퍼스널 클라우드 보안 Framework

윤가람, 이봉환
대전대학교 정보통신공학과
e-mail:kim03x@naver.com

Personal Cloud Security Framework

Ka-Ram Yoon and Bong-Hwan Lee
Department of Information & Commnun. Eng., Daejeon University

요 약

스마트폰 등 모바일 단말기의 보급이 확산되면서 퍼스널 클라우드 컴퓨팅을 이용한 개인화된 서비스에 대한 관심이 증가하고 있다. 퍼스널 클라우드 컴퓨팅 장점과 문제점인 기업의 기술과 서비스의 독점 및 종속성에 대한 문제점과 함께 보안 문제도 대두되고 있다. 본 논문에서는 퍼스널 클라우드에서의 보안 위협들을 살펴보고 보안 위협으로부터 대응을 위한 퍼스널 클라우드 보안 프레임워크를 제안하였다. 이는 향후 퍼스널 클라우드 서비스 제공 시 안전한 인프라를 설계하고 구현하는데 활용될 수 있을 것으로 예상된다.

1. 서론

퍼스널 클라우드(Personal Cloud)는 스마트폰, MID, PC, IPTV 등 개인의 디지털기기 종류가 증가하고, 블로그, 이메일, UCC, 소셜 네트워크 서비스 등 개인의 온라인 서비스가 급증하는 개인 정보화 시대에서, 모든 단말과 온라인 공간에 흩어져 있는 개인 콘텐츠를 클라우드 컴퓨팅 환경에 저장/통합/관리하여, 언제 어디서나 단말에 상관없이 독립적으로 접근할 수 있게 함은 물론, 콘텐츠의 분석 및 가공을 통해 고부가가치 개인화 서비스를 제공할 수 있게 해주는 미래 개인 컴퓨팅을 의미한다. 미래 IT 서비스 분야의 기본적인 인프라는 유무선 인터넷을 통합하는 웹(Web)이라 할 수 있다. 웹 환경에서 클라우드 컴퓨팅은 서비스를 제공하는 핵심 서비스 지원 기술로 진화 발전하고 있다. 이러한 진화 발전 과정에서 서비스를 지원받은 사용자 개인의 단말기의 형태도 기존의 개인용 데스크탑 PC에서 휴대와 이동이 가능한 UMPC(Ultra-Mobile PC), PDA, Netbook, Ipad 등으로 변천하고 있다. 최근에 휴대폰의 형태가 음성 통화와 단순 서비스의 피처(Feature)폰에서 스마트폰이라는 고기능 서비스의 지원이 가능한 모바일 단말기로 진화하고 있다[1].

따라서 퍼스널 클라우드는 서비스를 지원을 받기 원하는 모바일 단말기들을 그룹화하는 모델이라고 볼 수 있으며, 이러한 모바일 단말기들은 원하는 서비스를 클라우드를 통하여 지원받을 수 있다. 모바일 단말기에서 제공받는 서비스의 방법과 형태는 사용자의 능동적인 행동위에서 지원되는 것보다 클라우드 내에 있는 서비스 제공자의 능동적인 지원을 통하여 제공되는 형태이다. 현재 퍼스널 클라우드 환경에서 모바일 단말기 간에 서비스를 지원하기 위한 일부 모바일 어플리케이션들이 개발되어 적용되고 있다. 예를 들어, Mobile Gmail, Google Maps 및 일련의 네비게이션 응용 소프트웨어들이 이러한 모바일 클라우드 환경 내의 모바일 단말기에서 제공되고 있다. 하지만 퍼스널 클라우드는 클라우드 기술 특성상 다양한 보안 위협에 취약하다는 단점이 존재한다. 환경적으로도 관리가 쉽지 않은 지역에 분포되어 있는 경향이 많기 때문에 물리적인 공격을 비롯해 다양한 보안 위협 요인들을 잠재적으로 가지고 있다[1][2][3].

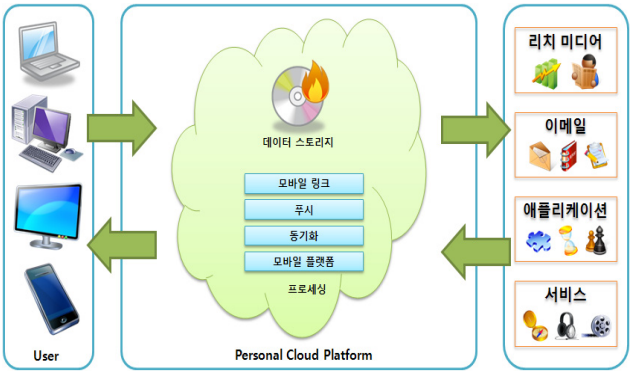
이러한 특성은 퍼스널 클라우드의 안전한 운영에 치명적인 오류를 일으키거나 잘못된 정보를 기반으로 서비스를 제공하게 되어 퍼스널 클라우드 서비스 자체를 무용지물화 시키는 결과를 초래할 수 있다. 이에 본 논문에서는 내·외부적인 위협 요소로부터 안전한 퍼스널 클라우드 구축을 위한 퍼스널 클라우드 보안 프레임워크를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 퍼스널 클라우드 구조를 살펴보고, 3장에서는 퍼스널 클라우드 보안 위협을 제시한다. 4장에서는 보안 프레임워크를 제안하고, 마지막으로 5장에서 결론을 맺는다.

2. 퍼스널 클라우드 컴퓨팅 서비스의 구조

퍼스널 클라우드 컴퓨팅은 클라우드 내에 크게 미디어 제공을 위한 데이터 스토리지 서버와 서비스를 처리하는 데이터 프로세싱 서버로 구성된다. 각 구성 요소들은 모바일 단말기에게 원하는 서비스 제공을 하는 인프라스트럭쳐 역할을 담당한다. 단말기 내에 내장되는 많은 응용 소프트웨어들은 혼자만이 동작되는 단순 응용 프로그램이 아닌 클라우드 내에 있는 서버들의 지원을 받아 원하는

서비스를 지원받는 형태 등으로 진화되고 있다. 즉 단말기 내의 저장 공간과 처리 기능을 활용하여 일부 기능은 수행하고, 클라우드 내의 서버들로부터 추가적인 기능을 지원 받아 서비스가 이루어진다. 그림 1은 퍼스널 클라우드 컴퓨팅의 서비스 구조를 나타낸다[1].



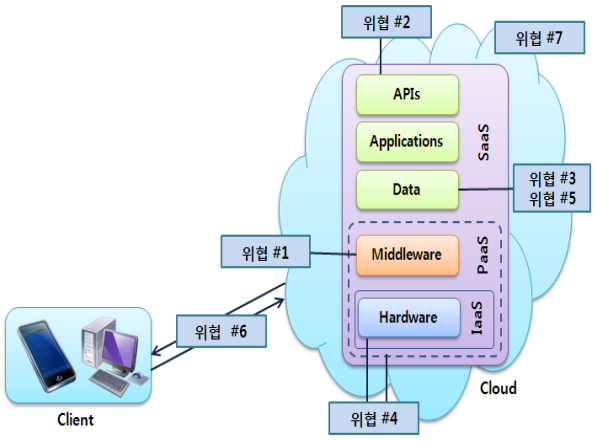
[그림 1] 퍼스널 클라우드 서비스 구조

그림 1과 같이 퍼스널 클라우드 서비스는 사용자의 각 디바이스 및 웹 서비스를 통해 분산되어 있는 개인 컨텐츠를 통합·저장하고 관리할 수 있는 환경을 제공하며, 컨텐츠 자동 변경(Contents Auto Revision) 기능을 통해, 한 기기에서 정보를 변경하면 변경된 정보를 클라우드(중앙 서버)로 보낸 다음 등록된 다른 모든 기기에 자동 업데이트를 하게 된다. 또 개인 콘텐츠 관리 쿨을 제공하고, 개인화된 검색 (검색, 위치 기반 자동 분류, 추천 등)을 가능하게 하기도 한다. 미래의 퍼스널 클라우드 컴퓨팅은 모바일 단말기의 저장 공간과 처리 능력을 확장하여 언제, 어디서나 필요한 데이터와 콘텐츠에의 접근을 허용하고 유니버설 프로세싱 기능을 지원하는 환경을 제공할 것이다.

3. 퍼스널 클라우드 보안 위협

퍼스널 클라우드 인프라에서 고려되어야 할 퍼스널 클라우드 컴퓨팅의 보안 위협 요소는 다음과 같이 7가지로 나눌 수 있다[5].

■ 위협 #1 : 클라우드 컴퓨팅의 오용과 비도적적인 사용 (Abuse and Nefarious Use of Cloud Computing)
- 악의적 목적으로 클라우드 도입 시, 가상공간에 정보가 존재하는 특성으로 기존 봇넷(botnet)보다 더욱 높은 위험성이 잠재



[그림 2] 퍼스널 클라우드 보안 위협[6]

■ 위협 #2 : 불안전한 인터페이스와 응용 프로그래밍 인터페이스 (Insecure Interfaces and APIs)
- 부가 가치 제공을 위하여 기존 코드의 재사용의 합성을 통한 응용프로그램 구축 시 복잡도 증가에 의한 보안 취약성 발생 가능

■ 위협 #3 : 악의적인 내부자 (Malicious Insiders)
- 클라우드 서비스 직원 채용 지침/기준의 부재로 해커, 조직범죄 등 악의적 목적을 지닌 사람의 채용가능성 증대는 서비스 내 데이터 유출 위험 발생

■ 위협 #4 : 기술 공유 문제(Shared Technology Issues)
- 인프라형 서비스 사업자는 공유 기술을 바탕으로 확장성을 제공하나, 다중 애플리케이션 아키텍처를 위한 효과적인 자원의 분리가 이루어지지 않을 경우 존재

■ 위협 #5 : 데이터 유실 또는 유출 (Data Loss or Leakage)
- 클라우드 환경의 구조적/운영적 특성으로 데이터 유출 위험 증가 (다양한 원인 존재)

■ 위협 #6 : 계정/서비스 하이잭킹 (Account of Service Hijacking)
- 피싱, 사기, 소프트웨어 취약성을 이용한 계정 접근은 일반적인 상황이며, 클라우드 환경에서의 계정정보의 유출은 모든 것을 내주는 것과 동일한 위협

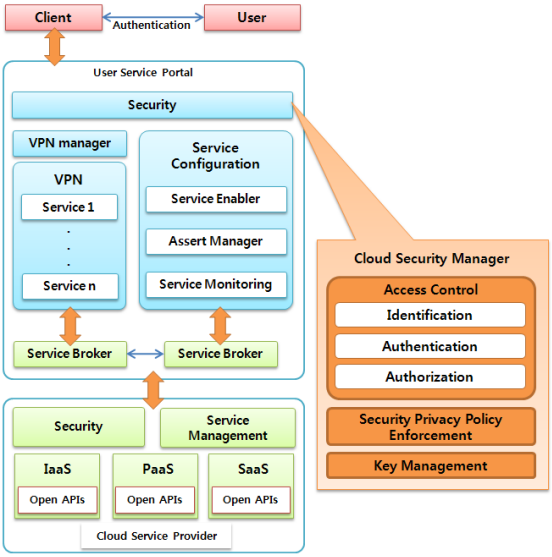
■ 위협 #7 : 알려지지 않은 위협 프로파일 (Unknown Risk Profile)
- 소프트웨어 버전, 코드 업데이트, 취약성 프로파일, 침입 시도 등은 기업의 보안현황 점검에 필수 요소

4. 퍼스널 클라우드 보안 프레임워크

전문가들은 3가지 클라우드 모델의 노출과 수위는 크게

다르므로, 어떤 계층에 대한 작업을 하고 있는지에 따라 보안을 해결하는 방법도 달라야만 한다는 점도 강조하고 있고, 보안 요구조건은 실제로 똑같지만, SaaS에서 PaaS나 IaaS로 옮겨가면 확보하고 있는 보안 제어 수준이 달라지고 논리적인 관점에서 보면 바뀐 것은 아무것도 없지만 물리적으로 어떻게 하는지가 바뀌게 된다. 서비스형 소프트웨어(SaaS)에서는 응용프로그램과 리소스 및 서비스 통합 문제, 사용자 데이터 관리, 접근제어, 리소스 모니터링에 대한 문제에 주의할 필요가 있다. 플랫폼형 소프트웨어(PaaS)에서는 접근제어에 대한 문제와 인프라형 소프트웨어(IaaS)에서는 서비스 인프라 관리 기술에 대한 문제를 보호할 필요가 있다. 클라이언트(단말)에서는 아이디 및 접근 제어, 응용프로그램 보안, 암호화 및 키관리에 대한 보안 대책이 요구된다[2][4].

그림 3은 퍼스널 클라우드에서의 3가지 모델(SaaS, PaaS, IaaS)에 따른 보안 프레임워크를 나타낸 것이다.



[그림 3] 퍼스널 클라우드 보안 프레임워크

5. 결론

클라우드 기술을 적용한 산업 및 서비스가 증가하는 상황에서 컴퓨팅 기술의 역할이 중요해지고 있고, 이와 관련하여 보안의 중요성 또한 증가하고 있다.

이에 본 논문에서는 퍼스널 클라우드 관련 보안 위협들을 분석하고 보안 위협으로부터 대응을 위한 퍼스널 클라우드 보안 프레임워크를 제안하였다. 이는 향후 퍼스널 클라우드 적용 시 안전한 인프라를 설계하고 구현함에 있어 참고 자료로 활용될 수 있을 것으로 사료된다.

Acknowledgement

본 연구는 한국연구재단의 지역혁신인력양성사업 및 한국산업기술평가관리원의 산업원천기술개발사업의 일환으로 수행된 연구결과임.

참고문헌

[1] 윤용익, 김스베를라나, “모바일 클라우드 컴퓨팅 기술 동향”, 정보통신산업진흥원 주간기술동향 통권 1429호, 2010. 3. 31.

[2] 은성경, 조남수, 김영호, 최대선, “클라우드 컴퓨팅 보안 기술”, 전자통신동향분석 제24권, 제4호, 통권 118호, pp.79-88, 2009년 8월.

[3] 이강찬, 윤용익, “모바일 클라우드 컴퓨팅”, OSIA standards & technology review, 2010년 제1호 제38권 통권76호, pp.28-40, 2010년 3월.

[4] 은성경, “클라우드 컴퓨팅 보안 기술 동향”, 情報保護學會誌 第20卷, 第2 號, 2010. 4.

[5] 임철수, “클라우드 컴퓨팅 보안 기술”, 정보보호학회지, 제 19권, 제 3호, pp 14-17, 2009년 6월.

[6] ″Cloud Security Alliance″, December 2009.