The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 4, pp.133-139, Aug. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.4.133
JIIBC 2014-4-20

암호화 알고리즘을 이용한 안전한 원격 EMR 의료정보 구현

Implementation of Secured Remote EMR Medical Information using Encryption Algorithm

양재수*, 이유식**, 홍유식***

Jaesoo Yang*, You-Sik Lee, Yousik Hong*****

요 약 요즈음, 원격 처방전 및 원격 진료가 시범적으로 운영되고 있다. 그러나 대부분의 원격지 병원에서 환자 생체 데이터를 암호화 하지 않고 전송하는 경우, 해커가 환자 처방전 데이터를 해킹해서 처방전 약물을 바꾸면 환자는 심각한 장애를 받을 수 있다. 따라서, 본 논문에서는, 이러한 문제점을 해결하기 위해 원격 처방전과 의료 정보시스템에 환자의 비밀번호, 개인 식별 정보, 바이오 정보 등을 암호화하는 알고리즘과 안전한 보안 구현 방안이 제시되었다.

Abstract Nowadays, telemedicine and remote prescription has been operating as a pilot basis. However, in case of remote hospitals without encrypting the biometric data transmission and its contents, the patient prescription data hacked from hackers who changed prescription medications can be serious obstacles to the patient. Therefore, in this paper, to solve this problem, password encryption, personal identification information, biometric data security on the patient's prescription and remote medical information system, and implementation of the encryption algorithm are proposed.

Key Words : Encryption Algorithm, Remote medical information system, Remote patient's prescription hacking, Secured Remote EMR

Ⅰ. 서 론

개인정보보호법에 대응하기 위한 병원들의 DB암호화 사업이 본격화 되고 있다. 이러한 정보보호를 구축하기 위해서, 전자 의무기록시스템(EMR), 의료영상정보저장전송시스템(PACS), CDW(Clinical DW), 주요 시스템에 암호화를 적용하는데 많은 연구를 하고 있다. 미래의 병원은 자동화로 원격처방전 및 원격 진료가 이루어지기 때문에 환자 정보는 매우 중요하다. 만약 해커가 환자 처방전 데이터를 해킹해서 처방전 약물을 바꾸면 환자는 심각한 장애를 받을 수 있다. 이러한 문제점을 해결하기 위해서는 원격 처방전 및 의료 정보시스템에 로그인할 때 이용하는 비밀번호 암호화를 비롯하여, 개인 식별 정보, 바이오 정보 등을 필수적으로 암호화 해야 한다[1-4].

특히, 많은 수의 환자를 보유한 종합병원이나 전문병원의 경우 개인정보가 유출될 경우 발생할 병원 신뢰도

*정회원, 단국대학교 전자전기공학부
**정회원, 펜타시큐리티시스템㈜
***종신회원, 상지대학교 컴퓨터 정보공학부 (교신저자)
접수일자 : 2014년 4월 23일, 수정완료 : 2014년 7월 29일
게재확정일자 : 2014년 8월 8일

Received: 23 April, 2014 / Revised: 29 July, 2014
Accepted: 8 August, 2014
*Corresponding Author: yshong@sangji.ac.kr
Dept. of Computer Science, Sangji University, Wonju, Korea

하락이나 천문학적인 손해 배상 금액을 고려한다면 내부자에 의한 정보유출 방지를 위한 보안 솔루션 도입이 시급하다[4-7].

본 연구과제에서는 WEB 기반에서 무선 통신기능을 이용하여서 환자와 한의사 간의 원격 진료를 할 경우에, 환자 신상 데이터 정보를 포함, 설진 및 맥진 암호화 과정을 구현하였다[8-13].

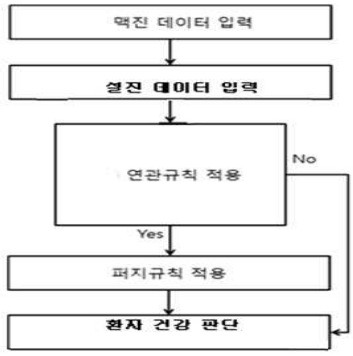
II. EMR챠트 기반 환자 건강상태 추론과 암호화

본 논문에서는 환자의 신체조건 및 나이조건 성별 조건 등을 고려해야하므로 질병 확신도에 관한 믿음값을 산출하는 알고리즘을 제안하였다. 첫째, 조건부확률 P(Hi|E) 를 알기 위해 사전확률 P(Hj)와, 조건부 확률 P(E|Hj)를 알아야 한다. 예를 들어, E가 환자의 몸에 나타나는 증상이고 Hi가 질병으로 추론될 경우에, 각 질병들의 증상 E가 나타날 확률 P(E|Hj)가 주어져야 하나 현실적으로 이들에 대한 데이터가 부족한 경우가 많다. 그러므로 본 논문에서는 퍼지규칙을 이용한 질병 확신도에 관한 믿음값을 다음과 같이 설정하였다[12,13]

RULE: (건강이 좋지 않은 Group)
IF S amp (진폭)이 MAX 이다.
AND 환자 맥박 속도가 Big 이다
AND 환자 맥박 강도가 High 이다
OR 환자 설태양이 High 이다.
Not 환자 설색이 분홍색이 아니다.
OR 환자 설색이 검정색 이다.
OR 환자 설색이 보라색 이다.
OR 환자 설색이 노란색 이다.
THEN 고혈압+ 당뇨+심장 질환환자
(5장 6부 : 나쁜 환자)

전처리 RULE: (건강이 좋은 Group)
IF S amp (진폭)이 MEDIUM 이다.
AND 환자 맥박 속도가 MEDIUM 이다
AND 환자 맥박 강도가 MEDIUM 이다
OR 환자 설태양이 MEDIUM 이다.
Not 설색이 검정색 이다.
Not 설색이 보라색 이다.
Not 설색이 노란색 이다.
THEN : 정상 환자
(5장 6부 : 좋은 환자)

그림1.에서는 환자의 질병을 보다 정확하게 산출하기 위해서 맥진 및 설진 데이터를 2개 이상 추론할 때 신체조건등에 의해서 정확한 추론이 어려울 경우에 퍼지규칙 및 통계기반 확률 데이터를 이용한 믿음값 을 이용한 최종 질병추론 산출과정을 설명하고 있다.



1. 지능형 맥파 알고리즘
Fig. 1. Intelligence pulse wave algorithm

Rule : IF A is t1 THEN C is B2
(Fu)
fact : A is t1' (Fr)
conclusion : C is t2'
(FC)
여기에서,
A : 임상 환자 상태
C : 추론 결과
Fu : 규칙의 불확실성을 나타내는 fuzzy number
Fr : 사실의 불확실성을 나타내는 fuzzy number
FC : 결론의 불확실성을 나타내는 fuzzy number
V1, V2, V1', V2' : 값 (values)
여기서 Fu은 확신율 (CF)를 나타내며, Fr은 가능척도를 나타낸다.

후처리 RULE (실맥)
IF Samp = Med And
Bmi = High And
H_Blood= High And
N time = Med And
Then
Strongwave = CNF 60

여기서 CNF 60이란 실맥 Strong(Excess syndrome) 파장으로서, RULE 의 확신도가 60%란 뜻이다. 만약, 퍼지규칙을 사용하지 않고 기존의 방법대로 확신도를 표

시한다면, 이러한 환자는 실맥으로 분류될 확률이 항상 100%로 간주된다. 본 논문에서는 BMI(체질량 지수;체중(kg)/키(m^2))와 H_Blood(최고혈압) 및 Samp(상승 파형), N time (절흔점 시간)을 고려해서 실맥 신뢰도를 60%로 판단하게 된다. 만약 사용자가 S amp = Low에 대한 확신도를 70이라고 주었으면 결론에 대한 확신도는 0.6 × 0.7 = 0.42가 된다.

질병의 맥진 파형도 환자의 성별이나 나이, 기타 신체 조건에 의해서 맥파의 강도 및 빠르기가 같지 않으므로 정확한 추론을 하기에는 매우 어려운 현상이 발생한다. 그러므로, 똑같은 질병의 맥진 데이터 결론이 두 개 이상의 서로 다른 추론값을 갖게 될 때에 정확한 추론을 하기 위해서 믿음값을 다시 계산하기 위해 사용하는 함수인 믿음값 결합함수를 사용하였다[12,13]. 요즈음 원격진료를 허용 할 때에 환자의 생체 데이터 및 영상데이터 음성데이터가 위조 및 변조되는 우려성 때문에, 원격진료를 꺼려하는 실정이다. 본 논문에서는 이러한 문제점을 해결하기 위해서, 위조 및 변조를 방지할 수 있는 알고리즘을 제안하였다. 표 1에서는 환자 생체 원본 데이터를 보여준다. Table 2에서는 Table 1에서 분석한 소중한 데이터를 인터넷상에서 DB로 저장 될 때에 해킹이나 변조를 예방하기 위해서 암호화된 과정을 보여주고 있다. 본 논문에서는 원격지에서, 환자 생체 데이터를 인증을 받을 때 환자의 생체 데이터가 유출되는 문제 방지와 보안성을 만족시키기 위해서 표 2에서 보는 것과 같이, 환자 데이터를 암호화하는 안전한 상호인증 프로토콜을 제안하였다.

1. 환자 생체정보 원본 데이터
Table 1. Patients body information source data

이름	맥진 데이터	설진 데이터	최고혈압	당뇨
홍길동	실맥	황갈색	178	123
박하나	평맥	정상	154	150
김기춘	허맥	정상	186	230
안재명	실맥	검정	176	310
박현일	평맥	자주색	125	156

표 2. 환자 생체정보 암호화 데이터
Table 2. Patient's body information encrypted data

이름	맥진 데이터	설진 데이터	혈압	당뇨
9b0775c440cd9e7d	06bf7ac487ed2f97	7b202af05b174aee	06bf7ac487ed2f97	cd9127635f75a09c
217d86c10e2ca4f5	06bf7ac487ed2f97	b006295f01478ec7	a878b99b3b0950e1	24ae98b2ced6ea43
facd60eb8e8d79ca	c42af71869e34b1b	b61e4845c8edf4c4	a878b99b3b0950e1	cd9127635f75a09c
5495153745 49b559	e89d039ed0abbbc4	6de5e7ce9e4e96a3	06bf7ac487ed2f97	cd9127635f75a09c
7e5253b7c35c031b	06bf7ac487ed2f97	43d3feac99e3b6af	a878b99b3b0950e1	b8b4be611036ba93

그림.2.에서는 스테가노 그래픽 기능을 이용해서 환자의 맥진 및 설진데이터가, 원격지에서 병원으로 전송 되었을 때에 데이터 위조여부를 확인 할 수 있는 기능을 설명하고 있다.

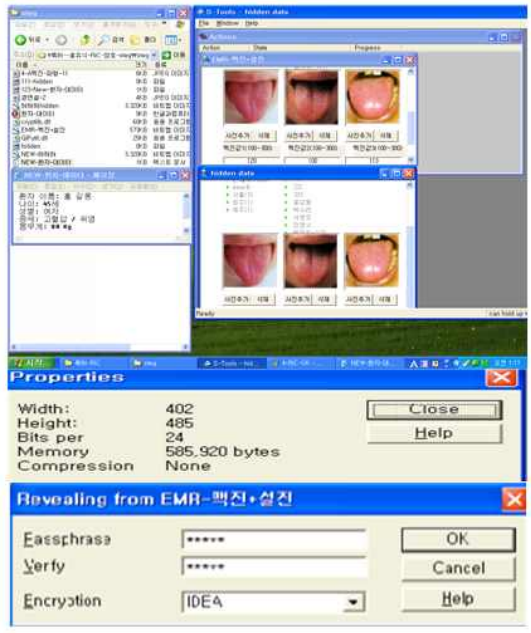


그림 2. 맥진 및 설진 데이터 암호화
Fig. 2. Pulse diagnosis and tongue diagnosis data encryption

스테가노 그래픽 기능을 실행하면, EMR-맥진-설진.bmp에 환자 데이터가 삽입되어 암호화되었으므로 해킹

및 환자데이터 위조 및 변조를 할 수 없는 장점을 제공하고 있다. 요즈음, 전자의무기록시스템(EMR)을 이용해서 환자의 진료기록을 보다 정확하고 신속하게 할 수 있다.

Ⅲ. 의료정보의 암호화

의료 정보는 법적으로 민감 정보로 분류되는 중요한 정보이며[1], 반드시 안전하게 전송 및 보관되어야 하므로[2] 본 논문에서도 암호화를 적용하여 안전성을 확보했다.

본 논문에서는 다음의 항목들에 대하여 암호화 및 보안을 적용하였다.

① 스마트폰과 헬쓰케어 단말기 간의 데이터 전송구간
② 스마트폰에서의 데이터 저장
③ 스마트폰과 웹 서버 사이의 전송구간
④ 웹 서버에서의 데이터 저장

1. 스마트폰과 헬스케어 단말기간의 데이터 전송 구간의 암호화

헬스케어 센서장비(맥박 센서, 혈압/혈당 센서, 심전도 센서, 적외선 온도 센서)를 통하여 측정된 생체정보는 H-Andro210에서 처리되어 스마트폰으로 무선네트워크(블루투스; Bluetooth)를 통하여 전송된다. 블루투스의 보안은 다음의 3가지 모드가 있다[3].

- Security Mode 1 : Non-secure.
- Security Mode 2 : A service level enforced security mode
- Security Mode 3 : The link level-enforced security mode

우리가 주목할 보안 목적은 기밀성이다. 즉, 전송되는 데이터를 전송하는 양단 이외의 타인(타기기)이 인지할 수 없도록 하는 것이다. 따라서, 헬스케어 장비의 Security Mode를 2나 3으로 설정하고 통신을 수행한다면, 소기의 목적을 달성할 수 있으므로 본 과제에서는 Bluetooth Protocol 본연의 보안 기능을 활용하여 기밀성을 보장했다.

2. 스마트폰에서의 데이터 저장시 암호화 방안

헬스케어 센서장비로부터 전송된 생체정보들은 스마트폰에서 안전하게 저장되어야 한다. 이를 위하여 암호화 기술을 적용해야 하고, 본 과제에서는 빠른 속도와 높은 안전성을 보장하는 블록 암호화 알고리즘 중 AES 256을 적용했다. AES는 다른 블록 암호화 알고리즘에 비하여 속도, 하드웨어 구현 용이성 등에서 비교우위를 점하고 있는 뛰어난 알고리즘임이 입증되었다[4,5].

암호 알고리즘은 단순한 수학적인 계산으로써, 그 자체만으로는 보안이라고 할 수 없으며, 키 생성, 보관, 폐기 등 안전하게 키의 Life Cycle을 관리하는 것이 보안의 핵심이다. 특히 우리가 사용하는 대칭키 알고리즘의 경우, 암호화 시 사용한 키가 복호화 시에도 그대로 사용되므로 안전한 키 보관이 문제가 된다. 즉, 암호화 시 사용한 키를 디스크나 메모리 영역 어딘가에 저장해 놓아야 복호화 시 다시 사용할 수 있다.

키 유도 방식을 사용하면 공격자가 키 파일을 탈취하거나 메모리 해킹 또는 실행파일을 Reversing하여도 실제 사용되는 키가 아니라 키를 유도하기 위한 Component 중 일부인 Salt 값이나 Iteration Number 만을 획득하여 완전한 키를 알 수 없다. 본 논문에서는, Fig.3 키 유도 및 암(복)호화 과정에서 보여주는 바와 같이, 공개키 암호 알고리즘 분야에서 사실상 표준(de facto standards)[5]으로 사용되는, RSA사의 PKCS 표준중 #5에 정의된 PBKDF2를 사용하여 키를 유도했다.

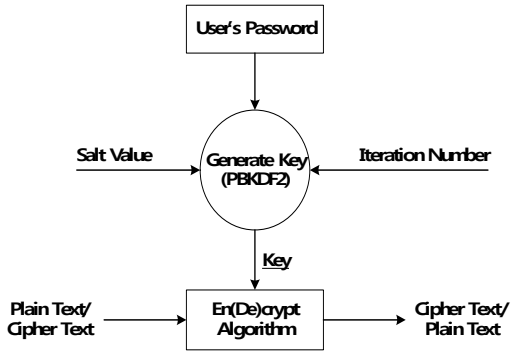


그림 3. 키 유도 및 암호화/복호화 과정
Fig. 3. Key derivation and encryption/decryption process

즉,

- 암복호 키 유도
  - $K_S = PBKDF2(PW, Salt, Iter)$

  여기서,
  K_S : SymmetricKey
  PW : User's password

Salt : Cryptographic salt
Iter : Iterations

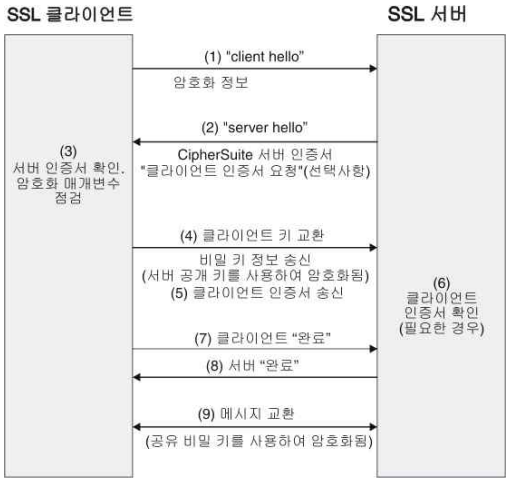
- 유도된 키를 이용한 암호화 또는 복호화
  - $C = E(K_S,P)$ or $P=D(K_S,C)$

여기서,
C : Cipher text
E( ) : Encryption function
P : Plain text
D( ) : Decryption function

의 과정으로 진행된다.

3. 스마트폰과 웹 서버 사이의 전송구간 암호화

일반적으로 스마트폰과 웹 서버 사이의 통신을 위하여 인터넷망을 사용한다. 인터넷 망은 누구나 접근할 수 있으며, 공격자가 손쉽게 전송되는 데이터를 획득할 수 있으므로 인터넷 망을 통하여 민감정보인 개인의 의료정보가 전송되는 것은 매우 위험하다. 따라서, 안전한 데이터 전송을 위하여 법이 정하는 수준 이상의 보안 조치가 필요하다[6].



4. SSL 동작 구조 (출처 : IBM)
Fig. 4. SSL enforcement behavior structure (Source: IBM)

본 논문에서는 보안서버의 구축을 통하여 민감 정보의 안전한 송수신을 보장했다. 보안서버란, 인터넷상에서 개인정보를 암호화하여 송수신하는 기능이 구축된 웹사이트를 말하며, 크게 SSL(Secure Sockets Layer) 방식과 응용프로그램 방식의 2가지로 구분된다[4-8]. 본 논문에서는 SSL방식의 보안서버를 선택, 적용하였다. 현재 SSL에 대한 공격들이 보고되고 있지만, 이는 SSL 자체에 대한 공격이라기보다는 악의적인 AP 설치, 가장(masquerading), 중간자 공격(Man-In- The-Middle Attack) 등 운영 상의 취약점에 대한 공격들이며, 본 논문의 범위를 벗어나는 주제들이므로 논하지 않는다[7-8].

SSL 적용시 웹 서버와 클라이언트는 위의 Fig.4. 같은 구조로 비밀키를 공유하고, 해당 비밀키를 사용하여 암호화 통신을 수행한다. SSL을 이용하여 보안서버를 구축하는 방법은 인증기관으로부터 SSL 인증서를 발급받아 서버에 설치하고 웹 서버 프로그램에 대하여 적절하게 설정을 변경하는 방식이다. 자세한 사항은 참고문헌을 참고한다[5-7].

4. 웹 서버에서의 데이터 저장시 암호화

시스템 내의 구성 요소에 대한 보안이 모두 중요하지만, 서버의 보안은 그 중 가장 중요하다. 단말의 보안이 훼손되면 한 개인의 정보가 유출되지만, 서버의 보안이 훼손된다면 서버에 저장된 모든 개인의 정보가 유출될 수 있기 때문이다. 공격자가 서버를 주로 공격하는 이유가 여기에 있다. 전술한 바와 같이 본 과제에서는 개인정보(의료정보)의 보호에 초점을 맞추고 있기 때문에 기밀성에 대해서만 논의하기로 한다. 본 논문에서 웹 서버에서의 암호화를 위하여 사용된 알고리즘들은 다음과 같다[17,18].

표 2. 웹 서버 암호화 적용 알고리즘
Table 2. 웹 서버 암호화 적용 알고리즘

종류	용도	알고리즘	키 길이	근거
난수생성기	키 생성	HASH_DRBG	-	ISO/IEC 18031(2011) NIST SP 800-90
블록 암호	데이터 암복호	AES	256	ISO/IEC 18033-3(2010) FIPS PUB 197
공개키 암호	키 암복호	RSAES	2048	ISO/IEC 18033-2(2006)
해시	공개키 암호 및 난수 생성시 내부 연산	SHA 256	-	ISO/IEC 10118-3(2004)

데이터베이스를 암호화하기 위해 사용된 키는 시스템 설치시 안전한 난수생성기를 통하여 생성한다. 해당 키는 시스템 설치 시 한 번만 생성되며, 키를 변경하기 위

해서는 전체 데이터를 복호화한 후, 변경된 키로 다시 암호화하는 과정이 필요하다. 데이터베이스를 암호화하기 위하여 데이터베이스에 데이터를 기록하는 시스템에서는 해당 키를 알고 있어야 하므로, 키의 저장이 불가피하다. 표 3에서는 본 논문에 적용한 웹 서버 암호화 알고리즘을 나타낸다. 키를 안전하게 저장하기 위해서 그림5.에서 보여주는 바와 같이 해당 키는 서버의 공개키로 암호화하여 저장한다. 이후 키를 사용하기 위하여 복호화하는 과정이 필요하며, 해당 키는 서버의 개인키로 복호화할 수 있다. 이 때 관리자의 비밀번호 입력 과정이 필요한데, 보안을 위해서 관리자의 개입은 반드시 필요하다.

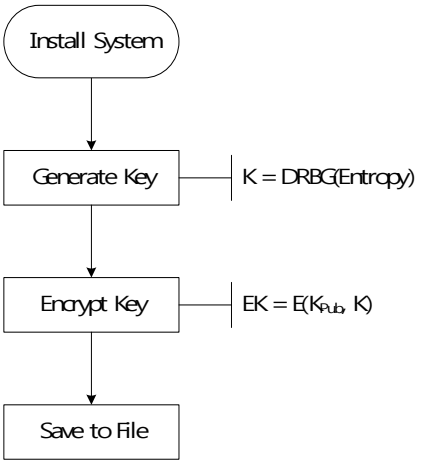


그림 5. 공개키 생성 및 암호화 저장
Fig. 5. Public key generation and Encrypted Storage

복호화된 키는 필요시 사용할 수 있도록 마스터키로 암호화하여 공유 메모리에 로딩된다. 데이터베이스에 접근하여 데이터를 기록, 조회할 때, 데이터베이스를 암호화하는 시스템(웹 서버)에서 해당 공유 메모리에 접근하여 키를 획득하여 사용할 수 있다. 그림 6은 암호화 키 메모리 적재 방법을 나타낸다.

기밀성을 훼손하는 각종 알려진 공격들에 대하여 효과적으로 방어할 수 있는 시스템이지만, 향후 실제 서비스를 제공하기 위해서는 접근제어, 헬스케어 센서장비에 대한 부채널 공격 방어, HSM 도입 등을 통한 Key Management System 구축 등 다양한 분야에 대한 대비 및 연구가 필요하다.

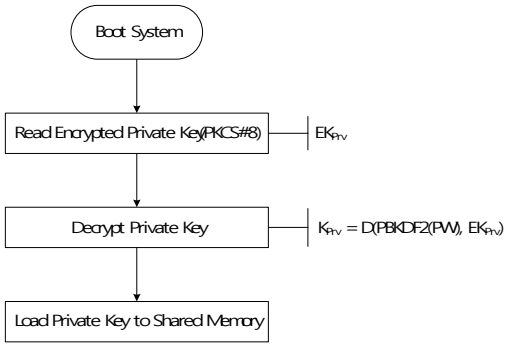


그림 6. 암호화 키 메모리 적재 방법
Fig. 6. Method of loading an encryption key memory

본 논문은 이상의 과정을 통하여 각 시스템을 구성하는 요소들, 또는 요소들 간의 통신 구간에 대하여 안전한 저장 및 송수신 체계를 구축하였다.

Ⅳ. 결 론

본 논문에서는 원격의료를 시행 할 경우에 원격지에서 환자의 맥진데이터 및 설진데이터를 암호를 이용해서 환자 생체데이터를 안전하게 전송하는 모의실험을 하면서, 이의 구간별 암호화 방안은 물론, 생체 데이터의 암호화 방안과 그 구현 방안에 대해 기술하였다. 원격진료를 허용 할 때에 환자의 생체 데이터 및 영상데이터 음성데이터가 위조 및 변조되는 우려성 때문에, 원격진료가 원격 의료진료 제도와 함께 어려움이 있다. 본 논문에서는 이러한 문제점을 해결하기위해서 ,위조 및 변조를 방지할 수 있는 알고리즘을 제안하였다.

특히, 본 논문에서는, ① 스마트폰과 헬쓰케어 단말기간의 데이터 전송구간, ② 스마트폰에서의 데이터 저장시, ③ 스마트폰과 웹 서버 사이의 전송구간, ④서버에서의 데이터 저장시 보안 암호화 방안에 대해 기술하였다. 또한, WEB 기반에서, 원격지에서, 환자 데이터가 병원으로 전송되는 동안에 맥진 및 설진, 혈압데이터 +심전도의 환자 진료 정보 (JPG, BMP)화일이 변조 및 해킹을 방지하기 위한 암호화 SW 과정을 모의실험하면서, 아이디 및 비밀번호 등의 노출이나 개인정보 노출을 막기 위한 보안기능 강화와 안전한 생체데이터 암호화 및 복호화 방안을 제안하였다.

향후, 본 연구의 결과를 기반으로 보안이 적용된 원격

지에서 암호화를 이용한 디지털 병원 시스템 구축에 대한 안전한 보안 알고리즘과 보안 시스템 적용에 도움이 되리라 본다.

References

[1] 23 of the Privacy Act and the Personal Information Protection Act Article 18.
[2] http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/index.jspTopic=% 2Fcom.ibm.mq.csqzas.doc%2Fsy10660_.htm
[3] Guide to Bluetooth Security, NIST Special Publication 800-121, pp. 11-12
[4] Performance Comparison of the AES Submissions, Bruce Schneier et al. February 1, 1999, Proc. Second AES Candidate Conference, NIST, pp. 15-34 March 1999
[5] RFC 2898-PKCS # 5: Password-Based Cryptography Specification Version 2.0, pp. 32, Sept., 2000
[6] The technical personal information Administrative protection measures based on Article 5
[7] security server deployment guide, Information and Communication, 2007
[8] New Tricks for Defeating SSL in Practice, Marlinspike, M., February 2009
[9] A. Kandal, L. Li, and Z. Cao, "Fuzzy Inference and Its Application to Control Systems," Fuzzy Sets and Systems, Vol. 48, No. 1, pp. 99-111, 1992
[10] http://article.joinsmsn.com/news/article
[11] Kim, gwanghwan, "A study on medical records and standardized format", Korea Institute of Venture Technology Conference, Proceedings Proceedings Part 2, pp. 507-508, 2010
[12] Hong You - Sik, "Intelligent maekjingi implementation ", The journal of the Institute of Internet Broadcasting and Communication vol.13 no.2, pp. 245-254, 2013
[13] Hong You - Sik, "smart tongue diagnosis electronic chart system", The journal of the Institute of Internet Broadcasting and Communi-cation v.12 no.2, pp. 243-249, 2012
[14] Jaesoo Yang, "Implementation of Secured Smart-Learning System using Encryption Function ", The journal of the Institute of Internet Broadcasting and Communication v.13 no.5, pp.195 - 201, 2013
[15] National Intelligence IT Security Certification Center, www.standard.go.kr/
[16] National Internet Development Agency of Korea, http://seed.kisa.or

소개

재 수(정회원)

- 1988년 8월 ~ 1993년 1월 : 미 NJIT 박사
- 1981년 3월 ~1981년 12월 : MIC 사무관
- 1982년 1월 ~ 2006년 1월 : KT
- 2006년 3월 ~ 2011년 10월 : 광운대 교수
- 2007년 2월 ~ 2011년 10월 : 경기도 정보화특보
- 2011년 11월 ~ : 단국대학교 부교수

이 유 식(정회원)

- 2009년 9월 ~ : 펜타시큐리티시스템 ㈜ 신기술개발팀장
- 2012년 9월 ~ : 고려대학교 정보보호대학원 박사과정

홍 유 식(종신회원)

- 1991년 ~ 현재 : 상지대학교 컴퓨터정보공학부 교수
- 1989년 ~ 1990년 : 삼성전자 종합기술원연구원
- 2006년 ~ 2010년 : 대한전자공학회 컴퓨터 소사이티 회장