ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 3, pp. 79-84, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.3.079

클라우드 환경에서 관리자 역할을 강화한 사용자 프라이버시 보호 모델

정윤수, 연용호*
목원대학교 정보통신융합공학부

User privacy protection model through enhancing the administrator role in the cloud environment

Yoon-Su Jeong, Yong-Ho Yon*
Department of information Communication Convergence Engineering, Mokwon University

요 약 클라우드 서비스는 다양한 매체를 통해 손쉽게 사용할 수 있어 많은 사용자로부터 많은 각광을 받고 있다. 그러나, 클라우드 서비스를 사용하는 사용자의 프라이버시를 악용하는 다양한 보안 피해가 증가하고 있어 이를 예방할 수 있는 기술들이 부족한 상황이다. 본 논문에서는 클라우드 환경에서 사용자의 프라이버시를 제3자가 불법적으로 악용하지 않도록 사용자의 프라이버시를 안전하게 보호하기 위한 보호 모델을 제안한다. 제안 모델은 중간 관리자와 클라우드 서버의 역할을 강화하기 위해서 사용자의 서명을 랜덤하게 분할 관리하고 있다. 제안 모델에서 사용자의 프라이버시 정보는 보안함수와 사용자 서명을 통해 클라우드 서버가 사용자에게 제공하고 있기 때문에 제3자에게 불법적으로 유출되는 것을 막고 있다. 또한, 사용자의 프라이버시 보호에 곱셈군의 랜덤수와 일방행 해쉬 함수를 해쉬체인으로 묶음으로써 사용자의 서명을 안전하게 사용할 수 있다. 성능평가 결과, 제안 모델은 기존 모델보다 데이터의 처리시간이 평균 24.5% 향상된 결과를 얻었고, 사용자의 프라이버시 정보를 그룹 관리하기 때문에 기존 모델보다 효율성이 13.7% 향상되었다.

주제어 : 클라우드 서비스, 사용자 프라이버시, 보안, 해쉬체인, 키 관리, 속성

Abstract Cloud services are readily available through a variety of media, attracting a lot of attention from users. However, there are various security damages that abuse the privacy of users who use cloud services, so there is not enough technology to prevent them. In this paper, we propose a protection model to safeguard user 's privacy in a cloud environment so as not to illegally exploit user' s privacy. The proposed model randomly manages the user 's signature to strengthen the role of the middle manager and the cloud server. In the proposed model, the user's privacy information is provided illegally by the cloud server to the user through the security function and the user signature. Also, the signature of the user can be safely used by bundling the random number of the multiplication group and the one-way hash function into the hash chain to protect the user's privacy. As a result of the performance evaluation, the proposed model achieved an average improvement of data processing time of 24.5% compared to the existing model and the efficiency of the proposed model was improved by 13.7% than the existing model because the user 's privacy information was group managed.

Key Words : Cloud Service, User Privacy, Security, Hash Chain, Key Management, Property

1. 서론

클라우드 컴퓨팅은 컴퓨터에 보관되어 있던 데이터를 인터넷 상에 존재하는 저장 공간에 보관함으로써 사용자가 필요할 때마다 각종 단말 장치를 이용하여 데이터를 불러올 수 있는 기술이다[1]. 이 기술은 최근 클라우드 기술 중에 매우 각광을 받고 있는 서비스 중에 하나로 꼽을 수 있다. 과거에는 클라우드 환경에 접속할 수 있는 달말

*Corresponding Author : Yong-Ho Yon(yhyon@mokwon.ac.kr)
Received May 14, 2018 Revised June 4, 2018
Accepted June 20, 2018 Published June 30, 2018

기가 컴퓨터밖에 없었지만 최근에는 스마트폰이나 태블릿 컴퓨터, 그리고 IPTV와 같이 인터넷에 접속해서 사용하는 장치들이 늘어나고 있다[2-4]. 클라우드 서비스를 제공하는 업체 또한 최근 클라우드 서비스 붐에 발맞추어 기하급수적으로 늘어나고 있다.

최근에는 클라우드 서비스를 통해 제공되는 데이터의 보호 및 사용자의 프라이버시를 보장하기 위한 암호문 액세스 정책이나 속성 집합과 연동된 암호문 액세스 정책을 많이 사용하고 있다[5]. 대부분의 클라우드 환경에서는 기업 차원에서 사용자의 데이터 및 프라이버시 정보를 보호하고 있지만 정부 차원에서 클라우드 서비스 관련 보호 정책이 필요하다[6].

본 논문에서는 다양한 장치를 통해서 클라우드 환경에 저장되어 있는 데이터를 자유롭게 서비스 받으려고 할 때 사용자의 프라이버시 정보를 제3자가 악의적으로 사용하려고 하는 것을 예방하기 위한 클라우드 보호 모델을 제안한다. 제안 모델의 목적은 클라우드 환경을 구성하고 있는 구성요소 중 게이트웨이 역할을 수행하는 중간 관리자의 역할을 강화하는 동시에 사용자의 서명을 랜덤하게 분할 관리하도록 서버의 역할을 강화하는데 있다. 이렇게 함으로써 제안 모델을 사용하는 사용자의 프라이버시 보호를 안정적으로 제공할 수 있다. 제안 모델에서는 사용자의 프라이버시 정보를 보안함수와 사용자 서명을 함께 제공함으로써 제3자에게 사용자의 프라이버시 정보를 유출시키지 않도록 하고 있다. 또한, 중간 관리자는 사용자의 서명을 랜덤하게 분할하여 사용자 프라이버시 보호에 사용할 수 있도록 곱셈군의 랜덤수와 일방행 해쉬 함수를 해쉬체인으로 안전하게 묶어 생성한다.

이 논문의 구성은 다음과 같다. 2장에서는 클라우드 서비스와 기존 연구에 대해서 알아본다. 3장에서는 클라우드 환경에 적합한 사용자 프라이버시 보호 모델을 제안하고, 4장에서는 제안 방법을 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

클라우드는 컴퓨팅 자원의 실체에 관계없이 사용자가 필요한 만큼 가져다 사용하고 사용한 만큼 비용을 지불하는 네트워크 서비스를 의미한다[1,3]. 클라우드 서비스는 지역적으로 모든 곳에 서비스를 제공할 수 있는 것은 아니지만 사용자가 요청을 할 경우 또는 클라우드 서비스를 제공하는 회사가 서비스할 수 없는 지역으로부터 요청을 받았을 경우에 다른 클라우드의 인프라에서 필요한 자원을 가져다 서비스를 할 수 있다. 클라우드의 전체적인 개념을 정의하면 Fig.. 1과 같다.

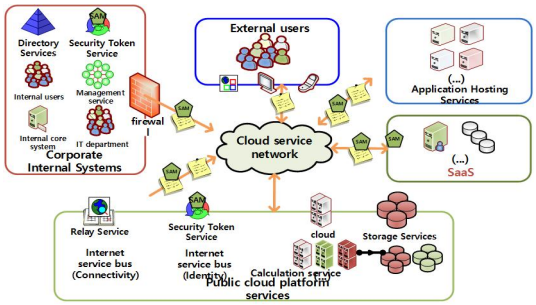


Fig. 1. Cloud computing environment

현재까지 연구되고 분석된 클라우드 서비스는 매우 다양하며 실제 운영 중인 클라우드 플랫폼도 매우 큰 규모로 운영되고 있다. 클라우드 서비스와 관련된 최근 연구 결과를 분석하면 다음과 같다[7-11].

S. Naaraj et al. 기법은 클라우드 네트워크 환경에서 송・수신되는 데이터를 암호화하는 프로세스를 개발하였다[7]. 이 기법은 일반 데이터 뿐만 아니라 보안이 설정되지 않은 채널을 통해 멀티미디어 데이터를 암호화하여 전송할 수 있도록 보안 기능을 향상시킨 것이 특징이다.

A. K. Dubey et al. 기법은 사용자와 클라우드 서버간 데이터를 암・복호할 때 RSA 기법을 사용한 양방향 클라우드 아키텍처를 제안하였다[8]. 그러나, 이 기법에서 클라우드 관리자는 사용자로부터 전달받은 키를 데이터가 업데이터할 때마다 갱신되어야 하는 문제점을 가지고 있다.

V. S. Mahalle et al.기법은 클라우드 사용자의 데이터를 안전하게 보호하기 위해서 RSA와 AES를 함께 사용한 하이브리드 접근방법을 제안하였다[9]. 그러나, 이 기법은 데이터를 보호할 때마다 반드시 공개키, 개인키, 비밀키 등 3개의 키를 사용해야 하기 때문에 대칭과 비대칭 알고리즘을 반드시 조합하여 사용해야 하는 문제점을 가지고 있다. 또한 RSA와 AES 암호 방법을 조합할 경우 사용자와 클라우드 데이터 간의 정보 전송 시간이 증가하는 문제점이 있다.

G. L. Prakash et al. 기법은 256 비트 대칭 키를 클라우드 환경에서 사용하는 암호화 기법을 제안하였다[10]. 이 기법은 클라우드 서버와 사용자가 공유한 비밀키를

이용하여 데이터를 재구성하기 때문에 민감한 데이터를 아웃소싱되는 것을 예방할 수 있는 특징이 있다.

S. Verma et al. 기법은 암호화와 암호 해독 측면의 균형을 유지하기 위한 RSA를 변형한 암호 기법을 제안하였다[11]. 이 기법은 클라우드 환경에서 사용되는 모든 데이터를 RSA 임베디드 프로토콜이 실행되는 환경에서 동작되도록 오프라인 생성기, 온라인 프록시 생성기 등을 사용한 것이 특징이다.

3. 사용자 프라이버시 보호를 위한 클라우드 보호 모델

이 절에서는 클라우드 환경에서 사용자의 프라이버시 정보를 악의적으로 사용하려고 하는 제3자로부터 사용자의 프라이버시 정보를 사전에 예방하기 위한 클라우드 보호 모델을 제안한다.

3.1 개요

최근 운영 중인 클라우드 서비스는 애플의 아이클라우드(iCloud), 아마존의 클라우드 인프라 등과 같은 글로벌 IT 업체에서 개인 사용자 중심으로 서비스가 바뀌고 있다[12-15]. 그러나, 보안 및 개인정보 보호를 위한 대책 등이 미비하기 때문에 안전한 퍼스널 클라우드 제공을 위한 준비가 많이 필요하다.

본 논문에서는 클라우드 환경에서 사용자의 프라이버시를 안전하게 보호하기 위한 보호 모델을 제안한다. 제안 모델은 Fig. 2와 같은 처리 과정을 통해 사용자의 개인 정보를 안전하게 처리하도록 정의하고 있다. Fig. 2처럼 제안 기법에서는 클라우드 서버에 등록하거나 저장되어 있는 사용자의 개인 정보를 암호화할 때 익명의 키를 생성한다.

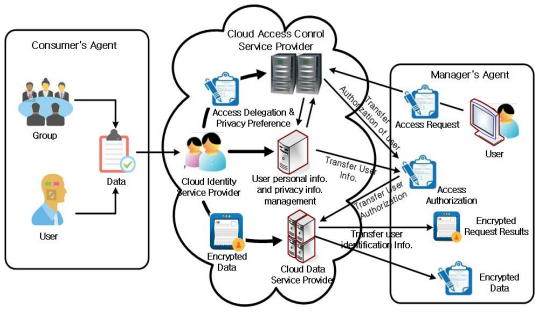


Fig. 2. Overall Process of Proposed Scheme

Fig. 2처럼 제안 모델은 클라우드 환경의 보안문제를 해결하고, 클라우드 컴퓨팅 활성화 및 산업발전을 위해서 클라우드 환경에서 수집 또는 생성되는 개인 정보를 보호할 수 있다. 제안 모델에서는 적절한 사용자 접근을 유지함으로써 사용자의 개인 정보에 대한 무결성을 보장한다. 제안 모델에서는 클라우드 서버가 클라우드 서비스를 사용하는 모든 사용자들을 신뢰적인 관계로 인식하여 처리한다고 가정한다. 제안 모델은 정보주체와 서비스 제공자 간에 사전 합의된 프라이버시 정책에 따라 개인정보의 안전한 처리를 통제하도록 사용자를 지원한다.

3.2 시스템 모델

제안 모델을 구성하는 시스템 구성요소는 Fig. 3처럼 사용자, 클라우드 서비스 제공자, 중간 관리자 등으로 구성된다.

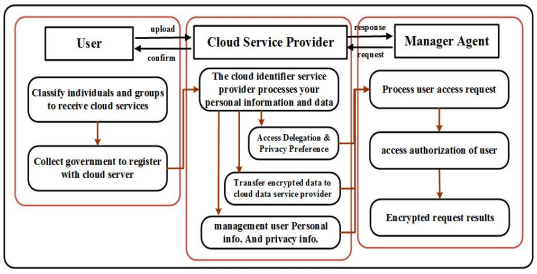


Fig. 3. System Model of Proposed Scheme

● 사용자

클라우드 서비스에서 처리되는 데이터를 수집 및 검색을 요청한다. 사용자는 클라우드 환경에서 처리되는 수 많은 데이터를 생성하는 역할을 수행한다.

● 중간 관리자

클라우드 서버에서 처리되는 데이터의 신뢰성을 보장 및 감시하는 역할을 담당한다. 사용자가 클라우드 서비스를 요청할 때 사용자의 신뢰 유·무를 감사하는 역할을 수행한다.

● 클라우드 서비스 제공자

클라우드 서버에 저장되어 있는 데이터를 사용자에게 제공하는 주체로써 클라우드 시스템을 운영 및 관리하는 역할을 담당한다. 클라우드 서비스 제공자는 사용자의 데이터를 저장 및 업데이트 할 수 있다.

3.3 사용자 프라이버시 접근 제어 과정

제안 모델은 사용자의 프라이버시를 보호하기 위해서 서비스 제공자의 권한 속성 정보를 바탕으로 사용자들에게 클라우드 서비스를 제공한다. 사용자는 클라우드 서비스를 제공받기 전에 데이터에 할당된 속성값에 따라 비밀정보를 할당받고 사용자의 프라이버시 정보를 등록한다. 이 때, 서버는 네트워크에 위치한 사용자와 가장 가까운 곳에 위치하여야 한다고 가정한다. 클라우드 서버는 중간 관리자의 속성과 타임스탬프 T에 따라 중간 관리자가 사용자의 프라이버시에 접근하는 것을 제어한다.

- 단계 1 : 사용자는 클라우드 서버에 자신의 아이디 ID_U와 패스워드 PW_U를 전달한 후 서버가 생성한 일회성 비밀키를 중간 관리자에게 전달한다.
- 단계 2: 클라우드 서버는 사용자가 소속된 클라우드 환경을 관리하는 중간 관리자의 속성정보를 추출한다. 이때, 중간 관리자의 속성정보가 $P_i = \{P_1, P_2, \cdots, P_n\}$이라고 가정하고, 중간 관리자의 모든 정보 중 일부 권한 속성 $\{P_1, P_2, \cdots, P_n\} \subseteq P_i$ $(i \leq n)$ 만이 클라우드 서비스를 제공받는 사용자의 프라이버시 접근 과정에 사용된다. 여기서 i는 중간 관리자의 권한 속성 수를 의미하고, n은 중간 관리자가 보유한 권한 속성의 전체 수를 의미한다.
- 단계 3 : 중간 관리자는 사용자의 아이디 ID_U와 패스워드 PW_U 그리고 중간 관리자의 속성 정보 P_i를 이용하여 사용자의 프라이버시를 보호하기 위한 사용자 프라이버시 인식 정보 UPI_U 를 생성한다.

$$UPI_U = h(,ID_U,\ PW_U\ ) \parallel h(SI_U,\ P_i) \qquad (1)$$

- 단계 4 : 중간 관리자는 클라우드 서버에게 사용자의 프라이버시 인식 정보 UPI_U 를 사용자의 아이디 ID_U와 매칭될 수 있도록 데이터베이스에 저장한다. 클라우드 서버는 사용자의 프라이버시 인식 정보 UPI_U가 정상인지를 파악한 후 사용자에게 프라이버시 인식 정보 UPI_U를 중간 관리자에게 전달한다. 이 같이 처리하는 이유는 서버가 중간 관리자의 속성 정보에 따라 사용자를 특정 클라우드 영역에 할당하고 중간 관리자에게 부여된 정책과 속성정보를 이용하여 사용자의 프라이버시에 불법적으로 접근하는 악의적인 공격자를 판별하기 위해서이다.

3.4 사용자 인증 과정

이 절에서는 사용자의 프라이버시 인식 정보 UPI_U 를 이용하여 사용자가 정상적인 사용자인지를 판별하는 과정을 수행한다.

- 단계 1 : 사용자는 중간 관리자에게 사용자의 프라이버시 인식 정보 UPI_U 와 사용자의 아이디 ID_U 를 전달한다.

$$Transfer \quad (UPI_U\ ,\ ID_U) \qquad (2)$$

- 단계 2 : 중간 관리자는 사용자로부터 전달받은 정보 쌍 $(UPI_U\ ,\ ID_U)$을 확인 한 후 해쉬함수 $h()$ 에 적용하여 사용자 프라이버시 인식 정보 UPI_U 가 맞는지 체크한다.
- 단계 3 : 중간 관리자는 사용자가 정상적인 사용자로 확인이 되면, 사용자의 확인 정보 $(SI_U\ ,\ ID_U)$를 사용자의 개인키로 암호화하여 서버에게 전달하고 그렇지 않으면 종료한다.
- 단계 4 : 클라우드 서버는 중간 관리자에게 사용자의 확인 정보 $(SI_U\ ,\ ID_U)$를 전달받은 후 중간 관리자에게 권한 정보를 보내기 위해서 소수 $\delta(\delta \geq n+1)$를 선택한 후 Z_δ 에서 임의의 랜덤 수 $r_i(1 \leq i \leq n)$를 생성하여 중간 관리자에게 전달한다.
- 5단계 : 중간 관리자는 클라우드 서버가 생성한 랜덤 수 r_i를 사용자의 프라이버시 인식 정보 UPI_U로 암호화하여 전달한다.

4. 평가

이 절에서는 제안 모델과 기존 모델을 비교평가하기 위해서 데이터 처리시간과 효율성을 중심으로 평가한다.

4.1 데이터 처리시간

Fig. 4은 클라우드 환경에서 사용자가 요청한 데이터를 중간 관리자와 서버간 처리되는 데이터의 처리시간을 기존 모델과 비교 분석하였다. Fig. 4의 결과처럼, 제안 모델은 사용자의 프라이버시를 보호하기 위해서 데이터에 할당된 속성 값에 따라 비밀정보를 사용하여 사용자의 프라이버시 정보를 등록하기 때문에 기존 모델에 비해 데이터의 처리시간이 평균 24.5% 향상된 결과를 얻었

다. 이 같은 결과는 클라우드 서버가 중간 관리자의 속성에 따라 사용자의 프라이버시 접근을 제어할 수 있기 때문에 나타난 결과이다.

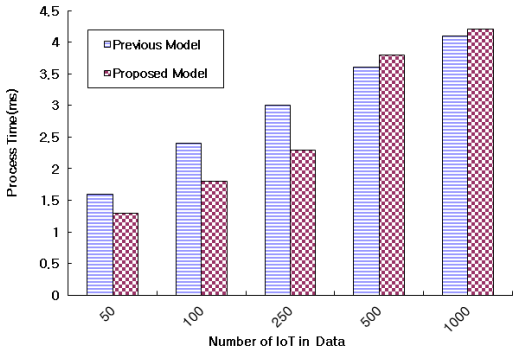


Fig. 4. Analysis of Data Process Time between previous model vs. proposed model

4.2 효율성

Fig. 5는 사용자의 클라우드 사용 목적에 따라 클라우드 서버에 존재하는 데이터가 처리될 때 발생되는 클라우드 서버의 효율성을 비교 분석하였다. Fig. 5의 실험 결과, 제안 모델은 기존 모델보다 효율성이 13.7% 향상되었다. 이 같은 결과는 사용자의 정보를 서버가 처리할 때 사용자의 프라이버시 정보를 그룹 관리할 수 있도록 속성 기반으로 데이터를 관리하기 때문이다. 또한, 제안 모델은 해쉬 체인으로 다중 서브넷 구조로 형성되는 사용자의 프라이버시 정보를 사용 목적에 따라 제어하기 때문에 기존 모델보다 효율성이 높게 나타났다.

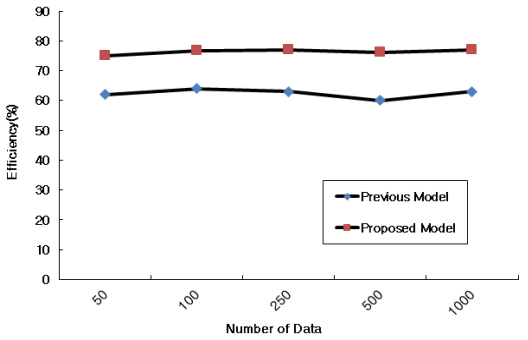


Fig. 5. Efficiency through number of Personal Privacy Information

5. 결론

최근 클라우드 서비스가 다양한 방법으로 사용자에게 제공됨에 따라 사용자의 프라이버시 보호와 관련된 연구가 필요하다. 본 논문에서는 클라우드 환경에서 사용자의 프라이버시를 보호하기 위한 사용자 프라이버시 보호 모델을 제안하였다. 제안 모델의 목적은 중간 관리자와 클라우드 서버의 역할을 강화함으로써 사용자의 프라이버시를 제3자가 불법적으로 악용하여 사용하지 못하도록 하는 것이다. 제안 모델은 사용자의 프라이버시 정보에 보안함수와 서명을 곱셈군의 랜덤수와 일방행 해쉬 함수를 사용해서 해쉬 체인으로 묶기 때문에 기존 모델보다 효과적이다. 성능평가 결과, 제안 모델은 기존 모델보다 데이터의 처리시간이 평균 24.5% 향상된 결과를 얻었고, 사용자의 프라이버시 정보를 그룹 관리하기 때문에 기존 모델보다 효율성이 13.7% 향상되었다. 향후 연구에서는 본 연구의 결과를 기반으로 실제 운영되고 있는 클라우드 서비스에 적용하여 성능 평가를 수행할 계획이다.

REFERENCES

[1] S. C. Lee & W. Y. Chung. (2014). A robust wearable u-healthcare platform in wireless sensor network. *Journal of Communications and Networks, 16, 4,* 465-474.
DOI : 10.1109/jcn.2014.000077

[2] T. W. Kim, K. H. Park, S. H. Yi & H. C. Kim. (2014). A Big Data Framework for u-Healthcare Systems Utilizing Vital Signs. *Proceedings of the 2014 International Symposium on Computer, Consumer and Control(IS3C)*, 494-497.
DOI : 10.1109/is3c.2014.135

[3] F. Touati, R. Tabish & A. Ben Mnaouer. (2014). Towards u-health: An indoor 6LoWPAN based platform for real-time healthcare monitoring. *Proceedings of the 2013 6th Joint IFIP Wireless and Mobile Networking Conference(WMNC)*, 1-4.
DOI : 10.1109/wmnc.2013.6548958

[4] Y. S. Lee, N. Bruce, T. Non, E. Alasaarela & H. Lee. (2015). Hybrid Cloud Service Based Healthcare Solutions. *Proceedings of the 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 25-30.

DOI : 10.1109/waina.2015.42

[5] H. Pan. J, J. H. Kim, K. Y. Chun & J. K. Ryu. (2013). Design of Portable Healthcare Gateway for Patient with Chronic Disease. *Proceedings of the 2013 International Conference on Information Science and Applications (ICISA)*, 1-2.
DOI : 10.1109/icisa.2013.6579337

[6] H. Hu, Y. Wen, T. S. Chua & X. Li. (2014). Toward Scalable Systems for Big Data Analytics: A Technology Tutorial. *IEEE Access*, 2, 652-687.
DOI : 10.1109/access.2014.2332453

[7] S. Nagaraj, Dr. G. S. V. P. Raju & V. Srinadth. (2015). Data Encryption and Authentication Using Public Key Approach. *Elsevier Procedia Computer Science*, 48, 126-132.
DOI : 10.1016/j.procs.2015.04.161

[8] 'A. K. Dubey, A. K. Dubey, M. Namdev & Shiv Shakti Shrivastava. (2016). Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. *IEEE*, 1-8.
DOI : 10.1109/CONSEG.2012.6349503.

[9] V. S. Mahalle & A. K. Shahade. (2016). Enhancing the data security in Cloud by implementing Hybrid (Rsa & Aes) Encryption Algorithm. IEEE, 146-149.
DOI : 10.1109/INPAC.2014.6981152.

[10] G. L. Prakash, Dr. M. Prateek & Dr. I. Singh. (2014). Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System. *International Journal Of Engineering And Computer Science*, 3, 4, 5216-5223.
DOI : 10.1109/icspct.2014.6884895

[11] S. Verma & D. Garg. (2015). Improvement in Rebalanced CRT RSA. *The International Arab Journal of Information Technology, 12, 6,* 524-531.

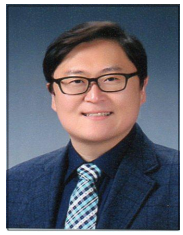
[12] Y. S. Jeong. (2012). RFID-based Authentication Protocol for Implantable Medical Device. *The Journal Of Digital Policy & Management, 10, 2,* 141-146.

[13] Y. S. Jeong & S. H. Lee. (2012). u-Healthcare Service Authentication Protocol based on RFID Technology. *The Journal Of Digital Policy & Management, 10, 2,* 153-160.

[14] Y. S. Jeong & S. H. Lee. (2012). U-Healthcare user's privacy protection protocol with Implantable medical Device of State Information. *The Journal of Korea Information and Communications Society(J-KICS), 37, 4,* 277-353.
DOI : 10.7840/kics.2012.37c.4.297

[15] D. G. Kim & I. G. Song. (2009). Need and Development of u-Healthcare Service. *Korean Society for Internet Information, 1, 3,* 9-17.

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 정보통신공학과 조교수
- 관심분야 : 유·무선 통신 보안, 정보보호, 헬스케어, 빅 데이터
- E-Mail : bukmunro@gmail.com

연 용 호(Yon, Yong Ho) [정회원]

- 1988년 2월 : 충북대학교 수학과 학사
- 1990년 2월 : 충북대학교 수학과 석사
- 1997년 8월 : 충북대학교 수학과 박사
- 2011년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 교수
- 관심분야 : 격자론, 격자암호, 양자논리
- E-Mail : yhyon@mokwon.ac.kr