디지털산업정보학회 논문지 제12권 제1호-2016년 3월
http://dx.doi.org/10.17662/ksdim.2016.12.1.081

퍼스널 클라우드 환경에서 사용자 관리를 위한 보안 프레임워크의 설계 및 평가

진 병 욱*·김 종 화**·차 시 호***·전 문 석****

Design and Evaluation of Secure Framework for User Management in Personal Cloud Environments

Jin Byungwook · Kim Jonghwa · Cha Siho · Jun Moonseog

〈Abstract〉

Cloud computing technologies are utilized and merged in various domains. Cloud computing technology-based personal cloud service technologies provide mobility and free access by using user centered storages and smart devices such like smart phones and table PCs. Therefore, we should overcome limits on the storage by solving the capacity problems of devices to provide security services in the personal cloud environments It can be addressable to provide the convenience of various security technologies. However, there are some security threats inherited from existing cloud environments and the possibilities of information leakage when devices are lost or stolen. Therefore, we designed a framework for providing secure cloud services by adding objects, such as user authorization, access tokens, set permissions by key generation, and key management assignments, for user management in personal cloud environments. We analyzed the stability of the proposed framework in terms of irreverent use and abuse, access to insiders, and data loss or leakage. And we evaluated the proposed framework in terms of the security with access control requirements in personal cloud environments.

Key Words : Personal Cloud, User Management, Secure Framework, Permission Management

Ⅰ. 서론

최근 클라우드 컴퓨팅 기술 관련 시장이 폭넓게 확대되고 있고 2015년에는 2014년 대비 21%가 성장하여 그 규모가 거의 6800억 원 규모로 형성되고 있다. 대형 글로벌 업체들은 매년 클라우드 솔루션의 매출 비중이 높아지고 있으며, 하이브리드 관련 사업의 규모를 확대해 나가고 있다. 또한 스마트폰의 보급이 확대됨에 따라 개인 이용자를 대상하고 하는 스토리지 공간 서비스가 제공되어 사용자들에게 편의성을 제공하고 있다[1].

그러나 퍼스널 클라우드 환경은 프라이버시나 개인정보 등의 보안 문제에 대한 보안 위협이 발생할 수

* 숭실대학교 컴퓨터학과 박사수료
** 한화탈레스 전술통신팀 선임연구원
*** 청운대학교 멀티미디어학과 교수(교신저자)
**** 숭실대학교 컴퓨터학과 교수

있으며, PC 중심의 클라우드 서비스와 달리 다양화된 스마트 기기에서 데이터 및 콘텐츠에 대한 접근성이 요구될 수 있다. 따라서 퍼스널 클라우드 환경에서는 사용자 접근관리의 보안성이 요구된다[2]. 또한 퍼스널 클라우드 컴퓨팅은 기존 클라우드 컴퓨팅 환경에서 발생하는 보안위협을 그대로 포함하고 있으며 다양한 스마트 환경의 공격이 발생할 수 있다[3, 6].

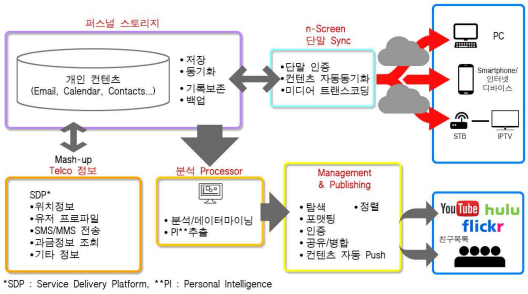
그러므로 본 논문에서는 이를 해결하기 위해서는 사용자 권한 부여, 접근 토큰, 권한별 키 생성 집합, 키 관리 배정을 추가하여 사용자 관리를 위한 보안 프레임워크를 설계하였다.

본 논문의 구성은 다음과 같다. 2장의 관련연구에서는 퍼스널 클라우드 서비스의 구성과 보안 요구사항에 대해서 기술하였다. 3장에서는 제안된 보안 프레임워크 및 서비스 수행 과정에 대해서 설명하였으며, 4장에서는 제안된 프레임워크의 안전성 분석 및 보안성을 비교 분석하였다. 5장에서는 결론 및 향후 연구방향을 제시하였다.

Ⅱ. 관련연구

2.1 퍼스널 클라우드 서비스의 구성

퍼스널 클라우드 서비스는 <그림 1>과 같이 서비스 범주와 2가지 필수 서비스로 구성되어 있다. 우선 서비스는 온라인 스토리지, 웹 기반 어플리케이션, 웹톱(WebTop)으로 구성될 수 있다. 사용자는 인터넷이 연결된 네트워크 환경에서 시간 및 장소에 제한을 받지 않고 개인화된 서비스를 이용할 수 있다는 특징이 있다. 또한 필수 서비스 요소는 개인화 콘텐츠 서비스와 프라이버시 서비스로서 사용자 개인의 정보, 데이터, 콘텐츠에 관한 안전성이 보장되어야 한다[3]. 퍼스널 클라우드 서비스를 구성하는 요소들에 대한 자세한 설명은 다음과 같다.



<그림 1> 퍼스널 클라우드의 서비스 구조

(1) 온라인 저장소(Online Storage)

온라인 저장소는 사용자가 언제 어디에서나 필요한 데이터를 업로드/다운로드할 수 있는 공간을 제공할 수 있는 서비스를 말한다. 그러나 중요 데이터는 바이러스, 다른 온라인 사용자의 악의적인 접근 또는 사용자의 부주의로 인한 손상에 대한 안전성이 요구되며, 실시간으로 서비스 할 수 있는 가용성을 보장받아야 한다[3-4].

(2) 웹 기반 어플리케이션(Web-Based Applications)

인터넷이나 인트라넷을 통하여 브라우저상에서 사용자가 손쉽게 이용할 수 있는 소프트웨어로 정의하고 있으며, 사용자의 사용량에 따라 수요가 점점 높아지고 있는 추세이다. 그로 인해 사용자가 사용을 원할 때 즉시 서비스를 제공하고 있으며, 사용자의 디바이스에 설치를 하지 않아도 유지할 수 있다는 장점이 있다[3-4].

(3) 웹톱(Webtop)

장소에 제약 없이 인터넷이 서비스가 되는 곳에서 사용자의 정보를 공유 기능을 통해 일관성 있게 지원할 수 있는 서비스를 말한다. 주소록, 전자메일, 파일을 사용자 정보 동기화를 통해 공유할 수 있다는 특

징이 있다[3].

(4) 개인화 콘텐츠 서비스(Personalized Content Service)

개인화 콘텐츠 서비스란 사용자의 메일 계정, 주소록, 일정 관리, 단말기 사용 이력과 같은 개인 정보와 사용자가 받은 미디어 콘텐츠, 공공용 콘텐츠의 관리 환경을 제공한다. 또한 관리 툴 및 개인화 검색 서비스를 제공하고 보유하고 있다. 그러나 각 디바이스 및 웹 서비스를 통하여 개인화 콘텐츠에 관한 관리 및 분산 시스템에 관한 서비스를 제공해야 한다[4].

(5) 프라이버시 서비스

개인 사용자 정보를 기반으로 서비스를 수행하고 있는 퍼스널 클라우드 서비스는 개인 정보 보호가 필요하다. 이로 인해 개인의 사용자 정보와 데이터 보호를 위하여 데이터를 송수신할 때 안전한 암호화를 수행하여야 한다. 또한 데이터 저장 및 관리 부분 측면에서 데이터 유출 및 유실이 발생하더라도 사용자의 데이터가 안전하게 보호되어야 한다[5].

2.2 퍼스널 클라우드 환경의 보안 요구사항

퍼스널 클라우드 환경에서의 주요 보안 요구사항들은 프라이버시 제공, 제3자의 인증기관, 제3자의 감사, 프라이버시 정책/접근 제어, 개인 서비스 네트워크라 할 수 있다. 이러한 보안 요구사항에 대한 자세한 설명은 다음과 같다[4, 7].

(1) 프라이버시(Privacy) 제공

퍼스널 클라우드 환경에서는 사용자의 콘텐츠 접근 및 공유에 대해서 안전한 관리가 요구되며, 사용자가 원하는 서비스에 맞춰서 알맞게 설정될 수 있어야 한다.

(2) 제3자의 인증기관

퍼스널 클라우드 서비스는 사용자의 정보를 기반으로 운영한다. 그러나 사용자의 정보를 제3의 기관에서 사용자 인증 후 식별 값을 통하여 활용되어야 한다[4].

(3) 제3자의 감사(Audit)

사용자의 이용 및 보안 정책에 따라서 올바른 서비스를 제공해주는 감사 기관이 필요하다. 신뢰된 제3자는 감사 기능에 따라 권한 부여를 수행할 수 있는 기능이 필요하다[4]. 서비스 제공, 데이터 및 프라이버시 보호, 환경에 알맞은 다중 암호화, 역할식별에 따른 제어기법이 요구되고 있다[9].

(4) 프라이버시 정책/접근제어

사용자의 직업, 역할, 정보에 따라 서비스의 권한이 다르게 부여된다. 사용자 정보 분석 후 역할에 따라 알맞은 권한 부여를 통하여 접근 제어 방법이 올바르게 정의되어야 한다[5, 8].

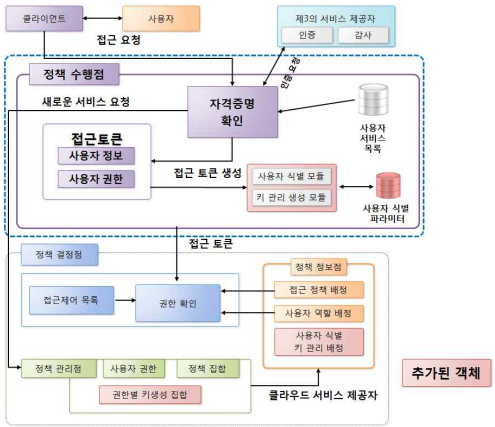
(5) 개인 서비스 네트워크

클라우드 서비스 환경이 발전하고 사용자들로부터 폭넓게 활용됨으로써 사용자 각각의 클라우드 서비스 환경이 구성된다. 그러나 정보 유출과 같은 피해가 발생하지 않도록 사용자를 위한 가상의 네트워크가 생성되어 안전하게 설정할 수 있어야 한다.

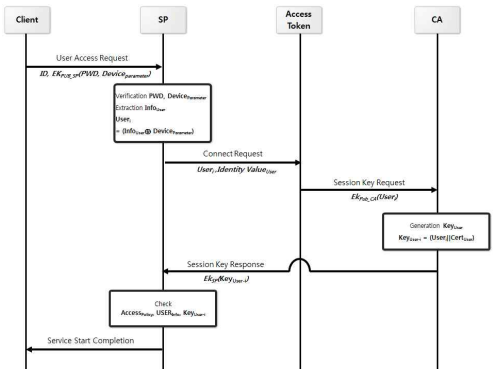
Ⅲ. 제안 보안 프레임워크 설계

본 논문에서 제안한 보안 프레임 구조는 <그림 2>와 같다. 퍼스널 클라우드 접근 제어 모델에서 빨간색 글자로 추가된 객체 및 모듈이 본 논문에서 제안한 프레임 워크로서 안전성 부분을 보완하였다. 추가

된 부분은 사용자 식별 모듈(User identity module), 키 관리 모듈 생성(Key management module generation), 사용자 식별(User identity), 키 생성에 의한 권한 집합(Permission set by key generation), 사용자 ID 관리 할당(Allocation of identity management of user)이다. 본 논문은 이들을 활용하여 사용자의 접근 제어 및 개인 프라이버시에 대한 정보 안전성을 강화하는 보안 서비스 수행절차에 대한 프로토콜을 설계하였다. <그림 3>은 본 논문에서 제안한 프레임워크에서 사용자에 대한 접근 제어 절차를 보인 것이다.



<그림 2> 제안된 보안 프레임 구조



<그림 3> 서비스 수행절차 과정

<그림 3>에서 보인 것과 같이 본 논문에서 제안한 프레임워크의 서비스 수행 절차는 다음과 같다.

1. 사용자는 클라이언트 디바이스를 통하여 통합 서비스 제공자에게 접근을 요청한다. 사용자가 초기의 접근을 요청할 때 ID, PW와 디바이스의 파라미터를 함께 전송한다.
2. 통합 서비스 제공자는 사용자의 자격 증명 확인(Verification of Credentials)을 위해 접근 토큰에 연결하여 사용자 정보를 확인한 후 사용자 파라미터를 활용하여 해쉬 값을 생성한다.

   $User_i = Hash(info_{User} \oplus Device_{Parameter})$
3. 사용자 ID와 PW를 이용하여 제3의 서비스 제공자로부터 인증을 수행한 후 인증 값을 부여받은 식별 값과 해쉬 값을 조합하여 사용자 권한 키(Key)를 생성한다.

   $Key_{User} = (User_i \| Cert_{User})$
4. 이후 클라우드 서비스 제공자는 정책 관리에서 키 생성에 의한 권한 집합을 확인한 후 결과 값을 정책 정보 객체로 데이터를 전송한다.

   $Data_{user-i} = User_i, Info_{User}$
5. 수신된 데이터를 받은 객체는 접근 정책, 사용자 역할, 사용자 식별 키 관리 값을 검색한 후 정책 결정 객체로 데이터를 전송한다.
6. 수신된 데이터를 받은 객체는 접근 제어목록을 확인한 후 사용자 권한에 알맞은 권한을 부여하여 서비스를 시작한다.

Ⅳ. 성능 평가

4.1 안전성 분석

본 논문에서 제안한 퍼스널 클라우드 환경에서 사용자 관리를 위한 보안 프레임워크에 대한 안전성은

TTAK. KO-10.0533[9]의 퍼스널 클라우드 환경에서 발생하는 공격기법을 기반으로 분석하였다. [9]에 기술된 대표적인 공격기법은 클라우드 컴퓨팅 남용 및 불손한 사용, 악의적인 내부자에 대한 접근, 데이터 유실/유출 등으로 이에 대한 분석 내용은 다음과 같다.

- 클라우드 컴퓨팅 남용 및 불손한 사용 : 악의적인 사용자가 클라우드를 도입하여 정보 관리에 피해를 입히고, 서비스 거부 공격을 수행하는 방법이다. 제안된 프레임에서는 사용자의 파라미터 값을 기반으로 생성한 $User_i$를 활용하여 위와 같은 공격을 무마할 수 있다.
- 악의적인 내부자에 대한 접근 : 정보 관리 측면에서는 권한이 없는 사용자의 접근으로 인하여 다양한 해킹과 공격들이 발생할 수 있다. 이를 해결하기 위해 사용자 접근 요청 과정에서 SP는 사용자의 정보를 분석한 후 정보를 검증한다. 이후 CA에서는 사용자의 정보를 기반으로 권한이 있는 사용자에게 Key_{user}를 부여한다.
- 데이터 유실 또는 유출 : 클라우드 컴퓨팅 서비스를 관리적인 측면에서 데이터 유실 및 유출에 대한 피해가 발생할 수 있다. 그러나 본 논문에서 제안한 프레임워크는 Key_{user}를 생성하여 서버 콘텐츠에 대한 올바른 접근 제어와 관리를 수행할 수 있다.

4.2 보안성 평가

본 절에서는 기존의 표준 프레임워크와 본 논문에서 제안한 프레임워크에 대하여 보안성을 비교분석하였다.

<표 1>은 앞에서 기술한 퍼스널 클라우드에 대한 접근 제어 요구 사항을 참고하여 비교 분석하였다. 기존 보안 정책과의 호환성에서는 클라우드 기반의 보안 정책 및 시스템을 활용하여 설계하였으므로 서비스의 제공이 가능하다. 또한 본 논문에서 제안한 퍼스널 클라우드 보안 프레임워크는 보안 요구사항의 사용자 데이터 관리를 적용하기 위하여 관련 표준기술인 KMIP(Key Management Interoperability Protocol) 기반의 키 관리 프로토콜과 사용자 식별 프로토콜을 설계하여 사용자 개인의 프라이버시를 보장하도록 하였다. 제안된 보안 프레임워크에서 클라우드 컴퓨팅 제공자 항목의 사용자 키 관리 배정, 권한 별 키 생성 집합을 설계하여 사용자로부터 독립적인 보안 정책을 수용할 수 있는 서비스를 제공하도록 설계하였다. 마지막으로 키 생성에 의한 권한 집합과 사용자 ID 관리 할당을 설계하여 SLA 기반의 접근 제어 정책을 수립하였다.

<표 1> 보안성 비교 분석[4-5]

	기존의 시스템	제안된 보안 프레임 워크
보안정책과 웹서비스의 유용성	지원	지원
독립적인 보안정책	지원안함	지원
프라이버시 보호	지원안함	지원
클라우드 서비스 레벨 협약	지원안함	지원

Ⅴ. 결론

본 논문에서는 퍼스널 클라우드 환경에서 사용자에 따른 권한 부여를 통하여 안전한 클라우드 서비스를 제공하기 위한 보안 프레임워크를 설계하였다. 제안된 프레임워크에서는 사용자의 식별 값을 접근 토큰에서 검증한 후 권한을 확인하여 서비스를 수행하는 방식을 사용하였다. 또한 사용자의 신원을 제3자로부터 인증을 수행하여 이를 기반으로 권한 키를 생성하여 권한을 부여하였다. 제안된 프레임워크의 타당성을 검증하기 위하여 본 논문에서는 클라우드 컴퓨팅 환경의 보안 요구사항을 기반으로 기존의 시스

템과 비교분석을 수행하였으며, 접근 제어 측면에서 발생하는 보안 위협에 관하여 안전성을 분석하였다. 그러나 제안된 시스템을 실제 클라우드 환경에 적용하기 위해서는 접근 제어와 권한 부여뿐만 아니라 메시지 전송 기법에 관한 연구가 필요하다. 또한 제안된 프레임워크를 세밀하게 설계 및 구현하여 효율성에 대한 비교분석이 필요하다. 따라서 향후 클라우드 컴퓨팅과의 융합된 환경에서 적용할 수 있는 프레임워크에 대한 추가적인 연구를 수행할 계획이며, 신규나 변종 보안 위협 사항에 대하여 안전한 통신을 수행할 수 있는 공격 유형에 따른 연구를 수행할 예정이다.

참고문헌

[1] 신동희, 김누리, “퍼스널 클라우드 기술동향,” 한국인터넷정보학회 학회지, 제15권, 제1호, 2014, pp. 38-473.

[2] Jose Rivera, “Cloud Computing for Personal Use,” the epoch times, 2010.

[3] Cloud Security Alliance, “Top threats to Cloud Computing v1.0,” 2010.

[4] TTAK. KO-10.0615, “Personal Clooud Access Control,” TTA, 2012.

[5] 최대선, 김승현, 진승헌, 이윤호, “스마트폰 환경에서 응용 보안을 위한 플랫폼 독립적인 보안 프레임워크,” 한국정보과학회 논문지, 제39권, 제1호, 2012, pp. 102-107.

[6] 신태환, 서광규, “국내외 클라우드 컴퓨팅 기반 융합사례,” 클라우드 지원센터, 2014.

[7] 양정모, “클라우드 컴퓨팅의 신뢰성 향상 방안에 관한 연구,” 디지털산업정보학회 논문지, 제8권, 제4호, 2012.

[8] 민소연, 진병욱, “차세대 무선 네트워크 환경에서 메시지 보호를 위한 통신 시스템 설계,” 한국산학기술학회 논문지, 제16권, 제7호, 2015, pp. 4884-4890.

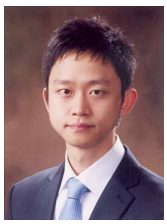
[9] TTAK. KO-10.0533, “Personal Cloud Security Framework,” TTA, 2011.

■ 저자소개 ■

진 병 욱
Jin Byungwook

2011년 3월~현재 숭실대학교 컴퓨터학과 박사수료
2011년 2월 숭실대학교 대학원 컴퓨터학과 (공학석사)
2010년 2월 청운대학교 멀티미디어학과 (문학사)

관심분야 : IoT, 인증 시스템, 접근제어
E-mail : quddnr4511@naver.com



김 종 화
Kim Jonghwa

2009년 1월~현재 한화탈레스 선임연구원
2009년 2월 고려대학교 전기전자전파공학부 (공학사)

관심분야 : IoT, 정보 보안, 빅 데이터
E-mail : jonghwa3. kim@hanwha.com

차 시 호
Cha Siho

2009년 3월~현재 청운대학교 멀티미디어학과 교수
1997년 7월~2000년 2월 대우통신 종합연구소 선임연구원
2004년 2월 광운대학교 대학원 컴퓨터과학과 (공학박사)
1997년 8월 광운대학교 대학원 전산계산학과 (이학석사)

관심분야 : 네트워크 관리, 차량통신 네트워크, 무선 센서 네트워크, IoT
E-mail : shcha@chungwoon.ac.kr

전 문 석
Jun Moonseog

1991년 3월~현재
숭실대학교 컴퓨터학과 정교수
1991년 2월 New Mexico State University
Physical Science Lab.
책임연구원
1989년 2월 University of Maryland
Computer Science 박사

관심분야 : 정보보호, 암호학, 네트워크 보안
E-mail : mjun@ssu.ac.kr

논문접수일: 2016년 2월 27일
수 정 일: 2016년 3월 11일
게재확정일: 2016년 3월 15일