Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 11 pp. 746-754, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.11.746
ISSN 1975-4701 / eISSN 2288-4688

스마트 헬스케어 기반의 디바이스 접근제어를 위한 키 생성 및 통신기법 설계

민소연[1*], 이광형[2], 진병욱[3]
[1]서일대학교 정보통신학과, [2]서일대학교 인터넷정보학과, [3]숭실대학교 컴퓨터학과

A Design of Key Generation and Communication for Device Access Control based on Smart Health Care

So-Yeon Min[1*], Kwang-Hyong Lee[2], Byung-Wook Jin[3]
[1]Dept. of Information and Communcation, Seoil University
[2]Dept. of Internet Information, Seoil University
[3]Dep. of Computer Science, Soongsil University

요 약 ICT기반의 융합산업인 스마트 헬스케어 시스템은 건강관리부터 원격진료 범위에 걸쳐 다양한 산업분야의 핵심 연구 주제이다. 스마트 헬스케어 환경은 웨어러블 디바이스를 통하여 사용자의 심박 수, 체온, 건강상태 등과 같은 생체정보를 주치의가 있는 병원 네트워크로 전달하는 기술을 의미하며 환자의 다양한 데이터를 수집하고 복합적인 정보를 추론할 수 있는 기술은 스마트 헬스케어 기술의 핵심기술이라 할 수 있다. 그러나 환자에 대한 개인의 의료정보를 다루는 만큼 정보관리에 대한 보안위협이 있으며, 무선 네트워크 환경에서 발생하는 공격기법에 대해서 취약점이 발생할 수 있다. 그러므로 본 논문에서는 스마트 헬스케어 기반의 디바이스 접근제어를 위한 키를 생성 후 생성한 키를 활용하여 안전한 통신 프로토콜을 설계하여 스마트 헬스케어 시스템의 보안성을 강화하였다. 성능평가에서는 스마트 헬스케어 환경에서 발생하는 공격기법에 대해서 안전성 분석을 하고, 기존의 키 암호화 방식과의 보안성 및 효율성을 분석하여 기존의 암호화 방식 대비 대략 15% 향상된 수치를 확인할 수 있었다.

Abstract Smart healthcare systems, a convergent industry based on information and communications technologies (ICT), has emerged from personal health management to remote medical treatment as a distinguished industry. The smart healthcare environment provides technology to deliver vital information, such as pulse rate, body temperature, health status, and so on, from wearable devices to the hospital network where the physician is located. However, since it deals with the patient's personal medical information, there is a security issue for personal information management, and the system may be vulnerable to cyber-attacks in wireless networks. Therefore, this study focuses on a key-development and device-management system to generate keys in the smart environment to safely manage devices. The protocol is designed to provide safe communications with the generated key and to manage the devices, as well as the generated key. The security level is analyzed against attack methods that may occur in a healthcare environment, and it was compared with existing key methods and coding capabilities. In the performance evaluation, we analyze the security against attacks occurring in a smart healthcare environment, and the security and efficiency of the existing key encryption method, and we confirmed an improvement of about 15%, compared to the existing cipher systems.

Keywords : Access Control, Key Generation Protocol, Key Management, Personal Information Security, Smart Health care

본 논문은 2016년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : So-Yeon Min(Seoil Univ.)
Tel: +82-10-6576-0726 email: symin@seoil.ac.kr
Received October 6, 2016 Revised November 2, 2016
Accepted November 10, 2016 Published November 30, 2016

1. 서론

최근 ICT기반의 융합기술 서비스가 점차 증가함에 따라 다양한 서비스가 점차적으로 확대되고 있는 추세이며, 헬스케어 산업은 모바일 네트워크의 급속한 발전과 범국가적으로 질 높은 의료서비스를 향상시키기 위해서 여러기관에서 연구되고 있다[1][7-8].

세계 각국에서는 ICT 기반의 헬스케어 솔루션 및 인프라를 지원하고 있으며 헬스케어 정책의 다각적인 연구를 통해, 고령화 인구사회에서 관리하는 의료서비스를 적용하도록 추진하고 있다. 스마트 헬스케어 서비스는 언제 어디에서나 네트워크를 통하여 주치의 및 의료진으로부터 진료 및 처방을 받을 수 있으며, 건강관리를 할 수 있는 서비스를 의미한다. 하지만 환자의 중요한 개인 건강정보를 관리함으로서 해커 및 악의적인공격자들의 표적이 되고 있다. 작년 한해 국내외에서 의료업계를 노리는 해커들의 공격사례들이 발생하고 있으며, 개인정보 및 데이터를 노리는 공격자들이 발생하고 있다[4][5][7][11].

본 연구에서는 스마트 헬스케어 기반의 환자의 건강정보, 개인정보에 대해서 안전하게 헬스케어 서비스를 수행할 수 있도록 키 생성 및 안전한 통신 시스템에 관하여 설계하였다. 그리고 디바이스 및 키 관리 프로토콜을 설계함에 따라서 송수신하는 메시지에 대한 안전성 및 보안성을 강화하였다.

2장에서는 스마트환경기반의 헬스케어 시스템 활용 및 보안위협 및 헬스케어 시스템 환경의 보안요구사항에 대해 관련연구를 서술하였다. 3장에서는 디바이스 등록 및 키 생성 절차, 메시지 통신절차, 키 갱신 및 관리 프로토콜에 대해서 서술하였으며, 4장에서는 안전성 분석 및 보안성 분석을 통하여 성능평가결과를 나타내었으며 5장 결론에서는 향후 연구방향을 제시하였다.

2. 관련연구

2.1 스마트환경기반의 헬스케어 시스템 활용 및 보안위협

과거에는 치료중심의 관리였으나 최근에는 관리 중심의 헬스케어 환경 분야로 변화되고 있다. 과거부터 현재까지 질병이 발생하고 치료하기 위해서 비용이 소모되었지만, 앞으로는 건강관리부분에 비용이 많이 들어가고 유지하도록 많은 부분이 요구되고 있다[3-4].

이러한 기술을 구축하기 위해서 ICT기반의 건강관리 기술 및 서비스가 발전되고 있으며, 원격의료 및 건강관리 분야가 활발히 연구되고 있다. IoT의 장비를 통하여 장소에 상관없이 언제 어디서든 환자의 건강상태를 모니터링하고 이상 증후 발생 시 즉각적으로 대응할 수 있다는 특징이 있다. 헬스케어 시스템 구성도는 [Fig. 1]과 같다[3][10].

서비스를 수행하는 정보는 주로 환자 개개인의 건강정보이면서 보안 및 개인정보보호 노출 및 유출과 같은 사례가 발생하여 문제점으로 부각되고 있다. 그리고 유무선 기반의 통신을 수행함으로서 기존의 취약점과 신규 및 다양한 공격기법이 존재한다.

이러한 공격기법을 방지하기 위해서 안전한 교화 및 공유 기술을 요구하고 있다. 즉, 멀웨어나 봇넷 등과 같은 사이버위협에 침해받고 있어 헬스케어환경에서 안전성의 대한 강화가 요구되고 있다[5].

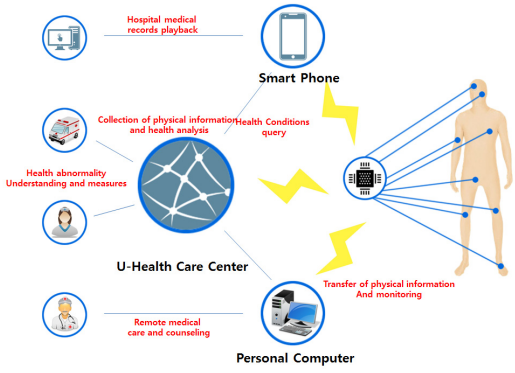

Fig. 1. Health Care Service Configuration

2.2 헬스케어 시스템 환경의 보안요구사항

헬스케어 환경에서 정보를 보호하기 위해 기술적인 요구사항은 다음과 같다.

- 개인 건강정보 수집, 저장 및 관리 단계에서 보호

사용자의 개인정보는 의료기관 내•외부의 단말기에서 수집되며, 다양한 의료서비스를 수행하기 위해서 저장 및 관리한다. 사용자의 건강정보를 분류, 접근 권한 관리, 중요정보 암호화, 통신을 수행할 때 관리 및 보호를 수행해야한다[1][4][9][12].

- 개인건강정보 폐기 단계에서 보호

데이터 형태로 저장되는 정보는 처리 시에 편리하고 다방면에서 손쉽게 사용할 수 있다는 장점이 있으나, 원본과 사본의 대한 식별부분이 어려움이 있어 기술적 보안요구사항을 다루고 있으며, ISO TS 22600-1 : Health informatics - Privilege management and access control-part 1 : Overview and policy management 표준문서를 참조한다[1][6].

- 개인건강정보 교류 단계에서의 보호

헬스케어 서비스를 수행하기 위해서는 의료서비스를 제공하는 종사자와 병원에서 정보교류가 활발히 이루어져야하고, 관련된 보안 요구사항을 충족해야한다[1][4-5].

- 개인정보 침해사고 예방 및 대응

의료서비스 영역에서 정보는 매우 민감하고 정확성이 요구되어야 하는 항목이다. 환자의 건강정보를 관리하기 위해서는 적절한 보고체계를 수립해야하며, 신속한 대응이 필요하다. 또한 건강정보를 처리하기 위해서는 주기적인 진단과 관리가 필요하다[4-6][9].

3. 스마트 헬스케어 환경의 키 생성 및 통신 프로토콜 설계

본 연구에서 제안하는 시스템은 사용자가 디바이스를 사용하여 병원 네트워크의 도메인 영역으로부터 등록 및 키를 부여받고 안전한 통신 서비스를 수행하는 것을 목표로 한다. 그리고 병원의 접근제어 서버에서는 디바이스 및 키 관리 프로토콜 수행하여 안전한 정보관리를 하도록 설계하였다. 본 논문의 가정 사항은 아래와 같으며 제안된 프로토콜의 약어표는 [Table 1]과 같다.

- 디바이스는 사용자가 사용하기 전에 Key Management Server에 Serial Number가 등록되어 있어야 한다.
- Service Provider와 Key Management Server는 파라미터값을 기반의 $Session_{Key}$ 생성 알고리즘을 공유하고 있다.

Table 1. Abbreviation

Sign	Description
$User_{ID}$	Identification Value of User
$User_{Code}$	Code Value of User
$Device_{nonce}$	Generate Device Nonce
$Device_{SN}$	Serial Number of Device
KMS_{Grade}	Granted Grade Value by Key Management Server
$Signature_{Device}$	Signature Value of Device
$Patients-code$	Generated Patients code by Service Provider
$Hospital_{code}$	Generated Code Value by Hospital Information Server
SP_{nonce}	Generated Nonce by Service Provider
$Device_{Info}$	Information of Device

3.1 디바이스 등록 및 키 생성 절차

사용자는 디바이스를 사용하여 Service Provider로부터 디바이스 등록을 수행한다. 이후 Certificate Authority로부터 사용자 정보, 디바이스 정보를 확인 후 검증받고 Key Management Server로부터 $Session_{Key}$를 검증받는다. $Session_{Key}$는 디바이스 및 사용자에 알맞은 등급값을 부여한다. 상세적인 절차는 [Fig . 2]와 같다.

1. 사용자는 디바이스를 사용하여 Service Provider로부터 등록요청 메시지를 전송한다.

$$E_{Pub-sp}(Device_{SN}), User_{ID} \quad (1)$$

2. Service Provider는 $User_{ID}, Device_{Sn}$ 을 검사하고 디바이스로부터 사용자 코드 메시지를 요청한다.

3. 디바이스에서 $Device_{nonce}$ 를 생성 후 사용자는 사용자 코드 값을 입력 후 디바이스에서는 해쉬함수를 수행하여 $Hash(User_{Code})$ 해쉬값을 생성한다. 코드값은 해쉬함수를 수행하여 안전하게 Service Provider로 사용자 코드 메시지를 전송한다.

$$Hash(User_{Code}), E_{pri-sp}(Device_{nonce}) \quad (2)$$

4. Service Provider는 Certificate Authority로 부터 해쉬값, 사용자 식별값, $Device_{SN}$이 첨부된 신원 검증 요청 메시지를 전송한다.

$$Hash(User_{Code}), User_{ID}, E_{pub-ca}(Device_{SN}) \quad (3)$$

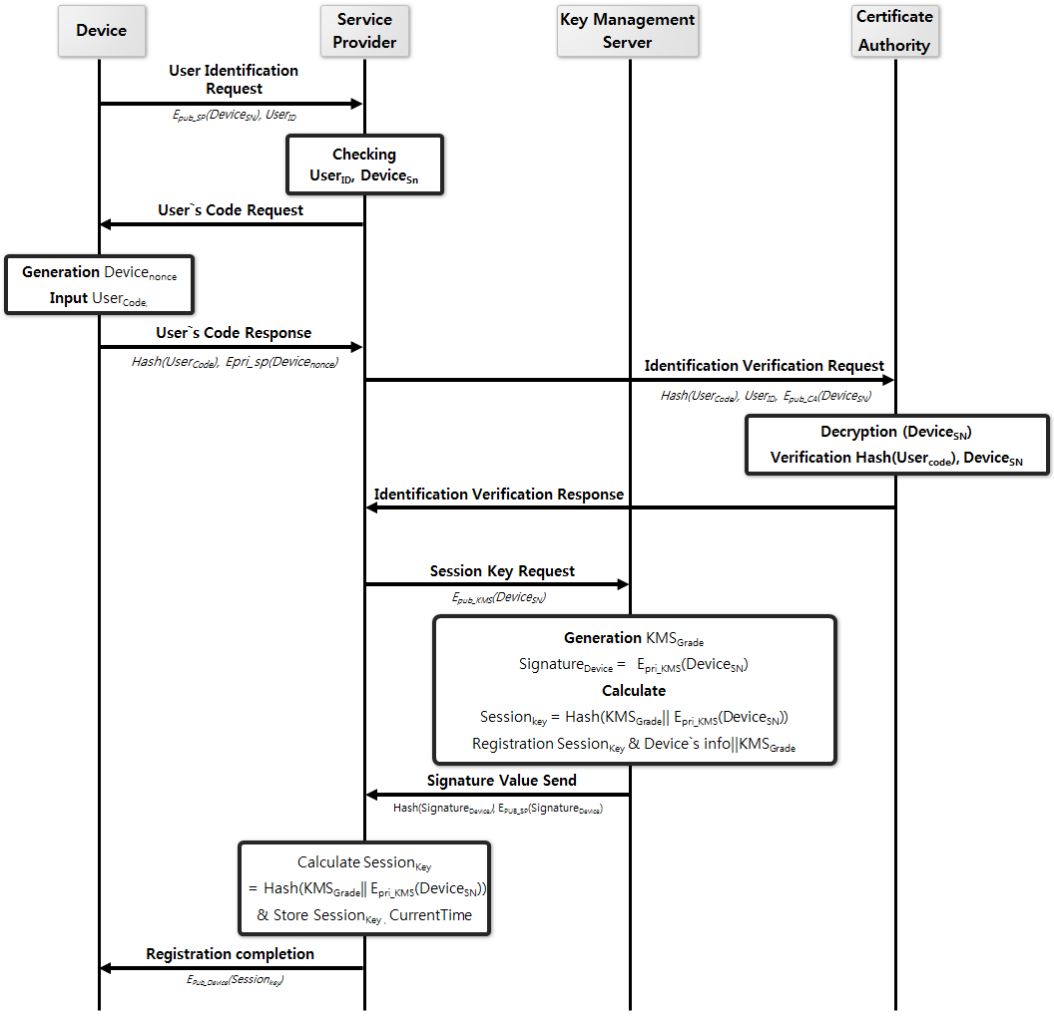

Fig. 2. Device Registration and Key Generation Phase

5. Certificate Authority는 신원 메시지를 복호화 한다. 이후 $Hash(User_{code}), Device_{SN}$ 에 대한 검증작업이 완료되면 응답메시지를 Service Provider로 전송한다.

6. Service Provider는 Key Management Server로부터 세션키 생성 메시지를 요청한다.

$$E_{Pub-KMS}(Device_{SN}) \quad (4)$$

7. Key Management Server는 KMS_{Grade} 를 생성 한 후 $Signature_{Device}$ 를 생성 한다. 이 후 $Session_{Key}$ 를 생성 후 Key Management Server는 $Session_{Key}$, $Device_{ID}$, KMS_{Grade}를 등록한다.

$$Signature_{Device} = E_{Pri-KMS}(Device_{SN}) \quad (5)$$

8. Key Management Server로 Signature Value값을 Service Provider로 전송한다. 이후 $Session_{Key}$ 를 계산 후 키와 현재시간을 저장한다. 디바이스의 공개키 값으로 암호화 후 $Session_{Key}$ 를 전송한다.

$$Session_{Key} = Hash(KMS_{Grade}||E_{Pri-KMS}(Device_{SN})) \quad (6)$$

3.2 메시지 통신 프로토콜 설계

본 절에서는 메시지 통신 프로토콜 설계에 대하여 기술하고자 한다. 사용자는 디바이스 등록 및 키 생성 절차에서 등록받은 세션 키를 기반으로 암호화 후 메시지를 전송한다. 이후 Hospital Information Server에서는 메시지를 수신하고 Key Management Server에서 확인 후 복호화 하여 사용자로부터 Feedback 메시지를 전송한다. 상세적인 절차를 [Fig. 3]에서 나타내었다.

1. 사용자는 디바이스를 활용하여 Service Provider로부터 건강정보 메시지를 전송한다.

$$Session_{Key}(Message), E_{\mathrm{Pri-Device}}(Device_{SN}), User_{ID} \quad (7)$$

2. Service Provider 복호화 후 수신된 메시지를 확인 후 메시지를 코드 변환작업을 수행한다. 그리고 Hospital Information Server로 환자 상태 보고 메시지를 전송한다.

$$Session_{key}(Message), E_{\mathrm{Pri-hip}}(patients-code), User_{info} \quad (8)$$

3. 수신된 메시지를 받은 Hospital Information Server는 Key Management Server로부터 키 검증 메시지를 전송한다.

4. Key Management Serve에서 $Device_{ID}$ 을 참고하여 Session Key를 검색한다. 이후 Hospital Information Server 공개키로 암호화하여 $Session_{Key}$를 Hospital Information Server로 전송한다.

5. Hospital Information Server는 수신된 메시지를 복호화하여 메시지를 확인한다. 이후 Service Provider로부터 온 $E_{pri-hip}(Patients-code)$를 검증 후 $Hospital_{Code}$ 를 생성한다.

6. Service Provider로 환자에 대한 피드백 메시지를 발송 후 Service Provider는 디바이스로 메시지를 전송한다.

$$E_{pub-sp}(Hospital_{Code}, Message) \quad (9)$$

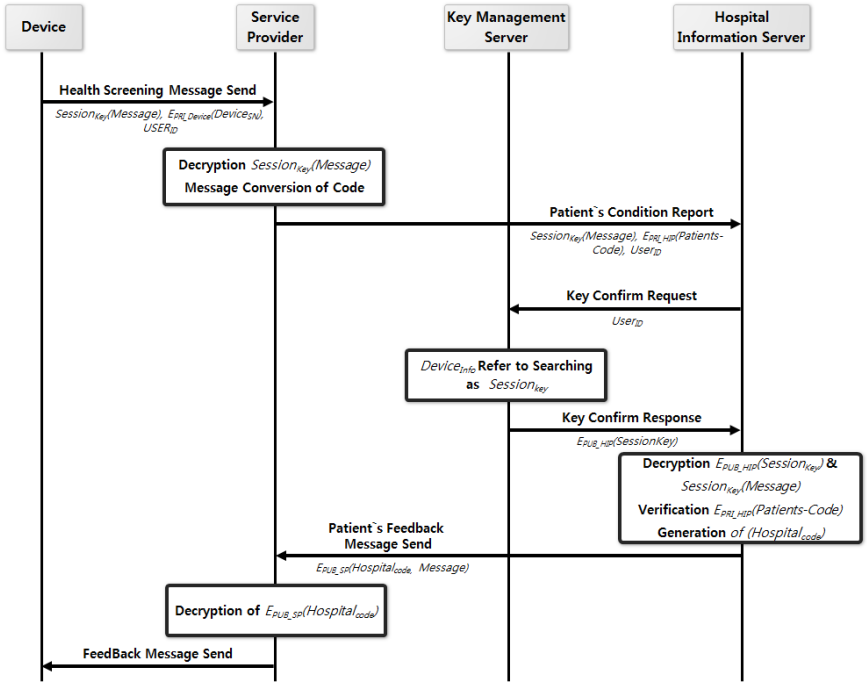

Fig. 3. Message Communication Protocol Design

3.3 키 갱신 및 관리 프로토콜 설계

키 갱신 및 관리 프로토콜은 주치의가 Hospital Information Server를 통하여 Key Management Server로 키에 대한 정보를 수신한다. 그리고 Key Management Server에서 유효기관, Service Provider에서 생성된 난수 값을 검증 후, 키 확인 메시지를 전송한다. 아래의 [Fig. 4]는 키 갱신 및 관리 프로토콜이다.

1. Hospital Information Server에서 Key Management Server로 디바이스 키 관리 메시지를 전송한다.

$$E_{pub-KMS}(Code), Hash(KMS_{Parameter}) \quad (10)$$

2. Key Management Server는 메시지를 복호화하여 해쉬값을 검증한다. 이후 Service Provider로부터 디바이스 제어 리스트 요청 메시지를 전송한다.

3. Service Provider는 디바이스로부터 상황 메시지를 통신 후 목록을 검사한다. 이후 Certificate Authority로부터 검증 요청 메시지를 전송한다.

$$Hash(User_{code}), E_{Pub-CA}(SP_{Nonce}) \quad (11)$$

4. Certificate Authority는 수신된 메시지의 $Hash(User_{Code})$, $E_{Pub-CA}(Sp_{Nonce})$를 검증 후 Service Provider로부터 검증 완료 메시지를 전송한다.

5. Service Provider는 Key Management Server로부터 Device Access List를 전송한다. 이후 Key Management Server에서는 Session을 검색 후 현재시간이 유효시간보다 크면 세션 키를 갱신하며, Hospital Information Server로 디바이스 키 관리 확인 메시지를 전송한다.

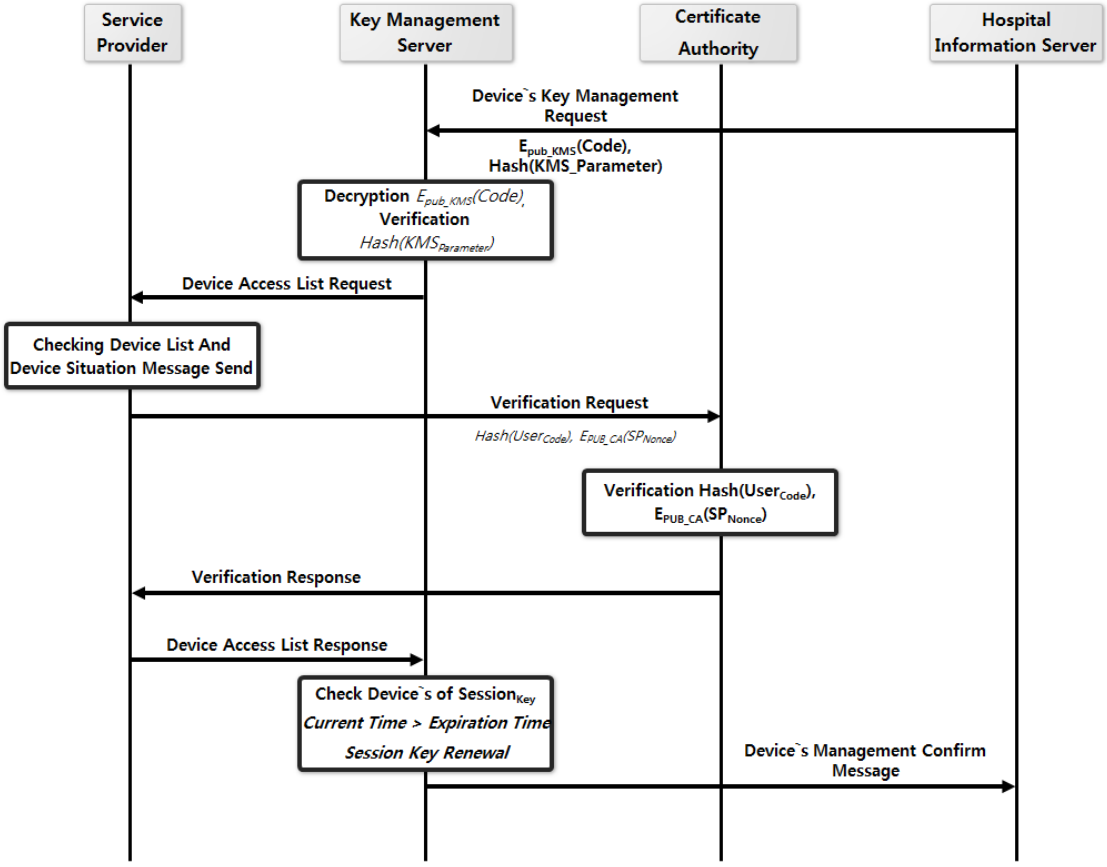

Fig. 4. Key Renewal and Management Protocol

4. 성능분석

4.1 안전성 분석

본 절에서는 제안된 프로토콜의 안전성을 분석하기 위해 기존의 U-Health 및 Smart-Health 환경에서 발생하는 공격기법을 기반으로 분석하였다. 위장공격, 중간자 공격, 재생공격이 Health Care환경에서 대표적인 공격기법이며, 개인정보유출, 부인방지에 대한 보안위협이 있다.

4.1.1 위장공격

위장공격은 악의적인 사용자가 불법 디바이스 이용하여 Hospital Server, Service Provider로 접속 후 정보를 도청하는 공격을 말한다. 이러한 위협에 대응하기 위해 등록과정에서 사용자 코드로 생성된 해쉬값 $Hash(User_{code})$ 와 Server Provider의 개인키 값으로 암호화된 $Device_{nonce}$ 값을 검증하여 망에 대한 접속을 막을 수 있었다.

4.1.2 중간자 공격

Smart Heath Care환경에서 Service Provider 도메인과 Key Management Server 도메인영역에 정보를 탈취하는 중간자 공격기법이 발생하는데, 이를 방어하기 위해 등록과정에서 생성된 $Session_{Key}$ 로 메시지를 암호화하여 전송하고 $Device_{Sn}$, $Hospital_{code}$ 로 검증한다.

4.1.3 재생공격

디바이스에서 생성된 사용자의 메시지를 가로채어 Service Provider, Key Management Server, Hospital Information Server로 공격하는 재생공격은 대표적인 공격기법이다. 그러나 키 관리 과정에서 디바이스의 정보를 수신하여 $Session_{Key}$ 를 관리하고, Hostpital Information Server에서는 $Session_{key}$ 를 Key Management Server에서 확인함으로써 재생공격이 실패한다.

4.1.4 개인정보유출

Smart Health Care 환경에서는 외부의 사용자가 디바이스를 이용하여 Hospital의 네트워크를 접속함으로써 사용자 정보를 탈취 후 유출 하는 보안위협이 발생할 수 있다. 이를 막기 위해서 $Session_{Key}$ 를 생성할 때 KMS_{Grade} 를 생성하여 사용자에 따른 등급을 부여하여 유출에 대한 피해를 막을 수 있다. 또한 사용자 정보를 등록함으로써 정보유출에 대한 추적이 가능하다.

4.1.5 부인방지

Service Provider와 Key Management Server에서 $Session_{Key}$ 로 암호화된 메시지를 검증받으며, 또한 공개키와 개인키로 $User_{code}$, $Device_{nonce}$, $Device_{SN}$ 및 해쉬함수를 통한 해쉬값을 검증 후 상호인증을 수행함으로써 부인방지에 대한 위협을 완화할 수 있다.

4.2 암호 성능 및 보안성 평가

제안된 프로토콜의 보안성 및 안전성을 평가하기 위해 TTA.KO-10.0304 개인건강정보 보호를 위한 기술적 요구사항 TTA 표준문서를 기반으로 보안성을 평가하였다. 개인건강정보 익명화, 개인건강정보 폐기, 개인건강정보의 내역관리, 개인건강정보 침해 사고와 관리에 대해서 비교분석하였으며, 기존의 시스템 환경과 제안 시스템의 보안성을 평가한 자료를 [Table 2]에서 나타내었다. 제안된 시스템에서는 사용자 건강 정보성에 대한 관리를 제공하여 진료가 끝나면 즉시 폐기할 수 있도록 설계하였으며, 키 관리 프로토콜을 제안된 시스템의 적용하여 사용자의 건강정보에 대한 침해부분의 보안성을 보완하였다.

Table 2. Security Requirement Comparison of Existing System and Proposed System

Requirement	Exist System	Proposed System
Personal health information Disposal	Not Support	Support
Management of the contents of the personal health information	Support	Support
Health information infringement accident and management of individual	Not Support	Support

제안된 시스템의 암호성능을 분석하기 위하여 Inter(R) Core i7-4970(3.6GHz), 8.00 GB, Windows Professional 64 bit환경에서 분석하였다. Java Cryptography Architecture

플랫폼을 활용하여 기존의 대칭키 암호 Triple-DES, SEED, AES, 제안된 암호화($Session_{Key}$)의 암호화, 복호화, 통신과정의 암•복호화 통합의 효율성 분석을 수행하였고, 수행속도를 비교분석한 수치를 [Table 3]과 [Fig. 5]에서 나타내었다.

Table 3. Numerical Analysis of Cryptographic Performance (unit :millisecond)

	T-DES	SEED	AES	Proposed Cryptography
Encryption	238	15	23	38
Decryption	12	13	12	13
Total	250	137	178	152

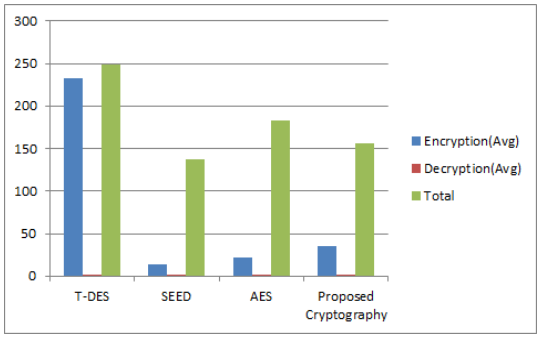

Fig. 5. Comparison Analysis of Exist Cryptography Method and Proposed Cryptography System

[Table 3]에서는 기존의 대칭키 암호화 방식인 T-DES, SEED, AES와 비교분석을 수행하였으며, 수치의 단위는 밀리 세컨드로 표시하였다. 제안된 암호화 수행방식에서는 5번의 암호화 복호화 수행과 해쉬함수를 수행하여 등록 프로토콜을 설계하였다. 기존의 인증과정에서 Certification과는 달리 해쉬함수를 수행하여 속도적인 측면에서는 속도가 떨어지지만, 해쉬함수에서 등급 및 권한 부여에 관한 파라미터를 첨부하여 통신과정에서 안전하게 수행할 수 있도록 하였고, 통신과정에서는 등록과정에서 설계된 $Session_{Key}$를 암•복호화 작업을 수행하여 기존 암호 시스템(AES)대비 통신과정에서 효율성이 향상된 것을 확인할 수 있었다.

Table 4. Performance System of Exist System and Proposed System

	Exist System	Proposed System
Registration Phase	4Encryption + 4Decryption + 1 Cert	5Encryption + 5Decryption + 5HASH(MD5)
Message Communication Phase	3 Encryption(AES) + 3 Decryption + 1 Cert	3 Encryption(Proposed Session Key) + 3 Decryption

[Fig. 5]에서 도시한 바와 같이 기존의 T-DES, SEED에 비하여 암호화 성능이 암•복호화 및 키 생성 수행속도에서는 높게 나왔지만, AES에서는 암•복호화 부분에서는 수치가 38% 증가하였음을 확인하였고, 키 생성속도 부분에서 기존보다 25% 증가하므로 총 수치에서는 15% 향상된 속도를 확인할 수 있었다. 그리고 키 생성과정에서 사용자의 등급 값과 디바이스 정보를 같이 저장함으로써 권한관리와 정보의 안정성과 보안성을 확인할 수 있었다.

5. 결론

본 연구에서는 스마트 헬스케어 기반의 정보유출 피해와 사용자의 디바이스를 접근제어 및 키 관리 프로토콜을 설계하여 통신을 시스템에 대해서 연구하였다.

제안된 프로토콜은 디바이스 등록 및 키 생성단계에서 사용자의 해쉬값과 Service Provider의 검증값을 기반으로 Key Management Server에서 세션키를 설계하였다. 이후 통신과정에서 세션키를 활용하여 안전한 통신을 수행할 수 있도록 프로토콜을 설계하였으며, 키 관리 프로토콜에서는 Hospital Information Server에서 Service Provider로 디바이스 접근 목록 및 킷값을 검증하여 갱신하는 프로토콜을 제안하였다.

성능평가의 안전성 분석에서는 Smart-Health Care환경과 기존의 U-Health Care환경에서 발생하는 공격기법에 대해서 안전성을 분석하였으며, 기존의 대칭키 암호화 방식인 Triple-DES, SEED, AES와 비교분석하여 AES 대비 대략 15% 향상된 수치를 확인할 수 있었다.

제안된 시스템을 Smart Health Care환경에 적용하기 위해서는 본 연구에서 제안된 키 관리와 디바이스 제어뿐만 아니라, 개인정보 정책 수립이 필요하며, 향후 다양

한 IoT 디바이스와 연동하여 Smart-Health Care 기반에서 효율성 높은 서비스를 위한 연동 프레임워크 설계 및 분산인증 알고리즘에 대한 연구를 진행할 계획이다.

References

[1] TTA.KO – 10.0304, “Technical Privacy and Security Requirements for Personal Health Record”, TTA, 2008. 12.

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

[3] TTA, Health Data Gateway, Server Protocol, 2011.6.

[4] TTA, u-Health Service Reference Model, TTA, 2010.12.

[5] M. Li, K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Communications, vol. 17, no. 1, pp. 51-58, Feb. 2010.
DOI: http://dx.doi.org/10.1109/MWC.2010.5416350

[6] Wearable Technology Market-Global Scenario, Trends, Industry Analysis, Size, Share And Forecast 2012-2018.

[7] Young-bok Cho, Sung-hee Woo, Sang-ho Lee, Jong-bae Park, “A Secure Telemedicaine System in Smart Health Environment using BYOD”, JKICE, vol. 19, no. 10, pp. 2473-2480, 2015.

[8] Jong-Jin Park, Gyoo-Seok Choi, Jeong-Lae Kim, In-Kyoo Park, Jeong-Jin Kang, Byeong-Ki Son, "Development of Mobile Healthcare App for Mental Health Management ? Focused on Anger Management-," The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), vol. 14, no. 6, pp. 13-18, Dec. 31, 2014.
DOI: http://dx.doi.org/10.7236/JIIBC.2014.14.6.13

[9] M Meingast, T Roosta, S Sastry, “Security and privacy issues with health care information technology”, 28th Annual International Conference of the IEEE, 2006. 9.
DOI: http://dx.doi.org/10.1109/iembs.2006.260060

[10] Jin Tae Park, Hyun Seo Hwang, Jun Soo Yun, Gyung Soo Park, Il Young Moon, “Application and Convergence Technique : User Motion Recognition Healthcare System Using Smart-Band”, Koni, vol. 18, no. 6, pp. 619-624, 2014.

[11] Jae-Man You, In-Kyoo Park, "Android Storage Access Control for Personal Information Security,"" The Journal of The Institute of Internet, Broadcasting and Communication, vol. 13, no. 6, Dec. 2013.
DOI: http://dx.doi.org/10.7236/JIIBC.2013.13.6.123

[12] Sang-Hyun Joo, Tae-Gil Kang, Woo-Suk Yang, "A Implementation of Iris recognition system using scale-space filtering," The Journal of The Institute of Webcasting, Internet Television and Telecommunication, vol. 9 no. 5, pp. 175-181, 2009.

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 임베디드 시스템

이 광 형(Kwang-Hyong Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 (공학사)
- 2002년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 인터넷 정보과 부교수

<관심분야>
멀티미디어 보안, 사물인터넷, 학습콘텐츠, 영상처리

진 병 욱(Byung-Wook Jin) **[정회원]**

- 2010년 2월 : 청운대학교 멀티미디어학과 (문학사)
- 2013년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과

<관심분야>
사물지능통신, USN, 네트워크 통신