우, 그림 2와 그림 5에서 나타낸 바와 같이 동적상황인증 과정을 진행한다. ID/PWD와 응급상태 알림을 통해 받은 인증문자를 입력하고 사용자 인증

을 수행한다. 인증서버에서는 사용자로부터 받은 ID/PWD, 인증문자를 확인함으로 써 사용자 인증을 수행한다. 사용자 인증이 완료되면 이동 단말기 인증을 진행한다. 이동 단말기 인증은 사용자의 역할, 근무시간, 근무위치를 통한 인증을 진행한다. 인증서버는 Staff테이블의 Role, W-Hours (Start-End), Loc을 확인한다. Role의 속성들(담당의사, 간호사, 보조간호사,...등)을 확인하여 각 속성들의 역할에 맞도록 환자의 의료정보를 등급별(레벨1, 레벨2, 레벨3,...등)로 제공한다. W-Hours속성을 확인하여 사용자의 근무시간을 현재 이동 단말기의 물리적 시간과 비교한다. Loc속성은 의료진인 사용자가 근무하는 장소에 설치된 WiFi들의 SSID집합이다. 이동 단말기로부터 받은 WiFi의 SSID가 Loc 속성에 포함되어 있다면 인증에 성공한다. Role, W-Hours, Loc의 인증은 한 번에 이루어지며 하나라도 인증조건을 벗어 날 시 인증실패로 재 인증 하거나 수동 인증 절차를 거치도록 하였다. 사용자와 이동 단말기 인증을 모두 마친 사용자는 인증된 이동 단말기를 사용하여 의료정보관리서버에 저장된 상위 등급의 환자의료정보를 접근할 수 있는 권한을 부여받는다.

(그림 9) 동적상황인증 기반 의료정보 접근 결과

(Figure 9) Accessing Results of Medical Information Based on Dynamic Context Authentication

그림 9와 같이 구현 모바일 애플리케이션에서 ID/PWD, 인증문자를 입력 후 사용자 로그인하면 동적상황인증이 이루어진다. 응급상태에서 인증될 경우 정상상태에서는 접근할 수 없었던 상위 등급으로 분류된 정보를 확인 할 수 있게 된다. 상위 등급의 정보의 예로서 환자의 만성 질환, 진료 내역, 처방 내역 및 PACS(Picture Archiving Communication System)과 연동한 영상정보 등과 같은 중요한 환자 개인 의료정보를 접근할 수 있도록 하였다. 응급 진료를 마친 후, 환자가 정상상태('N')가 되면 위 권한은 응급상태에서 정상상태로 전환된다. 따라서 응급상태에서 허가 되었던 동적상황인증이 자동 해제되며 접근 허가된 상위 등급의 의료정보에 접근이 또한 금지된다.

5. 결 론

최근 병원에서는 효율적 의료정보관리를 위한 u-의료정보시스템을 구축하고 있으며, 언제 어디서나 신속한 의료서비스가 가능하도록 의료정보를 공유 및 활용하고 있다. 그러나 담당 의료진 외에도 환자의 의료정보의 접근이 가능하여 개인정보의 유출이 대두됨에 따라 환자의 개인정보 및 의료정보의 접근에 대한 인증이 절대적으로 필요하다. 따라서 본 논문에서는 기존 ID/PWD만을 이용하는 정적 인증방법과는 달리 환자의 의료 상황 및 다양한 인증 요소들을 포함한 동적상황인증시스템을 제안하였다. 제안하는 시스템은 환자의 응급상태 여부에 따라 의료진에게 의료정보의 접근 권한을 차등 부여가 가능하도록 하였다. 환자의 상태가 응급상태일 경우 동적상황인증 시스템을 통해 환자의 상위 의료정보에 접근함이 가능하도록 구현하였으며, 이를 통해 u-의료정보시스템에서 환자의 개인정보 및 의료정보 접근에 대한 투명성을 보였다. 향후 연구로는 환자의 동적인증상황을 고려한 사용자와 이동 단말기의 자동인증 서비스 모델을 연구할 예정이다.

참고문헌(Reference)

[1] H. J. Sung, "A study on the Bio Information System (BT+IT+NT) about Accordance of Fusion Technology and Process of Industrialization In Ubiquitous Society", The Korea Society of Information Technology Applications, pp. 387-402, 2007.4.
http://www.ndsl.kr/ndsl/search/detail/article/articleSearchResultDetail.do?cn=NPAP08107912

[2] M. U. Aslam, A. Derhab, K. Saleem, and H. Abbas, “A Survey of Authentication Schemes in Telecare Medicine Information Systems”, Springer US, Journal of Medical Systems, Vol. 41, No. 1, article no.14, 2017. https://doi.org/10.1007/s10916-016-0658-3

[3] G. Abdelkader, H. S. Naima, and A. P. Adda, “Secure Authentication Approach Based New Mobility Management Schemes for Mobile Communication”, Journal of Information Process Systems, Vol. 13, No. 1, pp. 152~173, 2017.
http://doi.org/10.3745/ JIPS.03.0064

[4] J. W. Kim, HB Chang, “A Study on Design Security Management Evaluation Model for Small-Medium size Healthcare Institutions”, Journal of Society for e-Business Studies, Vol. 1, No. 23, pp. 89-102, 2018.
http://www.jsebs.org/jsebs/index.php/jsebs/article/view/304

[5] Y. S. Jeong, S. H. Lee, “A Study of Patient’s Privacy Protection in U-Healthcare”, Journal of the Korea Institute of Information Security & Cryptology, Vol. 22, No. 4, pp. 913-921, 2012.
http://journalhome.ap-northeast-2.elasticbeanstalk.com/journals/jkiisc/digital-library/2479

[6] S. C. Joo, “A Study of Dynamic Context Authentication Service for Accessing Medical and Healthcare Information”, Proceedings of the 36th KSII Fall Conference, Vol. 18, No. 2, pp. 193-194, 2017.

[7] S. C. Joo, “Design of Dynamic Context Authentication Scheme for Transparent Access of Medical Information”, Proceedings of the 36th KSII Fall Conference, Vol. 18, No. 2, pp. 192-193, 2017.

[8] G. S. Ham, O. J. Seo, S. C. Joo, “Implementation of Dynamic Context Authentication for Accessing Medical Information”, Proceedings of the 37th KSII Spring Conference, Vol. 19, No. 1, pp. 115-116, 2018.

[9] J. S. Choi, S. E. Kim, S. H. Lee, “Toward Ubiquitous Healthcare Services With a Novel Efficient Cloud Platform”, IEEE Transactions on Biomedical Engineering, Vol. 60 , No. 1 , pp 230 – 234, Jan. 2013.
https://ieeexplore.ieee.org/document/6324392/

[10] W. Li, C. Jung, J. Park, “IoT Healthcare Communication System for IEEE 11073 PHD and IHE PCD-01 Integration Using CoAP”, TIIS, Vol. 12, No. 4, pp. 1396-1414, 2018.
https://doi.org/10.3837/tiis.2018.04.001

[11] D. G. Korzun, A. V. Borodin, I. A. Timofeev. “Digital Assistance Services for Emergency Situations in Personalized Mobile Healthcare: Smart Space Based Approach”, International Conference on Biomedical Engineering and Computational Technologies (SIBIROCON), pp. 62-67, 2015.
https://doi.org/10.1109/sibircon.2015.7361852

[12] T. V. Prabhakar, Madhuri Sheethala Iyer, H. S. Jamadagni, P. R. Priyanka, Payal Mondal, V. V. S. Sasi Kiran, Vaishnavi Govindarajan, “Wearabkle Device for Healthcare Application” 2013 Texas Instruments India Educators’ Conference, pp. 91-96, 2013.
https://ieeexplore.ieee.org/document/6757121

[13] J. K. Lee, H. J. Kim, S. W. Kim, J. Y. Song, S. R. Yoon, “Deep Learning-Based Biological Signal Analysis for Assisting Cardiovascular Disease Diagnosis on Mobile Environment”, The Journal of Korean Institute of Communications and Information Sciences, Vol. 42, No. 7, pp. 1470-1476, 2017.
https://doi.org/10.7840/kics.2017.42.7.1470

[14] W. Y. Chung. “Multi-Modal Sensing M2M Healthcare Service in WSN”, TIIS, Vol. 6, No. 4, pp. 1090-1105, 2012.
http://www.itiis.org/digital-library/manuscript/335

[15] Ichiro Yamada, Guillaume Lopez, “Wearable sensing systems for healthcare monitoring”, Jun 2012 in 2012 Symposium on VLSI Technology (VLSIT), pp. 1-6, 2012.6.
https://doi.org/10.1109/vlsit.2012.6242435

[16] Usman Ahmad Usmani, Mohammed Umar Usmani, “Future Market Trends and Opportunities for Wearable Sensor Technology”, IJET Vol.6(4): 326-330 ISSN: 1793-8236, 2014.
https://doi.org/10.7763/ijet.2014.v6.721

[17] Y, Tian, B. Song, M. M. Hassan, E. N. Huh, ″A Privacy-aware Graph-based Access Control System for the Healthcare Domain″, TIIS, Vol. 6, No. 10, pp. 2708-2730, 2012.
http://www.itiis.org/digital-library/manuscript/427

[18] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Liu, J. Ma, "PRIAM: Privacy Preserving Identity and Access Management Scheme in Cloud", TIIS, Vol. 8, No. 1, pp. 282-304, 2014. https://doi.org/10.3837/tiis.2014.01.017

[19] S. K. Kim, H. J. Hwang, "Security Requirements of Personal Health Service", Journal of Institute of Korean Electrical and Electronics Engineers, Vol. 19, No. 4, pp. 548-556, 2015. https://doi.org/10.7471/ikeee.2015.19.4.548

[20] D. H. Moon, K. H. Kim, S. K. LEE, "Effects of Deep Breathing with Incentive Spirometer on Pulmonary Function and O2 Saturation by Time Process in Patients with Rib Fracture", Journal of the Korea Contents Association, Vol. 15, No. 3, pp. 174-183, 2015. https://doi.org/10.5392/jkca.2015.15.03.174

[21] I. K. Seo, S. H. Yang, "Analysis on the Interface Desing of Electronic Sphygmomanometer focused on User Experience", Journal of Digital Design, Vol. 13, No. 1, pp. 253-262, 2013. https://doi.org/10.17280/jdd.2013.13.1.025

◐ 저 자 소 개 ◑

함 규 성(Gyu-Sung Ham)
2018년 원광대학교 컴퓨터공학과(공학사)
2018년~현재 원광대학교 대학원 컴퓨터공학과(공학석사)
관심분야 : Distribute system, Security, Healthcare etc.
E-mail : ham1231@wku.ac.kr

서 원 정(Own-jeong Seo)
2018년 원광대학교 컴퓨터·소프트웨어공학과(공학사)
관심분야 : Distribute system, Security, Healthcare etc.
E-mail : eehrrhtldud@wku.ac.kr

◐ 저 자 소 개 ◑

정 호 일(Hoill Chung)

2010년 상지대학교 컴퓨터정보공학부(공학사)
2013년 상지대학교 대학원 정보통신공학과(공학석사)
2017년 상지대학교 대학원 정보통신공학과(공학박사)
2015년~2018년 (사)지역정보연구원 책임연구원
2018년～현재 원광대학교 컴퓨터·소프트웨어공학과 조교수
관심분야 : Data mining, Data Analysis, Artificial Intelligence(A.I), Healthcare etc.
E-mail : hijung1982@wku.ac.kr

주 수 종(Su-Chong Joo)

1986년 원광대학교 전자계산공학과(공학사)
1988년 중앙대학교 대학원 컴퓨터공학과(공학석사)
1992년 중앙대학교 대학원 컴퓨터공학과(공학박사)
1990년～현재 원광대학교 컴퓨터·소프트웨어공학과 교수
2007년~2009년 원광대학교 정보전산원장
2015년~2017년 원광대학교 공과대학 학장
1993년 미국 University of Massachusetts at Amherst, Dept. of EECE, Post-Doc
2003년, 2009년 미국 University of California at Irvine, Dept. of EECS, 방문교수
관심분야 : Distributed Middleware Computing, Multimedia Database System, Ubiquitous Computing (u-Home and Healthcare services)
E-mail : scjoo@wku.ac.kr