ISSN 2586-1816
Journal of Convergence for Information Technology
e-ISSN 2586-4440
Vol. 8. No. 3, pp. 63-69, 2018
DOI : https://doi.org/10.22156/CS4SMB.2018.8.3.063

클라우드 환경에서 헬스케어 데이터를 위한 효율적인 암호화 기법

조성남[1], 정윤수[2*], 오충식[3]
[1]한국과학기술정보연구원 학술정보공유센터
[2]목원대학교 정보통신융합공학부
[3]한국과학기술정보연구원 과학기술사이버안전센터

An Efficient cryptography for healthcare data in the cloud environment

Sung-Nam Cho[1], Yoon-Su Jeong[2*], ChungShick Oh[3]
[1]Korea Institute of Science and Technology Information
[2]Dept. of information Communication Convergence Engineering, Mokwon University
[3]Korea Institute of Science and Technology Information

요 약 최근 의료 서비스 분야는 사용자의 헬스케어 데이터를 효율적으로 관리하기 위해서 클라우드 서비스를 이용하고 있다. 그러나, 클라우드 환경에서 처리되는 사용자의 헬스케어 데이터의 안정성을 보장하는 연구는 미진한 상태이다. 본 논문에서는 클라우드 환경에서 헬스케어 데이터를 효율적으로 암호화하는 부분 랜덤 암호화 기법을 제안한다. 제안 기법은 병원 의료 서비스에 최적화하도록 사용자가 생성하는 랜덤키(p, q)를 2개 생성하여 공개키와 개인키 생성에 반영한다. 제안 기법에서 사용되는 랜덤 키는 데이터를 전체 암호화하지 않고 일부분만을 암호화하여 사용자의 헬스케어 데이터 처리 효율을 향상시켰다. 성능평가 결과, 제안 기법은 암호화 생성 비용을 평가한 결과 기존 기법에 비해 21.6% 낮추었고, 병원 내 사용자 헬스케어 데이터 처리 시간도 18.5% 향상된 결과를 얻었다.

주제어 : 클라우드, 헬스케어, 암호화, 인증, 키 생성

Abstract Recently, healthcare services are using cloud services to efficiently manage users' healthcare data. However, research to ensure the stability of the user's healthcare data processed in the cloud environment is insufficient. In this paper, we propose a partial random encryption scheme that efficiently encrypts healthcare data in a cloud environment. The proposed scheme generates two random keys (p, q) generated by the user to optimize for the hospital medical service and reflects them in public key and private key generation. The random key used in the proposed scheme improves the efficiency of user 's healthcare data processing by encrypting only part of the data without encrypting the whole data. As a result of the performance evaluation, the proposed method showed 21.6% lower than the existing method and 18.5% improved the user healthcare data processing time in the hospital.

Key Words : Cloud, Healthcare, Encryption, Authentication, Key Generation

1. 서론

최근 4차 산업 혁명이 대두되면서 클라우드 환경에서 처리되고 있는 데이터가 이기종 장치에 저장되어 서로 다른 네트워크 환경에서 손쉽게 사용할 수 있는 빅 데이터 서비스가 각광을 받고 있다[1,2]. 특히, 의료 서비스 분야에서는 의료 서비스의 질을 향상시키기 위해서 클라우드 서비스와 접목하는 연구가 활발해지고 있다[3]. 클라

*This research was supported by Korea Institute of Science and Technology Information(KISTI)
*Corresponding Author : Yoon-Su Jeong(bukmunro@mokwon.ac.kr)
Received May 15, 2018 Revised May 26, 2018
Accepted June 20, 2018 Published June 30, 2018

우드 기반의 의료 서비스는 의료 서비스의 인프라와 생체의료(biomedical) 시스템의 효율성을 개선하고자 많은 투자가 이루어지고 있다[4,5].

클라우드 환경에서 헬스케어와 관련된 최근 연구에서는 사용자 인증보다는 클라우드 환경에서 송·수신되는 수 많은 데이터들의 기밀성을 보장하는 연구에 초점을 두고 있으며, 사용자와 사용자 사이에 송·수신되는 헬스케어 데이터의 유출과 관련된 보안 문제가 발생 할 수 있다.

Phunchongharn 기법은 병원에 구축된 무선 LAN (WLAN, Wireless local area network) 환경을 기반으로 동작되는 E-헬스케어 애플리케이션 기법을 제안하였다[6,7]. 그러나, 이 기법은 무선 LAN 기술의 통신 거리 문제로 인하여 앰블러스와 같은 공간에서는 응급상황 대처가 원활하지 않는 문제점을 가지고 있다.

Shen 기법은 클라우드 환경에서 의료 센서와 인접한 무선 사용자와의 통신 채널을 통해 높은 수준의 전력으로 데이터를 전송하는 기법을 제안하였다[8]. 그러나, 이 기법은 높은 전력으로 데이터를 송·수신할 경우 의료 센서가 오·동작될 수 있는 문제점이 있다.

본 논문은 병원에서 처리되는 사용자의 헬스케어 데이터를 클라우드 환경에 적용하였을 때, 사용자의 헬스케어 데이터를 안전하게 보호하기 위한 부분 랜덤 암호화 기법을 제안한다. 제안 기법은 병원 의료서비스를 클라우드 환경에서 운영할 때 사용자의 의료 데이터를 제3자가 악의적으로 도용하지 못하도록 사용자가 생성한 2개의 랜덤키(p, q)를 공개키와 개인키에 반영함으로써 사용자의 데이터를 전체 암호화하지 않고 일부분만을 암호화할 수 있어 계산 비용을 기존 기법에 비해 많이 줄이고 있다. 제안 기법은 효율적인 암호화 기법을 보장하기 위해서 다음과 같은 3가지 목적을 가진다.

첫째, 병원에 설치된 무선 장치를 통해 사용자의 헬스케어 데이터를 제3자의 악의적인 도용없이 서버에 안전하게 전달함으로써 사용자의 의료 서비스를 안전하게 받을 수 있게 한다. 둘째, 사용자가 생성한 2개의 랜덤키는 공개키와 개인키에 각각 적용하여 공개키와 개인키로 인한 보안 공격을 예방할 수 있다. 셋째, 사용자의 헬스케어 데이터를 통해 의료 서비스 및 행정 처리의 절차를 최소화할 수 있다.

제안 기법은 사용자의 헬스케어 데이터를 실시간으로 통합 관리할 수 있도록 헬스케어 데이터를 부분 암호화하여 전달하기 때문에 변원내 의료 서비스 효율성을 향상시킬 수 있는 역할을 수행한다.

이 논문의 구성은 다음과 같다. 2장에서는 클라우드 의료 서비스 및 기존 연구에 대해서 알아본다. 3장에서는 부분 암호화 기법을 이용한 클라우드 헬스케어 데이터 암호 기법을 제안하고, 4장에서는 제안 기법과 기존 기법을 비교 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅은 Fig. 1처럼 언제, 어디서나 컴퓨팅 자원을 필요에 따라 차용하여 네트워크를 통해 다양한 방식으로 접근하는 서비스를 의미한다[9-11]. 클라우드 컴퓨팅에서의 보안 위협은 기존 컴퓨팅 환경과 달리 가상화 엔진 하이퍼바이저에 의한 보안 위협, 관리자에 의한 보안 위협, 네트워크 전송과정에서의 보안 위협 등이 있다[12].

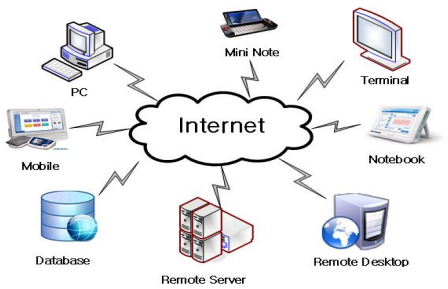


Fig. 1. Cloud Computing Environment

최근 클라우드 관련 연구에서는 특정 자원을 안전하게 공유하여 사용하는 방법들이 연구되고 있다[5]. 그러나 이 방법들은 특정 자원을 여러 사용자들이 빈번하게 사용할 경우 클라우드 환경의 전체 효율성에 많은 영향을 미칠 수 있는 문제점이 있다. 그 밖의 기법에서는 클라우드의 데이터 무결성을 보장하기 위해서 해쉬기반 대신 RSA 기반으로 ID 기반의 암호화 기법과 RSA 디지털 서명을 조합한 기법도 연구되고 있다[7]. 그러나, 이 기법은 데이터의 무결성을 보장하지만 사용자 정보를 저장하는 데이터 저장 공간이 높아지는 단점을 가지고 있다.

2.2 기존 연구

Z. A. Khattak et. al 기법은 공격자(adversary)가 사용자 신체에 부착된 장치에 접근시도를 할 경우 사용자가 지정한 연합 ID를 사용하여 안전하게 악의적인 공격을 예방하는 기법을 제안하였다[13]. 이 기법은 연합 ID 관리 시스템에 대한 보안 모델을 기반으로 클라이언트와 인식자 제공자 사이의 신뢰적 설립을 위한 상호 플랫폼을 사용하는 것이 특징이다.

H. Gao et. al 기법은 병원 시스템에서 사용하는 사용자의 인식자를 연합으로 생성하여 사용자의 인식자를 동적으로 관리하는 기법을 제안하였다[14]. 이 기법은 정적 정책 언어 대신 동적 신뢰 정책 언어를 사용하여 의료 시스템의 신뢰관계를 표현하는 정책을 사용하고 있다.

Y. Zhou et. al 기법은 의료 시스템에서 사용하는 서명키를 RSA와 소인수분해문제에 기반한 대리서명 기법을 제안하였다[15]. 이 기법은 직접 대리 서명키를 사용하여 위임장을 스스로 생성할 수 있는 것이 특징이다[15].

M. Mambo et. al 기법은 공개키 기반의 대리서명 기법을 제안하였다[16]. 이 기법은 대부분 RSA 전자서명 알고리즘을 사용하고 있어 이중의 서명 알고리즘이 가능한 장점이 있지만, 강한 위조 불가능성을 충족하지 못한다는 단점이 있다.

Yu et. al 기법은 소인수 분해 문제의 어려움에 기반 Rabin 기반 대리서명을 제안하였다[17]. 이 기법은 원 서명자가 대리서명자에게 위임장과 그에 대한 서명을 전송하면 대리서명자는 인증서의 유효성을 확인한다.

3. 클라우드 환경에서 처리되는 효율적인 헬스케어 데이터 암호 기법

이 절에서는 병원 내 설치된 무선 장치를 통해 사용자의 헬스케어 데이터를 서버에 안전하게 전달할 수 있는 암호화 기법을 제안한다.

3.1 개요

병원 환경에서 운영되고 있는 헬스케어 서비스는 무선 LAN (WLAN, Wireless local area network) 환경을 기반으로 대부분 동작되고 있다. 그러나, 휴대폰의 발달로 인하여 무선 LAN 이외에 다양한 무선 통신 기술이 사용되고 있다. Fig. 2는 제안기법의 전체 동작 과정을 보여주고 있다.

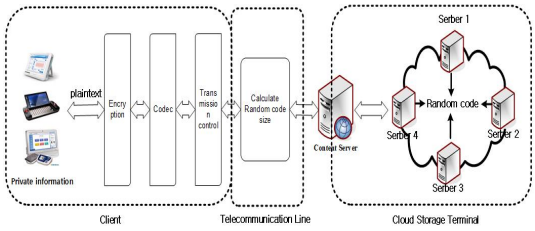


Fig. 2. Overall Process of Proposed Scheme

Fig. 2에서 제안 기법의 구성요소는 클라이언트, 통신라인, 클라우드 저장 터미널 등 3개 구성요소로 이루어져 있다. 각 구성요소에는 많은 모듈들이 구성되어 사용된다. 클라이언트는 대칭형 암호화 모듈, 임베디드 코딩 및 디코딩 모듈 및 네트워크 전송 제어 모듈로 구성되는 다양한 IT 터미널 제품을 포함하고 있다.

클라우드 스토리지 터미널은 클라우드 액세스 컨트롤러 및 클라우드 스토리지 리소스 메인 프레임이 포함된다. 통신 회선은 클라이언트와 클라우드 스토리지 터미널 간의 연결에 필요한 대칭 암호화 모듈이 사용된다. 대칭 암호화 모듈에 체크섬과 타임 스탬프가 사용된다. 네트워크 전송 제어 모듈은 클라이언트와 클라우드 스토리지 터미널 간의 인터페이스 한편으로는 올바른 데이터 업로드에 사용된다.

클라우드 액세스 컨트롤러은 완벽한 클라우드 스토리지 리소스 할당 및 저장소 정보 피드백. 사용자에 대한 청구 기능이 사용된다. 클라우드 스토리지 리소스는 사용자 정보를 저장하는 이동 통신사를 의미한다. 합법적인 사용자에게 특정 저장 공간을 할당하고 합법적 인 사용자에 대해 데이터 액세스 기능을 완료한다.

3.2 RSA 기반 암호 알고리즘 설계

이 절에서는 병원 내 사용자의 헬스케어 데이터를 안전하게 송・수신하기 위해 사용되는 전반적인 암호 알고리즘을 기술하고 있다. Fig. 3는 제안 기법에서 제안한 RSA 기반의 암호 알고리즘의 동작과정을 보여주고 있다. Fig. 3처럼 제안 기법에서 동작되는 RSA 기반의 헬스케어 데이터 암호 과정은 사용자의 헬스케어와 관련된 모든 데이터를 실시간으로 스트리밍이 가능하도록 사용자의 헬스케어 데이터를 전체 암호화하는 대신 사용자의

헬스케어 데이터를 일부 암호화하도록 처리함으로써 암호 처리과정의 효율성을 향상시켰다.

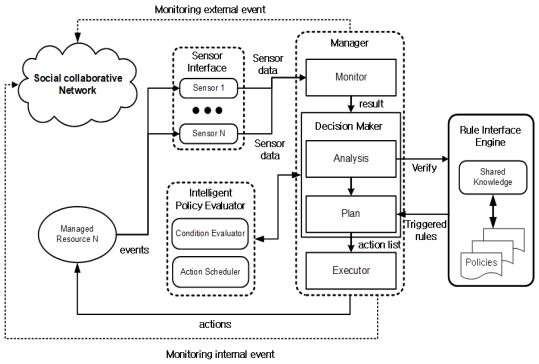


Fig. 3. RSA-based encryption Process of Proposed Scheme

Fig. 3에서 RSA 기반 암호 처리를 수행하기 위해서는 사용자의 헬스케어 데이터를 수집하기 위한 센서가 하나 이상 연결되어 있어야 하며, 각각의 센서로부터 수집된 헬스케어 데이터들은 실시간으로 서버에 스트리밍된다. 제안 기법에서 사용자의 헬스케어 데이터를 수집하는 센서와 사용자 간 통신은 이벤트 알림을 통한해 이벤트 트리거를 사용하기 때문에 가능하다.

3.3 헬스케어 데이터를 위한 키 생성 및 암/복호 알고리즘

이 과정은 제안 기법에서 암복호에 사용되는 공개키와 개인키를 사용자가 선택한 임의의 랜덤키를 이용하여 생성하는 키 생성 알고리즘을 기술하고 있다. 헬스케어 데이터를 사용자로부터 수집한 센서들은 서버에게 사용자의 헬스케어 데이터를 안전하게 암호화하여 전달해야 하는데, 이 때 헬스케어 데이터를 암호화하기 위한 키는 Table 1과 같은 RSA 기반의 키 생성 과정을 사용한다. 서버는 서버와 사용자가 임의로 선택한 비트 수열(0과 1로 구성된 수열)을 통해 N개의 가장 큰 소수 p, q를 생성한다. 여기서, p와 q는 p=2$q^{'}$+1와 q=2$p^{'}$+1을 만족하는 임의로 생성되는 큰 솟수를 의미한다. p와 q는 사용자의 개인키(p, q)와 공개키(n, e)를 생성하는데 사용된다.

Table 1. Key Generation Algorithm

Algorithm 1 Key Generation Algorithm

Input The Security parameter δ
Output Tuple (Sk, Pk) consisting of the secret key Sk and Public key Pk

1: **Procedure**: Key Generation
2: Generate $p(\cong (0,1)^{*}\rightarrow(0,1)^{N})$ and $q(\cong (0,1)^{*}\rightarrow(0,1)^{N})$
3: Select random prime numbers p(=2$q^{'}$+1) and q(=2$p^{'}$+1) and check that $p!=q$
3: Compute modulus $n = p \cdot q$
4: Compute phi, $\phi = (p-1)(q-1)$
5: Select public exponent e, $1 \le e \le \phi$ such that GCD(e, ϕ) = 1.
6: **end procedure**

데이터 암호 알고리즘은 Table 2처럼 공개키(n, e)를 이용하여 암호화 과정을 수행한다. 데이터를 0에서 (n-1) 사이의 정수로 나타낸다. 큰 데이터는 여러 블록으로 나눈 후 각 블록에 동일한 범위의 정수를 지정한다. 데이터는 $M^{e} \pmod n$를 통해 암호문 C가 생성이 된다. 암호문 메시지 C를 복호화하기 위해서는 암호화 키 (e, n)가 공개되어야 한다.

Table 2. Encryption Algorithm

Algorithm 1 Encryption Algorithm

Input a public key Pk and a plaintext P_i
Output Ciphertext C_i

1: **Procedure**: Encryption Process
2: Obtain the receipient's public key (n, e)
3: Represent the plaintext message as a positive integer m
4: Compute the ciphertext $c=M^{e} \pmod n$
5: **end procedure**

암호화 과정을 통해 서버로 전달되는 스트리밍 데이터는 해쉬 체인을 통해 사용자의 헬스케어 데이터의 보안 파라미터 ψ_1, ψ_2를 무작위로 선택하기 위해서 식 (1) ~ 식(3)의 과정을 수행한다.

$$\{h_i | d_i,\ i \in N\} \quad (1)$$

$$\psi_1 = g^{h_i} \quad (2)$$

$$\psi_2 = h_i \cdot g(\equiv p^{'} \cdot q^{'}) \quad (3)$$

서버는 생성된 해쉬체인 h_i, 보안 파라미터 ψ_1와 ψ_2, 사용자 인덱스 id를 XOR하여 SID를 생성한 후 데이터베이스에 저장한다. 제안 기법에서 데이터 복호 알고리즘은 Table 3처럼 복호화 키(d, n)를 이용하여 사용자에 의해 비공개로 유지된다. e, d 및 n에 적합한 값을 결정하기 위해서는 우선 두 개의 매우 큰 솟수 p와 q를 선택하여 n을 p・q와 동일하게 설정한다. GCD (d, ((p-1)・(q-1))) = 1과 같은 큰 정수 d를 선택한 후 $e \cdot d = 1 \pmod{((p-1)\cdot(q-1))}$가 되도록 e를 찾는다.

Table 3. Decryption Algorithm

Algorithm 1 Decryption Algorithm

Input a secret key Sk and a plaintext C_i
Output The corresponding plaintext P_i

1: **Procedure:** Decyption Process
2: Use his private key (n, d) to compute $m = c^d \pmod{n}$
3: Extact the plaintext from the integer representative m
4: **end procedure**

Table 3과 같은 복호화 과정에서는 사용자와 서버간 사용자 보안 정보가 정상적인 정보인지 검증하여 사용자가 정상적인 사용자일 경우 복호화가 정상적으로 수행한다. 서버는 데이터베이스에 저장되어 있는 사용자 정보 SI와 사용자가 생성한 SI'를 식 (4)처럼 비교함으로써 복호화 과정이 정상적인지를 확인한다. 만약 사용자 정보가 일치하지 않으면 사용자로부터 복호키를 다시 요청하여 복호화 과정을 다시 수행한다.

$$SI \cong SI' \bmod N \quad (4)$$

4. 평가

이 절은 NS-2.35 시뮬레이션을 사용하여 클라우드 환경에서 사용자의 헬스케어 데이터를 암호화하는 실험을 기존 기법들과 성능 분석을 수행하였다. 제안 기법의 실험환경은 Table 4와 같다.

Table 4. Simulation Environment

Topology	1000 × 1000
No of Nodes	50
Traffic flows	30 CBR flows
Packet Size	500 bytes
MAC	IEEE 802.11p MAC (12Mbps)
Propagation	Radio propagation
Sim.time	500s

Table 5는 제안 기법과 기존 기법과 처리량, 드롭율, 지연시간 등을 비교 평가하고 있다[6,7,8]. Table. 5의 분석 결과, 제안 기법은 사용자의 헬스케어 데이터를 부분 랜덤 암호화를 수행하기 위해서 사용자가 생성한 2개의 랜덤키(p, q)를 공개키와 개인키에 반영함으로써 사용자의 데이터를 전체 암호화하지 않고 일부분만을 암호화할 수 있어 기존 기법에 비해 성능 평가가 향상되었다. 이 같은 결과는 사용자의 헬스케어 데이터 암호화에 사용되는 추가적인 기능이 사용되지 않았기 때문에 나타난 결과이다.

Table 5. Simulation Evaluation

Protocol	Parameters		
	Throughput	Drop Rate	Delay(ms)
[6]	1025	55	101.45
[7]	1002	52	94.34
[8]	978	47	89.36
Proposed Scheme	935	42	83.75

Table 5처럼 제안 기법은 기존 기법에 비해 평균 9.6%의 처리량이 향상되었고, 지연시간은 21.1% 낮은 결과를 얻었다. 이 같은 결과는 제안 기법이 암・복호 과정에 사용되는 키를 사용자가 생성한 2개의 랜덤키(p, q)를 통해 공개/개인키를 생성하였으며, 또한 추가적인 암호 알고리즘을 사용하지 않았기 때문에 나타난 결과이다.

5. 결론

의료 서비스는 IT 기술이 발달하면서 병원내 진료 뿐만 아니라 원격의 환자 진료에도 많은 투자와 기술 연구

가 진행되오고 있다. 특히, 의료 서비스 분야에서는 클라우드 서비스와 관련된 인프라와 생체 의료 시스템을 개선하고자 많은 투자가 이루어지고 있다. 본 논문에서는 병원에서 처리되는 사용자의 헬스케어 데이터를 클라우드 환경에서 안전하게 보호하기 위한 부분 랜덤 암호화 기법을 제안하였다. 제안 기법은 사용자의 의료 데이터를 제3자에게 악용되지 않도록 사용자가 생성한 2개의 랜덤키(p, q)를 통해 공개키와 개인키를 생성하여 사용자의 데이터를 부분 암호화함으로써 사용자 데이터의 기밀성을 높이고 동시에 계산 비용은 낮추었다. 성능평가 결과, 제안 기법은 기존 기법에 비해 처리량, 드롭율, 지연시간 등이 향상되었다. 이 같은 결과는 제안 기법에서 사용자의 데이터를 암호화하는 키를 사용자가 생성한 2개의 랜덤키(p, q)를 사용하였기 때문에 암호 효율성을 향상시킨 결과이다. 향후 연구에서는 본 연구의 결과를 기반으로 클라우드 환경에서 사용되는 다양한 데이터 별 암호 효율을 향상시킬 수 있는 추가 연구를 수행할 계획이다.

REFERENCES

[1] R. H. Weber. (2010). Internet of Things: New Security and Privacy Challenges. *Computer Law & Security Review, 26(1)*, 23-30.
DOI : 10.1016/j.clsr.2009.11.008

[2] S. C. Choi, M. W. Ryu, M, Jin & J. H. Kim. (2014). Internet of Things platform and service trends. *Information and Communications Magazine(Information and Communication)*, *31(4),* 20-27.

[3] S. Haller, S. Karnouskos & C. Schroth. (2009). The Internet of Things in an Enterprise Context. *Future Internet-FIS 2008 Lecture Notes in Computer Science, 5468,* 14-28.
DOI : 10.1007/978-3-642-00985-3_2

[4] S. Raza, H. Shafagh, K. Hewage, R. Hummen & T. Voigt. (2013). Lithe: Lightweight Secure CoAP for the Internet of Things. *IEEE Sensors Journal*, *13(10),* 1-1.
DOI : 10.1109/jsen.2013.2277656

[5] Y. S. Jeong & S. H. Lee. (2012). U-Healthcare user's privacy protection protocol with Implantable medical Device of State Information. *Journal of the Korean Institue of Communicaitons and Information Sciences*, *37(4),* 277-353.
DOI : 10.7840/kics.2012.37c.4.297

[6] P. Phunchongharn, D. Niyato, E. Hossain & S. Camorlinga. (2009). An EMI-Aware Prioritized Wireless Access Scheme for e-Health Application in Hospital Environments. *IEEE transactions on information technology in biomedicine*, *14(5),* 1247-1258.
DOI : 10.1109/titb.2010.2047507

[7] P. Phunchongharn, E. Hossain & S. Camorlinga. (2011). Electromagnetic Interference-Aware Transmission Scheduling and Power Control for Dynamic Wireless Access in Hospital Environments. *IEEE Transactions on Information Technology in Biomedicine*, *15(6),* 890-899.
DOI : 10.1109/titb.2011.2164258

[8] Q. Shen, X. Liang, X. Shen, X. Lin & H. Y. Luo. (2004). Exploiting Geo-Distributed Clouds for a E-health Monitoring System With Minimum Service Delay and Privacy Preservation. *IEEE Journal of Biomedical and Health Informatics*, *18(2),* 430-439.
DOI : 10.1109/jbhi.2013.2292829

[9] X. Shen. (2012). Emerging technologies for e-healthcare. *IEEE Journals & Managines Network*, *26(5),* 2-3.

[10] H. B. Kim, Y. J. Jeon & S. J. Kim. (2011). Study on security management in cloud computing environment. *Kongju University KNU Management Consulting Institute, Management Consulting Review*, *2(1),* 127-144.

[11] H. S. Kim & C. S. Park. (2010). Cloud computing and personal authentication services. *Review of KIISC* , *20(2),* 11-19.

[12] K. H. Lee, H. S. Choi & Y. D. Chung. (2011). Massive Data Processing and Management in Cloud Computing: A Survey. *Journal of KIISE*, *38(2),* 104-125.

[13] Z. A. Khattak, S. Sulaiman & J. A. Manan. (2010). A study on threat model for federated identities in federated identity management system, *Proceedings of the 2010 International Symposium in Information Technology(ITSim)*, *2,* 618-623.
DOI : 10.1109/itsim.2010.5561611

[14] H. Gao, J. Yan & Y. Mu. (2010). Dynamic Trust Model for Federated Identity Management. *Proceedings of the 4th International Conference on Network and System Security(NSS)*, 55-61.
DOI : 10.1109/nss.2010.40

[15] Y. Zhou, Z. Cao & R. Lu. (2005). Provably secure proxy-protected signature schemes based on factoring. *Appl. Math. Comput.*, *164(1),* 83-98.
DOI : 10.1016/j.amc.2004.04.032

[16] M. Mambo, K. Usuda & E. Okamoto. (1996). Proxy signatures for delegating signing operation. *Proceedings*

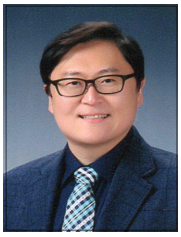
of the Third ACM Conference on Computer and Communications Security, 48-57.
DOI : 10.1145/238168.238185

[17] Y. Yu, Y. Mu, W. Susilo, Y. Sun & Y Ji. (2012). Provably secure proxy signature scheme from factorization. *Mathematical and Computer Modelling*, 1160-1168.

조 성 남(Cho, Sung-Nam) [정회원]

- 1992년 2월 : 전남대학교 전산통계학과(전산학사)
- 2004년 2월 : 고려대학교 소프트웨어공학과(전산학석사)
- 2017년 2월 : 광운대학교 경영정보학과(박사 수료)
- 1996년 ~ 현재 : 한국과학기술정보연구원 선임연구원
- 관심분야 : 정보화전략, 정보화투자성과, 정보기술아키텍처, IT거버넌스, 소프트웨어공학
- E-Mail : chosn@kisti.re.kr

정 윤 수(Jeong, Yoon Su) [정회원]



- 1998년 2월 : 대학교 전자계산학과 학사
- 2000년 2월 : 충북대학교 전자계산학과 석사
- 2008년 2월 : 충북대학교 전자계산학과 박사
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학[6,7,8]과 조교수
- 관심분야 : ICT 네트워크, 유·무선 통신, 정보보호, 헬스케어, 빅 데이터, 바이오인포매틱스
- E-Mail : bukmunro@mokwon.ac.kr

오 충 식(Oh, ChungShick) [정회원]

- 2004년 2월 : 충북대학교 전자계산학과(이학석사)
- 2013년 2월 : 충북대학교 컴퓨터공학과(공학박사)
- 1986년 ~ 현재 : 한국과학기술정보연구원 책임기술원
- 관심분야 : 정보보호, 개인정보보호, 유비쿼터스, 재난관리, 정보화
- E-Mail : ocs@kisti.re.kr