Journal of the Korea Industrial Information Systems Research Vol. 19, No. 3, Jun. 2014
http://dx.doi.org/10.9723/jksiis.2014.19.3.057

환자의 프라이버시 보호와 불법 접근 차단을 위한 RFID 기반 UHISRL 설계†

(An UHISRL design to protect patient's privacy and to block its illegal access based on RFID)

이 병 관[1], 정 은 희[2]
(Byung Kwan Lee and Eun Hee Jeong)

요 약 본 논문은 RFID를 이용하여 환자, 의료진, 의약품을 관리하는 UHISRL(Ubiquitous Healthcare Information System based on Real Time Location)을 제안하였다. 제안하는 UHISRL은 환자의 건강상태를 모니터링하고, 그 결과를 스마트 폰과 태블릿 PC로 확인할 수 있다. 또한, 본 논문에서 설계된 ERHL(Extended Randomized Hash Lock) 인증 기법을 사용하여 재전송공격과 스푸핑 공격을 차단하였고, 환자의 프라이버시는 CP-ABE(Cipher Text - Attributed based Encryption)기법을 이용하여 UHISRL DB 접근을 속성에 따라 제한함으로써 보안을 강화시켰다. 특히, UHISRL는 만성질환자의 응급 상황을 실시간으로 모니터링 함으로써 불의의 사고를 방지할 수 있도록 하였다.

핵심주제어 : UHISRL, RFID 인증, 질병 모니터링, 헬스 케어, 개인정보보호

Abstract This paper proposes the UHISRL(Ubiquitous Healthcare Information System based on Real Time Location) which manages patient, doctor, medicine by using RFID. The proposed UHISRL monitors the patient's health state, and enables us to confirm the result with Smart Phone and Tablet PC. Also, it can block Replay and Spoofing attack by using the ERHL(Extended Randomized Hash Lock) authentication scheme designed in this paper. A patient privacy is enhanced by limiting UHISRL DB access according to attributes with CP-ABE (Cipher Text - Attributed based Encryption) technique. Specially, UHISRL can prevent an unexpected accident by monitoring a chronic patient's emergency situation in real time.

Key Words : UHISRL, RFID authentication, Disease monitoring, Healthcare, Privacy security

1. 서 론

고령화 사회 진입과 정보기술의 진화로 헬스 케어 분야가 차세대 신 성장 산업으로 부각되고 있다. 특히, 21세기에는 질병의 치료는 물론, 예방 및 관리를 통해 건강한 삶을 영위하는 것으로 변화하다보니 통신, 전자회사 등이 새로운 헬스 케어 공급자로 부상하고 있다. 그리고 유비쿼터스의 중심 기술인 RFID(Radio Frequency IDentification)는 AIDC(Automatic Identification Data Capture)로 차세대 혁신적인 기술로써 인식되어왔으며, RFID를 헬스케어에 이용하여

† 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (NRF-2012R1A1A4A01012039)
1) 관동대학교 컴퓨터학과, 제1저자
2) 강원대학교 지역경제학과, 교신저자(jeongeh@kangwon.ac.kr)

환자식별(identification)과 위치(location)를 파악하거나 의료기기와 약품 등을 효율적인 관리함으로써 의료 서비스의 질을 크게 향상시킬 수 있다.

본 논문은 RFID를 이용하여 환자의 의료 정보, 의약품 재고 관리, 홈 헬스 케어 관리와 같은 전체적인 프로세스들을 설계하고, 처리 결과를 언제, 어디서나 스마트 폰이나 태블릿으로 확인할 수 있는 UHISRL (Ubiquitous Healthcare Information System based Real-time Location) 설계를 제안한다. 또한, 제안하는 UHISRL은 RFID로 인식된 환자의 ID에 따라 기본적인 정보를 제공하지만, 환자정보에 접근할 수 있는 권한을 제한함으로써 환자의 프라이버시를 보호하고, 홈 헬스 케어에 의해 수집된 환자 정보를 이용하여 환자 질병을 모니터링 함으로써 불의의 사고를 미연에 방지하고자 한다.

본 논문의 구성은 2장에서 관련연구를 살펴보고, 3장에서는 제안하는 UHISRL을 설명하고, 4장에서는 UHISRL를 분석한다. 그리고 5장에서 결론을 맺는다.

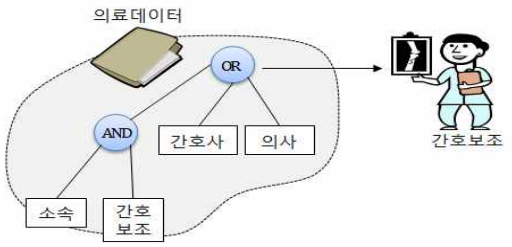
2. 관련연구

2.1 속성 기반 암호화

속성 기반 암호화(Attributed Based Encryption)는 2005년 Sahai와 Waters[1]에 의해 FIBE(Fuzzy Identity-based Encryption)로 제안되었다. 그리고 1년 뒤에 FIBE는 ABE를 이용한 접근 제어 기능을 제공하는 KP(key-Plice) ABE[2]를 제안하였다. 그 후에 KP-ABE와 유사하지만 역할(Role) 개념을 추가하여 좀 더 실용적인 응용을 고려한 CP(Ciphertext Policy)-ABE[3]가 제안되었다[4].

KP-ABE는 복호 가능한 속성집합으로 송신자가 암호화하고 수신자의 키 생성 시에 자신의 속성집합에 근거하는 접근 구조를 바탕으로 복호화하고, CP-ABE는 암호문 생성 시에 송신자가 접근 구조를 지정하여 수신자의 속성집합을 바탕으로 복호화 한다[1,5]. 메디컬 정보와 헬스 정보를 제공하는 헬스 케어 기관이 구성원들에게 특별한 역할을 할당하고, 그들의 역할에 따라 특별한 데이터 접근할 수 있는 권한을 제공하는 헬스 케어 시스템에서는 KP-ABE보다 CP-ABE이 더 효율적이고 수월하다[4,5].

CP-ABE는 암호문 생성시 송신자가 접근 구조를 지정하여 수신자의 속성 집합을 바탕으로 복호화를 한다. 예를 들어, 그림 1에서 개체가 [간호보조], [소속]이라는 속성을 가지고 있을 경우, 송신자는 암호문에 [간호보조이고 소속이라면 복호 가능]이라는 접근 구조 만들어 암호화 하면, 접근구조를 만족하는 개체만이 복호가 가능하다[5].



<Fig. 1> Access structure of CP-ABE

CP-ABE는 4개의 알고리즘인 전역 키설정(Setup), 암호(Encryption), 개인키 생성(Key generation), 복호(Decryption)이다[4,5,6].

- 전역키 설정 : 보안파라미터를 입력으로 전역 공개키 PK(Public Key)와 마스터 키 MK(Master Key)를 생성한다.
- Encrypt(PK, M, A) : 공개 키 PK와 메시지 M, 그리고 속성트리 A를 입력으로 메시지 M에 대한 암호 메시지 CT(Cipher Text)를 생성한다.
- Key Generation(MK, S) : 마스터 키 MK와 보유하고 있는 속성집합인 S를 입력하여 각 속성값에 대한 비밀키 SK를 생성한다.
- Decrypt(PK, CT, SK) : 공개 파라미터 PK, 암호문 CT, 그리고 개인키 SK를 입력으로 암호문 CT를 평문으로 복호화한다.

2.2 RFID용 정보보호기술

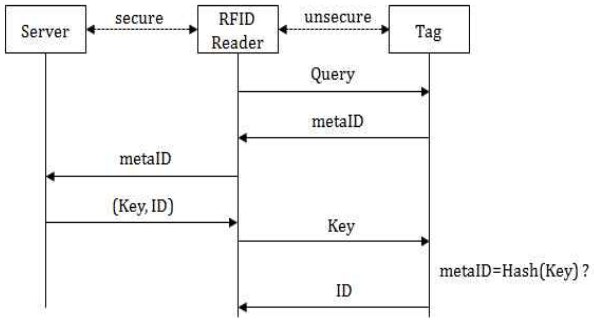
RFID용 정보보호기술로는 태그의 리더 인증, 위치 추적 방지를 통한 프라이버시 보호 등 다양한 기법들이 존재한다.

2.2.1.Hash Lock Protocol

S. A. Weis[7] 등은 전방향성을 특징으로 하는 해시

함수를 기반으로 HLP(Hash-Lock Protocol)을 제안하였다[8].

그림 2와 같이 HLP에서 태그는 리더의 쿼리에 대해 metaID로만 응답하고, 리더는 안전하다고 가정된 통신 채널을 통해 DB에서 metaID에 해당하는 태그 키와 ID 값을 가져 온다. 그리고 리더는 이 태그 키를 태그에 전달하면, 태그는 전달받은 키에 대한 해시를 계산한 후, 태그의 metaID와 같은 경우에만 리더에게 데이터를 전달함으로써 불법적인 리더가 태그 내용을 읽는 것을 방지한다.

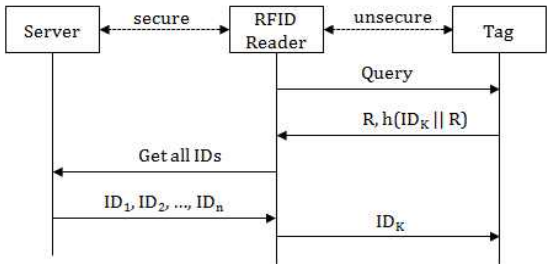


<Fig. 2> HLP authentication procedure

하지만 공격자가 metaID를 도청하여 정당한 리더로 전송하게 되면, 상호인증 단계가 없기 때문에 리더는 공격자에게 정당한 키를 전달하는 문제점이 있다. 또한 HLP에서는 metaID, Key, 태그의 ID를 아무런 제약 없이 전송하고, 리더의 질의에 대한 응답으로 항상 같은 metaID 값을 전송하기 때문에 도청, 스푸핑 공격, 재전송 공격 및 위치 추적에 취약하다[8,9,10,11]

2.2.2 Randomized Hash Lock Protocol

RHLP(Randomized Hash Lock Protocol)[7]은 HLP의 위치 추적 문제를 해결하기 위해 리더가 태그를 읽을 때마다 태그의 난수 생성기를 통하여 태그는 리더에게 항상 다른 값을 리턴하게 된다. 하지만, RHLP도 공격자가 도청으로 획득한 데이터를 이용하여 재전송 공격, 스푸핑 공격을 할 경우에 태그의 ID가 노출되는 문제점이 있다[8,9,10,12]. 그리고 RHLP는 리더에서 해시 함수를 반복적으로 수행해야 한다는 부담이 있으며, 한정된 응용 범위를 가지는 경우에는 사용 가능하지만, 많은 태그를 필요로 하는 경우에는 부적합하다.



<Fig. 3> RHLP authentication procedure

본 논문에서는 CP-ABE와 RHLP를 이용하여 환자, 의료진, 의약품 등의 정보와 위치를 파악할 때, 환자의 정보를 보호하고자 한다.

3. UHISRL 설계

제안하는 UHISRL(Ubiquitous Healthcare Information System based Real-time Location)은 RFID를 이용하여 환자와 의료진은 환자의 의료정보에 접근할 수 있고, 의약품과 의료기기는 위치와 재고현황을 파악할 수 있도록 설계한다. 또한 UHISRL은 환자와 의료진의 경우에는 환자의 상태를 언제, 어디서나 스마트 폰이나 태블릿으로 확인할 수 있고, 프라이버시 침해와 불법 접근을 차단하기 위하여 보안을 강화시키고자 한다.

제안하는 UHISRL은 다음과 같은 전제조건 하에 설계한다.

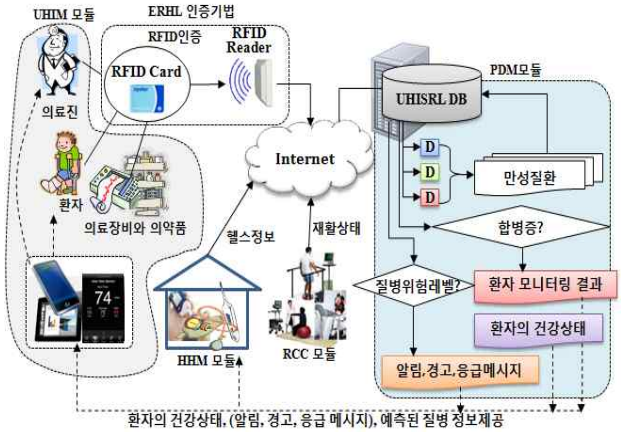
첫째, RFID에는 환자와 의료진의 고유 번호가 등록되어 있다.

둘째, 의료기기와 의약품에는 RFID 라벨이 부착되어 있고, 이 RFID 라벨에는 제품명, 유효기간, 취급등급 등의 기본적인 정보가 저장되어 있다.

셋째, 병원에는 RFID Reader기가 설치되어 있고, UHISRL DB에는 RFID와 연계되는 환자, 의료진, 의료기기와 의약품의 정보가 저장되어 있다.

UHISRL은 그림 4에서 설명하고 있듯이 환자, 의료진, 의약품에 대한 정보를 관리하는 UHIM(Ubiquitous Healthcare Information Management) 모듈, 환자, 의료진, 의약품에 대한 RFID를 검증하는 ERHL (Extended Randomized Hash Lock) 인증기법, 홈 헬스케어를 관리하는 HHM(Home Healthcare

Management) 모듈, 환자의 재활치료를 관리하는 RCC(Rehabiliation Clinical Control) 모듈, UHISRL DB에 저장된 환자 정보를 이용하여 환자의 질병을 모니터링하고, 환자의 건강상태를 스마트폰이나 태블릿 PC를 통해 환자 또는 의료진에 전달하는 PDM(Patient Disease Monitoring) 모듈로 구성된다.



<Fig. 4> UHISRL component and data flowchart

3.1 UHIM 모듈 설계

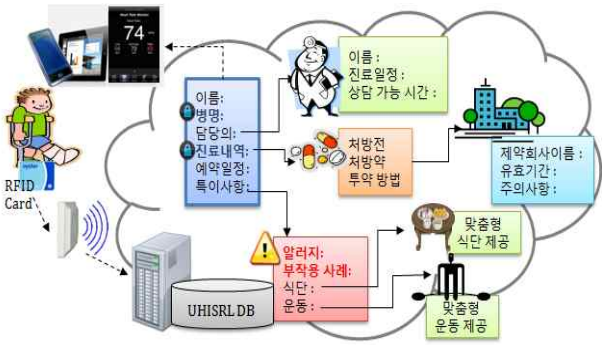
UHIM(Ubiquitous Healthcare Information Management) 모듈은 RFID를 사용하여 환자의 정보를 관리하는 PM(Patient Management) 서브 모듈, 의료진의 정보를 관리하는 MPM(Medical Personal Management) 서브 모듈, 그리고 의료장비와 의약품에 대한 정보를 관리하는 MEM(Medical Equipment Management) 서브 모듈로 구성된다.

3.1.1 PM 서브 모듈 설계

PM(Patient Management) 서브 모듈은 그림 5와 같이 RFID Reader기에 의해 인식된 환자의 고유번호를 이용하여 환자 정보를 관리한다.

[1 단계] PM 서브 모듈은 RFID Reader기로 환자의 고유 번호를 식별한 후, UHISRL DB에 접근하여 환자의 정보인 이름, 담당의사, 예약 일정, 특이 사항 등을 가져온다.

[2 단계] 이때 환자의 사생활 침해를 방지하기 위해 본인과 접근권한이 있는 의료진인 경우에만 병명, 진료내역을 확인할 수 있다. 반면에 인증 받지 못한 제3자인 경우에는 접근이 제한된다.



<Fig. 5> The process contents of PM sub module

[3 단계] PM 서브 모듈은 환자의 질병에 따라 식이요법, 맞춤형 식단 그리고 운동 방법 등의 정보를 제공한다.

[4 단계] PM 서브 모듈은 환자가 처방받은 약품에 대한 제약회사 정보, 유효기간, 주의사항을 스마트폰과 태블릿으로 제공한다.

[5 단계] PM 서브 모듈은 진료를 담당하는 담당의 상담 가능시간을 제공한다.

3.1.2 MPM 서브 모듈 설계

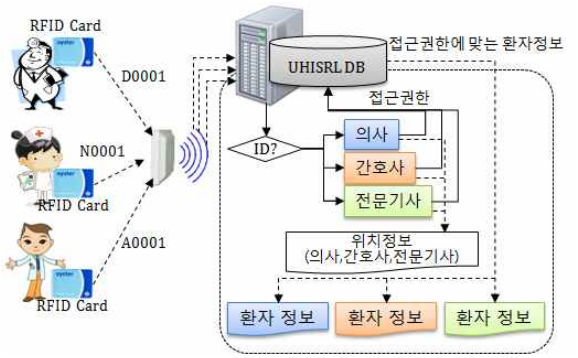
MPM 서브 모듈은 그림 6과 같이 내과의사, 간호사, 전문 기사 등의 의료진들은 ID가 등록된 RFID를 이용하여 의료진들의 위치를 추적하여 응급상황에 유연하게 대처할 수 있도록 한다. 또한 의료진의 역할에 따라 UHISRL DB에 접근 권한을 다르게 부여함으로써 환자의 프라이버시를 보호하고자 한다.

[1 단계] MPM 서브 모듈은 의료진 위치를 파악한다.

[2 단계] 응급상황 발생 시에 가까운 위치에 있는 의료진들이 적시에 배당한다.

[3 단계] MPM 서브 모듈은 주치의, 간호사, 전문기사 등의 역할에 따라 UHISRL DB에 접근할 수 있는 권한을 다르게 부여한다.

[4 단계] MPM 서브 모듈은 접근 권한에 따라 UHISRL DB에 저장되어 있는 환자의 의료정보를 확인할 수 있도록 환자의 정보를 제공한다.



<Fig. 6> The process flowchart of MPM sub module

3.1.3 MEM 서브 모듈 설계

MEM 서브 모듈은 의약품과 의료기기에 RFID 라벨을 부착하여 의약품과 의료기기의 위치와 재고현황을 관리자가 실시간으로 모니터링 할 수 있도록 설계한다. 특히, 주의가 필요한 의약품인 경우에는 자동으로 의약품의 위치와 개수가 집계되도록 설계하여 의약품 부주의로 발생할 수 있는 의료사고를 방지한다.

그림 7은 관리자가 PC, 태블릿을 이용하여 의약품을 관리하는 모듈의 정보 흐름을 설명한 것이다.

<Fig. 7> The process flowchart of MEM sub module

[1 단계] MEM 서브 모듈은 의료장비와 의약품의 RFID 라벨에는 의료 장비명과 약품명, 제조회사, 유효기간, 취급레벨 등의 기본적인 정보를 작성한다.

[2 단계] RFID 리더기로 의료장비와 의약품에 부착된 RFID 라벨을 읽은 후에 의료장비와 의약품의 위치, 제조회사, 유효기간, 취급 레벨 등을 파악한다.

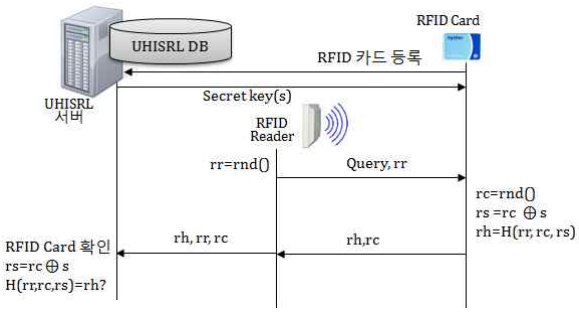
[3 단계] MEM 서브 모듈은 의약품의 유효기간이 지났거나, 기본 재고 수량보다 적게 비치된 의약품이나 의료장비들의 목록을 관리자 모니터링 할 수 있도록 UHIRSRL DB를 갱신하거나 저장한다.

[4 단계] MEM 서브 모듈은 관리자의 PC 또는 태블릿 을 이용하여 의료장비와 의약품의 현황을 확인할 수 있도록 정보를 제공한다.

3.2 ERHL 인증 기법 설계

본 논문에서 제안하는 UHISRL 서버는 RFID를 이용하여 환자, 의료진, 의약품 등 전반적인 관리를 하도록 설계한다. 그런데, RFID는 정보보안에 취약하므로, 본 논문에서는 ERHL(Extended Randomized Hash Lock) 인증 기법을 설계하여 RFID를 이용하는 환자, 의료진, 의약품 등의 정보를 보호하도록 다음과 같이 설계한다.

[1 단계] UHISRL 서버는 RFID에 의료진, 환자, 의약품 정보를 등록하기 전에 그림 8과 같은 절차로 UHISRL DB에 RFID의 비밀키(s)를 등록한다.



<Fig. 8> The authentication process of ERHL

[2 단계] RFID 리더기가 랜덤한 수(rr)를 생성하고, Query와 rr을 RFID에 전송한다.

[3 단계] RFID는 RFID 리더기로부터 Query를 전달받으면, 랜덤한 수(rc)를 생성하고, 비밀키(s)와 XOR 연산을 한다.

[4 단계] RFID는 RFID 리더기로부터 전달받은 rr과 rc, rs를 해시한다.

[5 단계] RFID는 해시한 값과 rc를 RFID 리더기에 전송하면, RFID 리더기는 RFID가 전송한 해시 값, rc,

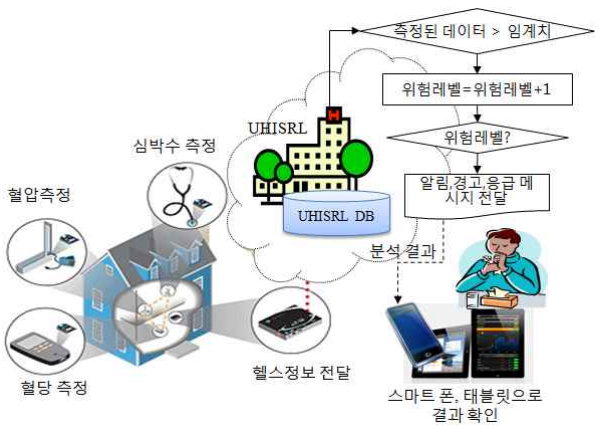
rr을 UHISRL 서버에 전송한다.

[6 단계] UHISRL 서버는 RFID 리더기가 전송한 rc, rr과 UHISRL 서버에 등록된 s를 해시한 값과, RFID 리더기가 전송한 해시값과 비교하여 RFID을 인증한다.

UHISRL 서버는 이렇게 RFID를 확인한 후에, 환자 정보, 의료진 정보, 의약품 정보에 접근하도록 함으로써 환자의 개인 프라이버시 침해, 의료정보 유출을 방지하고자 한다.

3.3 HMM 모듈 설계

HHM(Home Healthcare Management) 모듈은 가정에서 전용 단말기를 통해 자신의 건강 수치를 측정하고, 이 측정데이터를 실시간으로 분석해서 이 데이터들을 UHISRL DB 서버에 전송하여 만성질환자들의 건강상태를 확인하고 관리하는 모듈이다. 그림 9는 HHM 모듈의 처리절차를 설명한 것이며, 단계별 처리절차는 다음과 같다.



<Fig. 9> The process of HHM module

[1 단계] HHM 모듈은 고혈압, 당뇨 등 만성질환자들의 혈압/혈당의 자료를 가정에서 실시간으로 UHISRL DB에 전송한다.

[2 단계] UHISRL DB는 전달받은 환자의 헬스 정보로 환자의 질병 위험 레벨을 산출한다.

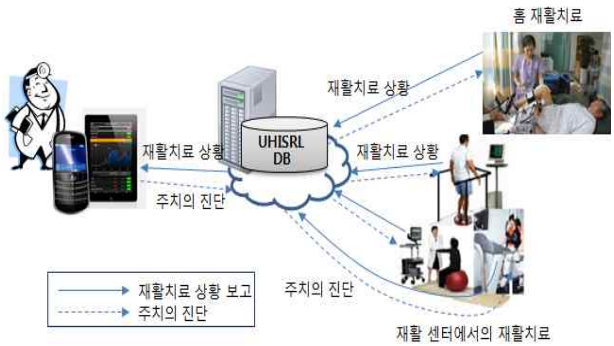
예를 들어, 고혈압 환자의 경우, 측정된 환자의 혈압이 임계치보다 클 경우 환자의 질병 위험 레벨을 한 단계 상승시킨다. 일정한 시간이 흐른 후에 측정한 환자의 혈압이 여전히 임계치보다 클 경우 질병 위험 레벨을 한 단계 더 상승시킨다.

[3 단계] 산출된 환자의 질병 위험 레벨에 따라 환자에게 알림메시지 또는 경고메시지를 스마트 폰에 전달한다.

예를 들어, 레벨 1단계일 경우에는 알림 메시지를 전달하고, 레벨 2단계일 경우에는 경고 메시지를 전달한다. 그리고 레벨 3단계일 경우에는 신속하게 인근 병원을 방문하도록 응급 메시지를 전달한다.

3.4 RCC 모듈 설계

RCC(Rehabiliation Clinical Control) 모듈은 개인별 맞춤 치료와 환자의 재활 치료 상태를 관리하는 모듈로써 실시간으로 재활 치료 상태를 환자에게 제공한다. 그림 10은 RCC 모듈의 처리절차를 설명한 것이다.



<Fig. 10> The process of RCC Module

[1 단계] RCC 모듈은 개인의 사전사후 ROM(관절 가동범위) 및 개인일상지수(바텔 지수) 등을 체크하고, UHISRL DB에 저장한다.

[2 단계] 주치의는 UHISRL DB에 접속하여 환자의 건강상태를 확인하고, 재활치료에 대한 소견서를 UHISRL DB에 저장한다.

[3 단계] 물리치료사는 UHISRL DB에 접속하여 환자에 대한 재활치료 소견서를 확인하고, 환자 개인별 맞춤치료를 하고, 치료 진행상황과 환자의 상태를 UHISRL DB에 저장한다.

[4 단계] RCC 모듈은 환자가 일상생활에서도 지속적으로 재활치료를 수행할 수 있도록 다양한 재활증진 정보를 제공한다.

3.5 PDM 모듈 설계

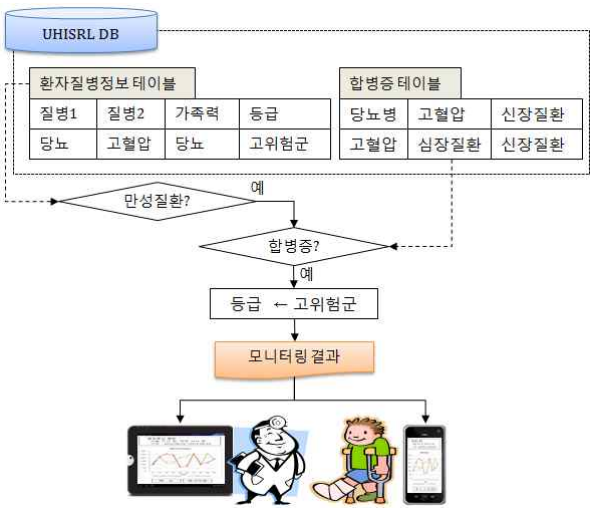
PDM(Patient Disease Monitoring) 모듈은 UHISRL DB에 저장된 환자의 질병에 따라 환자를 모니터링 하여 환자의 질병을 관리한다.

그림 11은 PDM 모듈의 환자 질병 모니터링 절차를 설명한 것이다.

[1 단계] PDM 모듈은 UHISRL DB에 저장되어 있는 환자의 질병을 파악한다.

[2 단계] PDM 모듈은 환자가 만성질환을 앓고 있을 경우에는 만성질환에 대한 합병증 발생 여부를 모니터링 한다. 예를 들어, 당뇨병 환자의 경우, 당뇨병의 합병증으로 의심되는 심장질환과 고혈압이 발생할 경우에는 고위험군으로 분류한다.

[3 단계] PDM 모듈은 고위험군으로 분류된 환자들의 정보를 주기적으로 모니터링하고, 그 결과를 환자와 주치의에게 전달한다.



<Fig. 11> The flowchart of PDM module

3.6 UHISRL DB 접근 제어 설계

본 논문에서는 의사, 간호사 등의 속성에 따라 환자의 의료 정보에 접근을 제한하도록 설계하였다.

UHISRL은 UHISRL DB에 구성원에 대한 RFID를 등록할 때, UHISRL DB 접근에 필요한 공개키, 마스터키를 등록하고, 이 키들과 구성원의 속성을 이용하여 다음과 같이 UHISRL DB에 접근 허가를 받은 후에 UHISRL DB에 접근할 수 있다.

[1 단계] RFID를 사용자에 발급할 때, RFID 사용자의 정보를 UHISRL DB에 저장한다.

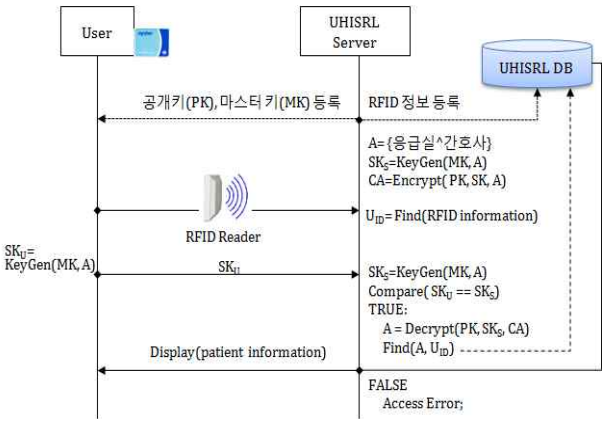
[2 단계] 이때, 사용자의 속성에 대한 정보를 암호화하여 UHISRL DB에 저장한다. 사용자의 속성은 {환자, 의사, 간호사, 간호보조, 전문기사}, {진료과, 소속부서, 직급} 중에서 각각 한 개씩 선택하여 생성한다. 예를 들어, 응급실에 근무하는 간호사일 경우, 사용자 속성(A)는 (응급실 ^ 간호사)이 된다.

UHISRL 서버는 마스터 키(MK)와 사용자 속성을 이용하여 비밀키 SK를 생성하고, 사용자 속성을 암호화 한다.

A=(응급실, 간호사)

SK=KeyGen(MK, A)

CA = Encrypt(PK, SK, A)



<Fig. 12> The access procedure of UHISRL DB

[3 단계] 사용자가 UHISRL DB에 접근하려고 할 때, 사용자의 RFID를 RFID 리더기가 읽어 사용자의 ID를 찾는다.

[4 단계] 사용자는 RFID 등록시 전달받은 마스터키 MK와 사용자 속성을 이용하여 비밀키 SK를 생성한다.

[5 단계] 사용자는 UHISRL DB 접근에 필요한 비밀키인 SK를 입력하면, UHISRL 서버는 사용자가 입력한 SK와 UHISRL 서버가 갖고 있는 SK와 비교한다.

[6 단계] 4단계의 비교 결과가 참이면, UHISRL 서버는 암호화된 사용자의 속성을 복호화 한다.

A = Decrypt(PK, SK, CA)

[7 단계] UHISRL 서버는 사용자의 속성이 (응급실, 간호사)인 것을 확인하고, 환자의 의료정보를 제공한다.

4. 성능 분석

의료정보가 디지털화되면서 민감한 개인 의료 정보를 데이터베이스에 보관하게 될 경우, 내부자 및 외부자로부터의 기밀성 유지가 필요하며, 특히 의료 서비스 사용자에 대한 프라이버시 보호가 필요하다.

본 논문에서는 ERHL 인증 기법과 CP-ABE기법을 이용하여 UHIRSL DB에 접근하는 권한을 속성에 따라 접근을 허용함으로써 환자의 프라이버시를 보호하도록 설계하였다.

4.1 UHIRSL의 보안성 분석

4.1.1 프라이버시 보호

RFID 리더와 RFID 사이의 데이터 전송은 무선 채널을 이용하여 도청공격을 받을 수 있지만, 본 논문에서 제안하는 ERHL 인증기법은 랜덤하게 생성된 난수를 이용함으로써 도청공격에 안전하다. 또한, RFID 리더기에 의해 수집된 RFID의 해시 값은 랜덤 하게 생성된 난수를 이용함으로써 RFID 리더기에 의해 수집된 해시 값으로는 위치추적을 할 수 없다. 단, UHIRSL 서버는 RFID의 비밀키인 s를 알고 있으므로 RFID의 위치는 UHISRL 서버만이 알 수 있으므로 환자의 프라이버시를 보호할 수 있다.

4.1.2 재전송 공격

RFID 리더기와 RFID 사이에 전송되는 데이터를 가로챈 공격자가 UHIRSL 서버에 접속하더라도 RFID 리더기와 RFID가 랜덤 하게 생성된 일회용 난수를 사용하는 RFID 인증 절차를 통과할 수 없으므로 재전송 공격으로부터 UHIRSL DB의 데이터를 보호할 수 있다.

4.1.3 스푸핑 공격

RFID 리더기와 RFID 사이에 전송되는 데이터를 가로챈 공격자는 UHISRL 서버에 데이터를 요청하지만, RFID 리더기와 RFID는 매번 랜덤하게 생성된 새로운 난수를 사용한 해시값을 사용하므로 RFID의 비밀키 s를 유추할 수 없다. 따라서 제안하는 ERHL 인증 기법은 스푸핑 공격으로부터 안전하다.

<Tabel 1>은 기존의 RFID 인증 프로토콜과 본 논문에서 제안하는 ERHL을 비교한 것이다.

<Table 1> Security comparison of protocol

프로토콜	위치추적	재전송공격	스푸핑공격
HLP	약함	약함	약함
RHLP	강함	약함	약함
ERHL	강함	강함	강함

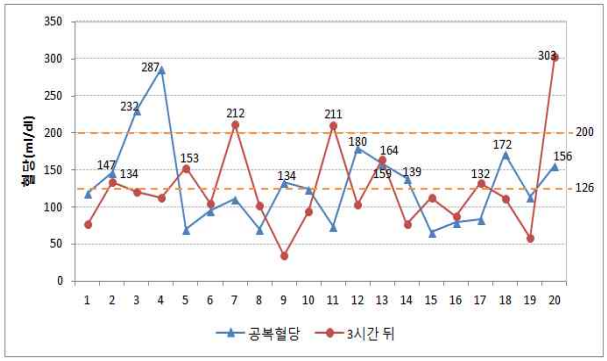
HLP은 항상 같은 metaID 값을 전송하기 때문에 위치 추적에 약할 뿐만 아니라, 데이터 도청으로 인한 재전송 공격, 스푸핑 공격에 약하다. 그리고 RHLP는 HLP와 달리 랜덤 하게 생성된 난수를 이용하기 때문에 위치추적에 강하지만, 공격자가 도청으로 획득한 데이터를 이용한 재전송 공격, 스푸핑 공격에는 약하다. 하지만, 본 논문에서 제안한 ERHL은 랜덤 하게 생성된 일회용 난수를 이용하므로 RFID 비밀키(s)를 유추할 수 없기 때문에 위치추적에 강할 뿐만 아니라, 데이터 도청으로 인한 재전송 공격, 스푸핑 공격에 강하다.

4.1.4 데이터베이스 보호

본 논문에서는 UHISRL DB에 접근할 수 있는 권한을 속성에 따라 부여하였고, 3.6절의 그림 12와 같이 RFID에 의해 식별된 ID에 따라 접근구조에 맞는 개체만이 UHISRL DB에 접근할 수 있으므로 UHISRL DB의 보안이 강화되었다.

4.2 모니터링 관리

환자의 질병 모니터링 실험은 당뇨병 환자의 데이터[13]를 이용하였으며, 공복혈당 평가 기준값은 126mg/dL이상일 경우 위험레벨을 1단계 올리고, 일정한 시간이 흐른 후에 다시 측정한 혈당이 여전히 126mg/dL 이상일 경우에는 위험레벨을 2단계로 올리고 경고 메시지를 전달한다. 이때 고혈당 기준값인 200mg/dL이상인 경우에는 응급메시지를 전달한다.



<Fig. 13> The result of monitoring(diabetes)

그림 13은 당뇨병환자의 저녁 식사 전의 공복혈당과 3시간 뒤의 혈당을 측정한 결과이다. 이 결과에 따라 PDM 모듈은 알림 메시지를 7회, 경고 메시지를 2회 그리고 응급 메시지를 5회 전달하였다.

따라서 UHISRL은 만성질환자의 응급 상황을 모니터링 함으로써 불의의 사고를 방지할 수 있다.

5. 결 론

본 논문에서는 환자의 프라이버시 침해와 불법 접근을 차단시킨 RFID 기반 UHISRL을 설계하였다.

첫째 UHISRL은 RFID를 이용하여 환자, 의료진, 의약품과 의료기기의 정보를 효율적으로 관리한다.

둘째, 만성질환자들의 건강상태를 점검하여 환자상태를 위험레벨로 분류하고, 위험레벨에 따라 알림, 경고, 응급 메시지를 전송함으로써 불의의 사고를 예방할 수 있다.

셋째, 환자의 재활 치료 상황을 UHISRL DB에 저장하여 환자, 의료진이 환자의 재활상태를 수시로 확인할 수 있다.

넷째, 수집된 환자의 상태를 분석하여 환자의 상태에 따라 알림, 경고, 응급 메시지를 스마트폰으로 전송함으로써 환자의 건강상태를 모니터링 할 수 있다.

다섯째, RFID를 인증함으로써 재전송 공격과 스푸핑 공격을 차단할 수 있다.

여섯째, 속성에 따라 UHISRL DB에 접속함으로써 환자의 프라이버시를 보호할 수 있다.

그 결과, 본 논문에서 설계한 UHISRL은 환자의 질병을 모니터링 함으로써 불의의 사고를 미연에 방지할 수 있을 뿐만 아니라 의료비도 절감 할 수 있다. 또한, 제안된 RFID 인증기법과 속성 기반 데이터베이스 접근 기법으로 환자, 의료진 등의 개인정보 대한 접근을 제한함으로써 u-Healthcare와 DB 보안을 강화시킬 수 있다.

References

[1] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption", In Advances in Cryptology-Eurocrypt, LNCS 3494, pp.475- 473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based Encryption for Fine-Grained Access Control of Encrypted Data", CCS'06 Proceedings of the 13th ACM Conference on Computer and Communications Security, 30 October 2006, pp.89-98.

[3] J. Bethencourt, A. Sahai, and B. Water, "Ciphertext - Policy Attribute - Based Encryption", In Proceedings of 2007 IEEE Symposium on Security and Privacy, 20-23 May 2007, pp. 321-334.

[4] Jong-Min Jeong, Tae-Kyoung Kwon, "Security Extension for Content-Centric Networks with Attribute-Based Encryption", Telecommunications Technology Association, the 6th Telecommunication Standardization, pp.78-93, 2010.

[5] Youjin Song, Kwangyong Park, "Attribute based encryption technology", Review of KIISC, Vol.20, No.2, pp.85-92, 2010.

[6] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE", CCS'07 Proceedings of the 14th ACM Conference on Computer and Communications Security, 28 October 2007, pp.456-465.

[7] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W.Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, 2003.

[8] Juseok Shin, Sejin Oh, Cheolho Jeong, Kyungho Chung, Kwangseon Ahn, "Improved An RFID Mutual Authentication Protocol Based on Hash Function", The Journal of KICS, Vol.37-C, No.3, pp.241-250, 2012.
[9] Dae-Jung Kim, Moon-Seog Jun, "Design of RFID Mutual Authentication Protocol using One Time Random Number", Journal of KIISE: Information Networking, Vol.35, No.3, pp.243-250, 2008.
[10] Jin-Seob Shin, Young-Ho Park, "An Authentication Protocol using the EXOR and the Hash Function in RFID/USN", Journal of the Korea Industrial Information Systems Research, Vol.12, No. 2, pp.24-29, 2007.
[11] Walid I. Khedr, "SRFID: A hash-based security scheme for low cost RFID systems", Egyptian Informatics Journal, Vol.14, Issue 1, pp.89-98, 2013
[12] Md Monzur Morshed, Anthony Atkins and Hongnian Yu, "Secure ubiquitous authentication protocols for RFID systems", EURASIP Journal on Wireless Communications and Networking, Vol.93, pp.1-13, 2012
[13] Diabetes Data, http://archive.ics.uci.edu/ml/datasets/Diabetes

이 병 관 (Byung Kwan Lee)

- 정회원
- 부산대학교 기계공학과 공학학사
- 중앙대학교 전자계산공학과 공학석사
- 중앙대학교 전자계산공학과 공학박사
- 관동대학교 공과대학 컴퓨터학과 교수
- 관심분야 : 네트워크 보안, IoT, 빅 데이터, 센서 네트워크

정 은 희 (Eun Hee Jeong)

- 정회원
- 강릉대학교 통계학과 이학사
- 관동대학교 전자계산공학과 공학석사
- 관동대학교 전자계산공학과 공학박사
- 강원대학교 인문사회과학대학 지역경제학과 부교수
- 관심분야 : 네트워크 보안, 인터넷보안, 전자상거래 보안, 빅 데이터

논 문 접 수 일 : 2014년 03월 26일
1 차 수 정 완 료 일 : 2014년 05월 07일
2 차 수 정 완 료 일 : 2014년 05월 26일
게 재 확 정 일 : 2014년 05월 28일