情 報 保 護 學 會 誌
第22卷 第7號, 2012. 11

퍼스널 클라우드 보안 표준화 동향

박 준 영*, 나 상 호*, 허 의 남**

요 약

퍼스널 클라우드는 클라우드 컴퓨팅에 대한 관심이 높아지고 활발한 연구가 진행되면서 개인 사용자들의 클라우드 서비스에 대한 욕구를 충족시키기 위한 서비스이다. 국내외에서 IT기업을 중심으로 퍼스널 클라우드 서비스를 제공하고 있다. 하지만 표준기술 없이 개발된 퍼스널 클라우드 서비스는 각 클라우드 서비스 제공자에 종속되어 호환성이 낮으며, 서비스 및 개인정보에 대한 보안 정책도 명확하지 않고 개인화 서비스를 제공하기 위한 보안 가이드라인도 부족하다. 따라서 본 논문에서는 퍼스널 클라우드 서비스에 대한 정의 및 요구사항과 퍼스널 클라우드 보안 기술에 대한 보안 표준화를 분석한다.

Ⅰ. 서 론

퍼스널 클라우드는 클라우드 컴퓨팅이 새로운 패러다임으로 주목받으면서 떠오른 사용자 중심형 서비스이다. 기존의 클라우드 컴퓨팅은 서비스 제공자를 중심으로 독자적인 클라우드 컴퓨팅 환경을 구축하여 종속적인 클라우드 서비스를 제공하였기 때문에 클라우드 서비스 사용자들은 다양하고 통합적인 클라우드 서비스를 제공 받기 힘들었다.

시장조사업체인 '포레스터 리서치'의 분석가인 *"Frank E. Gillette"*이 "퍼스널 클라우드"부문에서 "장치 중심에서 정보 중심으로 변화하는 개인 컴퓨팅"라는 주제로 보고서를 저술하였다. 그는 보고서를 통해, "디지털 기기와 서비스들은 퍼스널 클라우드를 통해 하나로 합해질 것이다." 라고 언급하면서 퍼스널 클라우드의 발전 방향을 제시하였다[2].

또한 세계적인 리서치 자문기관인 가트너(Gartner)는 "퍼스널 클라우드"를 "하이브리드 IT 및 클라우드 컴퓨팅"과 함께 2013년 10대 전략 기술[3]로 발표하면서 클라우드 컴퓨팅에서 퍼스널 클라우드를 세분화하면서 퍼스널 클라우드의 중요성을 입증하게 되었다.

국내에서는 정부기관의 지원하에 2010년부터 퍼스널 클라우드 개발 사업을 시작하였으며, 현재는 퍼스널 클라우드 서비스 및 보안 기술까지 표준화가 진행되고 있다.

본 논문에서는 국내 표준화 기관인 TTA(한국정보통신기술협회)에서 표준으로 제정한 퍼스널 클라우드 정의 및 서비스 참조모델과 현재 표준화가 진행중인 퍼스널 클라우드 접근제어, 퍼스널 클라우드 개인정보보호 모델 그리고 퍼스널 클라우드 보안 프레임워크를 살펴봄으로써 퍼스널 클라우드 서비스 및 보안 동향을 파악하고자 한다.

Ⅱ. 퍼스널 클라우드 개요[4]

퍼스널 클라우드는 서비스 제공자 및 사용자 단말에 독립적으로 사용자 정보기반의 개인화된 콘텐츠를 제공하는 사용자 중심형 클라우드 서비스이다.

최근에 스마트폰, 모바일기기, 퍼스널 컴퓨터, 넷북, IPTV 등 개인의 디지털기기 종류가 증가하고, 블로그, 이메일, 소셜 네트워크 서비스 등 개인의 온라인 서비스가 급증하는 개인 정보화 시대에서, 모든 단말과 온라인 공간에 흩어져있는 개인 콘텐츠를 클라우드 환경에 저장/통합/관리하여, 언제 어디서나 단말 독립적으로 접근할 수 있게 함은 물론, 콘텐츠의 분석 및 가공을 통해 고부가가치 개인화 서비스를 제공한다.

본 연구는 한국산업기술평가관리원의 산업원천기술개발사업(정보통신)의 연구결과로 수행되었음(1003532).
* 경희대학교 컴퓨터공학과 박사과정 ({parkhans, shna}@khu.ac.kr)
** 경희대학교 컴퓨터공학과 교수 (johnhuh@khu.ac.kr)

2.1. 퍼스널 클라우드의 특징

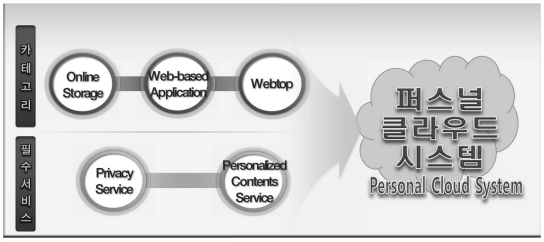
클라우드는 모든 컴퓨팅 자원을 서비스형태로 제공하는 새로운 컴퓨팅 방식으로써 네트워크, 가상화, 어플리케이션, 플랫폼 등 복합적이고 광범위한 복합적인 의미를 갖는다.

퍼스널 클라우드의 기본 특징은 다음과 같다.

- 사용 용이성과 디바이스 간 호환성
- 인터넷 기반의 즉각적인 이용성
- 개인화된 콘텐츠 제공 및 관리
- 소프트웨어(SaaS)-개인 콘텐츠(Data)간 연동

2.2. 퍼스널 클라우드의 서비스 분류

퍼스널 클라우드는 다음과 같은 3가지의 서비스 카테고리와 2가지의 필수 서비스가 필요하다.



〔그림 1〕 퍼스널 클라우드 시스템

2.2.1. 퍼스널 클라우드 서비스 카테고리

퍼스널 클라우드는 Online Storage, Webtop, Web-based Application의 3가지 종류의 카테고리로 나눌 수 있다[1]. 무한한 리소스, 웹기반 어플리케이션, 웹톱(Webtop)을 인터넷이 연결된 네트워크 환경에서 언제, 어디서나 개인화된 컴퓨팅 환경을 이용할 수 있다.

- **Online Storage**

Online Storage는 인터넷이 연결된 어느 곳에서나 사용가능하고 사용자에게 보안이 필요한 중요 정보를 보관하는 저장 공간을 제공한다.

- **Web-Based Application**

Web-based Application이란 서비스 제공자는 사용자 컴퓨터에 다운로드, 설치가 필요 없는 호스트 소프트웨어 어플리케이션을 제공하며, 사용자는 서비스 이용을 위해 자신의 컴퓨팅 자원을 사용할 필요가 없다. 구독료를 지불하는 것처럼, 웹기반 응용프로그램은 사용자가 사용을 원할 때 서비스를 제공한다.

- **Webtop**

Webtop은 사용자가 소유하고 있는 고사양의 데스크톱을 인터넷이 연결된 장소에서 재현하는 기술이다. 예를 들면, 사용자는 사용자 소유의 데스크톱의 정보나 환경을 Webtop에서도 똑같이 제공받을 수 있다.

2.2.2. 퍼스널 클라우드의 필수 서비스

- **개인화 콘텐츠 서비스**

사용자는 다수의 모바일 기기를 통해 개인화 콘텐츠(Personalized Content Service)를 보유하게 된다. 하지만 각 디바이스 및 웹 서비스를 통해 개인화 콘텐츠는 분산되기 때문에 개인화 콘텐츠 서비스가 이를 통합 저장 및 관리를 제공한다. 개인화 콘텐츠 서비스는 메일 계정, 주소록, 일정관리, 앨범 관리, 단말기 사용 이력 등에 관한 정보를 통합 저장 및 관리하며 사용자가 다운로드 받은 음악, 영화, 드라마 등의 공공용 콘텐츠(Public Content)의 저장, 재생 및 관리 환경을 제공한다. 또한 개인화 콘텐츠는 관리 툴(Tool) 및 개인화 검색 서비스(Personalized Retrieval)를 제공한다.

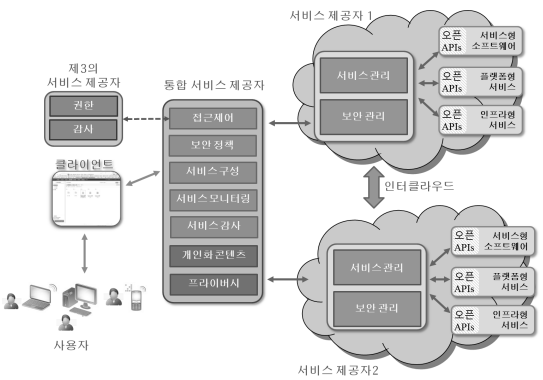
이를 위해 아래와 같은 기능이 필요하다.

- **서비스 간 콘텐츠 통합 관리 기능**; 분산되어 있는 개인 콘텐츠의 통합 저장 및 관리 환경
- **콘텐츠 동기화 기능**; 다양한 클라우드 서비스와 디바이스 간 콘텐츠 동기화 기능
- **콘텐츠 공유 기능**; 각 클라우드 서비스 콘텐츠를 OpenAPI를 이용한 클라우드 서비스 간 상호 운용성 제공 방안

- **프라이버시 서비스 (Privacy Service)**

프라이버시 서비스는 개인 사용자 정보를 기반으로 서비스를 제공하기 때문에 개인 정보 보호가 필요하다. 또한 개인 사용자 정보와 개인 데이터(동영상, 사진, 파일 등) 보호를 위해 사용자, 서비스 제공자, 데이터 감사자(Auditor) 간 데이터 이중암호화를 통해 데이터 유출 및 유실이 발생하더라도 안전하게 개인 데이터 보호가 가능해야 한다.

2.3. 퍼스널 클라우드 참조 모델



〔그림 2〕 퍼스널 클라우드 참조 모델

본 퍼스널 클라우드 참조 모델은 클라이언트(사용자), 제3의 서비스 제공자, 통합 서비스 제공자로 구분하면 각 기능은 다음과 같다.

- **클라이언트(사용자)** : 사용자가 클라이언트(브라우저)를 통해 서비스를 제공받는다.
- **제 3의 서비스 제공자** : 통합서비스 제공자가 사용자 식별 및 권한 승인 등과 같은 사용자 인증 서비스를 제공하고 이 기관은 공공기관 또는 공인된 인증기관이 될 수 있다.
- **통합서비스 제공자** : 사용자 정보를 고려하여 개인화 콘텐츠를 각 서비스 제공자에게 요청하여 서비스를 제공받고 이를 사용자가 사용할 수 있도록 구성하여 서비스를 제공한다.
- **서비스 제공자** : 사용자의 개인화 콘텐츠 저장 및 여러 콘텐츠를 보유하고 있으며 통합 서비스 제공자의 요청에 따라 서비스를 제공하며 모든 서비스는 오픈API로 구성한다.

Ⅲ. 퍼스널 클라우드 보안 표준화 동향

퍼스널 클라우드 보안 표준화는 퍼스널 클라우드 서비스 참조모델을 기반으로 진행되고 있으며, 국내 표준화 기구인 *TTA(한국정보통신기술협회) PG420(클라우드 컴퓨팅 그룹)*에서 활발히 표준화가 이뤄지고 있다. 본 장에서는 현재 표준화 제정 또는 진행되고 있는 퍼스널 클라우드 보안 표준화를 살펴본다.

3.1. 퍼스널 클라우드 접근제어 시스템

공공용/사설용 클라우드 접근제어와 퍼스널 클라우드 접근제어는 비슷한 컴퓨팅 환경을 제공하지만 접근제어의 목적은 다음과 같은 차이점을 보인다[5,10].

- **공공용/사설용 클라우드 접근제어**: 리소스에 대한 사용자의 접근을 관리 또는 제어하여 안전하고 끊김 없는 서비스를 제공한다.
- **퍼스널 클라우드 접근제어**: 사용자의 콘텐츠(데이터, 미디어, 어플리케이션 등)에 대한 안전한 접근과 개인 콘텐츠 보호를 및 개인 콘텐츠의 쉬운 접근 등을 제공하는 사용자 역할기반 접근제어이다.

3.1.1. 퍼스널 클라우드 접근제어 요구사항

- **기존 보안 정책과의 호환**

퍼스널 클라우드 서비스는 인터클라우드와 서비스 융합 등의 통합서비스를 제공하기 때문에 퍼스널 클라우드만의 접근제어 정책 및 시스템을 구축하기 보다는 기존의 웹 서비스 및 클라우드 서비스와의 보안정책 결정, 수립, 수행이 호환될 수 있어야 사용자에게 더 많은 서비스를 제공이 가능하다.

- **독립적인 보안 정책 수립**

클라우드 서비스 제공자들의 원활한 관리를 위해서 클라우드 서비스 제공자들의 독립적인 보안 정책을 수립하여 관리할 수 있어야 한다.

- **융합 클라우드 서비스와 인터클라우드**

클라우드 사용자는 인터클라우드와 같은 복수의 클라우드 서비스 제공자로부터 서비스를 제공받거나 복수개의 서비스를 융합하여 서비스 제공을 받기 때문에 퍼스널 클라우드 접근제어는 복수의 서비스 제공자와 서비스를 순차적이거나 동시에 접근 제어가 이루어져야 한다.

- **프라이버시 보장**

개인 사용자를 중심으로 제공하는 서비스이므로 개인정보 유출을 차단할 수 있는 명확한 방법이 제시되어야 한다. 또한 클라우드 서비스 제공자가 사용자 정보를 악용할 수 있기 때문에 퍼스널 클라우드 접근제어에서는 사용자의 개인정보를 보호해야 하며 클라우드 서비스 제공자는 개인 사용자를 분별할 수 없지만 서비스 이용 정보를 유지하여 사용자 경험을 토대로 서비스를

제공해야 한다.

• 제 3의 감사자

클라우드 서비스 제공자는 서로 독립적인 보안 정책을 통해 관리하고 있으며 타 클라우드 서비스 제공자와의 원활한 융합 서비스를 제공하기 위해서는 타 클라우드 서비스 제공자와의 통신에 대한 감사가 필요하다. 통합 서비스 제공자와 클라우드 서비스 제공자, 또는 클라우드 서비스 제공자간의 감사를 위해 신뢰하는 제 3의 감사자가 요구된다.

• SLA 기반의 접근제어

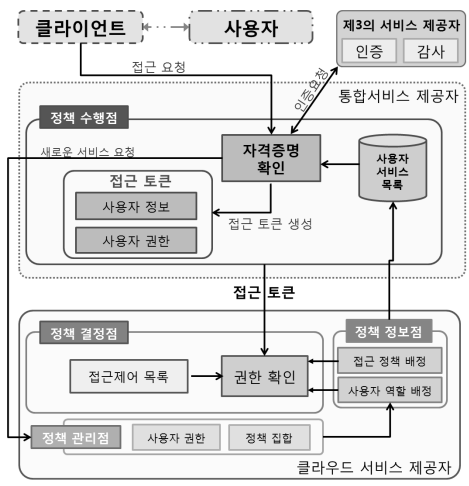
모든 서비스 제공자 (클라우드 서비스 제공자와 통합 서비스 제공자 등)는 사용자에게 사용자가 원하는 서비스를 제공하기 위해서 서비스 수준 협약(SLA)을 만족하는 접근제어 정책을 수립하여 제공해야 한다.

3.1.2. 퍼스널 클라우드 접근제어 참조모델

퍼스널 클라우드 접근제어 참조 모델은 클라이언트(사용자), 통합서비스 제공자, 클라우드 서비스 제공자, 제 3의 서비스 제공자로 구분한다.

사용자 인증은 통합서비스 제공자에서 리다이랙션을 통해 제 3의 서비스 제공자에게 사용자 인증을 요청하므로 통합서비스 제공자에는 사용자 정보가 남지 않아 사용자 정보 유출 및 유실을 방지 할 수 있다.

통합 서비스 제공자의 정책수행점에서는 인증된 사용자에 한하여 클라우드 서비스 제공자의 보안 정책과



〔그림 3〕 퍼스널 클라우드 접근제어 참조 모델

사용자 서비스 목록 등을 기반으로 서비스 접근을 위한 Access Token을 발행한다.

클라우드 서비스 제공자는 정책 결정점, 정책 정보점, 정책 관리점으로 구성되며 독립적인 보안 정책을 수립, 결정, 저장, 삭제 등이 가능하다.

제 3의 서비스 제공자는 통합 서비스 제공자에서의 접근 요청(리다이랙션)에 대해 사용자 인증을 수행하고 모든 서비스 제공자간의 감사(Audit)를 수행하여 사용자에게 원활한 서비스를 제공하는 역할을 수행한다. 인증 및 감사를 수행하는 기관이므로 신뢰할 수 있는 기관이 되어야 한다

3.2. 퍼스널 클라우드 개인정보보호 참조모델[6]

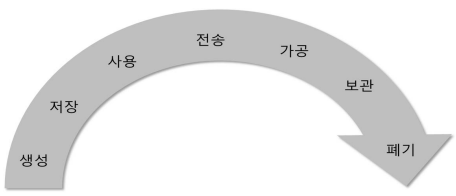
3.2.1. 개인정보 분류

퍼스널 클라우드 서비스에서 개인정보는 이용자가 서비스 제공자에게 자발적으로 제공하는 제공정보와 서비스 이용 또는 서비스 제공 시 필요에 의해 생성되는 이용정보로 나뉜다.

- **제공정보**: 이용자가 서비스 이용을 위하여 회원가입 절차 혹은 서비스 등록을 위해 사업자에게 제공하는 정보로 서비스 제공자에게 자발적으로 제공한다는 특징이 있다.
- **이용정보**: 사업자가 서비스를 제공하는 과정에서 생성되는 이용자에 관한 정보로 시스템에 의하여 자동으로 수집, 기록되는 특성을 가지는 이용자의 접속 기록, 접속로그 쿠키 등과 사용자가 업로드하는 데이터가 포함된다.

3.2.2. 퍼스널 클라우드 개인정보보호 참조모델

퍼스널 클라우드 개인정보보호 참조 모델은 개인정보 생명주기인 생성, 저장, 사용, 전송, 가공, 보관, 폐기



〔그림 4〕 개인정보 생명주기

의 절차를 따른다.

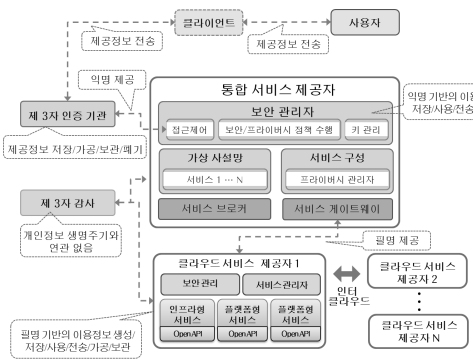
클라이언트에서는 이용자가 퍼스널 클라우드 서비스를 이용하기 위한 응용프로그램으로써 서비스 제공자와 제3의 인증 기관, 감사기관과 연동된다.

제3의 인증기관은 서비스 이용자로부터 개인 정보를 위임 받아 관리하고, 퍼스널 클라우드 서비스 제공 시 사용자로부터 입력된 정보를 바탕으로 인증을 수행하고 수행 결과만을 통합 서비스 제공자 혹은 클라우드 서비스 제공자에게 전달한다. 제공정보는 관리하나 일반적인 사용자의 서비스 이용과 관련된 정보는 수집하지 않으나 비정상적인 접근(로그인 정보 불일치 등)에 대해서 로그 기록을 남길 수 있다.

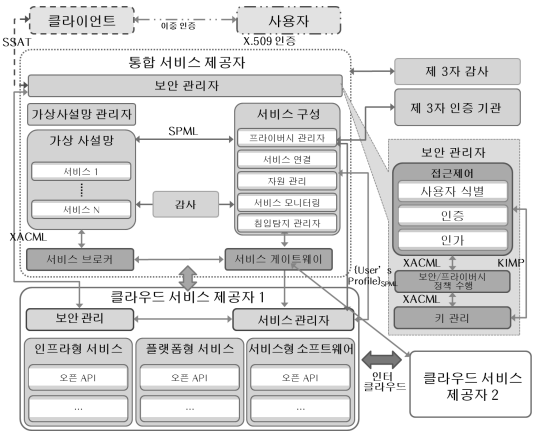
통합서비스 제공자는 다양한 퍼스널 클라우드 서비스의 중계자로서의 역할을 수행한다. 서비스 이용자는 퍼스널 클라우드 서비스 이용을 위하여 제3의 인증기관을 통해 등록된 정보를 바탕으로 다중 요소인증을 수행하고 통합 서비스 제공자는 제3의 인증기관의 인증 결과를 바탕으로 서비스 제공을 위한 익명성을 보장한다. 익명성 보장을 위해 필명과 같이 개인정보, 특히 제공정보가 포함되지 않은 이용정보를 생성한다.

클라우드 서비스 제공자는 토큰을 바탕으로 이용자를 특정 짓거나 구별할 수 없는 서비스 제공을 위한 아이디를 생성하고 이를 바탕으로 서비스를 제공한다.

제3의 감사자는 서비스 이용 중 필요한 제공 정보, 이용 정보에 대한 접근 또는 사용 없이 각 서비스 제공자, 제3의 인증 기관에서 정해진 법률과 정책에 입각하여 개인정보 생명주기 전반에 대한 관리 및 그 결과에 대하여 감사한다.



〔그림 5〕 개인정보보호 참조모델



〔그림 6〕 퍼스널 클라우드 보안 프레임워크

3.3. 퍼스널 클라우드 보안 프레임워크

퍼스널 클라우드 보안 프레임워크는 퍼스널 클라우드 참조 모델을 기반으로 접근제어, 개인정보보호, 서비스 감사 등의 퍼스널 클라우드 서비스를 이용하면서 필요한 모든 보안 시스템을 포함하고 있다.

사용자는 PDA, 랩톱 또는 모바일과 같은 다중인증을 제공하는 다양한 디바이스를 통해 클라이언트(예: 웹브라우저 또는 설치된 어플리케이션)에 접속한다. 통합서비스 제공자는 사용자에게 퍼스널 클라우드를 제공한다. 제 3의 인증기관 를 통해 다중 인증을 제공한다. 사용자 인증이 이뤄지면, SSAT(Single Sign Access Token)는 사용자 인증을 통해 생성된다. 그러면 사용자는 종단 사용자 서비스 포탈을 통해 서비스 공급자에 서비스를 요청하여 원하는 서비스를 제공받을 수 있다[7-9].

Ⅳ. 결 론

본 논문에서 퍼스널 클라우드 서비스 정의와 보안 기술에 대해 살펴보았다. 특히 각 보안기술들은 퍼스널 클라우드 참조 모델을 기반으로 하였기 때문에 서로 호환이 가능하고 기존의 보안 시스템의 보안 기술을 활용하여 호환성을 높였다.

그러나 현재의 클라우드 서비스는 각 기업에서 독자적인 클라우드 서비스를 경쟁적으로 제공하다 보니 많은 서비스들이 호환성이 낮은 서비스를 제공하게 되어 개인 사용자에게는 오히려 불편함을 초래하게 되었다.

이러한 문제들은 국내외에서 제정하는 표준 기술을 적용하여 호환성을 높이고 각 서비스 제공자에 독립적인 퍼스널 클라우드 서비스를 제공함으로써 해결될 수 있을 것이다. 또한 표준화 되어 있는 보안 프레임워크 및 기술들을 참조하여 퍼스널 클라우드 서비스의 특징을 고려한 보안 서비스를 제공할 수 있을 것으로 기대된다.

현재 국제 표준화 기관인 ISO, ITU-T에서는 클라우드 컴퓨팅에 대한 표준화는 아직 기본적인 단계에 머물러 있는 반면, 국내에서는 새로운 서비스 및 응용 기술에 대한 표준화가 진행되고 있어 원천기술을 선점할 수 있으며, 향후 국제 표준을 주도하기 위해서는 정부의 체계적인 정책지원이 필요하다.

참고문헌

[1] Jose Rivera, "*Cloud Computing for Personal Use*", The Epoch times, 2010

[2] Frank E, Gillett "*The Personal Cloud*" Forrester Research, 2009. 7.

[3] Michael Cooney, "*Gartner: Top 10 strategic technology trends for 2013*", ComputerworldUK, 2012

[4] TTA PG420 외, "*퍼스널 클라우드 서비스 정의 및 요구사항 분석*", TTAK.KO-10.0537, 한국정보통신기술협회, 2012

[5] TTA PG420 외, "*퍼스널 클라우드 컴퓨팅 접근제어*", 2011-388, 한국정보통신기술협회, 2012

[6] TTA PG420 외, "*퍼스널 클라우드 컴퓨팅 개인정보보호 참조모델*", 2011-389, 한국정보통신기술협회, 2011

[7] Cloud Security Alliance, "*Guidance for Identity & Access Management V2.1*" , 2009

[8] TTA PG420 외, "*퍼스널 클라우드 보안 프레임워크*", TTAK.KO-10.0533, 한국정보통신기술협회, 2011

[9] Zhang, Xinwen 외, "*Securing elastic applications on mobile devices for cloud computing*", CCSW '09, pp.127－134.

[10] David F. 외, "*Proposed NIST standard for role-based access control*", ACM Transactions on Information and Systems Security, 4(3): 224-274.

〈著者紹介〉

박 준 영 (Park Jun Young)
정회원

2010년 2월 : 한남대학교 컴퓨터공학과 졸업
2012년 2월 : 경희대학교 컴퓨터공학과 석사
2012년 3월~현재 : 경희대학교 컴퓨터공학과 박사과정
<관심분야> 클라우드 보안, 침입탐지, 프라이버시

나 상 호 (Na Sang Ho)
정회원

2008년 2월 : 경희대학교 컴퓨터공학과 졸업
2010년 2월 : 경희대학교 컴퓨터공학과 석사
2010년 3월~현재 : 경희대학교 컴퓨터공학과 박사과정
<관심분야> 클라우드 보안, 프라이버시

허 의 남 (Huh Eui Nam)
정회원

2002년 2월 : The Ohio University 전산학과 졸업(박사)
2002년~2003년 : 삼육대학교 컴퓨터공학과 조교수
2003년~2005년 : 서울여자대학교 컴퓨터공학과 조교수
2005년 ~ 현재 경희대학교 컴퓨터공학과 교수
<관심분야> 클라우드/그리드 컴퓨팅, 센서 네트워크, 네트워크 보안, 모바일 컴퓨팅, etc.