NFC 기반 U-Health 서비스 인증시스템 설계

윤지상*, 박석천**, 박준식***
*가천대학교 일반대학원 모바일소프트웨어학과
**가천대학교 컴퓨터공학과 정교수(교신저자)
***인성정보 개발서비스팀장
e-mail : yjs8237@naver.com

Design of U-Health Service Authentication System Based-on NFC

Ji-Sang Yun*, Seok-Cheon Park**, Jun-Sik Park***
*Dept of Mobile Software, Gachon University
**Dept of Computer Engineering, Gachon University
***Dept of Development Service, In-sung Information co., ltd

요 약

현재 많은 사람들이 스마트폰을 이용하고 있으며 스마트폰을 활용한 IT 기술들이 나날이 발전하고 있다. 또한 스마트폰을 이용 하여 사람들이 생활하는데 있어서 더욱 더 편리한 생활을 할 수 있도록 서비스 환경을 제공해준다. 그 중 대표적인 기술이 U-Health(Ubiquitous-Health) 기술 이며 U-Health 기술은 건강증진과 고령화 사회를 대비하기 위한 효과적인 문제해결 방안으로 주목받고 있다. U-Health 서비스는 스마트폰의 각종 센서를 활용하여 환자의 건강 상태를 체크하고 실시간으로 업데이트 하여 환자의 상태를 더욱 효율적으로 관리할 수 있다. 그러나 환자와 병원 서버 간에 데이터 단일화, 통신문제 등으로 인해서 아직까지는 많이 활용되고 있지 않는 현실이다. 또한 스마트폰으로 인한 환자의 개인신상 정보가 쉽게 노출될 수 있다는 단점이 있다. 따라서 본 논문에서는 NFC(Near Field Communication) 기반에서 환자와 병원간에 신뢰성 있는 데이터 전송을 위한 인증 시스템을 설계 하였다.

Ⅰ. 서 론

현재 스마트폰의 사용자가 급증하고 있다. 스마트폰의 사용자가 점점 늘어남에 따라 스마트폰을 활용한 IT 기술 또한 다양하고 급속하게 발전하고 있다. 또한 스마트폰의 하드웨어 규격이 점점 고용량 시스템으로 진화하고 있기 때문에 스마트폰으로 서비스 할 수 있는 기술들은 더욱 더 화려해지고 높은 품질의 서비스가 이루어 질 수 있다. 스마트폰은 모바일 망을 통해 항상 네트워크에 접속해 있기 때문에 하드웨어의 규격은 더욱 중요하다고 볼 수 있다. 또한, 스마트폰의 경우 여러 가지 센서 들이 탑재되어 있다. 이러한 센서 들을 활용하여 사용자의 현재 상황을 감지할 수 있게 되며 이를 통해 얻은 데이터는 다른 곳으로 전송 될 수 있다. 이러한 스마트폰의 센서를 통한 가장 대표적인 기술이 U-Health 시스템 이라고 볼 수 있다. U-Health 시스템은 센서를 이용하여 사용자의 현재 상태, 운동량, 스트레스 등의 데이터를 추출하여 이 데이터를 기반으로 사용자의 건강 상태를 실시간으로 체크하고 관리할 수 있다는 큰 장점이 있다. 하지만 실시간으로 사용자의 개인 정보를 전송하기 때문에 보안측면에서 도청 위협에 대해 노출되어 있다는 단점이 있다. 특히 스마트폰을 사용하는 사용자들의 보안 의식이 높지 않아서 악의적으로 사용자의 데이터를 이용하려 한다면 쉽게 사용자의 개인 정보를 이용할 수 있다.

따라서, 본 논문에서는 NFC 기반 U-Health 서비스의 보안 위협에 대비하기 위하여 NFC기반 AS (Authentication Server) 와의 인증 시스템을 설계한다.

Ⅱ. 관 련 연 구

2.1 U-Health

U-Health 시스템은 현재 IT기술의 발전으로 실시간 데이터를 빠른 시간 내에 전송할 수 있다는 장점이 있기 때문에 현재에도 꾸준하게 기술 개발이 이루어지고 있다.

IT분야에서의 정보교환기술은 다른 많은 분야의 기술들과 통합되어 가고 있다. 그 중 의료분야와 IT기술을 접목시킨 U-Health 기술이 특히 대두 되고 있다. U-Health 기술의 가장 큰 장점은 “anytime and anywhere” 이다. 말

그대로 언제, 어디서나 항상 사용자의 건강 상태를 체크하고 관리 할 수 있다는 점이 가장 큰 장점이라고 할 수 있다. U-Health 기술은 댁내에서 사용되는 RFID, USN 센서를 이용하기도 하며, 현재 많이 사용되고 있는 스마트폰을 이용하여 서비스 할 수도 있다[1]. 센서를 활용한 U-Health 서비스는 댁내에 있는 센서들로부터 사용자의 움직임 등을 체크하여 그 날 하루의 칼로리 소모, 스트레스 유무 판단, 운동 효과 등을 확인할 수 있다. 하지만 센서 기반으로 한 시스템은 데이터의 손실등 데이터를 전송하는데 있어서 신뢰성이 떨어진다는 단점이 있다. 항상 신뢰성있는 데이터의 전송을 위해서 데이터 전송의 성공여부를 꾸준히 체크해주는 관리가 필요하다[2]. 스마트폰을 활용한 U-Health 서비스는 스마트폰에 탑재되어 있는 각 센서들을 이용하여 사용자의 운동량, 움직임의 패턴등을 확인할 수 있다.

2.2 NFC

NFC는 무선태그(RFID) 기술 중 하나로 13.56MHz 대역의 통신 주파수에서 106Kbps에서 424Kbps의 통신 속도를 제공하는 통신범위 약 10cm 이내의 근접거리 무선 통신 기술이다. 통신거리가 짧기 때문에 다른 통신 기술에 비하여 보안성이 우수하고 가격이 저렴해 많은 주목을 받고 있다[6]. NFC는 근거리 무선 통신들의 다양한 성질들을 결합하여 다음과 같이 세 가지 모드로 동작 가능하다. 아래에 있는 모드들은 각각 RFID와 같이 데이터를 읽고 수정할 수 있는 모드, 블루투스 등과 연결하여 데이터 통신 서비스 가능 모드, 특정 카드에 탑재되어 비접촉식의 카드 성질을 지원하는 기능을 수행할 수 있는 서비스 들이 가능하다. NFC의 동작모드는 크게 3가지로 분류된다[6,7].

2.2.1 Reader / Writer 모드

NFC가 탑재되어 있는 디바이스는 NFC 트랜스폰더에 저장된 데이터를 읽고 수정할 수 있다. 즉, 다시 말해서 NFC 디바이스가 카드 Reader기와 writer기로 동작하는 모드이다.

2.2.2 Peer-to-Peer 모드

Peer-to-Peer 모드는 두 개의 NFC 디바이스간의 링크 수준의 통신을 지원한다. 기존의 Bluetooth 통신 서비스와 비슷하게 NFC가 탑재 된 두 단말간의 데이터전송 및 통신을 지원하는 모드이다.

2.2.3 Card Emulation 모드

Card Emulation 모드는 카드의 기능을 지원하는 서비스를 한다고 볼 수 있다. 스마트폰을 기준으로 스마트폰에 탑재되어 있는 NFC 기능으로 교통카드, 카드결제 서비스 등 카드로 할 수 있는 서비스들을 모두 지원해주는 모드이다.

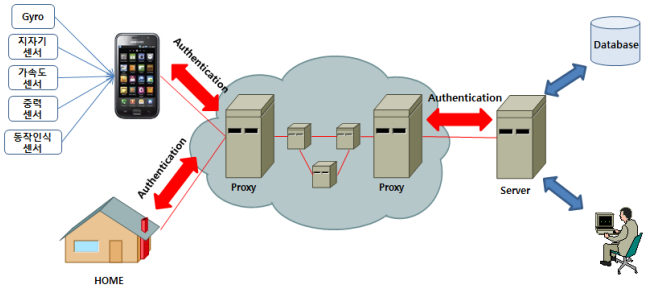
III. 인증시스템

3.1 U-Health 서비스의 보안 위협

현재 댁내기반 및 외부에서 서비스되고 있는 U-Health 시스템은 환자의 건강 데이터를 관리하는 병원의 서버로 전송될 때 위협을 받고 있다. 그리고 NFC 기술도 보안의 위협이 항상 도사리고 있다. NFC 리더기와 NFC 디바이스 간에 데이터 전송이 이루어지는 부분에도 데이터가 안전하게 전송되는 보안적인 이슈도 있지만 로컬 내에서 사용되는 데이터가 아니라 외부에서 전송되는 데이터이기 때문에 보안의 위협은 항상 있다고 볼 수 있다. 스마트폰 기반의 U-Health 서비스는 모바일 망을 사용하기도 하고 Wi-Fi 망을 사용하기도 하기 때문에 공중 네트워크망에서 사용되는 보안 알고리즘을 적용한 시스템이 필요하다. 네트워크망에서 사용되고 있는 다이제스트 인증 알고리즘을 사용하여 병원서버와 환자의 NFC 리더기 사이에 Proxy 서버를 두어 서버와 서버 사이에 인증이 이루어져야만 환자의 데이터를 신뢰성 있게 병원 서버로 전송할 수 있다. 이에 본 논문에서는 NFC 리더기와 NFC 디바이스 간에 보안대책과 기존 네트워크망에서 사용되고 있는 Digest 인증 알고리즘을 적용한 U-Health 인증 시스템을 설계 하고자 한다. NFC 의 보안 위협으로는 도청, 데이터 손상 및 중간자공격등 크게 세 가지로 분류된다.

3.2 시스템 전체 구성

현재 고령화 시대가 되고, 의학분야 기술의 발전으로 인해 우리나라 평균 수명 나이가 점점 높아지고 있다. 이와 같은 시점에서 U-Health 서비스는 앞으로 없어서는 안될 중요한 서비스로 자리매김 하고 있다. 하지만 U-Health 의 편한 서비스만 생각하고, 정작 개인 신상정보등 사용자의 중요한 정보가 누출될 수도 있기 때문에 사용자 정보 보안은 반드시 필요하다. 다음 그림 1은 본 논문에서 제안하는 U-Health 인증 시스템의 전체 구성도를 나타낸다.



(그림 1) U-Health 인증 시스템 전체 구성도

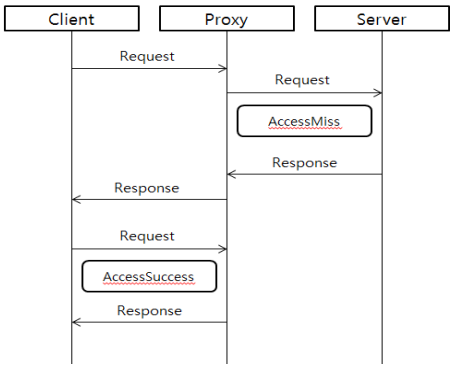
위 그림1에서 나타내듯이 스마트폰기반의 사용자 데이터와 댁내 기반의 사용자 데이터가 최초 전송될 때 Public망 내에 존재하는 Proxy 서버로 데이터가 모이게 되고, NFC를 이용하여 사용자의 인증이 이루어지게 되면 데이터가 병원내 서버로 전송되어 의사 혹은 관리자가 사용자의 데이터를 통해 진단하고 관리할 수 있는 시스템이다. 본 논문에서 제안하는 인증 시스템은 NFC 기반의 RF 보안이 100% 안전하지 않다는 단점을 극복하기 위해 설계하였다. 무선상의 RF 데이터 전송은 사용자 관점에서는 매우 편리하고 간편하다는 가장 큰 장점이 있는 반면에, 관리자 입장에서는 데이터를 보안 위협으로부터 신뢰성 있는 전송을 보장하기 어렵다는 단점이 있다.

3.3 Digest 사용자 인증

Digest 사용자 인증 방법은 데이터를 전송하려는 Sender가 데이터를 받는 Receiver 에게 Request 메시지를 보내면 서버에서는 challenge 메시지에 nonce 와 같은 랜덤 정보와 realm 정보를 보내주게 되고, 이 정보를 받은 Sender는 Receiver로부터 받은 정보와 자신의 Password, ID 값을 이용하여 해쉬함수를 통해 생성된 인증정보를 Receiver 에게 보내게 된다. Receiver 는 Sender에게 받은 정보를 가지고 해쉬함수를 통해 생성된 값을 비교하여 값이 같으면 인증을 하게 된다.

3.4 인증시스템 설계

본 논문에서 제안하는 인증시스템은 NFC 기반의 U-Health 서비스에서 환자 정보가 안전하게 병원 서버로 전송되는 것을 보장한다. 원격 진료가 가능한 U-Health 서비스는 네트워크망의 보안 위협으로부터 데이터가 보호되어야 한다. 스마트폰을 통해 수합한 데이터는 병원 서버로 바로 전송되는 것이 아니라 Proxy서버에서 임시적으로 보관 후 병원 서버로 전송한다. 다이제스트 인증은 NFC 리더기와 Proxy서버, Proxy 서버와 병원 서버 간에 인증을 지원하므로 네트워크망 안에서 생기는 예상 못한 변수에 대해 대비를 할 수 있다. 다음 그림 2는 본 논문에서 제안하는 인증 시스템의 데이터 전송 절차를 나타낸다.



(그림 2) 인증시스템 Sequence다이어그램

최초 클라이언트(NFC 리더기)가 서버에게 데이터 전송 요청을 하고 인증이 되지 않은 클라이언트는 인증을 하기 위한 응답 메시지를 받는다. 응답 메시지를 받은 클라이언트는 인증을 위해 인증 정보가 포함된 요청 메시지를 재차 전송하고 Proxy 서버는 서버로부터 받은 인증 키 값과 비교하여 키 값이 맞으면 세션을 맺는다. 다이제스트 인증을 통해 NFC 기술의 보안 취약점을 이용한 보안 위협으로부터 데이터를 안전하게 보호 할 수 있다.

Ⅳ. 결 론

현재 IT 기술이 급격히 발전하고 있다. IT 기술이 발전하는 만큼 IT 기술과 다른 분야가 융합되는 IT 융합기술 또한 많은 주목을 받고 있다. 향후 스마트 U-City 로 발전하기 위해서는 IT 융합기술이 현재의 기술보다 더 발전해야 하고, 다른 분야의 기술과 융합이 되어 더욱더 편리하고 간편한 서비스가 많이 개발이 되어야한다. 그 중 U-Health 서비스는 스마트 U-City 로 거듭나기위해 간과해서는 안 될 중요한 기술이며 고령화사회를 대비해서 현재의 기술력 보다 더 좋은 기술력을 제공하기 위해 끊임없이 연구되어야 할 분야이다. 본 논문에서는 U-Health 서비스에서 전송되는 사용자 개인정보에 대한 보안을 위해서 인증 메커니즘을 적용한 U-Health 시스템을 제안하였다. 네트워크 망에서의 인증 메커니즘을 적용함으로써 NFC 자체가 가지고 있는 보안적인 단점 요소를 보완해주어 신뢰성 있는 데이터 보안을 유지할 수 있도록 하였다.

참고문헌

[1] Martinez, J. Escayola, M. Martinez-Espronceda, “Standard-based Middleware Platform for Medical Sensor Networks and u-Health”, 2008

[2] Oh-young Kwon, Su-hong Shin, Seung-jung Shin, Woo-sung Kim, “Design of U-Health System with the Use of Smart Phone and Sensor Network”, 2010

[3] Hui Wang, Hyeok-soo Choi, Nazim Agoulmine, M. Jamal Deen, James Won-ki Hong, “Information-Based Sensor Tasking Wireless Body Area Networks in U-Health Systems”, 2010

[4] 김병주, 문형만, 박창선, 황정환, 서정민, “스마트 폰 기술을 활용한 학습형 U-Health 시스템 설계”, 2010

[5] 민병원, 오용선, 한동수, 구종영, “모바일 U-Health 서비스 플랫폼 설계”, 2009

[6] 이민구, 김동완, 손진수, “NFC를 활용한 능동형 인증 방법”, 2011

[7] 임선희, 전재우, 정임진, 이옥연, “NFC 보안 기술 분석 및 UICC 적용 효과 연구”, 2010

[8] 김선배, 김형국, 윤희용, “NFC 에서의 보안 취약점 분석”, 2011