모바일 헬스케어 시스템에서 USIM 을 사용한 인증 메커니즘

장동희*, 김강석*, 홍만표*
*아주대학교 대학원 지식정보공학과
e-mail : ddam2002@ajou.ac.kr

A User Authentication Mechanism using USIM ID in Mobile Healthcare System

Donghee Jang*, Kangseok Kim*, Manpyo Hong*
*Dept. of Knowledge Information Engineering, Graduate School of Ajou University, Suwon, Korea

요 약

모바일 환경의 발달과 스마트 폰 사용자가 증가하면서 의료서비스 환경에도 큰 변화를 가져왔다. 시간과 장소에 구애 받지 않고 실시간으로 의사와 환자의 소통이 가능해졌다. 하지만 무선환경에서 환자의 의료정보가 허가되지 않은 사용자에 의해 유출 되고 개인의 사생활의 침해가 우려되고 있다. 또한 헬스케어의 데이터는 환자의 건강과 밀접한 관계가 있어 데이터 위/변조가 일어날 경우에는 환자의 생명에도 영향을 미칠 수 있다. 따라서 본 논문에서는 스마트 헬스케어(Smart Healthcare)의 스마트보안 기술 핵심요소인 기밀성, 무결성, 사용자인증, 모바일 보안에 적합한 시스템을 설계하였다.

1. 서론

모바일 환경의 빠른 발달로 2001 년 10 월말 에는 2000 만 명을 넘고 2012 년 08 월에는 3000 만명을 돌파하였으며, 40~50 대의 신규 가입자도 작년대비 3.4 와 3.9 증가하였다[1]. 스마트폰 사용자가 전 연령층으로 대중화 되어가고 있는 가운데 최근 의료 환경은 병원 중심의 환경에서 환자 편의 중심으로 진료 방식이 바뀌고 있다. 의료서비스 중 일부인 진료지원, 질병의 판단 및 처방은 IT 의 활용성이 증대되고 있다. 이를 위해 정부는 2002 년 의료법 개정을 통해 원격지원 및 전자의무기록에 관한 활성화를 위해 노력을 기울이고 있다[3]. 하지만 무선 환경에서의 개인 프라이버시 정보를 주고 받는 것은 매우 위험하다. 헬스케어의 데이터는 주로 건강정보를 실시간으로 의사와 소통하기 때문에 데이터의 유출 및 위/변조가 일어날 경우에는 환자에게 물질적 피해와 더 나아가 생명에도 위협이 될 수 있다..

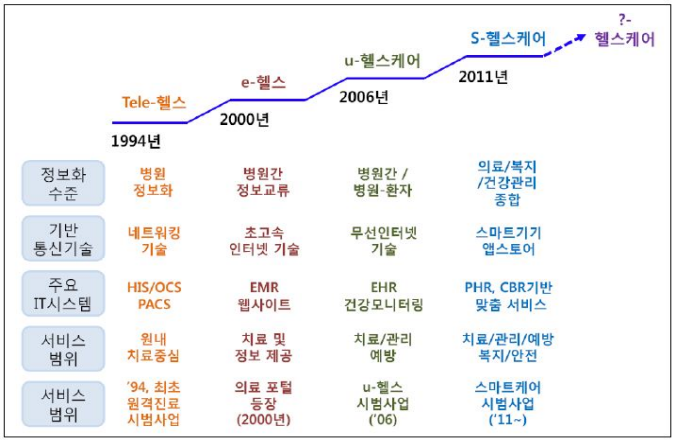
본 논문에서는 아이디/패스워드 와 USIM ID 정보를 이용한 자신이 소유한 물건을 통한 인증을 같이 사용함으로써 사용자인증의 안전성을 제공 하도록 설계하고 접근 권한에 있어서 모든 사용자가 아닌 의사에게 권한을 부여 받은 사용자만이 모바일 헬스케어 시스템에 접근할 수 있도록 설계 하여 보다 안전한 서비스를 제공 받을 수 있다. 또한 안전한 키 교환 방식을 제시함으로써 기밀성, 무결성, 사용자 인증, 모바일 보안 등의 안전성을 제공한다.

본 논문의 구성은 다음과 같다. 2 장 관련연구에서 기존 시스템의 문제점 및 해결방안, 3 장에서는 본 논문에서 제시하는 제안기법을 설명한다. 4 장에서는 안전성 분석 5 장에서는 결론 및 향후 연구 과제를 기술하였다.

2. 관련연구

2.1 스마트 헬스 케어(Smart Healthcare)

보건의료서비스는 IT 기술과 접목하면서 병원 중심의 원격의료 단계에서 점차 환자 중심의 e-헬스케어로 진화 되었고, 스마트시대의 도래와 함께 s-헬스케어의 단계로 진화 하였다[2].

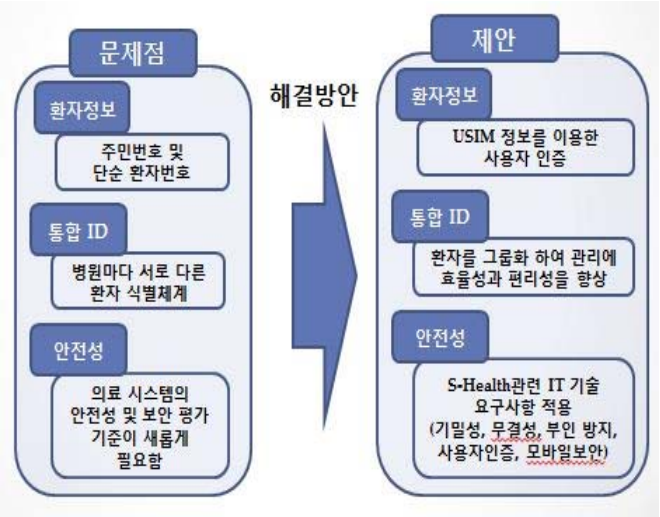


(그림 1) 헬스케어 진화 과정

* 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원 사업"의 연구결과로 수행되었음.

2.2 기존 시스템과 비교분석

기존의 u-Health 에서는 사용자 인증에 대한 문제점과 병원마다 서로 다른 환자 식별체계에 따른 환자 관리 그리고 시스템 안전성에 대한 평가기준에 대한 문제점이 있었다.



(그림 2) 기존 시스템의 문제점

(그림 2)에서 보다시피 본 논문에서 제안한 시스템에서는 USIM 정보를 사용한 사용자 인증, 환자를 그룹화 하여 의사가 환자를 관리하는데 있어서 효율성및 편의성 향상하였고, s-Health 관련 IT 기술 요구사항을 적용하였다.

2.3 사용자 인증기법의 유형

기존에 사용하고 있는 인증 기법으로는 세가지로 분류 할 수 있다. 첫째 생체인식(Biometrics)를 이용한 목소리식별, 망막검사, 지문검사 등 신체 일부를 통해 인증받는 방식이고, 둘째 본인이 소지하고 있는 물건들로 인증 받는 방식으로 OTP, 스마트카드, USB 토큰 등이 있다. 셋째로는 지식기반을 이용한 인증방식으로 대표적으로 아이디/패스워드 및 PIN 기반인증, 그래피컬 패스워드 등이 있다[5].

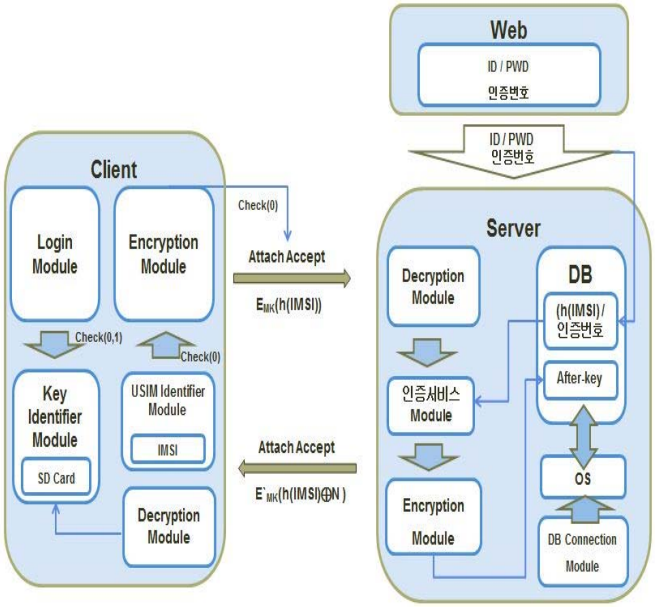
3. 제안기법

본 논문에서 제시하는 방안은 스마트 헬스케어 요구사항에 맞추어 기밀성, 무결성, 사용자인증, 모바일 보안에 맞추어 설계하였다.

3.1 시스템 구상도

본 논문에서 제시한 시스템은 클라이언트와 서버 안에 각각의 기능을 하는 모듈로 구성되어 있다.

- Login Module : 사용자가 아이디/패스워드를 입력하면 의사에게 인증 유/무를 확인하고 접근허가가 가능한 환자 일 경우 USIM Identifier Module 에서 USIM ID 정보를 전송한다.
- Key Identifier Module : 서버로부터 받은 인증 키를 관리하는 모듈이며, 현재 시스템은 USIM 메모리를 임의로 데이터를 변경 할 수 없기 때문에 SD Card 로 대체 사용하고 있다.
- USIM Identifier Module : 최초 기계내에 장착 되어있는 USIM ID 정보를 추출하여 가지고 있는 모듈이다. 최초 접속 사용자 일 경우 서버에 USIM ID 정보를 보내준다.
- Encryption Module : 추출된 USIM ID 정보를 이용하여 환자 인증에 필요한 인증 키를 생성 하는 모듈이다. 항상 새로운 임의의 난수를 USIM ID 정보와 mod 연산을 통해 클라이언트에게 전송한다.
- Decryption Module : 암호화 되어있는 인증 키를 복호화 하는 모듈
- 인증 Module : 인증 모듈은 서버 측에만 존재하며 Decryption Module 을 통해 복호화 된 값을 이전 값과 비교하는 모듈



(그림 3) 헬스케어 시스템 구성

3.2 사용자 인증

본 연구에서 제안된 프로토콜에 사용될 용어의 표기법을 <표 1>과 같이 정의 한다. (그림 3)에서는 등록단계, 로그인 단계, 키 교환 과정을 설명 하였다.

<표 1> 주요 약어 및 표기법

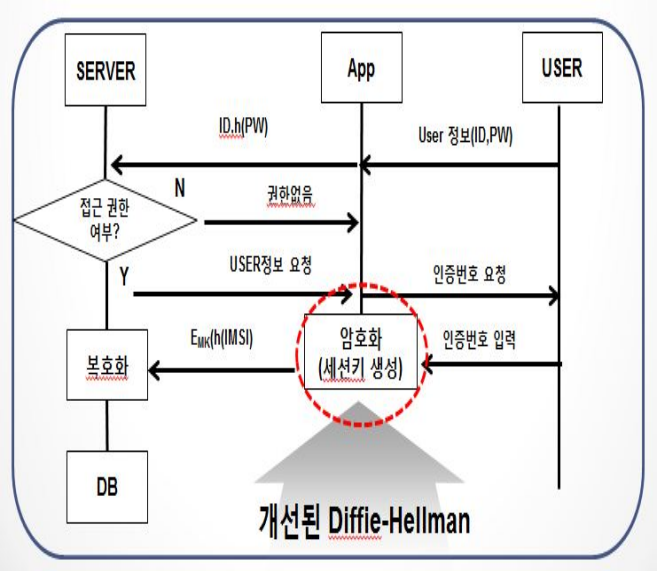
	용어	설명
Parameters	MK	사전에 인증 서버와 공유된 키 값으로 외부에 노출되지 않음 (Master Key)
	ID	사용자 ID
	PW	사용자 PWD
	IMSI	USIM ID 정보
	h(·)	해쉬함수
	N	랜덤 난수(Nonce)
	$E_{mk}(\cdot)$	Encryption Module 을 사용하여 MK 암호화된 인증키

3.2.1 등록 단계

Step 1. 서버는 의사에게 사용자가 접근권한을 부여 받았는지 체크 하고, 접근 가능한 사용자에 대해서 인증정보 요청을 한다.

Step 2. 세션 키 E_{MK} 로 IMSI 정보를 암호화 한 후 서버에 전송

Step 3. 서버는 대칭 키로 복호화 한 후 디비에 저장 한다.



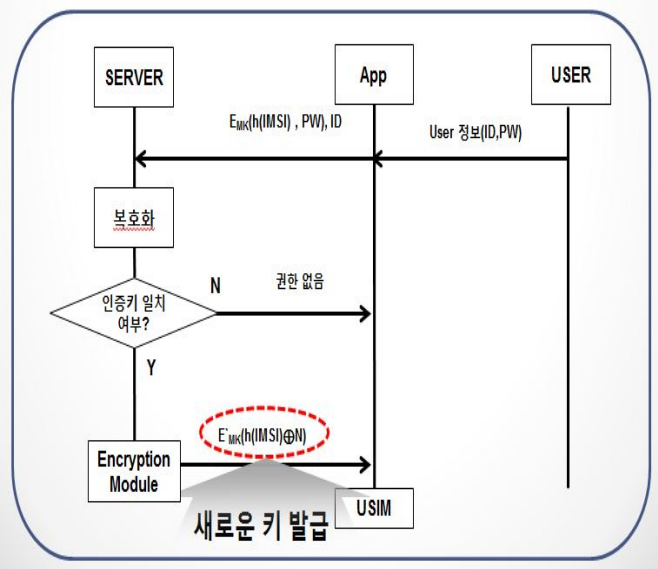
(그림 4) 등록과정

3.2.2 로그인 단계

Step 1. 사용자가 ID/PWD 를 입력하면 서버에게는 3 가지(IP/PW/E_{MK}(h(IMSI)⊕N)) 정보가 넘겨준다.

Step 2. 서버는 인증 키를 복호화 후 ID/PW 와 같이 인증 모듈을 통해 검증 받는다.

Step 3. 서버에서는 인증 단계가 끝나면 난수 값과 IMSI 값을 XOR 연산을 통하여 새로운 인증 키를 생성한다.



(그림 5) 로그인 과정

3.3 개선된 Diffie-Hellman

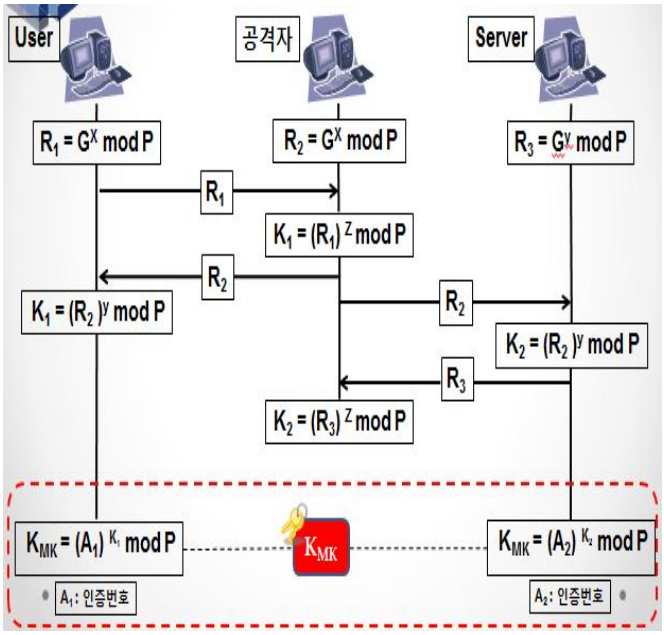
기존의 Diffie-Hellman 의 문제점인 중간자 공격을 해결하기 위한 방안이다.

Step1. 공격자에 의하여 사용자와 공격자 사이에 K_1 이라는 키가 생성된다.

Step2. 공격자에 의하여 공격자와 서버 사이에 K_2 라는 키가 생성된다.

Step3. 사용자와 서버는 각각 가지고 있는 인증 번호를 사용하여 다시 한번 연산을 함으로써 각각 K_{MK} 생성 하게 된다.

Step4. 공격자는 사용자에게 K_1 키로 암호화 값을 사용자에게 전송하게 되면 K_{MK} 로 복호화가 불가능하기 때문에 중간 침입을 감지 할 수 있다.



(그림 6) 개선된 Diffie-Hellman

4. 안전성 분석

4.1 패스워드 공격

사용자의 정보를 추측하거나 무차별 공격으로 패스워드가 유출이 될 경우 제안기법에선 USIM ID 정보를 사용하여 인증을 하기 때문에 패스워드가 유출 되었을 경우에도 기밀성을 보장할 수 있다.

4.2 재전송공격(Replay Attack)

클라이언트가 서버에게 자신을 증명할 인증 키를 보낼 때 공격자가 이를 가로채 다음 접속 시 재사용 할 경우 본 논문에서는 매 접속 시 서버 에서 새로운 키를 생성하여 클라이언트 에게 전송 하기 때문에 재전송 공격에 안전 할 수 있다.

4.3 중간자 공격(Man-in-the-Middle-Attack)

기존의 세션 키가 공격자에 의해 노출 되었을 경우에도 인증 번호를 이용하여 사용자와 서버간의 새로운 세션 키를 가지고 있기 때문에 중간에 공격자가 자신의 세션 키로 데이터를 암호화 한다면, 사용자 A 와 세션 키가 불일치 하기 때문에 인증이 불가능하다.

4.4 요구사항에 대한 안정성 평가

s-Health 에서 제시하는 스마트 보안 기술 핵심 요소를 기반으로 안전성 분석을 하였다. 기밀성, 무결성, 사용자 인증, 모바일 보안 이렇게 4 가지로 구분 되어 있다.

<표 2> 안전성 분석

분류	설명
기밀성	IMSI 정보를 사용하기 때문에 패스워드가 유출이 되어도 다른 허가 받지 않은 사용자는 접속 할 수 없다.
무결성	인증번호를 이용하여 세션 키를 암호화 하기 때문에 외부 공격자가 침입해 데이터를 위/변조할 수 없다.
사용자인증	아이디/패스워드와 IMSI 를 이용하여 Two-Facter 방식으로 인증을 실시하며, 중간자 공격에 대비하여 세션 키 안전성을 강화 하였다.
모바일 보안	다른 디바이스에서 어플리케이션에 접속을 시도 할 때 사용자의 정보와 IMSI 정보가 일치 하지 않기 때문에 접속이 불가능하다.

5. 결론

본 논문에서는 무선환경에서의 환자의료 정보보호를 위해 사용자 인증을 통한 어플리케이션의 접근 시스템을 제안하고 이를 모바일 헬스케어 시스템에 적용함으로써 환자에게 보다 안전하고 믿을 수 있는 서비스를 제공 한다. 기존 사용되고 있는 헬스케어 시스템들은 아이디/패스워드가 유출 될 경우 환자의료 정보의 유출이나 위/변조에 대한 문제점이 있다.

본 논문에서는 환자가 의사에게 수락요청을 하고 의사는 환자를 수락 해 줌으로써, 기밀성을 유지하고 디피 헬먼 키 분배 방식의 최대 약점인 중간자 공격을 해결 하였다. 또한 회원가입 시 인증번호를 입력받아 세션 키 생성 시 2 차적인 mod 연산을 통하여 전자서명 같이 복잡하고 별도의 비용의 발생 없이 시스템의 안전성을 높였다. 현재 시스템은 스마트 헬스케어 보안 요구 사항은 충족 하지만 아직 성능 평가는 이루어 지지 않았다. 또한 부인방지에 헬스케어 시스템에서의 부인방지에 대한 명확한 기준을 새워 이에 대한 해결책도 필요하다. 제안한 인증 메커니즘을 구현하여 그 안전성 및 성능을 증명 할 계획이다.

참고문헌

[1] 방송통신위원회, “제 5 차 스마트폰 이용실태 조사(2012 년 상반기)”, 방송통신위원회 보도자료, 2012.08.28

[2]한국정보화진흥원 “스마트 공공보건의료 서비스 도입 방안”, 2011. 06.07

[3]W. Diffie and M.E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, 1976.11, pp. 644-654

[4] 문영순 ”의료서비스에서의 정보보호 필요성”, 10.02.03

[5] 금융결제원 금융결제연구소, “최근 인증기술 관련 현황”, 2012.01

[6] 김성제, 조용환, 이태우 “모바일 환경에서 USIM ID 를 이용한 어플리케이션 인증기법” 충북대학교 2011 추계학술대회 논문집, 2011.11, pp.99-106

[7] 이윤진,이재근,조인준 “이동전화기를 이용한 Diffie-Hellman 키 교환기법의 개선방안” 한국해양정보통신학회논문지, 2009.10.26

[8] 이윤석,김은,정민수” USIM 기반 안드로이드 플랫폼에서의 어플리케이션 라이센스 관리 기법” 멀티미디어학회논문지 제 14 권 제 2 호, 2011.2, pp.238-248