M2M에서 U-Healthcare환경을 위한 생체인식 이용 인증시스템 설계

송충건, 이근호*
백석대학교 정보통신학부

Design of Authentication System using Biometrics for U-Healthcare Environment in M2M

Chung-Geon Song, Keun-Ho Lee*
Information and Communication, Baekseok University

요 약 현재 u-healthcare서비스가 활발하게 이루어지기 위해서는 통합의료정보시스템이 갖추어져야한다. 또한 통합의료정보시스템이 안전한 환경에서 구현되기 위해서는 인증시스템이 기반이 되어야 한다. 하지만 아직 여러 가지 요구사항을 개발하는 단계에 있다. 본 논문에서는 통합의료정보시스템에 한발 나아갈 수 있도록 u-healthcare 서비스를 위한 생체인식 이용 인증시스템을 설계하여 제안하고자 한다.

• **주제어** : 유헬스케어, 사물통신, 통합병원정보시스템, 인증시스템, 보안

Abstract An integrated medical information system should be equipped for the activation of u-healthcare service. In addition, the integrated medical information system should be based on an authentication system to be implemented in a safe environment. However, several requirements are being developed yet. In this paper, biometric authentication system will be designed and proposed for u-healthcare services for the integrated medical information system to go one step further.

• **Key Words** : U-Healthcare, M2M, Integration Hospital Information System, authentication system, Security

1. 서론

u-healthcare는 유비쿼터스 헬스케어의 약자로 언제 어디서나 실시간으로 의료서비스를 받는 것을 말한다. 이런 u-healthcare는 원격에서 네트워크 통신망을 통해 이루어지기 때문에 다양한 해킹공격의 대상이 될 수 있다. 이런 해킹공격으로 인한 시스템의 오류는 사용자의 건강악화나 사망으로 이어지기 때문에 이를 막기 위한 강력한 보안이 필요하다.

해킹사고로부터 시스템을 보호하는 우선적인 방법으로 서비스에 대한 접근제어를 구축하는 것이 있다. 접근제어란 제 3자가 시스템에 접근하여 정보를 열람하거나 시스템을 망가트리는 것을 막고 특정 인증시스템 아래에서 정당한 사용자를 분별하여 서비스를 제공하는 것을 말한다.

이런 접근제어를 실행하기 위해선 인증시스템이 필요한데 인증시스템의 종류와 방식은 다양하며 서비스마다 적절한 인증방식을 선택해야 한다. 또한 암호문을 복호화 할 수 있는 키의 관리문제도 고려해야 한다.

현재 의료정보시스템들은 병원들의 독단적인 서비스와 병원마다 다양한 인증시스템을 이용하고 있다. 이러

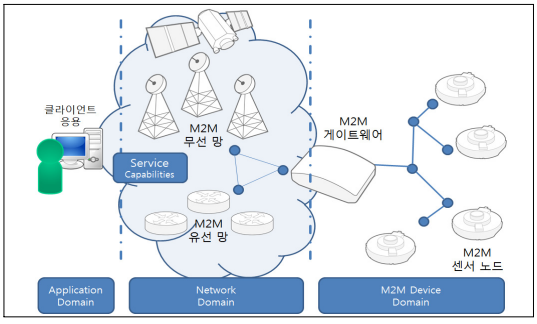
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2012년 2월 5일 수정일 2012년 3월 25일 게재확정일 2012년 4월 10일

한 현황은 미래 u-healthcare에서의 통합의료정보시스템으로 발전하는 궁극적 목표로 가기위한 많은 제약을 가지고 있다[1][5].

이런 병원들의 다양한 의료정보시스템들의 독단적인 서비스와 다양한 인증시스템을 통일하고 미래 u-healthcare에서의 통합의료정보시스템으로 한발 나아갈 수 있도록 하나의 키로 여러 의료 시스템으로부터 인증 받을 수 있는 생체인식을 이용한 인증시스템을 제안하고자 한다.

2. 관련연구

2.1 사물지능통신(M2M)

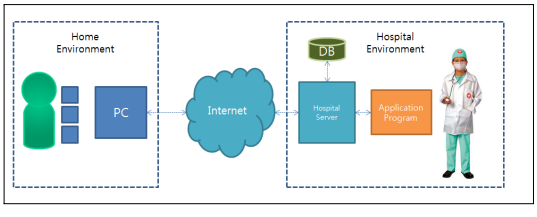


[Fig. 1] Architecture of ETSI M2M

사물지능통신(M2M)이란 인간의 직접적인 개입 없이 사물 간 자동적으로 이루어지는 통신을 말한다. [Fig. 1]은 ETSI의 M2M 구조를 간략하게 나타낸 그림이다. 그림과 같이 M2M Device에서 인간의 직접적인 개입 없이 수집된 데이터는 네트워크를 통해 이동하고 서비스 제공자에 의해 가동된 후 정보의 형태로 사용자에게 제공된다[4].

U-Healthcare도 이런 M2M을 이용한 응용서비스 중 하나이다.

2.2 U-Healthcare 서비스

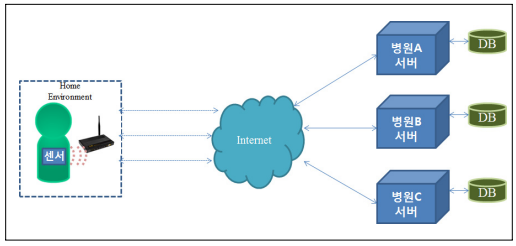


[Fig. 2] Architecture of Remote Healthcare Service

[Fig. 2]는 u-healthcare의 대표적인 서비스인 원격의료서비스의 구조를 나타낸다. 원격의료서비스는 센서가 부착된 디바이스를 통해 사용자의 신체정보를 획득한 후 자동적으로 네트워크를 통해 병원서버로 이동되어 진다. 병원 서버는 이러한 데이터를 가공하여 의사에게 제공하고 의사는 데이터를 토대로 환자를 진료하여 진단정보를 다시 네트워크 망을 통하여 환자에게 보낸다[3].

이러한 u-healthcare는 현재 발전초기 단계로 법적인 제한과 사람들의 인식 문제로 발전에 제약이 많다. 이러한 u-healthcare가 발전하기 위해서는 안정적인 인증과 보안이 요구되는 실정이다.

2.3 기존 병원 시스템 구조



[Fig. 3] Architecture of Exist Authentication System

현재 u-healthcare 환경에서 이루어지는 병원의 많은 의료 서비스들은 [Fig. 3]과 같이 단일 병원 단위로 이루어지며 병원마다 인증시스템이 다르기 때문에 병원마다 키를 하나씩 가지고 있어야 하므로 개인이 여러 가지 키를 관리해야하는 불편함이 있다. 심지어는 아직 의료정보시스템 자체가 제대로 구축되지 않은 병원이 많이 남아있다. 이런 실정은 여러 가지 유용한 의료서비스 개발에 많은 제약을 주고 있다. 그 결과로 M2M 의료계는 응용서비스인 U-Healthcare 서비스의 안전성에 확신을 가지지 못하고 개발과 상용화가 느리게 진행되고 있다. 또한 법적인 한계로 인해 사용자를 직접적으로 캐어하는 부분에 제한이 있다.

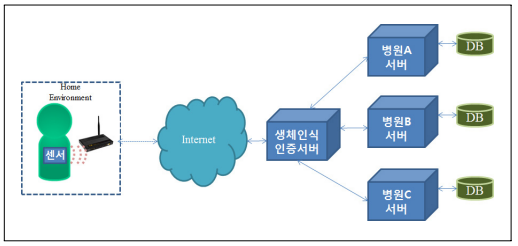
그러므로 u-healthcare 환경에서 이루어지는 여러 가지 유용한 의료서비스를 개발하고 상용화하기 위해선 앞에서 언급하였던 기존 의료정보시스템의 문제점을 해결할 효율적인 방안이 필요하다.

3. 제안하는 인증시스템

본 장에서 여러 병원에서 이루어지는 사용자 인증을

통합한 통합인증시스템을 제한한다. 또한 제한하는 인증 시스템의 구조와 구성요소들 사이에서 데이터가 이동하는 과정을 살펴본다.

3.1 제안 인증시스템 구조



[Fig. 4] Architecture of the Propose Authentication System

제안하는 인증 시스템에서는 [Fig. 4]와 같이 인터넷 망과 병원 서버 사이에 여러 병원들의 인증 시스템을 통합하는 인증 서버가 존재한다. 그러므로 U-Healthcare서비스에서 이동하는 모든 데이터는 이 인증 서버를 통과하게 된다.

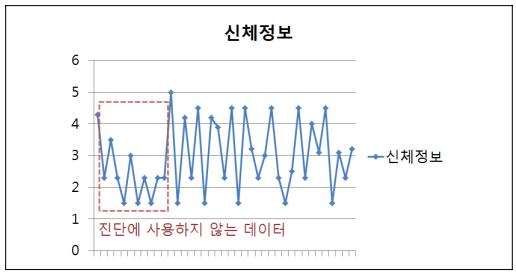
사용자의 정보를 보관하는 데이터베이스는 병원마다 하나씩 존재하며 병원에 귀속되어 병원 서버에만 보관된다.

3.2 제안 인증시스템 인증방법

제안 인증시스템에서는 U-Healthcare 서비스에서 이용하는 사용자의 신체정보를 통하여 인증을 수행한다. 위의 여러 인증시스템을 통합하고 동일한 인증키를 사용하기 위해서 신체정보를 인증키로 사용한다. 신체정보는 사람마다 고유한 값을 가지며 U-Healthcare에서 스마트 카드와 같이 추가적인 키의 소유가 필요 없이 사용자의 데이터만으로 인증을 수행할 수 있어 편리하고 보안성도 우수하여 실제 신체정보를 인증시스템의 인증 수단으로 적용한 사례도 많이 있다.

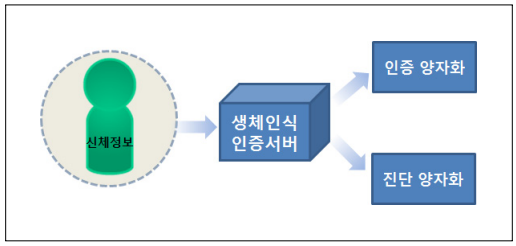
이런 신체정보를 통해 인증을 수행하는 방법은 [Fig. 5]와 같이 센서가 부착된 단말기에서 얻는 신체정보를 2차 평면그래프로 나타낸다.

아날로그 데이터를 디지털화 할 경우 부호화와 양자화를 거치게 되는데 초기 단말기에서 데이터가 보내길 때 양자화 폭을 넓게 하여 진단에 사용되지 않는 부분을 찾아 여러 가지 정보를 스테가노그래피 형식으로 숨긴다. 제 3자는 이러한 복잡한 2차 평면그래프에서 정보가 숨겨져 있다는 사실을 알 수 없으며 매번 변하는 데이터에서 어떤 부분에 데이터가 숨겨져 있는지도 알 수 없다. 그러므로 이 부분은 데이터의 안정성을 위해 활용할 수 있다.



[Fig. 5] Input of Information using Steganography

이렇게 넓은 폭으로 양자화 된 데이터는 인증서버에 도착한 이후 [Fig. 6]와 같이 2가지 형태의 목적으로 다시 좁은 폭의 양자화를 거칠 필요가 있다.



[Fig. 6] Divide of Propose for Body Information

첫 번째로 신체정보는 인증을 목적으로 양자화 된다. 도착한 신체정보를 통해 이동한 정보가 해당 환자의 정보가 맞는지 판단하게 된다.

두 번째로 의사의 진단을 위한 형태로 양자화 된다. 의사가 부호화만을 거친 복잡한 형태의 신체정보를 가지고 진단하는 것은 의사입장에서 매우 불편하므로 특정 질병을 진단하기에 알맞은 형태로 양자화를 거칠 필요가 있다.

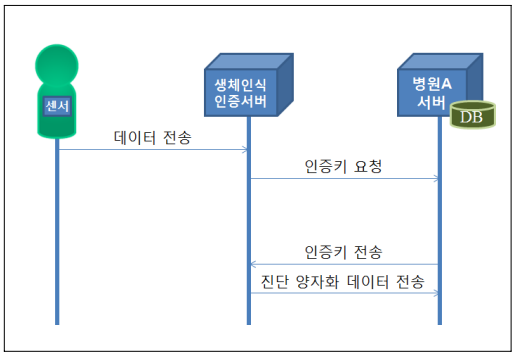
3.3 제안 인증시스템 인증절차

제안 인증시스템은 2가지 인증이 이루어진다. 첫 번째로 사용자의 정보가 병원의 의사에게 전송될 때 사용자를 확인하는 인증이 있고 다음으로 병원들 사이에서 사용자 정보가 이동할 시 사용자를 확인하는 인증이 있다.

3.3.1 사용자와 병원 사이의 인증

사용자의 정보가 병원으로 보내질 때 보내진 정보에

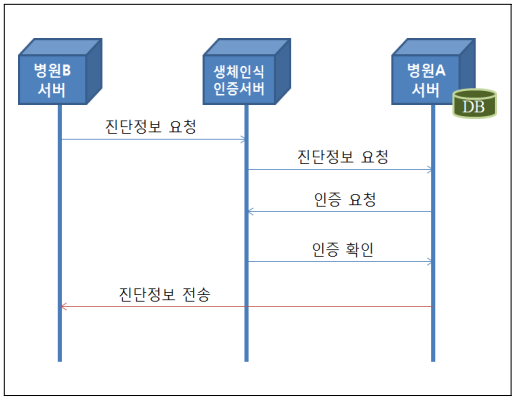
대한 인증이 이루어져야 한다. 사용자가 데이터를 보낼 경우 이는 생체인식 인증서버에 보내지지만 인증 시 비교대상이 되는 정보는 해당 병원의 데이터베이스에서 관리하기 때문에 병원에게 등록된 정보를 요청한다.



[Fig. 7] Process of Authentication User to Hospital

그 후 사용자가 보낸 정보에 대한 인증이 확실하게 이루어진 다음 진단을 목적으로 양자화 된 데이터가 병원으로 보내진다.

3.3.2 병원들 사이에서의 인증



[Fig. 8] Process of Authentication Hospital to Hospital

사용자가 병원A에서 병원B로 이동할 경우 병원B에서는 병원A에서 받은 검사를 중복으로 하는 것은 불필요하다. 위의 인증은 이렇게 병원들 사이에서 진료의 효율성을 위해 사용자정보를 이동시킬 시에 필요한 인증이다. 통합된 인증서버는 중간에서 요청한 병원의 사용자에 대한 인증을 수행하여 안전한 정보 교류를 도와준다.

4. 성능분석

4.1 안전성 분석

제안한 인증 시스템의 안전성을 정보보안의 3대 요소인 기밀성, 무결성, 가용성으로 나누어 분석하였다.

4.1.1 기밀성

병원마다 인증시스템을 따로 운영할 경우 경제적인 이유로 보안이 미흡한 병원을 통해 환자의 개인정보가 외부에 노출될 위험이 있다. 하지만 인증 서버를 통일하여 적용함으로 인증 시스템의 기밀성을 동등하게 보장할 수 있다.

4.1.2 무결성

서비스 도중 사용자의 신체정보가 수정될 경우 의사의 잘못된 진단으로 이어지기 때문에 무결성은 매우 중요한 요소 이다. 제안 인증시스템에서는 사용자의 정보가 2차 평명그래프 형태로 보내질 때 진단에 사용되지 않는 정보에 해쉬값을 숨겨 수정여부를 확인할 수 있을 뿐만 아니라 해커가 어떤 부분에 어떤 데이터가 숨겨져 있는지 알 수 없어 해쉬값에 대한 기밀성도 보장된다.

4.1.3 가용성

기존 의료정보 시스템에서는 경제적인 문제로 각종 DDoS공격에 노출되어 있는 병원이 있었다. 제안 인증시스템에서는 IDS와 IPS를 설치하여 이에 대응하여 연결되어 있는 모든 병원의 인증서비스를 보호할 수 있다. 하지만 하나의 인증 서버가 마비될 경우 전체 서비스의 마비로 이어지기 때문에 여러 대의 미러 서버를 운영함으로 만일의 사태에 대비해야한다.

[Table 1] Comparison of the Propose System

기밀성	병원마다 동등한 보안기술 적용
무결성	해쉬값이 함께 이동하여 무결성 보장 해쉬값을 안전하게 이동할 수 있음
가용성	통합된 서버의 보안기술로 전체에 적용 미러서버를 통해 위급상황 시 적절하게 대응

4.2 효율성 분석

지능형사물통신(M2M)에서는 특정 기간에 지속적으

로 통신이 이루어지기 때문에 가벼운 통신이 요구된다. 제안 인증시스템은 인증키나 해쉬값을 데이터에 숨김으로 안전성뿐만 아니라 이동하는 데이터의 크기도 줄일 수 있다. M2M의 응용분야인 U-Healthcare에 매우 적합한 방법이라 할 수 있다.

5. 결론

본문에서 여러 병원들의 구조적인 문제를 해결하기 위해 통합인증시스템을 설계해 제시해 보았다. 제시한 인증시스템은 기술적인 부분이 미흡하여 실현가능성을 확신할 수 없지만 여러 가지 요구사항들을 분석하고 이를 실현할 기술을 접목시킴으로 병원 의료정보시스템의 통합인증이 실현되어 u-healthcare 서비스가 활력을 얻기를 기대한다. 더 나아가 사람들이 서비스에 대한 신뢰도를 가지고 인식 변화하여 통합의료정보시스템을 구축을 위해 한걸음 더 나아가기를 기대해본다.

감사의 글

"이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2012-0003141)"

REFERENCES

[1] BoSoo Kim, "U-Healthcare & Medical Information System of Status and Operative Challenges for Integrated Medical Information System", The Korea Society of Digital Policy & Management, Vol. 9, No. 3, 2011.

[2] Cory Cornelius, "On Usable Authentication for Wireless Body Area Networks", HealthSec, 2010.

[3] ChungGeun Song, "Threat to Security of Remote-Controlling Medical Care Service and Countermeasure Under U-Healthcare Environment", 2nd ICCT, pp. 319-321, 2012.

[4] David Boswarthick, "M2M Activities in ETSI", SCS Conference, 2009.

[5] YongSik Jung, "Implement Plan of Integrated Medical Information System for Ubiquitous Healthcare Service", KOREA SOCIETY OF INDUSTRIAL INFORMATION SYSTEMS, Vol. 15, No. 2, 2010.

저자소개

송 충 건(Chung-Geon Song) [정회원]

· 2010년 3월 ~ 현재 : 백석대학교 정보통신학부

<관심분야> : 정보보호, U-Heahthcare, 사물지능통신

이 근 호(Keun-Ho Lee) [종신회원]

· 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)

· 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원

· 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호