http://dx.doi.org/10.14400/JDC.2015.13.5.219

u-health 시스템을 이용한 사용자 인증 프레임워크 설계

추연수*, 진병욱*, 박재표**, 전문석*
숭실대학교 일반대학원 컴퓨터학과*, 숭실대학교 정보과학대학원 정보보안학과**

Design The User Authentication Framework Using u-health System

Yeun-Su Choo*, Byung-Wook Jin*, Jae-Pyo Park, Moon-Seog Jun***
Dept. of Computer Graduate School Soongsil University*
Graduate School of Information Sciences Soongsil University**

요 약 OTP(One Time Password)는 인터넷 뱅킹 등에서 사용자의 인증을 위해서 많이 사용되는데 이를 위해 사용자는 OTP 발생기 또는 보안 카드 등을 소지하여야 한다. 또한 OTP 발생기 또는 보안 카드를 분실하였을 경우 OTP가 노출될 수 있는 가능성이 있다. 본 논문은 사용자 인증을 위해 사용되는 OTP 분실 및 복제에 대한 단점을 대체하기 위해서 USN의 한 분야인 u-Health의 다양한 기술을 이용하여 수집된 개인의 건강 정보를 활용한 사용자 인증 프레임워크를 제안한다. 본 논문에서 제안하는 사용자 인증 프레임워크는 분실 위험이 없으며, 개인의 건강 상태가 매일 달라지기 때문에 여러 가지 항목들을 조합한다면 충분히 OTP로서의 활용 가치가 있다. 또한 제안하는 프로토콜은 신뢰하는 기관들의 인증서로 암호화되어 서비스 제공자에게 전달되기 때문에 노출에 안전하며 OTP 생성을 위한 기기 및 카드를 소지할 필요가 없기 때문에 기존 OTP를 사용하는 은행, 쇼핑몰, 게임 사이트 등에서 유용하게 사용할 수 있다.

주제어 : OTP, USN, u-health, 사용자 인증, 건강정보

Abstract OTP(One Time Password) is for user authentication of Internet banking and users should carry their security card or OTP generator to use OTP. If they lost their security card or OTP generator, there is at risk for OTP leak. This paper suggests a new User Authentication Framework using personal health information from diverse technology of u-Health. It will cover the problem of OTP loss and illegal reproduction A User Authentication Framework is worthy of use because it uses various combinations of user's physical condition which is inconstant. This protocol is also safe from leaking information due to encryption of reliable institutes. Users don't need to bring their OTP generator or card when they use bank, shopping mall, and game site where existing OTP is used.

Key Words : OTP, USN, u-health, User Authentication, Health Information

1. 서론

USN(Ubiquitous Sensor Network)[1]이 발전하면서 USN 기술을 이용한 다양한 형태의 서비스가 제공되고

Received 17 March 2015, Revised 20 April 2015
Accepted 20 May 2015
Corresponding Author: Moon-Seog Jun
(Dept. of Computer Graduate Soongsil University)
Email: mjun@ssu.ac.kr

ISSN: 1738-1916

있다. 특히 USN 기술을 이용한 u-Health[2,3] 분야는 웨어러블 디바이스(Wearable Device)[4]를 이용하여 실시간으로 사용자의 건강 상태를 체크, 상담 및 처방을 통하여 질병을 조기에 발견하여 사용자 삶의 질을 높일 수 있는 유익한 분야이다. u-Health 기술을 이용하여 수집한 건강 정보는 사용자가 섭취하는 음식, 주거환경, 업무환경 등의 여러 가지 원인에 따라 변화무쌍하게 변하게 된다. 또한 이러한 건강 정보는 항목별(혈압, 당수치 등)로 일정한 구간을 형성하지만 매일 변하게 된다. 따라서 이러한 항목들을 이용하여 개인인증을 위한 OTP(One Time Password)로 충분히 사용할 수 있다. OTP[5,6,7,8]는 한번만 사용하는 패스워드를 말하며 인터넷 뱅킹과 같이 중요한 결제 시스템 등에 사용된다. 이러한 OTP를 위해서 OTP 발생기를 소지하거나 인증번호 조합을 위한 코드표를 활용한다. 이 때 발생기 또는 코드표를 분실하거나, 복제된다면 사용자 인증을 위한 OTP는 그 기능을 상실하게 되고 더 나아가 악의적인 목적으로 활용될 가능성도 있다. 따라서 본 논문에서는 u-health 기술을 이용하여 수집되는 개인 건강 정보를 이용하여 위와 같은 OTP의 단점을 대체하기 위한 사용자 인증 프레임워크를 제안한다. 제안하는 프레임워크는 화장실의 세면대와 변기, 웨어러블 디바이스 등을 이용하여 수집된 개인 건강 정보와 신뢰할 수 있는 기관에서 발급한 개인 인증서, 서비스 제공자의 인증서들과 함께 연동되어 사용자를 인증하는 요소로 활용된다. u-health 기술을 이용하여 수집되는 개인 건강정보는 수집하는 종류가 매우 다양하며 매일 수집되기 때문에 그 양이 매우 방대하므로 사용되는 건강정보의 날짜와 항목을 조합하면 매우 다양한 결과를 OTP 정보로 활용할 수 있게 된다. 이렇게 도출된 개인정보들을 서로 간단한 연산을 거치게 되면 건강정보로서의 의미도 상실하게 되어 개인의 건강 정보가 다른 분야 또는 다른 서비스에 활용되지 않을 수 있다.

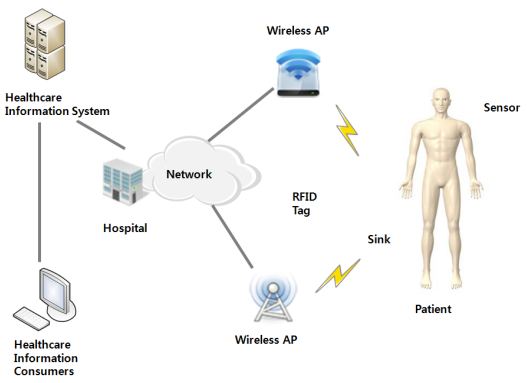
본 논문의 구성은 2장에서 관련연구로 u-health 기술과 OTP에 대해서 서술하고 3장에서는 제안하는 u-health를 이용한 사용자 인증 프레임워크에 대해서 기술하고 4장은 제안하는 사용자 인증 프로토콜의 안전성을 기존의 사용자 인증 시스템들과 비교한 후 5장에서 향후 연구 방향을 기술한 후 결론을 맺는다.

2. 관련연구

2.1 u-health Care

2.1.1 u-health Care Service

u-health Care 서비스는 공간적, 시간적 제약 없이 언제 어디서나 환자가 생활공간 속에서 다양한 의료 장비를 통하여 수집된 사용자의 생체 정보를 중앙의 원격 의료 서비스 시스템으로 통신하는 서비스를 말한다. 또한 u-health Care는 다양한 기술이 융합된 기술로서 모니터링 센서를 이용한 기기를 통해 수집한 환자의 건강 정보를 이용하여 의료진들이 사용자의 건강 피드백을 제공해 준다. 환자와 의료진 및 관련 응용 서비스 등으로 구성될 수 있다. 무선 의료기기 및 센서를 활용하여 데이터를 수집 후 전송하는데, 대표적으로 활용되고 있는 기술로는 Zigbee[9]나 UWB(ultra wideband)[10] 방식의 센서 통신 프로토콜이 사용될 수 있으며 WLAN이나 3GPP, 이더넷 등이 있다. 아래의 [Fig. 1]은 u-health care Service 구성도이다. 이와 같이 u-health care Service는 다양한 센싱 기술과 무선 기술들이 융합되어 환자의 건강상태를 실시간으로 체크하며, 상담 및 처방까지 할 수 있는 아주 유용한 서비스이다. 하지만 u-health Care System으로 송신된 데이터는 환자의 건강상태, 생활패턴 등에 관한 정보이며, 지극히 환자의 사적인 정보이므로 보호가 필요하다.



[Fig. 1] U-Healthcare Service Diagram

2.1.2 u-health Care 보안요구사항

u-health Care는 개인의 생체 정보 및 주변 환경에 관한 모니터링 정보 등 개인적인 정보를 주로 다루고 있고

유무선 네트워크와 절대적으로 밀접한 연관을 맺고 있어 보안 및 프라이버시 측면에 대한 보완사항이 요구되고 있다. u-health 서비스들은 유무선 네트워크 기반 서비스를 통하여 데이터를 송수신하므로 기존에서 발생하던 보안상 취약점 및 공격이 존재하고 있다. 따라서 안전성, 신뢰성 보장 및 데이터 보호를 위한 기술적 대안이 기본적으로 요구되고, 아래와 같은 기존의 다른 서비스와는 다른 보안 요구 사항들이 존재한다[11].

1. 개인 의료 정보권한 관리 및 위임, 기술적, 법제도적 지원책의 요구

정확한 진료를 받기 위해 환자개인의 생체 정보를 포함한 질병 내력, 가족력, 신체적 특징 등의 개인 의료 정보가 충분히 제공되어야 한다. 또한 중복된 검사 및 반복적인 의료 조치를 막기 위해 정보가 공유되어야 한다. 하지만 개인 정보가 타당한 대상자에 의해 의료 서비스 목적에 맞게 최소한의 공유가 이루어지기를 기대해야 한다. 그러므로 의료 정보에 대한 프라이버시 차원에서 개인 의료 정보권한에 대한 보완 지원책이 요구되어야 한다[11,12].

2. 내부자에 의한 정보 유출 위험성의 대책

내부자 및 의료진의 불법적인 의료 정보 열람과 이용을 막고 책임 소재를 판단하기 위해서는 보안 감사 체계가 필요하다. 대부분의 병원에서는 데이터 습득 이후 개인정보보호 관리에 대한 의무사항 준수가 미약하므로 감사 체계가 보완되어야 한다[11,13].

3. 독립성을 보장하는 인증서비스 및 책임을 부여하기 위한 기술 요구

향상된 수준의 의료 서비스와 개인의 의료 건강 정보에 대한 접근성을 용이하게 하기 위하여 향후 다양한 병원 정보 서버 간 환자 건강 정보 공유가 빈번하게 이루어진다. 이에 따라 다양한 의료 도메인 간 개인의 건강 및 의료 정보를 교환 시, 인증된 도메인 간에 가용한 정보만을 안전하게 송수신 할 수 있는 보안 기술이 요구된다[11,13].

4. 국가 통합형 ID 관리 시스템 모델 설계

병원마다 서로 다른 환자 식별 체계가 사용되고 있어 다수 사용자의 ID 정보를 관리해야하는 필요성이 있다. 병원 간 건강/의료 정보 공유 시, 환자를 포함한 인가 받은 정보 소비 주체들이 불필요한 개인 정보 노출 없이 익명성을 보장받으면서도 정상적으로 인증 및 식별 가능한 ID 관리 체계가 필요하다[11,14].

2.2 OTP(One Time Password) 생성방식 및 보안 요구사항

2.1.1 OTP 생성방식

OTP 생성 방식은 OTP 토큰과 인증 서버 간의 동기화 여부에 따라 비동기화 방식과 동기화 방식으로 나누어진다. 비동기와 형식에는 질의-응답 방식이고, 동기화 방식에는 시각 동기화, 이벤트 동기화, 조합 방식이 있다[15].

1. 비동기화 방식

비동기화 방식은 OTP 토큰과 인증 서버 간에 인증 요청 시 사용자가 직접 임의의 난수값을 OTP 토큰에 입력하여 OTP 를 생성하는 방식을 말한다. 대표적인 예로는 질의- 응답(Challenge- Response) 방식으로 사용자가 OTP 인증 요청 시 인증서버로부터 받은 질의 값을 직접 OTP 토큰에 입력하여 응답 값(난수 형태)을 생성하는 방식이다[5,6].

2. 동기화 방식

동기화 방식은 OTP 토큰과 인증 서버 간에 미리 공유된 비밀 정보와 동기화 정보에 의해 OTP 가 생성되는 방식이다. 비동기화 방식에 비해, OTP 토큰과 인증 서버간에 반드시 동기화가 이뤄져야하며 사용자 입력 불편, 기존 ID/패스워드 애플리케이션과의 호환 어려움 등 비동기화 방식의 한계점을 개선하였다. 동기화 방식은 동기화 정보에 따라 대표적으로 시각 동기화, 이벤트 동기화, 조합 방식으로 나눌 수 있다. 이때 OTP 입력 값으로 시각 동기화 방식은 현재시각과 공유된 비밀 키 값을 받고, 이벤트 동기화 방식은 이벤트 카운터 값과 공유된 비밀 키 값을 받으며, 조합 방식은 시각 값, 이벤트 카운트 값, 공유된 비밀 키 값을 받는다. 시각 동기화 방식 시각 동기화 방식은 서버와 OTP 토큰 간에 동기화된 시각 정보를 기준으로 특정 시간 (보통 1 분)마다 변하는 비밀번호를 생성하는 방식이다[5,8].

2.1.2 OTP 생성 알고리즘 보안 요구사항

OTP 생성 알고리즘은 표준 알고리즘을 기본적으로 사용하여야 한다. OTP 생성 알고리즘이 만족해야 하는 보안 요구 사항은 아래 <Table 1>과 같다[15].

〈Table 1〉 OTP Creating Algorithm Security Requirements

Security Requirements	Details
standard algorithm for creating algorithm	- Use creating pseudo random numbers algorithm tested for recommended or required standard (Satisfy unpredictability) - Use seed value more than 126bit entropy
recommended standard algorithm for OTP creating algorithm	-Use standard cipher algorithm more than intensity of 112bit for symmetric cipher algorithm - Use Hash algorithm more than intensity of 112bit for one-way Hash algorithm - Using HMAC(Hash-based Message Authentication Code) is recommended which is more safe. Enter OTP key more than 160bit
OTP should have more than 6-digit number of decimal number	output at least 6-digit number of decimal number

3. 제안하는 u-health 시스템을 이용한 사용자 인증 프레임워크

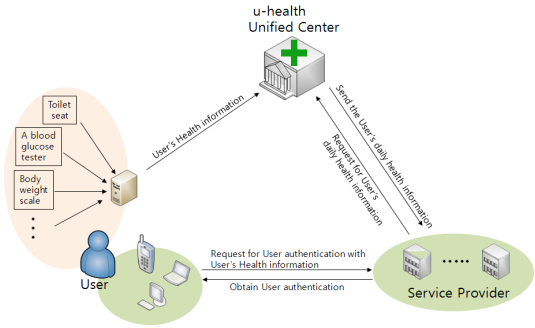
금융 사이트 등에서 안전한 거래를 위한 사용자 인증 과정은 인증서 이외에 추가적인 요소들과 복수 채널을 이용한다. 이에 발생하는 번거로움을 해결하기 위하여 사용자의 health 정보를 이용하는 사용자 인증 프레임워크를 제안한다. 제안하는 방법은 특별한 형태의 서비스에 귀속되지 않고 사용자 인증을 필요로 하는 곳이면 어디든 사용할 수 있도록 설계하였다. 제안하는 프레임워크에는 가정 사항이 몇 가지 있다. 본 논문의 가정 사항은 다음과 같다.

- USN을 기반으로 한 u-health 시스템의 인프라가 구성되어 있으며, 보안상의 문제가 없다.
- 사용자 인증을 위한 개인의 health 정보는 사용자 인증을 위해 사용될 뿐 사용자 인증을 요청하는 기관 및 업체에서 보관하지 못한다.
- 국가 및 의료보험공단 등 신뢰성 있는 기관에서 u-health 시스템을 통해 얻어진 정보를 통합 관리한다.
- 서비스 제공자는 신뢰성 있는 인증기관에 자신을 등록하여 악의적인 목적으로 제작된 사이트가 아님을 인증 받아 인증서를 보유하고 있다.

3.1 제안하는 프레임워크의 구조

제안하는 프레임워크는 사용자 인증을 위해서 u-health 시스템을 통해 획득한 개인 health 정보를 이용한다. 제안하는 사용자 인증 프레임워크의 전체적인 구조는 [Fig. 2]와 같이 통합 u-health 센터(HUC : u-Health Unified Center), Service Provider(SP), 사용자의 집에 설치된 u-health 시스템(UHS : User's u-Health System)과 SP에게 서비스를 요청하기 위한 여러 디바이스(UD : User's Device)들로 구성된다. 미리 가정한 것과 같이 HUC와 UHS의 정보교환은 보안상 문제가 없다.

UHS는 매일 변하는 사용자의 health 정보를 수집하여 HUC로 전송한다. UHC는 사용자들의 health 정보를 매일 수집하여 개인 DB에 저장하여 보관하며, 개인 건강을 관리한다.

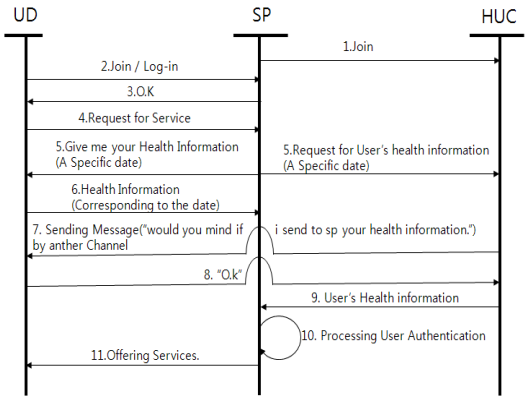


[Fig. 2] The overall structure of The proposed framework

사용자는 UD를 통하여 SP에게 서비스를 요청하면 SP는 사용자 인증을 위해서 사용자와 HUC에 해당 사용자의 건강 정보를 요청한다. 매일 변하는 사용자의 건강정보는 기존에 사용하던 하나의 OTP(One Time Password)의 역할로 활용된다. 사용자의 건강정보는 혈당, 혈압, 체중 등 상당히 다양한 정보를 수치화 할 수 있으며, 매일 변하기 때문에 OTP로서 충분히 사용가능하다.

3.2 사용자 인증 프로토콜

USN을 기반으로 구축된 UHS은 HUC와 UD에게 매일 아침 사용자의 건강정보를 송신한다. 사용자의 다양한 건강정보는 UHS와 UD에 날짜별로 저장되며. UD는 작은 저장 공간으로 인하여 특정 기간을 정하여 정해진 기간만 사용자의 건강정보만 보관한다. [Fig. 3]은 사용자의 건강정보를 이용하여 SP가 서비스 요청을 하는 사용자를 인증하는 과정이다.



[Fig. 3] User Authentication Protocol.

1) 서비스 제공자 등록

SP는 자신이 제공하려는 서비스 사이트가 악의적인 사이트가 아니라는 것을 증명하기 위하여 모두가 신뢰하는 인증기관에 자신을 등록하고 인증서를 이용하여 HUC에 자신을 등록한다.

2), 3) 사용자 회원가입 및 로그인

사용자는 서비스 받으려는 사이트에 회원가입을 하고 로그인 한다.

4) 서비스 요청

사용자는 원하는 사이트에 로그인 후 원하는 서비스를 요청한다.

5) 사용자 인증 정보 요청

SP는 자신에게 서비스를 요청하는 사용자에게 사용자만 가지고 있는 사용자 인증정보, 즉 사용자의 건강 정보를 요청하고, 사용자가 보내온 사용자 인증정보를 확인하기 위하여 HUC에게 사용자의 건강정보를 요청한다. SP는 자신의 인증서를 이용하여 요청 메시지를 서명하여 보낸다. 이 때, 사용자와 HUC에게 보내는 사용자 인증 정보는 특정 날짜를 랜덤하게 선택하여 요청하며, 사용자의 다양한 건강 정보 중 랜덤하게 선택하여 2개 이상 요청한다.

6) 사용자 인증 정보 전송

사용자 인증정보를 요청받은 사용자는 SP의 공개키를 획득하여 SP를 확인한 후 요청받은 사용자 인증정보를 자신이 보유한 UD에서 찾아 SP에게 전송한다. 자신의 사용자 인증정보를 SP에게 전송할 때 사용자는 획득한 SP의 공개키를 이용하여 자신의 건강정보를 암호화한 후 전송한다.

7), 8) HUC의 사용자 건강정보 제공 여부 확인

SP에게서 사용자의 건강정보를 요청받은 HUC는 자신이 가지고 있는 사용자의 건강정보를 SP에게 제공해도 되는지 사용자에게 확인한다. 이 때, 사용자의 정보 제공에 대한 동의 메시지는 공개된 인터넷 채널이 아닌 유선 전화 및 휴대전화를 이용한다.

9) 사용자 건강정보 SP 제공

HUC는 사용자의 동의를 획득한 후 SP에게 요청받은 특정날짜의 특정정보 2개 이상을 전송한다. 이 때, HUC는 SP의 공개키를 획득한 후 SP의 사용자의 건강정보를 암호화하여 전송한다.

10), 11) 사용자 인증 정보 조회 및 서비스 제공

SP는 자신의 개인키로 UD와 HUC가 보내온 사용자 인증정보를 복호화하여 두 정보가 일치하는지 확인한 후 사용자 인증 과정을 마무리한다. 사용자 인증과정이 끝나면 SP는 사용자 인증에 인증정보를 영구히 삭제한다. 사용자 인증이 성공적으로 마무리되면 SP는 사용자가 요청한 서비스를 제공한다.

UHS로부터 매일 수집된 사용자의 건강정보는 상황과 환경, 먹는 음식들에 따라 다르게 변하게 된다. 이렇게 매일 다양하게 변화하는 사람의 건강정보들은 어느 것보다 랜덤한 정보가 되며, 이러한 정보는 OTP로서의 충분한 가치를 가지게 된다. 이 정보들을 이용하여 개인을 인증할 수 있다.

4. 비교분석

본 장에서는 앞 장에서 제안한 인증 프레임워크와 기존의 OTP를 이용한 사용자 인증 시스템과의 안전성을 비교 분석한다. 시스템 구조에 따른 비교분석하였다. 아래의 표는 기존 OTP 인증시스템과 제안한 인증시스템과의 비교분석한 내용이다.

〈Table 2〉 Security Analysis On OTP Based Authentication System and Proposed Authentication System

	OTP Based Authentication System	Proposed authentication System
Impersonation Attack	△	○
Identification and authentication means	×	○
Impossible to replication	×	○
Replay Attack Prevention	△	○
MITM : Main-In-The-Middle Prevention	×	○
Personal Information Management	×	○

1) 가장공격(Impersonation Attack) 방지

본 논문에서는 사용자의 건강정보를 기반으로 인증 시스템을 설계하였으므로, 가장 공격이 불가능 하다. 만약 공격자가 사용자의 건강정보를 가로챈 후 가장 공격을 하는 경우, SP에서는 사용자로부터 단 하나의 건강정보 값이 아닌 특정한 일자의 건강정보 값을 랜덤형식의 값을 활용하여 인증한다. 그리고 인증과정이 완료되면 사용자의 정보를 폐기함으로써 가장공격은 실패한다.

2) 식별 및 인증수단

(Identification and authentication means)

기존의 OTP 기반 인증 시스템은 별도의 OTP 장비가 필요하다. 또한 공격자에 의해 OTP 목록이 유출 및 탈취가 되면 안정성에서 매우 취약하다는 단점이 있다. 하지만 제안한 인증 시스템에서는 사용자의 건강정보를 활용하여 인증함으로서 기존 OTP의 휴대성을 보완할 수 있으며, Password 목록 유출 및 탈취에 대한 취약점도 사용자의 모든 건강 정보가 유출 및 탈취되는 것이 아니기 때문에 상대적으로 안전하다.

3) 복제 불가능(Impossible to replication)

USN을 기반으로 구축된 UHS은 HUC와 UD에게 매일 아침 사용자의 건강정보를 송신 후 이를 기반으로 각각의 다른 패턴으로 생성하여 SP로 인증을 받는 시스템이다. 사용자 고유의 건강정보를 사용하고 인증 후 바로 폐기함으로써 복제공격에 대한 피해를 막을 수 있다.

4) 재전송 공격 방지(Replay Attack Prevention)

인증과정에서 HUC는 SP에서 사용자 정보를 확인하고, 자신이 가지고 있는 사용자의 건강정보를 상호간에 확인함으로써 재전송 공격이 실패하게 된다. 또한 사용자 정보제공에 대한 메시지는 2 Channel 인증방식을 사용함으로써 안전성이 강화된다. 마지막으로 기존의 OTP 인증 방식은 장비를 분실을 해서 공격자가 악용하여 재전송공격을 할 수 있으나, 본 논문에서 사용자 기반의 건강정보를 활용하여 장비에 대한 분실에 대한 악용 피해를 막을 수 있다.

5) 중간자 공격 방지

(MITM : Main-In-The-Middle Prevention)

공격자는 SP의 개인키를 알 수 없으므로 SP 위장하여 사용자의 개인정보 및 데이터를 탈취하는 중간자 공격을 할 수 없다. 그러므로 SP의 개인키 값을 알 수 없으므로 SP의 공개키로 암호화된 사용자의 건강정보를 UD, HUC로 복호화 할 수 없으므로 중간자 공격에 실패한다.

6) 사용자 측면의 개인정보 관리

사용자의 개인정보유출시 심각환 사생활 침해들이 발생할 수 있으므로 의료기관 환자의 건강정보관리 필요성에 대하여 대두되어지고 있다. 하지만 제안한 프레임워크에서는 SP가 받게 되는 건강정보는 어떤 건강 정보인지 알 수 없다. 어떤 항목의 건강 정보인지 알 수 없기 때문에 SP는 건강정보로서의 활용가치가 없다. 단지 인증을 위한 정보만 전달받게 된다. 또한 SP가 HUC와 UD로부터 수신한 정보는 확인 후 인증절차가 완료되면 인증정보를 영구히 삭제하여 개인정보유출에 관한 피해를 방지한다.

5. 결론

본 논문은 u-health System에서 개인의 건강 체크를 위해 수집하는 건강 정보를 이용하여 사용자를 인증할 수 있는 프레임워크를 제안하였다. 제안하는 사용자 인증 프레임워크는 매일 변화하는 자신의 건강 정보들을 이용하기 때문에 기존 OTP를 사용할 때 OTP 발생기 및 보안 카드 등을 소지할 필요가 없다. 이로서 기존의 OTP를 사용할 때 발생했던 불편함과 OTP 노출 위험은 비교 분석에서 기술한 것처럼 제안하는 사용자 인증 프레임워크가 우수하다.

하지만 제안 프레임워크는 u-health system 인프라가 제공되어야하며, 만약 개인이 u-health system에 매일 자신의 건강 상태를 체크해야만 하는 불편함이 있을 수 있다.

또한 본 논문에서 가정하고 있는 u-health system의 보안상 문제점이 발생하면 개인 건강 정보가 노출될 수 있는 문제가 발생하게 된다. 개인 건강 정보를 이용하여 사용자를 인증할 때, 인증에 필요한 정보가 개인 건강 정보라는 것을 알지 못하도록 관리하여야 한다. 따라서 개인의 건강 정보를 이용한 개인 인증 시에 개인 정보 노출 방지 방안이 향후 연구로 필요하다.

REFERENCES

[1] Buratti Chiara, Conti Andrea, Dardari Davide, Verdone Roberto, "An Overview on Wireless Servor Networks Technology and Evolution", Sensor, vol.9, no.8, pp.6869-6896, 2009

[2] TTA, u-Health Service Reference Model , TTA, 2010.12

[3] So-Yeon Min, Byung-Wook Jin, "Disign of Integrated Authentication S초듣 랙 Safe Personal Information Management in a U-Health Wnvironment", Journal of the Korea Academia-Industrial cooperation Society, Vol 15, No 6, pp.3865-3871, 2014

[4] Billinghurst, Mark and Thad Starner, "Wearable Devices : new ways to manage information.", Computer, vol. 32, no. 1, pp 57 -64, Jan. 1999.

[5] TTA, Road map for the one time password standards,TTA, 2011.12

[6] DOI: http://www.ietf.org/rfc/rfc2289.txt

[7] DOI: http://www.ietf.org/rfc/rfc4226.txt

[8] DOI: http://www.ietf.org/rfc/rfc6238.txt

[9] Kwangho Won, JeaHo Kim, JunJea Yu, "ZigBee", Journal of TTA, Vol. 94, pp 112-121, 2004

[10] Lei Zhu, Sheng Sun, and Wolfgang Menze, "Ultra-Wideband(UWB) Bandpass Filters Using Multiple-Mod Resonator", IEEE Microwave and Wireless Components Letters, vol. 15, no. 11, pp.1-3, Nov. 2005

[11] A Development of Standard and Bio-Authentication Technology for Telemedicine, KISA, 2007.12

[12] TTA, Information Security Reference Model for u-Health Service, TTA, 2010.12.

[13] TTA, Information Security Reference Model for u-Health Service, TTA, 2011.6

[14] TTA, u-Health Service Reference Model , TTA, 2010.12

[15] TTA, Security Requirements for the OTP Token, TTA, 2010.12

추 연 수(Choo, Yeun Su)

- 2003년 8월 : 호서대학교 컴퓨터공학과(공학사)
- 2005년 8월 : 숭실대학교 컴퓨터학과(공학석사)
- 2005년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정
- 관심분야 : 컴퓨터통신, 정보보안, 사용자 인증, 암호학
- E-Mail : lets-priase@hanmail.net

진 병 욱(Jin, Byung Wook)

- 2010년 2월 : 청강대학교 멀티미디어학과 (문학사)
- 2013년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정
- 관심분야 : 네트워크 보안, 인증 시스템, 사물지능통신
- E-Mail :quddnr4511@naver.com

박 재 표(Park, Jae Pyo)

- 1998년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2004년 9월 ~ 2009년 8월 : 숭실대학교 정보미디어기술연구소 전임연구원
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학 교수
- 관심분야 : 컴퓨터 통신, 정보보안, 포렌식, 암호학
- E-Mail : pjerry@ssu.ac.kr

전 문 석(Jun, Moon Seog)

- 1981년 2월 : 숭실대학교 전자계산학과 (공학사)
- 1986년 2월 : University of Maryland Computer Science (석사)
- 1989년 3월 : University of Maryland Computer Science(박사)
- 1989년 3월 ~ 7월 : Morgan State University 조교수
- 1989년 9월 ~ 1991년 2월 : New Mexico State University Phsical Science Lab 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 교수
- 관심분야 : 정보보호., 전자여권, 전자상거래
- E-Mail : mjun@ssu.ac.kr