ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 2, pp. 77-82, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.2.077

다중 사용자를 위한 효율적인 클라우드 보안 기법

정윤수
목원대학교 정보통신융합공학부

An efficient cloud security scheme for multiple users

Yoon-Su Jeong
Department of information Communication Convergence Engineering, Mokwon University

요 약 최근 클라우드 서비스가 일반 사용자에게 대중화되면서 클라우드 환경에 사용되는 정보 중 사용자의 정보가 자유롭게 송・수신되기 때문에 사용자의 정보 노출과 관련된 보안 문제가 발생되고 있다. 본 논문에서는 클라우드 서비스를 사용하는 다중 사용자의 개인 정보를 사전에 예방할 수 있도록 클라우드 서버에 저장되어 있는 개인 정보와 공유 정보에 접근하는 키를 각각 만들어 다중 사용자의 개인 정보를 안전하게 보호하기 위한 기법을 제안한다. 제안 기법에서 사용되는 첫 번째 키는 사용자의 개인 정보에 접근하기 위한 키로써, 개인정보와 연관된 정보들을 다중 계층의 형태로 운영하기 위해 사용된다. 두 번째 키는 개인 정보 이외의 다른 사용자에게 오픈되는 정보들에 접근한는 키로써, 클라우드를 사용하는 다른 사용자와 연계하기 위해 필요한 키다. 제안 기법은 클라우드 환경에서 사용되는 수많은 종류의 정보들을 다중처리하기 위해서 다중 해쉬체인으로 개인 정보를 익명화하도록 구성한다. 성능평가 결과, 제안 기법은 다중 형태의 구조로 처리되는 다중 사용자의 개인 정보를 제3자가 안전하게 접근하여 처리할 수 있도록 동작하기 때문에 개인 정보 관리 비용이 13.4% 단축된 결과를 얻었다. 제안 기법의 효율성은 기존 기법보다 19.5% 향상되었다.

주제어 : 클라우드, 다중 사용자, 보안, 해쉬체인, 키 관리

Abstract Recently, as cloud services become popular with general users, users' information is freely transmitted and received among the information used in the cloud environment, so security problems related to user information disclosure are occurring. we propose a method to secure personal information of multiple users by making personal information stored in the cloud server and a key for accessing the shared information so that the privacy information of the multi users using the cloud service can be prevented in advance do. The first key used in the proposed scheme is a key for accessing the user 's personal information, and is used to operate the information related to the personal information in the form of a multi - layer. The second key is the key to accessing information that is open to other users than to personal information, and is necessary to associate with other users of the cloud. The proposed scheme is constructed to anonymize personal information with multiple hash chains to process multiple kinds of information used in the cloud environment. As a result of the performance evaluation, the proposed method works by allowing third parties to safely access and process the personal information of multiple users processed by the multi - type structure, resulting in a reduction of the personal information management cost by 13.4%. The efficiency of the proposed method is 19.5% higher than that of the existing method.

Key Words : Cloud, Multi User, Security, Hash Chain, Key Management

*Corresponding Author : Yoon-Su Jeong(bukmunro@mokwon.ac.kr)
Received February 20, 2018 Revised April 05, 2018
Accepted April 20, 2018 Published April 30, 2018

1. 서론

스마트폰과 같은 휴대용 장치가 대중화되면서 클라우드 서비스와 같은 인터넷 서비스의 인기가 증가하고 있는 추세이다[1-3]. 특히, 클라우드 서비스는 중요 데이터를 개인 컴퓨터에 저장하지 않고 클라우드 서버에 저장하기 때문에 위치에 상관없이 언제 어디서나 사용자가 손쉽게 자료를 서비스 받을 수 있다[4-7].

Tatebayashi et al. 기법은 디지털 모바일 통신 시스템에서 사용되는 키를 모바일 통신 시스템에 따라 여러 개로 분배하는 기 분배 기법을 제안하였다[8]. 이 기법은 데이터를 보호하기 위한 비밀키를 제3자가 불법으로 가로채는 것을 예방하는 장점을 가지고 있지만 통신 객체 중 하나의 객체자 타협되면 키가 노출되는 단점을 가지고 있다.

Eschenauer et al. 기법은 분산 센서 네트워크 환경에서 클라이언트 서버의 인터 네트워크 시스템보다 강한 인증을 사용하기 위해서 패스워드의 수와 속성을 통합하여 인증을 수행할 수 있는 키 관리 기법을 제안하였다. 이 기법은 기존 클라이언트-서버 방식의 인증보다 강한 인증을 제공하는 것이 특징이다[9].

Park et al. 기법은 모바일 네트워크 환경에서 인증을 수행하기 위한 키 분배 기법을 제안하였다[10]. 그러나, 이 기법은 데이터를 평문으로 전달하기 때문에 제3자로부터 쉽게 공격에 노출되는 문제점을 가지고 있어 실시간 클라우드 컴퓨팅 환경에는 부적합하다.

본 논문에서는 클라우드 환경에서 사용되고 있는 다양한 서비스를 사용자가 안전하게 사용하기 위해서 사용자의 개인 정보를 대내·외적으로 처리되어야 하는 키를 n개 생성하여 사용자의 개인정보를 안전하게 보호하기 위한 기법을 제안한다. 제안 기법은 클라우드 서버에 등록되거나 저장되어 있는 사용자의 개인정보를 내·외부에서 접근하영 사용할 수 있도록 분류한 후 개인 정보를 그룹으로 묶을 수 있도록 n개의 키를 사용한다. 내·외부 그룹으로 묶은 개인 그룹 정보는 역할과 상황에 따라 개인 정보를 보호할 수 있도록 키를 n개 생성하여 개인정보를 0과 1로의 16진수 값으로 최소 32비트에서 최대 256비트로 구성하도록 한다. 제안 기법은 클라우드 환경에서 사용되는 수많은 종류의 개인 정보들을 그룹별 다중처리하기 위해서 해쉬체인을 다중으로 생성하여 개인정보를 익명화하도록 구성한다. 제안 기법은 클라우드 환경에서 개인 정보를 대내·외적으로 사용 목적에 따라 분류하기 위한 익명 키 정보를 n개 키를 조합하여 생성하는 것이 가장 큰 특징 중에 하나이다.제안 기법은 클라우드 서비스를 사용하는 사용자의 개인 정보를 안전하게 수집·보관·관리·처리 하도록 함으로써 제3자가 불법적으로 개인 정보를 악용하지 않도록 한다. 제안 기법은 개인 정보를 보호하는 기존 기법과 비교해서 다음과 같은 특징을 가진다. 첫째, 제안 기법은 개인 정보가 클라우드 환경에서 처리되는 것을 손쉽게 추적 및 모니터링할 수 있다. 둘째, 개인 정보를 대·내외적으로 사용하도록 분류한 후 처리 목적에 따라 개인정보를 보호한다. 셋째. 개인 정보는 2개의 키를 조합하여 클라우드 환경에서 사용하는 익명 키로 보호할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 클라우드 서비스 및 보안에 대해서 설명한다. 3장에서는 다중 사용자를 위한 클라우드 환경의 개인 정보보호 기법을 제시하고, 4장에서는 제안 기법의 성능 평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 관련연구

클라우드 환경에서 제일 중요시하고 있는 부분은 보안이다[11-12]. 클라우드 환경에서는 보안과 관련해서 서비스 측면에서 많이 다루고 있다. 클라우드 컴퓨팅 보안은 크게 응용 레벨, 호스트 레벨, 네트워크 레벨에서 다루어지고 있다. 특히, 위에서 언급한 3개 레벨(응용 레벨, 호스트 레벨, 네트워크 레벨)에서는 Fig. 1과 같은 많은 종류의 위협이 존재한다.

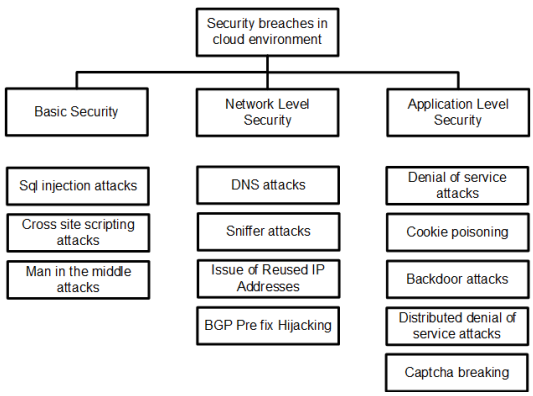

Fig. 1. Security breaches in cloud environment

현재까지 연구되고 분석된 보안 공격 중 클라우드 환경의 가상 및 클라우드 플랫폼과 관계된 보안 공격은 예방하기 매우 어려운 공격 방법으로 알려져 있다. 클라우드 서비스를 이용하는 기업은 가상 및 클라우드 플랫폼과 관계된 보안 공격을 통해 기업 내 중요 데이터를 노출시킬 수 있어 IT 관리자의 역할이 중요시되고 있다. 기업에서 사용하는 가상화 서버는 매우 큰 규모로 운영되고 있어 서비스되고 있는 가상화 서버가 문제가 있더라도 패칭 작업은 결코 쉬운 일이 아니다. 또한, 가상화 서버의 문제로 인하여 해커들이 가상화 서버의 정보를 탈취하거나 트래픽 공격을 통해 취약한 시스템의 정보를 훔칠 수 있는 여지를 제공할 수 도 있다.

3. 클라우드 서비스를 위한 다중 사용자 보안 기법

이 절에서는 클라우드 서버에 등록되거나 저장되어 있는 사용자의 개인정보를 내·외부에서 접근하여 사용할 수 있도록 분류한 후 개인 정보를 그룹으로 묶을 수 있도록 n개의 키를 사용한다. 내·외부 그룹으로 묶은 개인 그룹 정보는 개인 정보의 역할과 상황에 따라 개인 정보를 관리하거나 분류하기 위해서 n개의 키를 생성하여 개인 정보를 0과 1의 16진수 값으로 최소 32비트에서 최대 256비트로 구성한다.

3.1 개요

클라우드 환경에서는 단일 사용자 보다는 다중 사용자를 중심으로 서비스가 주로 운영된다. 개인 입장에서는 사용자 위주로 클라우드 서비스가 동작된다고 생각되지만 클라우드 서비스의 동작과정을 보면 클라우드 서버에 접속하여 서비스를 요구하는 다중 사용자의 정보를 관리하고 있다. 이때, 클라우드 서버가 다중 사용자를 관리 할 때 가장 중요하게 처리되어야 하는 부분 중 하나가 보안이다.

본 논문에서는 클라우드 환경에서 사용자의 정보를 안전하게 보호하기 위해서 Fig. 2와 같은 과정에서 n개의 키를 생성하여 사용자의 개인 정보를 대내·외적으로 처리하도록 정의하고 있다. Fig. 2처럼 제안 기법에서는 클라우드 서버에 등록하거나 저장되어 있는 사용자의 개인정보를 처리하기 위해서는 개인 정보를 서브넷으로 그룹화 한후 정보를 암호화할 때 n개 키를 이용하여 익명의 키를 생성한다.

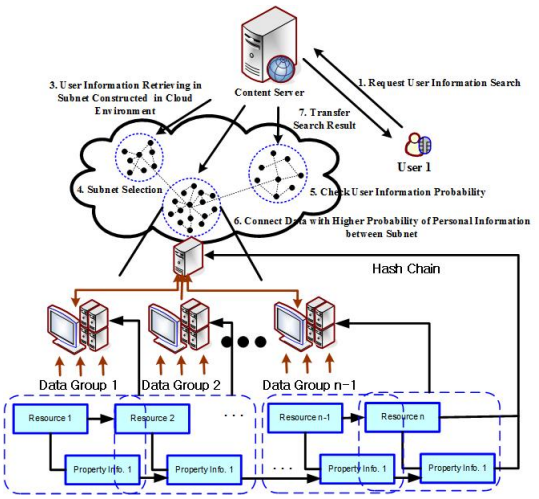

Fig. 2. Overall Process of Proposed Scheme

Fig. 2의처럼 제안 기법은 클라우드 환경에 존재하는 사용자의 모든 개인 정보를 직·간접 통신을 통해 접근이 가능하다. 또한, 네트워크간 서브넷을 구성하는 클러스터링 알고리즘은 안전한 통신 설정을 할 수 있도록 확장 가능하도록 설계하고 있다. 제안 기법에서는 클라우드 서버가 클라우드 서비스를 사용하는 모든 사용자들을 신뢰적인 관계로 인식한다고 가정한다.

3.2 익명 키 생성과정

이 절에서는 클라우드 서비스를 제공받는 사용자의 개인정보를 보호하기 위해서 2개의 키를 이용하여 대내·외적으로 사용하는 익명 키를 생성하는 과정을 다음과 같이 4가지 과정으로 구분하여 동작된다.

3.2.1 키 생성

제안 기법에서 익명 키 생성을 위해 필요한 키 n개를 생성하기 위해서는 우선 사전분배 방식을 통해 사용자와 클라우드 서버간 공유된 키와 서브넷 간 사용자 정보 인증을 위해 사용되는 키가 필요하다. 서브넷을 구성하는 정보 중 사용자 개인의 정보는 신뢰적이지만 적은수의 키만을 이용하지만 서브넷을 구성하는 사용자들은 많은 수의 키를 가지고 있지만 신뢰적이지는 못하다고 가정한다.

익명 키를 생성하기 위해 필요한 2개의 키는 클라우드

서비스를 필요로 하는 서로 다른 n개의 개인정보 데이터 셋을 모두 포함하는 $n-1$차 다항식이 식 (1)처럼 만들어진다. 식 (1)처럼 로 다른 n개의 개인정보 데이터 셋을 모두 포함하는 $n-1$차 다항식은 (x_1, y_1), (x_2, y_2), (x_3, y_3), ・・・, (x_n, y_n)을 xy편면상의 x좌표가 서로 다른 n개의 개인 정보 데이터 셋으로 나타낼 수 있다.

$$y = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \quad (1)$$

여기서 x_n는 데이터 셋의 수를 의미하고 y_n는 데이터 셋에 포함된 개인 정보의 키를 의미한다.

식 (1)에서 x_1, x_2, ・・・, x_n은 식 (2)처럼 서로 다른 n개의 데이터 셋으로 만들어진다.

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & & \cdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} \neq 0 \quad (2)$$

위 내용을 바탕으로 제안 기법에서는 클라우드 환경에서 개인 정보를 보호하기 위한 서브넷의 키를 생성하기 위해서는 $(x_j - x_i)$들의 곱 형태로 식 (3)처럼 나타낼 수 있다.

$$\det V_n = \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & & \cdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 < i \le j \le n} (x_j - x_i) \quad (3)$$

3.2.2 서브넷 생성

제안 기법에서 서브넷을 생성하기 위해서는 사용자의 개인정보가 대・내외적으로 사용하는 목적에 따라 사용자의 개인 정보를 계층적으로 서브넷을 생성한다. 서브넷을 구성하는 사용자가 식 (4)처럼 N명이라고 가정할 경우, 제안 기법에서 서브넷을 구성하기 위한 사용자의 개인 정보는 식 (5)처럼 $\hat{U} \subseteq U$와 같게 된다.

$$U = \{u_1, u_2, ..., u_N\}, \ i \in [1,N] \quad (4)$$

$$U_i = \{\hat{U} \subseteq U \mid i \in [1,N]\} \quad (5)$$

식 (5)를 통해 서브넷에 포함된 사용자의 정보 $I_i (i \in [1,N])$는 식 (6)처럼 개인 정보 i_i를 N개 샘플링하여 개인 정보 데이터셋(dataset) I_i를 만들기 위식 (7)처럼 데이터셋을 $I_i (i \in [1,N])$ 로 설정하며, 샘플링되는 데이터 셋는 $I_i \subseteq I$와 같다.

$$I = \{i_1, i_2, ..., i_N\}, \ i \in [1,N] \quad (6)$$

$$I_i = \{I_i \subseteq I \mid i \in [1,N]\} \quad (7)$$

3.2.3 개인 정보 송·수신

클라우드 서버는 서브넷으로 분류된 사용자의 개인 정보를 서로 연계하여 연계 확률이 가장 높은 개인 정보 $\vec{I}$에 대해서 속성 정보 p_i를 부여한다. 서브넷으로 구성된 개인 정보에 속성 정보가 부여되면 개인 정보의 종류, 기능, 특성에 따라 개인 정보의 속성 집합 $\bar{d}$를 식 (8)처럼 생성한다. 식 (8)에서 개인 정보의 연계 정보 CI_i는 개인 정보 $\vec{I}$와 개인 정보의 속성 집합 $\bar{d}$을 해쉬 함수 $H()$에 적용하여 생성한다.

$$CI_i = H(\vec{I}, \bar{d}), \quad 1 \le i \le n \quad (8)$$

4. 평가

제안 기법을 기존 기법과 비교평가하기 위해서 성능과 보안 측면에서 나누어 제안 기법을 평가한다.

4.1 성능평가

4.1.1 개인 정보 관리 비용

Fig. 3은 클라우드 환경에서 다중 사용자의 개인 정보를 효율적으로 관리하기 위한 비용을 기존 기법과 비교 분석하였다. Fig. 3의 실험 결과, 제안 기법이 다중 서브넷 구조로 다중 사용자의 개인 정보를 처리하기 때문에 개인 정보 관리 비용이 13.4% 단축된 결과를 얻었다. 이 같은 결과는 서브넷으로 구성된 사용자의 개인정보를 사용 목적에 따라 해쉬 체인으로 다른 서브넷에 존재하는 개인정보와 연관되도록 동작되기 때문에 나타난 결과이다.

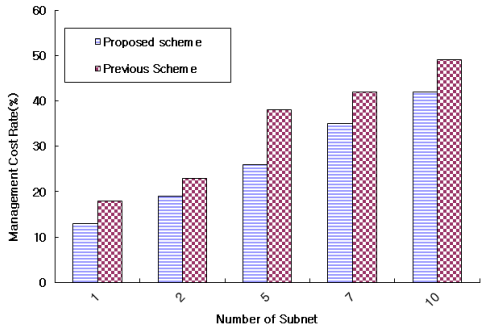

Fig. 3. Analysis of Personal Management Cost per Subnet

4.1.2 효율성

Fig. 4는 클라우드 환경에서 다중 서브넷에 사용목적에 따라 사용자의 개인정보를 클라우드 서버에서 처리하는 효율성을 비교 분석하였다. Fig. 4의 실험 결과, 제안 기법은 기존 기법보다 효율성이 19.5% 향상되었다. 이 같은 결과는 사용자의 정보를 n개의 키로 익명 키를 생성하기 때문에 클라우드 서버에 등록하거나 저장되어 있는 사용자의 개인정보를 기존 기법보다 다양하게 그룹관리가 가능하기 때문이다.

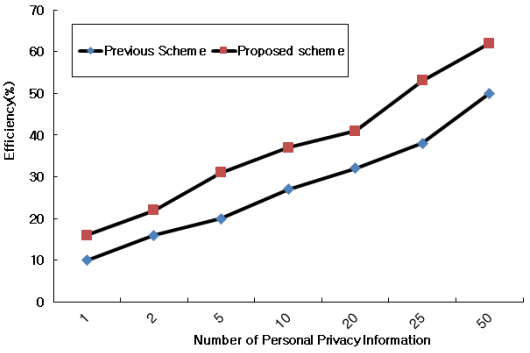

Fig. 4. Efficiency through number of Personal Privacy Information

4.2 보안 평가

제안 기법은 사용자의 개인 정보를 클라우드 서버에 등록된 후 다수의 서브넷으로 사용자의 개인정보를 액세스하기 위해서 개인 정보를 n개의 키로 생성된 익명의 키로 처리하기 때문에 클라우드 서비스를 끊김없이 제공받도록 사용자의 무결성을 보장받는다. 특히, n개의 키를 생성하여 개인 정보를 0과 1의 16진수 값으로 최소 32비트에서 최대 256비트로 구성하기 때문에 클라우드 서버와 사용자간 공유된 정보를 제3자가 쉽게 얻을 수 없어 사용자의 개인정보에 대한 안전성과 신뢰성이 보장받는다.

5. 결론

최근 클라우드 보안과 관련하여 많은 연구가 진행되고 있다. 본 논문에서는 사용자의 개인 정보를 대내·외적으로 처리되어야 하는 키를 n개 생성하여 사용자의 개인정보를 안전하게 보호하기 위한 기법을 제안하였다. 제안 기법은 개인 정보를 서브넷 그룹으로 묶어 상황에 따라 개인 정보를 보호할 수 있는 키를 0과 1의 16진수 값으로 최소 32비트에서 최대 256비트로 n개 생성한다. 제안 기법은 개인 정보를 그룹별 다중처리를 위해서 해쉬체인을 사용하여 개인 정보를 익명화하도록 하였으며, 사용자의 개인 정보를 안전하게 수집·보관·관리·처리 하도록 하여 제3자가 불법적으로 개인 정보를 악용하지 않도록 하였다. 성능평가 결과, 제안 기법은 다중 형태의 구조로 처리되는 다중 사용자의 개인 정보를 제3자가 안전하게 접근하여 처리할 수 있도록 동작하기 때문에 개인 정보 관리 비용이 13.4% 단축된 결과를 얻었다. 제안 기법의 효율성은 기존 기법보다 19.5% 향상되었다. 향후 연구에서는 본 연구의 결과를 기반으로 실제 운영되고 있는 클라우드 서비스에 제안 기법을 적용하여 성능 평가를 수행할 계획이다.

REFERENCES

[1] Y. S. Jeong. (2017). A Study on improving manufacturing environment using IoT technology in small business environment. *Journal of Convergence for Information Technology, 7(2),* 83-90.
DOI : 10.22156/cs4smb.2017.7.2.083

[2] J. S. Lee. (2017). A Study on the Effects of the Cooperative Philosophy between SMEs to the Cooperative Activities and Performance. *Journal of the Korea Convergence Society, 8(9),* 301-309.

[3] A. S. Oh. (2015). Smart Factory Logistics Management System Using House Interior Position Tracking Technology Based on Bluetooth Beacon. *Journal of the Korea Institute of Information and Communication Engineering, 19(11),* 2677-2682.

DOI : 10.6109/jkiice.2015.19.11.2677

[4] Y. S. Jeong. (2016). A Study of An Efficient Clustering Processing Scheme of Patient Disease Information for Cloud Computing Environment. *Journal of Convergence Soceity for SMB, 6(1),* 33-38.
DOI : 10.22156/cs4smb.2016.6.1.033

[5] Y. S. Jeong. (2010). An Efficiency Management Scheme using Big Data of Healthcare Patients using Puzzy AHP. *Journal of Digital Convergence, 13(4),* 227-234.
DOI : 10.14400/jdc.2015.13.4.227

[6] Y. S. Jeong. (2016). Design of Prevention Model according to a Dysfunctional of Corporate Information. *Journal of Convergence Soceity for SMB, 6(2),* 11-17.
DOI : 10.22156/cs4smb.2016.6.2.011

[7] M. Tatebayashi, N. Matsuzaki & D. B. Newman. (1999). Key distribution protocol for digital mobile communication systems. *Advances in Cryptology-CRYPTO'89,* 324-334.
DOI : 10.1007/0-387-34805-0_30

[8] L. Eschenauer & V. D. Gligor. (2002). A key-management scheme for distributed sensor networks. *Proceedings of the 9th ACM conference on Computer and communications security,* 41-47.
DOI : 10.1145/586110.586117

[9] C. Park, K. Kurosawa, T. Okamoto & S. Tsujii. (1993). On key distrubution and authentication in mobile radio networks. *Advances in Cryptology-euroCrypt'93,* 461-465.

[10] Y. S. Wu, B. Foo, Y. Mei & S. Bagchi. (2003). Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS. In Computer *Security Applications Conference, 2003. Proceedings. 19th Annual* (pp. 234-244). IEEE.
DOI : 10.1109/csac.2003.1254328

[11] S. T. Zargar & J. B. D. Joshi. (2010). A Collaborative Approach to Facilitate Intrusion Detection and Response against DDoS Attacks. *Proceedings of the 6th international Conference on Collaborative Computing: Networking, Applications & worksharing, collaboratecom.*
DOI : 10.4108/icst.collaboratecom.2010.46

[12] F. Y. Leu & Z. Y. Li. (2009). Detecting DoS and DDoS Attacks by using an Intrusion Detection and Remote Deterrence System. *Proceedings of the Fifth International Conference on Information Assurance and Security, IEEE,* 251-254.
DOI : 10.1109/ias.2009.294

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 : ICT 네트워크, 유·무선 통신, 정보보호, 헬스케어, 빅 데이터, 바이오인포매틱스
- E-Mail : bukmunro@mokwon.ac.kr