The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 19, No. 4, pp.77-83, Aug. 31, 2019. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2019.19.4.77
JIIBC 2019-4-12

전천 후 생활보조 시스템을 위한 안전하고 경량화 된 인증기법

A Secure and Lightweight Authentication Scheme for Ambient Assisted Living Systems

이명규[*], 최현철[**], 황보택근[***]

Myung-Kyu Yi[*], Hyunchul Choi[**], Taeg-Keun Whangbo[***]

요 약 인구 증가로 인해 노인 인구가 날로 증가하고 있다. 이런 노인들에겐 다양한 보살핌이 필요하지만, 노인들을 돌볼 수 있는 의료 종사자가 부족한 상황이다. 전천후 생활보조는 고령자의 안전과 건강한 삶을 보장하고, 고령자가 자신이 선호하는 환경에서 독립적으로 살 수 있는 기간을 연장하는 것을 목표로 한다. 전천후 생활보조는 스마트 장치, 의료 센서, 무선 네트워크, 건강관리 모니터링을 위한 컴퓨터 및 소프트웨어 응용 프로그램으로 구성된 시스템을 제공한다. 전천후 생활보조는 노인들의 건강과 건강 상태를 예방, 치료 및 개선하는 등의 다양한 목적으로 사용될 수 있다. 정보 보안 및 개인 정보 보호는 전천후 생활보조 시스템 사용자가 보호받을 수 있도록 보장하는 데 중요하지만, 이러한 특성을 고려한 연구는 미미하다. 본 논문에서는 전천후 생활보조 시스템을 위하여 안전하고 경량화 된 인증기법을 제안한다. 제안된 인증기법은 전천후 생활보조 시스템에서 요구되는 중요한 보안 요구 사항들을 지원할 뿐만 아니라 다양한 유형의 공격으로부터 안전하다. 또한 제안된 인증 기법이 기존의 인증 기법들보다 더 안전하고 효율적이라는 것을 보여주기 위하여 보안 분석 결과를 제시한다.

Abstract With the increase in population, the number of such senior citizens is increasing day by day. These senior citizens have a variety of care needs, but there are not enough health workers to look after them. Ambient Assisted Living (AAL) aims at ensuring the safety and health quality of the older adults and extending the number of years the senior citizens can live independently in an environment of their own preference. AAL provides a system comprising of smart devices, medical sensors, wireless networks, computer and software applications for healthcare monitoring. AAL can be used for various purposes like preventing, curing, and improving wellness and health conditions of older adults. While information security and privacy are critical to providing assurance that users of AAL systems are protected, few studies take into account this feature. In this paper, we propose a secure and lightweight authentication scheme for the AAL systems. The proposed authentication scheme not only supports several important security requirements needed by the AAL systems, but can also withstand various types of attacks. Also, the security analysis results are presented to show the proposed authentication scheme is more secure and efficient rather than existing authentication schemes.

Key Words : AAL, healthcare, wearable computer, security, authentication

[*]정회원, 가천대학교 IT융합대학 컴퓨터공학과
[**]정회원, 가천대학교 공과대학 건축학과
[***]정회원, 가천대학교 IT융합대학 컴퓨터공학과 (교신저자)
접수일자 2019년 6월 27일, 수정완료 2019년 7월 27일
게재확정일자 2019년 8월 2일

Received: 27 June, 2019 / Revised: 27 July, 2019 /
Accepted: 2 August, 2019
[*]Corresponding Author: tkwhangbo@gachon.ac.kr
Dept. of Computer Engineering, Gachon University, KOREA

Ⅰ. 서 론

평균수명의 증가와 출산율 감소로 인해 전 세계적으로 인구 고령화가 급속히 진행되고 있다. 유럽연합의 경우 80세 이상 초 고령자가 지난 10년 동안 급속히 증가하였으며, 2020년까지 65세 이상의 인구는 7천 5백만이 넘을 것으로 예상된다. 또한, 고령 인구 비중이 가장 높은 일본의 경우 90세 이상 인구가 처음으로 200만 명을 넘어섰고, 100세 이상 인구도 가파른 증가세를 보이고 있다. 초 고령자는 유럽 선진국과 일본을 중심으로 급격히 증가하여 왔으나, 향후에는 우리나라, 중국 등의 국가에서 증가 속도가 가속화될 것으로 예상된다. 따라서 이러한 고령화 문제를 해결하기 위해보다 새롭고 효율적인 기술이 필요하게 될 것이다. 전천후 생활보조(Ambient Assisted Living, 이하 AAL)는 고령자 혹은 만성 질환을 앓고 있는 사람들이 일상 및 직장생활 환경에서 정보 통신 기술을 사용하여 활동적이고 독립적인 생활이 가능하도록 도와주는 것을 목표로 한다. 집안에 설치된 다양한 센서와 장비를 활용해 거주자의 움직임을 실시간으로 분석하고, 병원이나 보건소 같은 의료진과 연계하여 모니터링 함으로써 독거노인의 낙상사고와 생활 패턴 이상 징후 등을 조기에 발견하여 응급 상황을 대비할 수 있다. 최근 AAL 기술은 일상생활에서 신체적 또는 인지적 능력이 감소한 사람들을 모니터링하고 지원함으로써 간병인의 업무를 보완하는 수단으로 받아들여지고 있다. 진보된 센서 기술은 다양한 기능의 센서를 환경에 내장 할 수 있게 되었으며, 단순히 온도나 조명을 켜고 끄거나 단계를 조절하는 단계를 넘어 소리와 영상을 기록하고 분석하는 보다 복잡한 형태의 내장형 센서를 통해 거주자의 환경 특성을 감지할 수 있다. 또한, 거주자의 물리적 또는 인지적 상태는 활동이 추론 될 수 있으며, 이러한 추론을 바탕으로 거주자의 건강관리가 이루어질 수 있다.

AAL 시스템의 기본적인 구성은 그림 1과 같다. 다양한 AAL 센서가 거주자의 부엌, 침실, 욕실 및 화장실을 포함한 환경에 배치될 수 있다. 식탁에 설치된 센서는 의자에 앉아 있는 사람을 감지하여 식사 행위에 대한 인식에 도움을 줄 수 있다. 침실의 침대 바로 아래 있는 센서는 거주자의 수면상태를 분석하는 역할을 할 수 있으며, 부엌에 설치된 화염 센서는 특정 파장의 광 감지 기능을 소유하고 있어서 적색 불꽃을 감지 할 수 있도록 설계되어 있으므로 화재 상황의 인식에 역할을 한다. 부엌 창문 앞에 설치된 센서는 비가 내릴 때 열려있는 창문을 잠그는 데 사용되며, 욕조가 목욕할 수 있는 물의 온도를 감지하는 데 사용될 수 있다. 또한, 위와 같은 환경정보 뿐 아니라 생체정보를 측정·분석하여 건강관리 정보를 제공할 수 있다. 혈당, 혈압 및 맥박과 같은 거주자의 신체상태 변화를 감지할 수 있는 센서들은 수집되는 각종 거주자의 생체정보를 AAL 게이트웨이를 통해 AAL 서버에 실시간으로 전송하여 거주자의 건강상태를 점검하는 데이터베이스로 활용하게 되며, 이를 토대로 의료진이 AAL 사용자에게 개인 맞춤 건강관리 서비스를 제공할 수 있다.

그림 1. AAL 시스템 구성도
Fig. 1. The architecture of the proposed AAL systems

이와 같이 AAL 시스템을 통하여 교환되는 정보는 매우 민감한 의료 및 민감 정보를 포함하여 있으며, 보안 및 프라이버시가 중요한 문제로 대두되고 있지만, 아직까지 보안에 대한 연구는 미미한 상태이다[1,2]. 본 논문에서는 AAL 시스템에서 요구하는 다양한 보안 요구사항을 만족하기 위하여 안전하고 경량화 된 인증 기법을 제안하고자 한다. 제안된 인증 기법은 AAL 센서가 가지고 있는 하드웨어 자원의 제약을 고려하여 설계되었다. 제안된 인증기법은 제한된 계산 능력과 저장 공간을 가진 AAL 센서의 특성을 감안하여, XOR와 해쉬와 같은 간단한 연산만을 포함하여 빠른 속도를 지원할 뿐 아니라 다양한 유형의 공격에 대비할 수 있다.

본 논문의 구성은 다음과 같다. 2장은 관련 연구 및 보안 요구조건을 설명하고, 3장은 제안된 인증기법을 설명한다. 4장은 제안된 기법에 대한 효율성과 안전성을 분석한다. 5장에서는 결론을 도출한다.

Ⅱ. 관련 연구

최근, 건강관리 시스템 및 AAL 시스템을 위한 인증

관련 연구들은 다음과 같다[3-12]. He[8]는 AAL 시스템을 위한 인증 프로토콜을 제안했다. 하지만, 사용자의 입력을 필요로 하므로 고령자를 고려해야 하는 AAL 시스템에서 적합하지 않다. 인증 프로토콜은 고령자인 사용자의 특성을 고려하여 설계되어야 한다. Yi[9]는 AAL 시스템을 위한 경량 인증 프로토콜을 제안했다. 하지만, 제안된 인증 프로토콜은 공개키 기반 암호화 알고리즘을 기반으로 하고 있어서 하드웨어로 구현할 경우 속도가 느리고 복잡한 단점을 가진다. Yi[10]는 AAL 데이터의 특성을 고려한 적응적 인증 프로토콜을 제안하였다. 하지만, 제안된 기법은 민감 데이터와 비민감 데이터를 구분하기가 쉽지 않은 단점을 가지고 있다. AAL 시스템은 모든 정보가 공개된 채널을 통해 전송되기 때문에 인증 기법은 보안이 취약할 수밖에 없는 단점을 가지고 있다. 따라서 다양한 유형의 공격을 차단할 수 있도록 안전할 뿐 아니라 경량화 된 인증 기법을 설계해야 한다. AAL 시스템에서 필수적으로 만족되어야 할 보안 요구 조건은 다음과 같다.

- 상호 인증 : 상호 인증은 통신 링크의 두 객체가 서로의 신분을 확인시켜 주는 양방향 인증 방법이다. 인증된 객체만이 AAL 시스템에서 수집한 데이터에 접근할 수 있도록 하려면 AAL 센서와 AAL 게이트웨이 사이의 상호 인증이 필요하다.

- 비 추적성 : AAL 데이터가 암호화 되더라도 악의적인 상대방이 통신 및 정보 흐름을 추적 할 수 있으며, 이를 통하여 사용자에 대한 정보를 추측할 수 있다. 따라서, 비 추적성은 AAL 시스템에서 중요한 보안 요구사항이다.

- 완전 순방향 비밀성(Perfect Forward Secrecy) : 완전 순방향 비밀성은 이 전의 비밀 키가 노출되더라도 다음의 키 분배 과정에서 얻는 세션 키의 안전성에는 영향을 미칠 수 없어야 하는 보안 요구사항이다. 새로운 키 정보를 수학적으로 예전의 키 정보와 관련이 없도록 설계하여, 누군가 예전 세션 키를 탐지하더라도 그 키를 사용해서 새로운 세션 키를 추측할 수 없어야 한다.

- 공격 저항(Attack Resistance) : 보안 통신을 보장하기 위해 인증 프로토콜은 재생 공격, 위장 공격, 중간자 공격, 위조/변조 공격 측면과 같은 다양한 공격을 견딜 수 있어야 한다.

III. 제안된 인증기법

본 장에서는 제안된 안전하고 경량화 된 인증기법에 대해서 설명한다. 그림 2와 같이 자세한 등록절차는 다음과 같다.

1) 스마트 폰을 포함한 AAL 센서는 센서의 임시비표 N_s를 생성한다.
2) AAL 센서는 타임스탬프 T_s를 생성한다.
3) AAL 센서는 N_s와 센서와 게이트웨이 간의 비밀 키 K_s를 연접한 값의 해쉬 값 A를 구한다.
4) AAL 센서는 N_s와 K_s를 XOR 연산한 결과 값인 B를 구한다.
5) 마지막으로, AAL 센서는 계산된 A와 B를 XOR 연산한 결과 값인 C를 구한다.
6) AAL 센서는 센서의 ID인 ID_s, B, C, T_s를 AAL 게이트웨이에게 전송한다.
7) AAL 게이트웨이는 수신된 B와 비밀 키인 K_s를 XOR 연산하여 N_s'을 구한다.
8) AAL 게이트웨이는 계산된 N_s'와 K_s를 연접한 값의 해쉬 값인 A'를 구한다.
9) AAL 게이트웨이는 수신된 B와 C를 XOR 연산하여 A를 구한다. 만약 수신된 A와 A'가 일치하지 않으면 무결성이 유지되지 않으므로 인증절차를 중단하고 종료한다. 두 값이 일치한다면 인증절차를 계속한다.
10) AAL 게이트웨이는 타임스탬프 T_s'를 생성한다.
11) AAL 게이트웨이는 게이트웨이의 임시비표 N_g를 생성한다.
12) AAL 게이트웨이는 N_g와 K_s를 연접한 값의 해쉬 값 D를 구한다.
13) AAL 게이트웨이는 N_g와 K_s를 XOR 연산한 결과 값인 E를 구한다.
14) 마지막으로, AAL 게이트웨이는 계산된 D와 E를 XOR 연산한 결과 값인 F를 구한다.
15) AAL 게이트웨이는 E, F, 타임스탬프 T_s'를 AAL 센서로 반환한다.
16) AAL 센서는 수신된 E와 비밀 키인 K_s를 XOR 연산하여 N_g'값을 구한다.
17) AAL 센서는 계산된 N_g' 와 K_s를 연접한 값의 해쉬 값인 D'를 구한다.
18) AAL 센서는 수신된 E와 F를 XOR 연산하여 D를 구하고, D와 D'의 값을 비교한다.

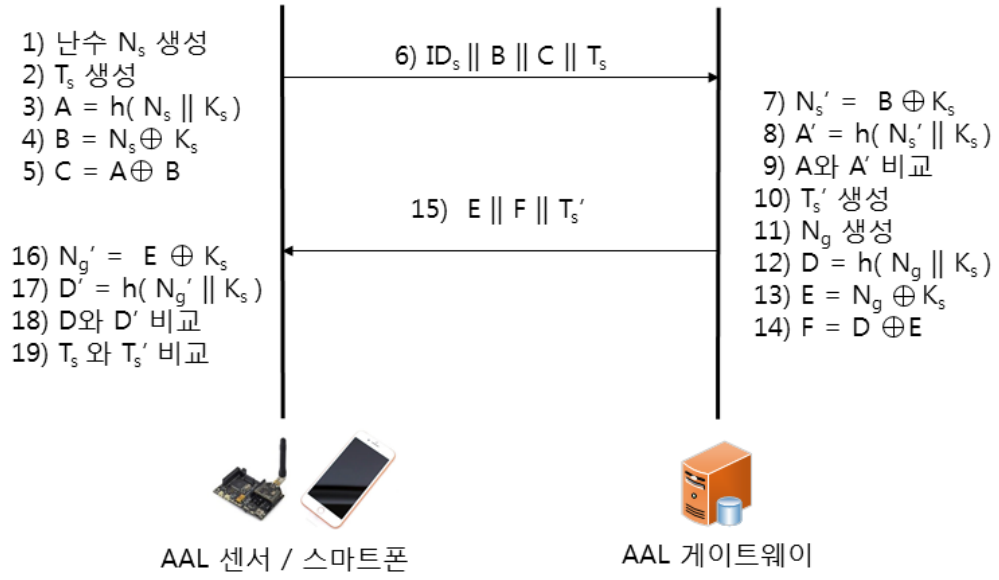

그림 2. AAL서비스를 위한 안전한 경량화 된 인증절차
Fig. 2. The lightened secure authentication procedure for AAL service

19) 만약 D와 D'이 일치하고, 수신된 T_s'이 T_s보다 크다면 무결성이 유지되며 인증절차가 성공적으로 이루어지게 된다. 만약 D와 D'가 일치하지 않거나 수신된 T_s'가 T_s보다 크지 않다면 무결성이 유지되지 않으므로 인증절차를 중단하고 종료한다.

이와 같은 과정을 통하여 인증을 수행한 후, 세션이 종료되면 새로운 난수와 임시비표를 생성하고 이전 난수와 임시비표는 제거한다.

IV. 제안된 인증기법 분석

본 장에서는 제안한 경량 인증 기법의 효율성과 안정성을 분석하고자 한다. 경량화된 보안 인증 기법의 효율석 분석을 위하여 표 1과 같이 계산 비용을 위한 표기를 정의한다[7-9].

표 1. 계산 비용을 위한 표기
Table 1. Natation for computational costs

표기법	설명
T_h	해쉬, 타임스팸프, 임시비표, XOR 연산 수행시간
T_{sym}	대칭키 암호화 혹은 복호화연산 수행시간
T_{asym}	비대칭키 암호화 혹은 복호화연산 수행시간
T_{mm}	모듈러 곱 연산 수행시간

X. Cao et. al[4] 과 J. Huang et al.[7]의 연구를 통하여 각각 (1)~(3)식과 같이 정리할 수 있다.

$$T_h \cong 0.4\ T_{mm} \quad (1)$$
$$T_{sym} \cong 0.4\ T_{mm} \quad (2)$$
$$T_{asym} \cong 29\ T_{mm} \quad (3)$$

제안된 인증 기법에서 AAL 센서는 1번의 임시비표 생성, 1번의 타임스탬프 생성, 3번의 XOR 연산, 그리고 2번의 해쉬 연산을 수행한다. 따라서, 사용자 측에서 발생하는 수행시간은 표 2와 같다. (1)~(3)식을 사용하면, Debiao He et. al.[8]인증방식은 88.6 T_{mm}로 계산될 수 있다. Yi et al[9]인증방식은 59.2 T_{mm} 으로 계산될 수 있으며, Yi et al[10] 인증방식은 비민감 데이터의 경우 0.8

표 2. 연산 비용 비교
Table 2. Computational cost comparisons

인증 프로토콜		사용자 측 인증시간	
Debiao He et. al.[8] 인증 기법		$2T_h + 2T_{sym} + 3T_{asym}$	88.6 T_{mm}
Yi et al[9] 인증 기법		$3T_h + 2T_{asym}$	59.2 T_{mm}
Yi et al[10] 인증 기법	민감 데이터	$2T_h + 2T_{asym}$	0.8 T_{mm}
	비민감 데이터	$2T_h$	58.8 T_{mm}
제안된 인증 기법		$7T_h$	2.8 T_{mm}

T_m, 민감 데이터의 경우 58.8 T_{mm}로 계산될 수 있다. 제안된 인증기법은 2.8 T_{mm}로 계산될 수 있다. 따라서 제안된 인증기법은 보다 효율성이 좋다고 말할 수 있다.

제안된 인증 기법의 보안요구 사항을 고려한 안정성을 분석하면 다음과 같다.

• 사용자 위장 공격 : 사용자 위장 공격은 공격자가 정당한 사용자의 센서로 위장하는 공격을 말한다. 센서에서 게이트웨이로 보내지는 메시지를 공격자가 가로챈 후, 취득한 타임스탬프 T_s를 이용하여 게이트웨이로 전송하여 정당한 사용자로 위장한다고 하자. 이러한 경우 정당한 사용자의 센서로 위장하기 위해서는 B와 C값을 생성해야 하는데, 제안기법에서는 임시비표 N_s와 비밀 키 K_s의 XOR 연산 및 일방향 해쉬 함수를 사용하여 B와 C값을 생성하였기 때문에, 공격자가 정당한 B와 C값을 생성할 수 없다. 따라서 제안기법은 사용자 위장 공격에 안전하다.

• 서비스 제공자 위장 공격 : 서비스 제공자 위장 공격은 공격자가 정당한 서비스 제공자인 게이트웨이로 위장하는 공격을 말한다. 게이트웨이에서 센서로 보내는 메시지를 공격자가 가로챈 후, 취득한 타임스탬프 T_s'를 이용하여 게이트웨이로 위장한다고 하자. 제안기법에서 임시비표 N_g와 비밀 키 K_s의 XOR 연산 및 일방향 해쉬 함수를 사용하여 E와 F값을 생성하였기 때문에, 정당한 서비스 제공자의 게이트웨이로 위장하려고 해도 공격자가 정당한 E와 F값을 생성할 수 없다. 따라서 제안기법은 서비스 제공자 위장 공격에 안전하다.

• 상호 인증 : 상호 인증은 인증에 참여하는 참여자들 사이에 서로 올바른 참여자임을 인증하는 것이다. 게이트웨이는 상호 공유하고 있는 비밀 키 K_s과 센서가 생성한 임시비표 N_s값을 이용하여 센서로부터 받은 값과 같은지 비교하여 센서를 인증하고, 센서는 상호 공유하고 있는 비밀 키 K_s과 게이트웨이가 생성한 임시비표 N_g값을 이용하여 게이트웨이로부터 받은 값과 같은지 비교하여 게이트웨이를 인증할 수 있다. 인증이 끝나면 새로운 임시비표를 생성하고 이전 임시비표는 제거된다. 따라서 상호 인증 조건을 만족한다고 볼 수 있다.

• 재전송 공격 : 재전송 공격은 전송된 메시지를 탈취해서 공격자가 다시 전송하는 공격을 말한다. 제안기법에서는 타임스탬프를 사용하여 자동적으로 증가되는 값을 이전 값과 비교함으로써 재전송 공격으로부터 보호할 수 있다. 또한, 제안기법에서는 사용자인 센서와 서비스 제공자인 게이트웨이 사이에 메시지를 전송할 때마다, 현재의 임시비표와 타임스탬프 값을 포함하고 메세지를 받으면 항상 임시비표와 타임스탬프를 확인 한다. 만약 공격자가 전송 메세지에서 타임스탬프 만 바꿔서 전송한다고 해도 전송하는 메세지에 임시비표를 포함하고 있기 때문에 임시비표도 타임스탬프에 맞게 다시 생성해야 한다. 하지만 앞의 위장 공격 안전성 분석에서 살펴본바와 같이 XOR 연산 및 일방향 해시함수에 의해 공격자가 임시비표를 다시 생성할 수 없기 때문에 제안 기법은 재전송 공격에 안전하다.

• 중간자 공격 : 중간자 공격은 통신 중간에서 도청을 하거나 전송되는 메시지의 내용을 바꿔서 전송하는 공격을 말한다. 공격자가 도청을 하여 B와 C를 알아낸다 하더라도 XOR 연산 및 일방향 해쉬 함수의 특성으로 인해 B와 C로부터 임시비표 N_s값을 계산하기 불가능하다. 마찬가지로, 공격자가 도청을 하여 E와 F를 알아낸다 하더라도 XOR 연산 및 일방향 해쉬 함수의 특성으로 인해 E와 F로부터 임시비표 N_g값을 계산하기 불가능하다. 또한, 중간자 공격을 통해 공격자가 임의로 선택한 메시지를 전송한다고 하더라도, 공격자는 비밀 키 K_s를 알 수가 없다. 따라서 위조된 메시지에 대해서 각 센서와 게이트웨이가 수행하는 인증과정을 통과하지 못하기 때문에 공격자가 수행한 중간자 공격은 성공할 수 없다. 따라서 제안 기법은 중간자 공격에 안전하다.

• 위조/변조 공격 : 센서와 게이트 사이에 데이터를 전송 및 수신하는 경우, 비밀 키 K_s를 이용하여 수신된 값과 계산된 해쉬 값을 비교함으로써 전송된 데이터의 변조나 위조는 쉽게 검출될 것이다. 따라서 제안된 기법은 변조/위조 공격에 안전하다고 말할 수 있다.

위에서 살펴본 바와 같이 제안된 기법은 효율적일 뿐 아니라 다양한 유형의 공격으로부터 데이터를 보호할 수 있다.

V. 결 론

최근, 의학이 발달하고 식생활이 향상됨에 따라 사람들의 평균 수명이 길어져서 고령자가 차지하는 비율이 점차 높아지고 있으며, 정년 연장이나 노인 복지 따위의

안건이 사회의 중요 문제로 대두되고 있다. 따라서, 사회 각 분야에서 고령화에 대비한 다양한 연구와 효과적인 대응이 필요한 상황이다. AAL 시스템의 주요 목적은 정보통신기술을 사용하여 노인 또는 장애인이 선호하는 환경에서 독립적으로 생활 할 수 있는 시간을 연장하는데 있다. 정보 보안 및 개인 정보 보호는 AAL 시스템 사용자가 보호받을 수 있도록 보장하는 데 중요하지만, 이러한 특성을 고려한 연구는 미미한 상황이다. 따라서, 본 논문에서는 AAL 시스템에서 요구하는 다양한 보안 요구사항을 만족하기 위하여 AAL 센서가 가지고 있는 하드웨어의 제약특성을 고려한 안전하고 경량화 된 인증 기법을 제안하였다. 제안된 인증 기법은 AAL시스템에 필요한 보안요구 사항을 지원할 뿐만 아니라 효율적이며, 다양한 공격에 안전하다.

References

[1] Personal Health Records and the HIPAA Privacy Rule.

[2] Myung-Kyu Yi, Hee-Joung Hwang, "A Study on Security Weakness and Threats in Personal Health Record Services", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.15, No. 6, pp.163-171, Dec. 31, 2015.
DOI : https://dx.doi.org/10.7236/JIIBC.2015.15.6.163

[3] C. Yeh, H. Chen, and J. Lo, "An Authentication Protocol for Ubiquitous Health Monitoring Systems," J. Medical and Biological Engineering, vol. 33, no. 4, 2013
DOI : 10.5405/jmbe.1478

[4] X. Cao and W. Kou, "A Pairing-Free Identity-Based Authenticated Key Agreement Scheme with Minimal Message Exchanges," Information Sciences, Vol. 180, pp. 2895-2903, 2010

[5] J. Liu et al., "Certificateless Remote Anonymous Authentication Schemes for WirelessBody Area Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, pp. 332-342, 2014.
DOI: https://doi.org/10.1109/TPDS.2013.145

[6] Z. Zhao, "An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem," J. Medical Systems, vol. 38, no. 2, 2014.
DOI 10.1007/s10916-014-0013-5

[7] J. Huang et al., "Robust and Privacy Protection Authentication in Cloud Computing," Int'l. J. InnovativeComputing, Information and Control International, Vol. 9, No. 11, pp. 4247-61, 2013

[8] Debiao He, Sherali Zeadally, "Authentication protocol for an ambient assisted living system", IEEE Communications Magazine, Vol. 53, No 1, pp. 71-77, Jan. 16, 2015
DOI: 10.1109/MCOM.2015.7010518

[9] Myung-Kyu Yi, Taeg-Keun Whangbo, "A Lightweight Authentication Protocol for Ambient Assisted Living Systems", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.17, No. 5, pp.9-16, Oct. 31, 2017.
DOI : https://dx.doi.org/10.7236/JIIBC.2017.17.5.9

[10] Myung-Kyu Yi, Hyunchul Choi, and Taeg-Keun Whangbo, "An Adaptive Authentication Protocol for Ambient Assisted Living Systems", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.18, No. 4, pp.19-26, Aug. 31, 2018.
DOI : https://doi.org/10.7236/JIIBC.2018.18.4.19

[11] Myung-Kyu Yi, Hee-Joung Hwang, "Design of Secure Personal Health Record Management Systems", The Journal of Korean Institute of Information Technology, Vol. 13, No. 8, pp.71-80, 2015
DOI : https://doi.org/10.14801/jkiit.2015.13.8.71

[12] Baek, Jong-Kyung, Park, Jae-Pyo, "A study of analysis and improvement of security vulnerability in Bluetooth for data transfer", Journal of Korea Academy Industrial Cooperation Society(JKAIS), Vol. 12, No. 6, pp. 2801-2806, 2011.
DOI : https://doi.org/10.5762/KAIS.2011.12.6.2801

저 자 소 개

이 명 규(정회원)

- 2005년 2월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 10월~현재 : 가천대학교 IT 융합대학 컴퓨터공학과 연구교수
- TTA 유헬스 프로젝트그룹 개인건강정보 표준화 전담반 위원

- 주관심분야 : u-Health, Big Data, Medical Informatics, Security, Ubiquious Computing

최 현 철(정회원)

- 2002년 2월 : 서울대학교 건축학과(공학석사)
- 2008년 8월 : 서울대학교 건축학과(공학박사)
- 2017년 2월 ~ 현재 : 가천대학교 공과대학 건축학과

- 주관심분야 : IT in Architectural Field, Parametric Design, AAL Healthcare Service

황 보 택 근(정회원)

- 1988년 CUNY 컴퓨터공학 졸업 (공학석사)
- 1995년 Stevens Institute of Technology 컴퓨터공학 졸업 (공학박사)
- 1997년~현재 가천대학교 IT대학융합 컴퓨터공학과 교수
- 주관심분야 : 영상처리, 패턴인식, 컴퓨터그래픽스, 3D 게임엔진, 의료정보

※ 이 연구는 2019년도 국토교통과학기술진흥원 연구비 지원에 의한 결과의 일부임
(과제번호 : 19RERP-B090228-06)