ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 5, pp. 107-113, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.5.107

블록 체인 기반의 다중 그룹 요소를 이용한 사용자 프라이버시 관리 모델

정윤수[1], 김용태[2], 박길철[3*]
[1]목원대학교 정보통신융합공학부 조교수
[2]한남대학교 멀티미디어학과 부교수
[3]한남대학교 멀티미디어학과 교수

User Privacy management model using multiple group factor based on Block chain

Yoon-Su Jeong[1], Yong-Tae Kim[2], Gil-Cheol Park[3*]
[1]Assistant Professor, Department of information Communication Convergence Engineering, Mokwon University
[2]Associate professor, Department of multimedia, Hannam University
[3]professor, Department of multimedia, Hannam University

요 약 IT 기술 중 빅 데이터와 인터넷 기술이 급속하게 발달함에 따라 중요 데이터를 USB와 같은 외부 저장장치에 저장하지 않고도 인터넷이 연결되어 있는 곳이면 어디든지 클라우드 환경에 저장된 데이터를 사용할 수 있는 환경으로 바뀌어 가고 있다. 그러나, 클라우드 환경에서 처리되는 데이터가 손쉽게 일반 사용자들이 처리할 수 있는 환경으로 바뀌가면서 사용자의 프라이버시 정보에 대한 보호의 중요성이 점점 증가하고 있다. 본 논문에서는 클라우드 환경에서 사용되는 정보를 제3자에게 노출시키지 않으면서 사용자의 서비스 질을 향상시킬 수 있는 관리 모델을 제안한다. 제안 모델은 다양한 클라우드 환경에서 처리되고 있는 데이터들 중에서 사용자의 프라이버시 정보를 제3자가 악의적으로 처리하지 못하도록 사용자 그룹을 가상의 환경으로 그룹핑한 후 identity 속성과 접근제어 정책을 블록 체인으로 처리한다. 특히, 클라우드 환경에서 처리되는 데이터의 처리 효율성에 대한 성능을 향상시키기 위해서 개인 정보와 계산 집약적인 암호 정책은 오프 체인에서 실행하도록 하였다.

주제어 : 클라우드, 사용자 프라이버시, 다중 그룹, 해쉬체인, 속성

Abstract With the rapid development of big data and Internet technologies among IT technologies, it is being changed into an environment where data stored in the cloud environment can be used wherever the Internet is connected, without storing important data in an external storage device such as USB. However, protection of users' privacy information is becoming increasingly important as the data being processed in the cloud environment is changed into an environment that can be easily handled. In this paper, we propose a user-reserving management model that can improve the user 's service quality without exposing the information used in the cloud environment to a third party. In the proposed model, user group is grouped into virtual environment so that third party can not handle user‘s privacy information among data processed in various cloud environments, and then identity property and access control policy are processed by block chain.

Key Words : Cloud, User Privacy, Multiple Group, Hash Chain, Property

*This paper has been supported by 2018 Hannam University Research Fund.
*Corresponding Author : Gil-Cheol Park (gcpark@hnu.kr)
Received September 12, 2018 Revised September 27, 2018
Accepted October 20, 2018 Published October 31, 2018

1. 서론

최근 몇 년동안 클라우드 컴퓨팅은 사용자의 요구사항을 충족시키기 위해서 많은 변화와 발전을 거듭하고 있다. 클라우드 컴퓨팅은 온 디맨드 셀프 서비스, 유비쿼터스 네트워크 액세스, 위치 독립적 자원 풀링, 신속한 탄력성 등의 특징을 통해 컴퓨팅 자원을 제어 및 최적화하는 특징이 있다[1]. 특히, 클라우드 컴퓨팅은 인터넷 상에 존재하는 데이터를 사용자가 필요로 할 때마다 다양한 단말 장치를 통해 이용할 수 있기 때문에 클라우드 서비스를 제공하는 기관이나 업체가 기하급수적으로 늘어나고 있다[2-4]. 그러나, 클라우드 환경에서 제공되는 다양한 서비스는 사용자의 제어권이 상실될 경우 데이터의 무결성 및 기밀성이 심각하게 위협받을 수 있는 문제점이 있다.

대부분의 클라우드 환경에서는 기업 차원에서 사용자의 데이터 및 프라이버시 정보를 보호하고 있지만 급속하게 성장하고 있는 클라우드 환경을 기업은 완벽하게 제어하기 어렵다. 클라우드 컴퓨팅 환경에서는 권한이 없는 사용자가 서버에 존재하는 민감한 데이터를 불법적으로 접근하거나, 암호문 액세스 정책 및 속성 집합과 연동하여 불법적인 접근을 시도한다.

클라우드 환경에서 처리되고 있는 수 많은 데이터를 서버에서 안전하게 처리하기 위해서는 사용자의 동의없이 사용자의 프라이버시 보호에 대한 정책이 필요하다. 특히, 중요 데이터를 USB와 같은 외부 저장장치에 저장하지 않고 인터넷이 연결된 클라우드 환경에 저장할 수 있는 방법이 필요하다.

본 논문에서는 다양한 장치들을 통해서 사용자의 데이터를 클라우드 환경에서 처리할 때 사용자의 프라이버시를 제3자로부터 안전하게 보호하기 위한 다중 그룹 기반의 클라우드 관리 모델을 제안한다. 제안 모델은 클라우드 환경에서 사용되는 정보를 제3자에게 노출시키지 않도록 블록체인 기반의 다중 그룹 요소를 사용한다. 특히, 제안 모델은 사용자의 프라이버시 정보를 가상의 환경에서 그룹핑한 후 ID(identity) 속성과 접근제어 정책을 블록 체인한다. 제안 모델에서는 클라우드 환경에서 처리되는 데이터의 처리 효율성을 향상시키기 위해서 개인 정보와 계산 집약적인 암호 정책을 오프 체인으로 처리한다.

이 논문의 구성은 다음과 같다. 2장에서는 클라우드 환경에서 발생할 수 있는 사용자 프라이버시 보호를 위한 기존 연구에 대해서 알아본다. 3장에서는 다중 그룹 요인을 이용하여 클라우드 연합에 필요한 사용자 프라이버시 정보 보호 관리 모델을 제안하고, 4장에서는 클라우드 환경에서 발생할 수 있는 보안 공격 측면에서 제안 모델을 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

클라우드 환경에서 사용자 프라이버시와 관련된 연구는 스토리지 그룹화, 사용자 프라이버시 보안 문제, 프로세스 및 메모리 보안 문제, 클라우드 시스템의 IoT 노드 등을 중심으로 많은 연구가 진행되어 왔다. 클라우드 컴퓨팅은 과거에 비해 인터넷 환경이 급변하면서 많은 양의 데이터를 가상의 스토리지에서 저비용으로 구축하기 때문에 사용자의 편리성이 향상되는 장점은 있지만 그에 따른 다양한 보안 문제가 발생하는 단점도 존재한다.

Singh et al. 은 클라우드 환경을 구성하고 있는 다양한 요소들의 연관 관계에서 발생할 수 있는 다양한 보안 문제와 Focusses 클라우드 보안 등의 보안 이슈들을 연구하였다[5]. Singh et al.은 클라우드 환경을 구성하고 있는 다양한 요소들의 연관 관계에서 발생할 수 있는 다양한 보안 문제를 효율적으로 해결할 수 있는 3계층 보안 구조를 제안하고 있다[6]. Zhang et al.은 클라우드 환경에 최적화된 알고리즘을 분석하여 클라우드 환경의 보안 문제를 분석하는 연구를 진행하였다[7]. Varadharajan et al. 은 클라우드 환경에서 유연한 보안 서비스를 사용자에게 제공하기 위한 연구를 수행하였다[8].

Iera et al.은 클라우드 환경에서 사용하고 있는 IoT 장치들을 마이그레이션 한 후 특정 IoT에 최적화된 기법을 제안하였다[9]. Saha et al.은 클라우드 환경에서 동작되는 다양한 장치들(자율제어, IoT 등) 뿐만 아니라 유・무선 상의 동기화 문제에 대해서 제안하고 있다[10]. Celesti et al.은 Saha et al.[10]가 제시한 내용을 기반으로 경량화된 IoT 클라우드 서비스 장치를 구현하였다[11]. Dar et al. 은 클라우드 환경에서 사용하고 있는 다양한 플랫폼의 가용성을 측정하기 위한 가상화 프레임워크를 제안하였다[12].

L. Echenauer et al. 기법은 클라우드 서비스에 필요한 사용자 키를 확률적으로 분배처리하기 위한 공유키 생성

방법을 제안하였다[13]. 이 기법은 공유키를 찾는데 많은 시간이 소비되는 문제점이 있지만 클라우드 서비스를 이용하는 많은 사용자의 키 보안성을 향상시킬 수 있는 장점이 있다.

H. Chan et al. 기법은 클라우드 서비스를 이용하는 사용자를 n그룹으로 나누어 공유키의 사용 효율성을 높이는 방법을 제안하였지만 공유키 사용에 필요한 메모리의 낭비가 높은 단점을 가지고 있다[14]. S. Zhu et al. 기법은 클라우드 서버에서 발생되는 부하를 줄이기 위한 공유키 생성기법을 제안하였다. 그러나, 이 기법은 공유키를 공유한 사용자간 상호인증 때문에 세션키가 노출될 수 있는 문제점이 존재한다[15]. A. Khalili et al. 기법은 사용자의 공개키와 개인키를 ID 기반으로 암호화하는 기법을 제안하였다[16]. 그러나, 이 기법은 개인키를 임계계수만큼 수집해야하기 때문에 중간자 공격에 취약한 문제점이 있다.

3. 다중 그룹 요소를 이용한 개인 정보 관리 모델

최근 IT 기술이 급속하게 발전하면서 클라우드 서비스를 제공받는 사용자가 급속하게 증가하고 있다. 클라우드 서비스를 제공받는 사용자의 정보(데이터, 실행 코드 등)들은 손쉽게 제3자에게 악용되는 피해가 빈번하게 발생되고 있다. 제3자에게 사용자의 정보를 악용되지 않도록 다양한 연구가 활발하게 진행되고 있지만 사용자를 만족시킬 수 있는 서비스의 질은 아직까지 미진하다. 이 절에서 클라우드 환경에서 사용되는 정보를 제3자에게 노출시키지 않으면서 사용자의 서비스 질을 향상시키기 위한 관리 모델을 제안한다. 제안 모델은 클라우드 환경에서 처리되는 다양한 장치들의 데이터나 실행 가능한 코드들의 무결성을 보장한다. 제안 모델은 사용자의 프라이버시 정보를 보호하기 위해서 사용자 그룹을 가상의 환경으로 그룹핑한 후 identity 속성과 접근제어 정책은 블록 체인으로 저장한다. 그러나, 개인 정보와 계산 집약적인 암호 정책은 non-블록체인에서 실행하여 서버의 부하를 줄이고 있다.

3.1 개요

클라우드 환경에서 사용되는 서비스는 사용자의 요구사항에 따라 다양하게 그룹화하여 제공되고 있다. 그러나, 현재 운영중인 클라우드 서비스는 사용자의 접근 권한에 따라 운영되고 있기 때문에 특별한 정책 지원 없이도 클라우드 서비스를 제공받을 수 있는 문제점이 있다. 본 논문에서는 클라우드 환경에서 제공되는 정보 중 사용자의 프라이버시 정보를 다중 그룹 요소로 사용하여 클라우드 연합을 위한 효율적인 관리 모델을 제안한다. 제안 모델은 클라우드 환경에서 사용자의 개인정보 중 ID 속성과 접근 정책은 블록체인으로 처리하고, PID, 사용자 권한 관리 등은 non-블록체인으로 처리할 수 있도록 쌍대 비교 행렬로 나타낸다.

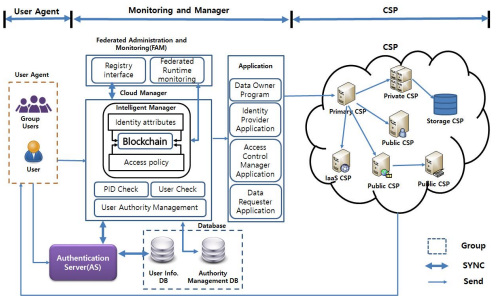

Fig. 1. Overview Process of Proposed Model

그림 1은 제안 모델의 전체 시스템 구조를 보여주고 있다. 그림 1은 사용자의 프라이버시를 안전하게 보호하기 위해서 클라우드 환경을 사용자 에이전트(User Agent), 모니터링과 관리자(Monitoring and Manager), 컨텐츠 서비스 제공자(CSP, Content Service Provider) 등으로 구분하도록 설계하였다. 사용자 에이전트는 클라우드 서비스를 제공받는 사용자를 단일 사용자(1인으로 구성)와 그룹 사용자 (2인 이상으로 구성)로 구분하여 사용자 에이전트를 구성하도록 하였다. 모니터링과 관리자는 사용자의 프라이버시를 보호하기 위해서 우선 ID 속성와 접근 정책을 블록체인으로 처리할 수 있도록 지능적 관리자(Intelligent Manager)가 관리하는 부분과 PID나 사용자를 체크하거나 사용자 권한을 관리할 수 있는 클라우드 관리자 부분으로 나누어 모니터링을 수행한다. 클라우드 관리자에 의해서 처리되는 정보는 사용자의 프라이버시 정보를 데이터베이스에 저장한 후 애플리케이션을 통해 컨텐츠 서비스 제공자에게 제공한다. 애플리케이션은 데이터 사용자 프로그램(Data Onner Program), 인식자 제공자 응용프로그램(Identity Provider application),

접근 제어 관리자 애플리케이션(Access Control Manager Application), 데이터 요청자 애플리케이션(Data Requester Application) 등으로 구성된다. 컨텐츠 서비스 제공자는 사용자에게 클라우드 서비스를 제공하기 위한 다양한 컨텐츠 서비스 제공자들로 구성된다. 그림 1에서 사용자는 CSP가 제공하는 서비스의 등급에 따라 접근 권한 등급이 부여되며, 클라우드 관리자에 의해 서비스 등록이 처리된다. 인증 서버는 사용자 등록과 동시에 사용자의 권한에 따라 접근 제어키와 비밀키를 생성하여 사용자 관리 테이블에 저장한다.

3.2 블록체인을 이용한 프라이버시 관리

이 절에서는 클라우드 환경에서 사용자의 프라이버시 정보를 효율적으로 관리하기 위해서 사용자의 프라이버시 정보를 블록체인에 적용하여 프라이버시의 중요도를 산출하는 과정을 기술하고 있다.

3.2.1 사용자 프라이버시 계층화

클라우드 환경에서 사용되고 있는 다양한 장치들(휴대폰, 태블릿, PDA 등)을 이용하여 클라우드 서비스를 제공받는 사용자의 프라이버시를 안전하면서 효율적으로 보호하기 위해서는 사용자의 프라이버시 중요도를 산출하는 것이 중요하다. 제안 모델에서는 사용자의 프라이버시에 대한 중요도를 산출하기 위해서 사용자의 프라이버시를 쌍대비교 행렬에 적용하고 있다. 제안 모델에서 사용되고 있는 사용자의 프라이버시 정보는 클라우드 구조적 특징에 상관없이 다양하게 적용될 수 있다. 제안 모델은 쌍대비교 행렬을 통해서 얻은 사용자의 프라이버시 중요도를 계층적으로 관리함으로써 사용자 프라이버시에 접근하는 제3자의 접근 권한을 제한한다. 사용자의 프라이버시 중요도를 쌍대비교 행렬을 통해 구한 결과값은 계층적으로 표현하며, 전체 n개의 사용자의 프라이버시 정보를 $n(n-1)/2$ 회 만큼 비교 횟수가 가능하도록 구성한다. 이 같이 하는 이유는 사용자의 프라이버시 정보를 계층적으로 구성하기 위해서이다.

3.2.2 사용자 프라이버시 연계

제안 모델에서 사용자 프라이버시 중요도는 안전한 해쉬함수(H_U: {0,1}→Z_N)로 표현하며, 사용자 프라이버시 연계를 다중으로 처리해야 하는 다중 사용자의 프라이버시 중요도는 H_U: $0,1^* \times Z_N \rightarrow Z_P$ 으로 나타낸다. 제안 모델에서 사용자 프라이버시를 계층적으로 나타낼 경우 K번째 위치의 사용자 프라이버시의 중요도는 식 1처럼 구할 수 있다. K번째 위치한 사용자의 프라이버시 정보는 사용자의 액세스 정보들과 프라이버시에 대한 중요도를 쌍으로 연계한다.

$$I[1,\ k] = \prod_{i=2}^{k} UPCI_i \qquad (1)$$

여기서, $I[1,\ k]$ 는 첫 번째 사용자 프라이버시 정보 계층에 대한 k번째 계층 요소의 종합 가중치를 의미한다. $UPCI_i$는 추정되는 사용자 프라이버시 정보의 w 벡터를 구성하는 행을 포함하는 $n_{i-1} \cdot n_i$ 행렬을 의미한다. n_i는 i번째 계층의 사용자 프라이버시 정보 수를 의미한다.

3.2.3 쌍대 비교 행렬을 이용한 사용자 프라이버시 중요도 처리 과정

클라우드 환경에서 처리되는 정보 중 사용자의 프라이버시를 탐지하여 처리하기 위해서 제안 모델에서는 사용자의 프라이버시를 중요도에 따라 가상 환경에서 사용자의 프라이버시 정보를 안전하게 처리하도록 블록체인과 non-블록체인을 조합하여 사용자의 프라이버시를 처리하도록 다음과 같이 3단계를 수행한다.

- 1 단계 : 가상환경에서 처리되어야 할 데이터 속성 정보 수집

제안모델에서는 클라우드 환경에서 처리되는 데이터를 효율적으로 처리하기 위해서 서버에서 데이터를 처리하기 전에 가상환경을 구축하여 클라우드 환경에서 처리하는 데이터를 사전 처리하도록 데이터를 식 (1)과 같이 수집한다. 식 (1)에서 처리되는 데이터는 클라우드 환경에서 처리되는 데이터의 속성정보들을 상관관계 행렬로 처리한다.

$$Att_i = \begin{pmatrix} 0 & \cdots & w_{1k} \\ \vdots & \ddots & \vdots \\ w_{k1} & \cdots & 0 \end{pmatrix} \qquad (1)$$

여기서, k는 데이터의 속성 정보의 개수를 의미하며, k의 범위는 1부터 9가지를 의미한다. w_{mn}은 데이터의 속성정보 Att_x와 Att_y사이의 상관 정보를 의미한다. w_{mn}와 w_{nm}는 m이 0이상이고 n이 1미만인 조건에서 동일하다.

만일 w_{mn}이 0이면 속성 정보 Att_x와 사이의 상관관계는 없다는 의미가 된다.

클라우드 서버는 사용자의 속성정보들을 통해 가상환경에서 처리되어야 할 데이터를 식 (2)처럼 추출한다.

$$AttInfo_i=\{Att_i|Att_i\in Att,\ 1\le i\le L\} \quad (2)$$

여기서 L은 클라우드 환경에서 처리되어야 할 정보의 총 개수를 의미한다. 단, $AttInfo_i$은 $Att_1\cup Att_2\cup\cdots\cup Att_n$ 이고 $\varnothing= Att_1\cap Att_2\ \cap\cdots\cap Att_i$을 의미한다.

- 2 단계 : 쌍대비교 행렬을 통한 사용자 프라이버시 중요도 계층화 후 연계

제안 모델에서 사용자의 프라이버시 중요도를 쌍대비교 행렬을 통해 구한 결과값을 전체 사용자의 프라이버시 정보 수 만큼 계층화 한다. 제안 모델에서는 사용자의 프라이버시 중요도를 $n\times n$ 행렬로 정의된 a_{ij}의 관계 성분으로 나타내기 때문에 사용자의 프라이버시 중요도에 대한 산출이 기존 방법에 비해 효율적으로 처리될 수 있다. 제안 모델에서 사용자의 프라이버시 중요도 a_{ij}(i와 j는 1, 2, ・・・ ,n)는 상대적 평가 요소 (w_1, w_2, ・・・, w_n)를 w_i/w_j= 1 / (w_j/w_i)처럼 사용한다.

- 3 단계 : 중요도에 따른 사용자 프라이버시 연계

제안 모델에서는 중요도에 따라 사용자의 프라이버시를 연계하기 위해서 중요도를 안전한 해쉬함수 : {0,1}으로 표현한다. 사용자 프라이버시 정보를 계층적으로 다중 연계를 하기 위해서 다중 사용자의 프라이버시 중요도를 $I[1,\ k]=\prod_{i=2}^{k}UPCI_i$ 처럼 사용하도록 연계한다. 제안 모델에서 클라우드 서비스를 사용하는 사용자의 프라이버시를 계층적으로 나타낼 경우 번째 위치의 사용자 프라이버시의 중요도를 사용자의 액세스 정보들과 쌍으로 연계하여 처리하도록 한다.

4. 평가

제안 모델은 다중 그룹 요인을 이용한 클라우드 연합을 위한 개인 정보 보호를 평가하기 위해서 다단계 서비스 접근인증에 따른 공격, 사용자 프라이버시 공격, Blackhole /Sinkhole 공격, Hello 플로우 공격, 웜홀 공격 등에서 평가를 수행한다.

제안 모델에서는 사용자 프라이버시 보호를 위해서 불법적으로 클라우드 환경에 접근하는 제3자를 허용한도록 계층적 다단계의 서비스 인증과정을 수행한다. 제안 모델에서는 계층적 다단계의 서비스를 수행하기 위해서 가상의 환경에 사용자의 프라이버시를 그룹핑한 후 사용자 프라이버시 정보 중 identity 속성과 접근제어 정책 등을 블록 체인으로 저장한다. 따라서, 제안 모델은 계층적 다단계의 인증 서비스를 수행하기 때문에 클라우드 환경에서 발생할 수 있는 다단계 서비스 접근인증 공격에 안전하다.

제안 모델은 사용자의 프라이버시 정보에 대한 중요도를 안전한 해쉬함수(H_U: {0,1}→Z_N)로 표현하고 있다. 제안 모델에서는 클라우드에 접근하는 다중의 사용자 프라이버시의 중요도를 H_U: $0,1^*\times Z_N\rightarrow Z_P$로 나타냄으로써 사용자의 프라이버시 공격을 예방하고 있다. 특히, 제안 모델에서 사용하는 사용자의 프라이버시 정보는 사용자의 액세스 정보들과 프라이버시에 대한 중요도를 쌍으로 연계하여 처리하기 때문에 사용자 프라이버시 공격에 안전하다. 또한, 제안 모델에서는 사용자의 프라이버시 정보를 손쉽게 관리할 수 있도록 연계정보를 $I[1,\ k]=\prod_{i=2}^{k}UPCI_i$와 같이 처리하기 때문에 사용자 프라이버시에 대한 가용성을 보장받을 수 있다.

제안 모델에서는 클라우드 환경을 구성하는 다양한 장치의 동작과정에서 발생할 수 있는 Blackhole/Sinkhole 공격을 예방하기 위해서 블록체인과 비블록체인을 조합하여 다양한 프라이버시 정보를 사용하고 있다. 이 같이 사용하는 이유는 불법적인 통신을 원하는 제3자가 플로딩 기반의 프로토콜을 사용하는 통신 사이에서 패킷 패싱과 같은 공격을 예방하기 위해서이다. 제안 모델에서는 클라우드 환경을 구성하는 장치들이 사용하는 인증키들을 주기적으로 갱신하고 있기 때문에 Blackhole/Sinkhole 공격을 예방할 수 있다.

제안 모델에서는 다중 사용자의 프라이버시 중요도를 $I[1,\ k]=\prod_{i=2}^{k}UPCI_i$ 를 이용해서 Hello 공격을 예방하고 있다. 사용자 프라이버시를 예방하기 위해 사용되는 다양한 인덱스 정보 및 인증 키들은 클라우드 환경을 구성하는 장비에서 주기적으로 갱신하고, 장비간 안전한 통

신을 통해서 사용자의 프라이버시를 송・수신하기 때문에 Hello 플로우 공격을 예방하고 있다. 또한 제안 모델에서는 사용자 프라이버시의 중요도를 계산하는 정보들을 주기적으로 변경하기 때문에 무결성 및 최신성을 제공한다.

제안 모델에서는 클라우드 환경에서 송・수신되는 정보들의 패킷(또는 비트) 정보를 제3자가 불법적으로 수집하여 추적할 때 발생하는 웜홀 공격을 예방하기 위해서 클라우드 환경을 구성하는 장치 간 서로 정보를 동기화하기 때문에 웜홀 공격을 예방하고 있다. 또한, 제안 모델은 클라우드 환경에서 처리되는 데이터의 속성 정보들을 상관관계 행렬로 처리하기 때문에 웜홀 공격에 안전하다.

5. 결론

최근 클라우드 컴퓨팅은 사회적 요구사항을 반영하여 많은 변화와 발전을 거듭하고 있다. 클라우드 컴퓨팅은 인터넷 상에 존재하는 데이터를 다양한 장치를 통해서 이용하기 때문에 개인 및 기관에 상관없이 많이 이용되고 있다. 그러나, 다양한 장치를 통해서 클라우드 환경에 존재하는 데이터를 사용하기 때문에 데이터의 무결성 및 기밀성이 제3자로부터 악용될 수 있는 문제점이 존재한다. 본 논문에서는 클라우드 환경에 저장되에 있는 사용자의 데이터를 안전하게 보호하기 위해서 사용자의 데이터를 다중 그룹으로 연합하여 사용자의 프라이버시를 보호하는 관리 모델을 제안한다. 제안 모델은 클라우드 환경에서 사용되는 정보를 제3자에게 노출시키지 않기 때문에 사용자의 프라이버시를 안전하게 보호할 수 있다. 특히, 제안 모델은 사용자의 프라이버시 정보를 가상의 환경으로 그룹핑한 후 ID 속성과 접근제어 정책은 블록체인으로 처리하기 때문에 제3자의 악의적 공격에 안전하다. 제안 모델에서는 클라우드 환경에서 처리되는 데이터의 처리 효율성을 향상 시키기 위해서 개인 정보와 계산 집약적인 암호 정책은 오프 체인에서 실행하도록 하였다. 제안 모델은 다양한 클라우드 환경에서 사용자가 서비스를 제공받도록 데이터나 실행 가능한 코드들의 무결성을 보장하고 있다. 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, June). A Big Data Framework for u-Healthcare Systems Utilizing Vital Signs. *Proceedings of the 2014 International Symposium on Computer, Consumer and Control(IS3C).* (pp. 494-497).
DOI : 10.1109/is3c.2014.135

[3] F. Touati, R. Tabish & A. Ben Mnaouer. (2014, April). 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).* (pp. 1-4).

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

[5] A. Singh & K. Chatterjee. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

[6] S. Singh, Y. S. Jeong & J. H. Park. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, 200-222.
DOI : 10.1016/j.jnca.2016.09.002

[7] J. Zhang, H. Huang & X. Wang. (2016). Resource provision algorithms in cloud computing: A survey. Journal of Network and Computer Applications, 64, 23 - 42.

[8] V. Varadharajan & U. Tupakula. (2014). Security as a service model for cloud environment. IEEE Transactions on Network and Service Management, 11(1), 60 - 75.
DOI : 10.1109/tnsm.2014.041614.120394

[9] A. Iera, G. Morabito & L. Atzori. (2016). The internet of things moves into the cloud. Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW). (pp. 191 - 191).
DOI : 10.1109/ic2ew.2016.54

[10] H. N. Saha, A. Mandal & A. Sinha. (2017). Recent trends in the internet of things. Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop

and Conference (CCWC). (pp. 1-4).
DOI : 10.1109/ccwc.2017.7868439

[11] A. Celesti, D. Mulfari, M. Fazio, M. Villari & A. Puliafito. (2016). Exploring container virtualization in iot clouds. Proceedings of the 2016 IEEE International Conference on Smart Computing (SMARTCOMP). (pp. 1-6).
DOI : 10.1109/smartcomp.2016.7501691

[12] K. S. Dar, A. Taherkordi & F. Eliassen. (2016). Enhancing dependability of cloud-based iot services through virtualization. Proceedings of the 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), 2016. (pp. 106 - 116).
DOI : 10.1109/iotdi.2015.38

[13] L. Echenauer & V. D. Gligor. (2002, Nov). A Key-Management scheme for Distributed sensor networks. Proceedings of the 9th ACM conference on Computer and communications security. (pp. 41-47).

[14] H. Chan, A. Perrig & D. Song. (2003, May). Random key predistribution schemes for Sensor networks. Proceedings of the 2003 IEEE Symposium on Security and Privacy. (pp. 197-213).
DOI : 10.1109/secpri.2003.1199337

[15] S. Zhu, S. Setia & S. Jajodia. (2002). A distributed group key managemet protocol for ad hoc networks. Unpublished manuscript. George Mason University.

[16] A. Khalili, J. Katz & W. A. Arbaugh. (2003, Jan). Toward Secure key Distribution in Truly Ad-Hoc Networks. Proceedings of the 2003 Symposium on Applications and the Internet Workshops(SAINT'03 Workshops). (pp. 342-346).
DOI : 10.1109/saintw.2003.1210183

정 윤 수(Yoon-Su Jeong) [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, 바이오인포매틱, 헬스케어, 빅 데이터, 클라우드 컴퓨팅
- E-Mail : bukmunro@gmail.com

김 용 태(Yong-Tae Kim) [정회원]

- 1984년 2월 : 한남학교 계산통계학과 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 통 신보안
- E-Mail : ky7762@naver.com

박 길 철(Gil-Cheol Park) [정회원]

- 1983년 2월 : 한남학교 계산통계학과 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 분과원장
- 관심분야 : Multimedia And Mobile Communication, Network Security
- E-Mail : gcpark@hnu.kr