Journal of the Korea Convergence Society
Vol. 10. No. 12, pp. 23-28, 2019

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2019.10.12.023

이질적인 클라우드 환경에 적합한 사용자 서명 보호 모델

정윤수[1], 김용태[2], 박길철[2*]
[1]목원대학교 정보통신융합공학부 교수, [2]한남대학교 멀티미디어학과 교수

User Signature Protection Model for Different Cloud Areas

Yoon-Su Jeong[1], Yong-Tae Kim[2], Gil-Cheol Park[2*]
[1]Professor, Department of information Communication Convergence Engineering, Mokwon University
[2]Professor, Department of multimedia, Hannam University

요 약 클라우드 서비스는 서로 다른 분야의 업무를 좀 더 다양한 사용자들에게 광범위하게 서비스하기 위해 개발된 서비스이다. 그러나, 클라우드 서비스는 서로 다른 사용자들의 요구 사항을 반영하도록 설계되었지만 그에 따른 다양한 보안 피해가 증가하고 있어 이를 해결하기 위한 기술들이 필요한 상황이다. 본 논문은 이질적인 클라우드 환경에서 제3자가 사용자의 서명을 악용하지 못하록 예방하는 사용자 서명 관리 모델을 제안한다. 제안 모델은 계층적 클라우드를 구성하는 중간 장치들의 기능을 강화하는 동시에 분할 사용되는 사용자의 서명 정보를 통합 관리한다. 성능평가 결과, 제안 모델은 사용자의 서명 관리를 분산 처리할 뿐만 아니라 중간 장치들이 사용자의 서명 처리를 분산 처리하기 때문에 효율성이 평균 8.5% 향상되었고, 사용자의 인증 처리를 수행할 때 사용자의 서명 지연 시간은 평균 13.3% 단축되었다. 사용자의 서명 처리를 중간 장치들이 처리할 때 발생하는 오버헤드는 기존 기법보다 평균 10.1% 낮았다.

주제어 : 클라우드, 보안, 사용자 서명, 인증, 암·복호

Abstract Cloud services are services developed to serve a wider variety of users in different fields. However, although cloud services are designed to reflect the needs of different users, a variety of security damages resulting from them are increasing and technologies are needed to address them. This paper proposes a user signature management model that prevents third parties from exploiting the user's signature in a heterogeneous cloud The proposed model strengthens the functionality of the intermediate devices that make up the hierarchical cloud while also managing the signature information of the partitioned user. As a result of the performance assessment, the proposed model not only distributed user signature management, but also improved efficiency by 8.5% on average because intermediate devices distributed user signature processing, and reduced the user's signature latency by 13.3% on average when performing user authentication processing. On average, the overhead generated by intermediate devices processing a user's signature was 10.1 percent lower than that of conventional techniques.

Key Words : Cloud, Security, User Signature, Authentication, Encryption·Decryption

*This paper has been supported by 2019 Hannam University Research Fund.
*Corresponding Author : Gil-Cheol Park(gcpark@hnu.kr)
Received October 1, 2019 Revised October 30, 2019
Accepted December 20, 2019 Published December 28, 2019

1. 서론

IT 기술이 발전하면서 클라우드 서비스의 중요성이 점점 증가하고 있다[1]. 클라우드 서비스는 서로 다른 분야의 업무들이 서로 광범위하게 제공받을 수 있는 하이브리드 클라우드 환경을 의미한다.

클라우드 서비스가 지역적으로 한 곳에서 모든 서비스를 제공받을 수 없기 때문에 특정 서비스는 지역적으로 분산 처리하여 서비스한다[2,3]. 그러나, 지역적으로 분산되어 있는 클라우드 서비스는 사용자의 서명을 중앙에서 직접 통합 관리할 수 있는 계층형 구조를 가진다. 그러나, 계층형 통합 관리 구조는 중앙에 저장되어 있는 사용자의 서명을 제3자가 악의적으로 사용하거나 침해당한다면 사용자의 피해가 증가할 수 있다. 최근 클라우드 서비스는 사용자의 서명을 지역적으로 분산 처리하는 분산 처리 구조로 운영하고 있다. 그러나, 지역적으로 분산 처리되는 사용자의 서명은 관리하기가 쉽지 않고 사용자의 부주의로 인하여 서명 분실과 같은 문제점이 발생할 수 있다.

최근 사용자 서명과 관련하여 다양한 연구를 진행되고 있다. 클라우드 환경에서 처리되는 데이터는 기밀성을 보장하기 위해서 RSA와 AES를 확장한 암호기법을 사용한다[4-6]. 클라우드에서 처리되는 사용자의 정보는 클라우드 환경의 범위에 따라 사용되는 키를 공개키와 개인키 이외에 비밀키를 포함하여 사용하기 때문에 사용자의 정보를 보호할 수 있다[7-9]. 그리고, 클라우드를 구성하는 게이트웨이 역할을 하는 중간장치의 보안을 향상시키기 위해서 RSA 기법을 변형한 암호 알고리즘을 임베디드 시스템에 적용한 연구도 있다[10-12].

본 논문은 이질적인 클라우드 환경에 적합한 사용자 서명 분할 관리 모델을 제안한다. 클라우드 범위와 상관없이 제안 모델은 사용자의 서명을 곱셈군 Z_n^*과 일방향 해쉬 함수만을 사용한 분할 처리한다. 이 같은 처리는 게이트웨이 역할을 수행하는 중간 장치의 효율성을 향상시키기 위해서이다. 제안 모델은 게이트웨이 역할을 수행하는 중간 장치가 사용자의 서명을 랜덤하게 분할 처리하도록 함으로써 사용자의 정보를 제3자에게 유출시키지 않는다. 또한, 제안 모델은 게인트웨이 역할을 수행하는 중간 장치가 사용자의 서명을 분산 처리하기 때문에 전체 클라우드 서비스의 처리 지연시간을 향상시킬 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 사용자 서명과 관련된 기존 연구에 대해서 알아본다. 3장에서는 이질적인 클라우드 환경에 적합한 사용자 서명 기법을 제안하고, 4장에서는 제안 기법을 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

S. Naaraj et al. 은 멀티미디어 데이터를 암호화하기 위한 클라우드 보안 기법을 제안하였다[4]. 그러나, 이 기법은 멀티미디어 데이터를 암호화할 때 사용자가 임의로 생성된 키를 사용하기 때문에 서버에서 키를 처리할 때 발생되는 오버헤드가 증가하는 문제점이 있다.

A. K. Dubey et al. 과 P. Yellapa 은 클라우드 환경에서 사용되는 키를 RSA 알고리즘을 사용하영 양방향 통신이 이루어지게 하는 아키텍처 기법을 제안하였다[5,6]. 그러나, 이 기법은 사용자가 생성한 키를 클라우드 환경에서 업데이트하도록 처리하기 때문에 제 3자의 중간자 공격이 가능한 문제점이 있다.

V. S. Mahalle et al. 은 사용자의 정보를 보호하기 위해서 RSA와 AES를 함께 사용하는 하이브리드 접근 방법을 제안하였다[7,8]. 그러나, 사용자의 정보를 보호하기 위해서 3개의 키(공개키, 개인키, 비밀키 등)를 사용하기 때문에 서버의 오버헤드가 증가 할 뿐만아니라 대칭과 비대칭 알고리즘을 조합할 때만 안전성을 보장하는 문제점이 존재한다.

N. Khanezaei 은 클라우드 서비스의 처리 시간을 줄이기 위한 RSA/AES 암호 기법을 제안하였다[9]. 이 기법은 사용자간 공유된 데이터에 한해서 RSA/AES 암호 방법을 조합하여 사용하기 때문에 정보 전송 시간을 줄이는 특징이 있다.

A. Priya et al. 은 클라우드에 저장되어 있는 사용자의 정보를 안전하게 처리할 수 있는 프레임워크를 제안하였다[10]. 이 프레임워크 기법은 기밀성을 중요시하기 때문에 프레임워크 내에서 처리하는 보안 프로세스를 중요시한다.

G. L. Prakash et al. 은 서버로부터 전달받은 공유키를 통해 데이터를 암호화하는 기법을 제안하였다[11]. 이 기법은 서버의 데이터를 재구성하기 위해서 256 비트의 대칭키를 사용하기 때문에 데이터의 아웃소싱을 예방할 수 있다.

S. Verma et al. 은 RSA 기법을 변형한 암호화 기법을 제안하였다[12]. 이 기법은 RSA 임베디드 프로토콜 환경에 적합하기때문에 온라인/오프라인의 프록시 생성기에서 사용된다.

3. 확률 기반의 IoT 사용자 프라이버시 보호 기법

이 절에서는 이질적인 클라우드 환경에서 사용자들에게 제공되고 있는 수 많은 서비스 중에서 사용자의 서명 정보를 효율적으로 처리할 수 있는 확률 기반의 IoT 사용자 서명 정보를 통합 관리하는 모델을 제안한다.

3.1 개요

최근 IT 기술이 발전하면서 IoT와 빅 데이터 등 최신 기술들이 서로 융합되면서 클라우드 서비스를 사용하는 사용자의 서명 정보들이 무분별하게 사용되고 있다. 그러나, 클라우드 서비스에 사용되는 사용자 서명 정보의 안전성은 아직까지 명확하게 보장되지 않고 있다.

본 논문에서는 클라우드 환경에서 이질적인 위치에 존재하는 클라우드 서비스를 사용할 때 서명 정보의 확률 정보를 확적으로 처리한 서명 통합 관리 모델을 제안하고 있다. 제안 모델은 사용자의 서명들을 곱셈군 Z_n^*과 일방향 해쉬 함수만을 사용하여 사용자의 서명 정보를 효율적으로 관리하는 것이 목적이다. 제안 모델은 게이트웨이 역할을 수행하는 중간 장치의 효율성을 향상시킬 뿐만 아니라 중간 장치에서 처리되는 정보 부하량을 줄일 수 있도록 사용자의 서명을 분할 처리하도록 하고 있다.

Fig. 1에서 클라우드 서비스 환경은 사용자의 정보가 제3자에게 유출되지 않도록 게이트웨이 역할을 수행하는 중간 장치의 역할을 위한 네트워크 구성을 보여주고 있다. 제안 모델은 곱셈군 Z_n^*과 일방향 해쉬 함수를 통해 처리된 사용자의 서명 정보를 다중 처리하게 함으로써 제3자에게 사용자의 서명 정보가 유출되지 않도록 하고 있다.

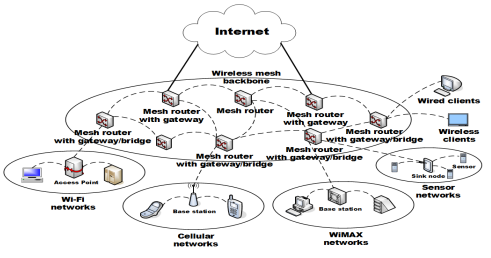

Fig. 1. Network Conponent in Proposed Model

3.2 동작 과정

Fig. 2에서 제안 모델은 클라우드 서비스 환경에서 사용자의 서명 정보를 생성하고 처리한 후 전달하기 위한 과정을 보여주고 있다.

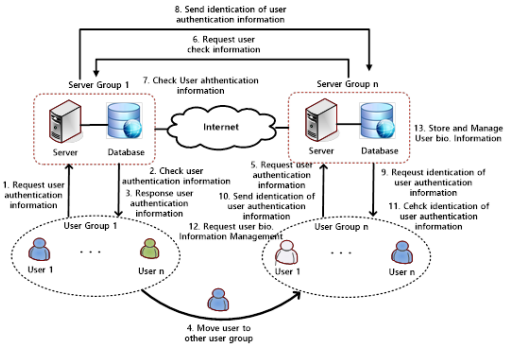

Fig. 2. Overall Operation Process of Proposed Model

Fig. 2는 서로 다른 이질적인 환경에 존재하는 사용자와 서비스 센터가 서로 통신을 통해 서비스를 송·수신받을 때 발생하는 사용자의 서명 정보를 효율적으로 보호하기 위해서 기존 일반 암호 기법 이외에 사용자의 서명 정보를 확률적으로 분할한 결과 값을 암호화한다. 기존 연구에서는 클라우드 서비스 관리자가 특정 사용자에게 요청할 경우에만 사용자의 서명 정보 값을 임의의 랜덤 값으로 생성하였지만 제안 모델에서는 클라우드 서비스를 구성하는 중간 장치의 속성 값과 비밀 값을 사용자의 서명값과 분할 처리하여 다중으로 서로 묶어 보안 정보(SI, Security Information) 값을 할당받기 때문에 비트 형태로 계층적으로 분산 배치된 사용자의 서명 정보들을 안전하게 처리할 수 있다. 또한, 클라우드 서비스 구성요소 중 중간 장치들의 역할 강화 및 부하를 낮출 수 있다.

3.3 사용자 서명정보의 속성 값 생성

제안 모델은 클라우드 환경에서 사용되고 있는 사용자의 서명 정보를 서로 연계하기 위해서 곱셈군 Z_n^*과 일방향 해쉬 함수를 통해 사용자 서명 정보의 속성 값을 생성한다. 제안 모델은 클라우드 서비스의 개수와 종류에 따라 사용자의 서명 정보의 무결성을 보장받기 위해서 속성 값을 사용한다. 사용자 서명 정보의 속성 값 생성과정은 다음과 같다.

· 1단계 : 사용자 서명 정보 생성

사용자의 서명 정보 생성과정은 사용자의 서명 정보 $\vec{s}$

를 식 (1)처럼 생성한다. 여기서, n은 사용자의 서명 정보 수를 의미한다.

$$\vec{S} = (s_1, s_2, \cdots, s_n) \quad (1)$$

식 (1)처럼 생성된 사용자의 서명 정보는 클라우드 서비스 환경을 구성하는 중간 장치에게 전달한다. 여기서, 공유키 sk는 사전에 안전한 경로를 통해 공유하였다고 가정하고 있다

· 2단계 : 사용자 서명 정보 연결

제안 모델은 사용자의 서명 정보를 S_U:{0, 1} → Z_N처럼 나타낸 후 사용자 서명 정보의 그룹 정보를 S_G: {0, 1}*× Z_N → Z_G와 같이 나타낸다. 제암 모델에서는 클라우드 서비스를 구성하는 중간 장치들이 서로 사용자의 서명정보를 인터리브하도록 해쉬 체인으로 묶는다. 게이트웨이 역할을 수행하는 중간 장치는 식 (2)처럼 서명 정보들의 연결값을 행렬로 나타내어 계층적 구조를 나타낸다.

$$US_x = \begin{Bmatrix} us_{00} \cdots us_{0j} \\ \vdots \quad \ddots \quad \vdots \\ us_{i0} \cdots us_{ij} \end{Bmatrix}, \ x=1,2,..,n \quad (2)$$

여기서, US_x는 게이트웨이 역할을 수행하는 중간 장치간 인터리브하도록 해쉬 체인한 값을 의미한다.

· 3 단계 : 서명 정보의 그룹 인덱스 정보 GI_i 생성

이 단계에서는 사용자로부터 전달된 사용자의 서명 정보를 묶어 그룹 인덱스 정보 GI_i로 생성한다. 그룹 인덱스 정보 GI_i는 식 (3) ~ 식 (4)와 같이 해쉬 정보 생성 후 그룹 인덱스 정보를 생성한다.

$$HI_i = H(US_i, \vec{S_i}), \ 1 \le i \le n \quad (3)$$

$$GI_i = H(HI_i) \in L, \ 1 \le i \le n \quad (4)$$

여기서, L은 사용자 서명 정보를 추출할 때 사용된 해쉬 길이를 의미한다.

· 4 단계 : 그룹 인덱스 정보 GI_i 등록

이 단계에서는 중간 장치가 사용자의 서명 정보를 그룹으로 인덱스한 정보 GI_i를 서버에 등록한다. 그룹 인덱스 정보 GI_i 등록 정보가 서버에 등록되고 나면 사용자의 서버가 관리하고 있는 클라우드 서비스를 안전하게 사용한다.

3.4 사용자의 서명 정보 계층화

클라우드 서비스를 사용자가 효율적으로 사용하기 위해서 사용자 서명 정보의 중요도에 따라 서비스를 계층화함으로써 서비스의 중요도를 추출할 수 있다. 제안 모델에서는 클라우드 서비스 간 사용자의 서명정보의 가중치 확률을 부여하여 클라우드 서비스의 중요도를 선택한다. 사용자의 서명 정보의 중요도에 대해서 최상위 계층에서 k번째 떨어진 하위 계층의 중요도은 식 (5)처럼 계산한다.

$$C[1,k] = \prod_{i=2}^{k} SI_k \quad (5)$$

여기서, $C[1,k]$는 사용자의 서명 정보가 위치한 k번째 클라우드 서비스의 위치 정보들을 계층화 한 가중치를 의미한다. SI_k는 k번째 사용자의 중요 서명정보의 수를 의미한다.

4. 평가

4.1 효율성

Fig. 3은 이질적인 클라우드 환경에 위치한 사용자의 서명정보 사용에 따른 게이트웨이 역할을 수행하는 중간 장치의 효율성을 평가한 결과이다. Fig. 3에서 사용자의 서명 정보에 대한 중간 장치의 효율성은 서명 정보를 분할 처리하지 않았을 때보다 평균 8.5% 높게 나타났다. 이 같은 결과는 사용자의 서명정보를 분할 처리함으로써 중간 장치의 부하를 낮추었기 때문에 중간 장치의 처리 시간이 단축 되었을 뿐만 아니라 사용자의 서명 정보의

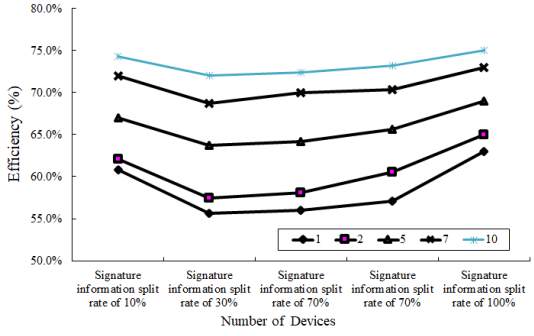

Fig. 3. Efficiency of intermediate devices for user signature information

처리시간 또한 단축되었기 때문이다. 또한, 제안 모델은 사용자 정보의 무결성을 보장받기 위해서 곱셈군 Z_n^*과 일방향 해쉬 함수를 통해 그룹 인덱스 정보 GI_i가 생성되기 때문에 사용자의 서명 정보를 분할하지 않았을 때보다 효율성이 높게 나타났다.

4.2 처리 지연시간

Fig. 4은 사용자의 서명 정보를 분할한 후 클라우드 서비스를 계층화할 수 있도록 사용자의 서명 정보의 중요도에 따른 사용자 서명 정보에 따른 중간장치의 처리 지연시간을 비교한 결과이다. 실험 결과, 사용자의 서명 정보의 중요도에 따른 중간 장치의 처리 지연시간은 기존 모델보다 평균 13.3% 향상된 결과를 얻었다. 이 같은 결과는 클라우드 서비스 간 사용자의 서명정보의 가중치 확률을 부여하여 클라우드 서비스의 중요도를 선택하여 사용하였기 때문에 나타난 결과이다. 또한, 사용자의 서명 정보를 중간 장치들이 서로 인터리브하도록 해쉬 체인으로 서로 묶어 사용하였기 때문에 나타난 결과이다.

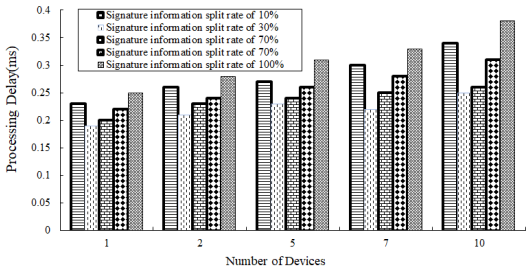

Fig. 4. Process delay of intermediate devices for user signature information

4.3 서비스 중요도에 따른 중간 장치의 오버헤드

Fig. 5는 클라우드 서비스 중요도에 따른 중간 장치의 오버헤드를 평가하고 있다. 그림 5의 결과처럼, 제안 모델은 서비스의 중요도에 따라 중간 장치의 오버헤드가 기존 모델보다 평균 10.1%로 낮게 나타났다. 이 같은 결과는 클라우드 서비스 간 사용자의 서명정보의 가중치 확률을 부여하여 클라우드 서비스의 중요도를 선택하였기 때문에 나타난 결과이다. 또한, 표 1의 결과를 기반으로 사용자의 서명 정보를 계층적으로 분산 배치할 경우 클라우드 서비스를 제공하는 중간 장치들의 역할 강화 및 부하를 낮추는 결과를 얻었다.

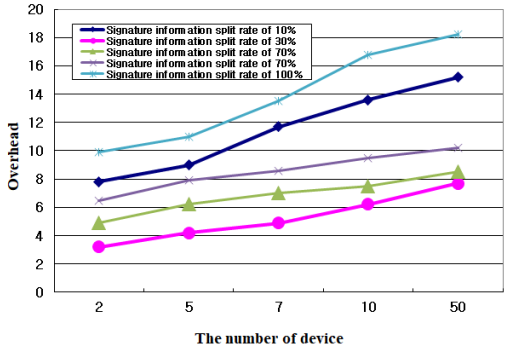

Fig. 5. Overhead of Intermediate Device

5. 결론

최근 클라우드 서비스는 서로 다른 분야의 업무들을 서로 광범위하게 서비스하고 있지만, 보안과 관련된 다양한 문제들이 여전이 존재하고 있다. 본 논문은 클라우드 환경에 적합한 사용자 서명 관리 모델을 제안하였다. 제안 모델은 사용자의 서명을 곱셈군 Z_n^*과 일방향 해쉬 함수만을 사용한 분할 처리하여 게이트웨이 역할을 수행하는 중간 장치의 효율성을 향상시켰다. 제안 모델은 사용자의 서명을 랜덤하게 분할 처리함으로써 사용자의 정보를 제3자에게 유출시키지 않는다. 제안 모델은 중간 장치의 역할을 강화하는 동시에 사용자의 서명을 분산 처리하기 때문에 전체 클라우드 서비스의 처리 지연시간을 낮출 수 있었다. 성능평가 결과, 제안 모델은 사용자의 서명 관리를 분산 처리할 뿐만아니라 중간 장치들이 사용자의 서명 처리를 분산 처리하기 때문에 효율성이 평균 8.5% 향상되었고, 사용자의 인증 처리를 수행할 때 사용자의 서명 지연 시간은 평균 13.3% 단축되었다. 사용자의 서명 처리를 중간 장치들이 처리할 때 발생하는 오버헤드는 기존 기법보다 평균 10.1% 낮았다. 향후 연구에서는 본 연구의 결과를 기반으로 클라우드 환경에서 IoT 사용자의 서명을 이용한 서비스 플랫폼에 적용할 계획이다.

REFERENCES

[1] H. Abwnawar & R. S. Janicke. (2017, July). Towards location-aware access control and data privacy in inter-cloud communications. *IEEE EUROCON 2017-17th International Conference on Smart Technologies* (pp. 739-744). Macedonia : IEEE

DOI : 10.1109/EUROCON.2017.8011209

[2] J. J. Yang, J. Q. Li & Y. Niu. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation Computer Systems. 43(44),* 74-86.
DOI : 10.1016/j.future.2014.06.004

[3] D. P. Gayathri. (2013). Overview of RSA and its enhancements. *International Journal of Innovative Research and Development, 2(11),* 306-310.

[4] 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

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

[6] P. Yellapa, C. Narasimham & V. Sreenivas. (2013). Data Security in Cloud using RSA. *IEEE.* p. 1-6.
DOI : 10.1109/ICCCNT.2013.6726471

[7] V. 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

[8] A. Kahate. (2010). *Cryptography and Network Security.* Tata McGraw Hill Education Private Ltd., New Delhi.

[9] N. Khanezaei & Z. M. Hanapi. (2016). A framework based on RSA and AES encryption algorithms for cloud computing services. *IEEE.* 58-62.
DOI : 10.1109/SPC.2014.7086230

[10] A. Priya, Y. K. Rana & B. P. Patel. (2015). Design and Implementation of an Algorithm to Enhance Cloud Security. *International Journal of Computer Applications. 113(12),* 41-46.
DOI : 10.5120/19882-1896

[11] 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

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

[13] Y. S. Jeong, Y. T. Kim & G. C. Park. (2017). A hierarchical property-based multi-level approach method for improves user access control in a cloud environment. *Journal of the Korea Convergence Society. 8(11),* 7-13.

[14] Y. S. Jeong & Y. H. Yon. (2018). User privacy protection model through enhancing the administrator role in the cloud environment. *Journal of Convergence for Information Technology. 8(3),* 79-84

[15] Y. S. Jeong. (2018). User Privacy Security Scheme using Double Replication Key in the Cloud Environment. *Journal of the Korea Convergence Society. 9(4),* 9-14.

정 윤 수(Yoon-Su Jeong) [정회원]

· 2000년 2월 : 충북대학교 전자계산학과 이학석사
· 2008년 2월 : 충북대학교 전자계산학과 이학박사
· 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
· 2012년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 조교수
· 관심분야 : 유무선 통신 보안, 정보보호, 빅 데이터, 헬스케어 서비스
· E-Mail : bukmunro@gmail.com

김 용 태(Yong-Tae Kim) [정회원]

· 1984년 2월 : 한남학교 계산통계 학과 학사
· 1988년 2월 : 숭실학교 자계산 학과 석사
· 2008년 2월 : 충북학교 자계산 학과 박사
· 2002년 12월 ~ 2006년 2월 : (주)가림정보기술 이사
· 2010년 10월 ~ 현재 : 한남학교 멀티미디어학부 교수
· 관심분야 : 모바일 웹서비스, 정보 보호, 센서 웹, 모바일 통신보안
· E-Mail : ky7762@hnu.kr

박 길 철(Gil-Cheol Park) [정회원]

· 1983년 2월 : 한남학교 계산통계 학과 학사
· 1986년 2월 : 숭실학교 자계산 학과 석사
· 1998년 2월 : 성균학교 자계 산학과 박사
·2006년 : UTAS, Australia 교환교수
· 1998년 8월 ~ 현재 : 한남학교 멀티미디어학부 교수
· 2005년 2월 : 한국정보기술학회 이사 멀티미디어 분과 원장
· 관심분야 : Multimedia And Mobile Communication, Network Security
· E-Mail : gcpark@hnu.kr