클라우드 서비스의 프라이버시 침해 요인에 관한 연구★

전정훈*

요 약

최근 클라우드 컴퓨팅 기술은 전 세계적으로 중요한 이슈로 부각되고 있으며, 기술과 서비스에 있어, 많은 주목을 받고 있다. 또한 클라우드 서비스는 기존의 웹 사이트(web site)를 이용한 단순 서비스 형태에서 여러 모바일 기기 및 통신 서비스(카카오톡, 페이스북 등)들을 이용한 다양한 유형의 형태로 진화해 가고 있다. 특히 서비스를 이용한 사용자 정보의 수집이 용이하게 됨에 따라, 사용자의 취향 및 선호도를 함께 분석할 수 있게 되었으며, 여러 장점들로 인해 점차 우리의 생활 깊숙이 자리잡아가고 있다. 그러나 클라우드 컴퓨팅의 긍정적인 측면과는 달리, 여러 취약점들로 인해, 해킹기술의 진화에 따른 다양한 공격과 피해가 예상되고 있다. 따라서 본 논문은 클라우드 서비스의 프라이버시 위협 요인에 대해 취약성과 공격 사례연구를 분석함으로써, 향후, 클라우드 컴퓨팅 서비스의 프라이버시 보안과 대응을 위한 자료로 활용될 것으로 기대한다.

A study on the Privacy threats factors of Cloud Services

Jeon Jeong Hoon*

ABSTRACT

Recently, The cloud computing technology is emerging as an important issue in the world, and In technology and services, has attracted much attention. Cloud services have evolved from simple forms to complex forms(using multiple mobile devices and communication services(Kakao talk, Facebook, etc.). In particular, as the cloud is especially facilitated the collection of user information, it can now be analyzed with the user's taste and preference. And many of the benefits of the cloud became increasingly closely with our lives. However, the positive aspects of cloud computing unlike the includes several vulnerabilities. For this reason, the Hacking techniques according to the evolution of a variety of attacks and damages is expected. Therefore, this paper will be analyzed through case studies of attack and vulnerability to the privacy threats factors of the cloud computing services. and In the future, this is expected to be utilized as a basis for the Privacy security and Response.

Key words : Cloud computing services, Privacy Threats factors, Cloud computing security, Security vulnerability

접수일(2015년 8월 31일), 수정일(1차: 2015년 9월 15일), 게재확정일(2015년 9월 25일)

★ 본 논문은 2014년도 동덕여자대학교 학술연구비 지원에 의하여 수행된 것임.

* 동덕여자대학교/컴퓨터학과

1. 서 론

최근 클라우드 컴퓨팅(cloud computing) 기술은 다양한 서비스 형태로 일상생활에 깊숙이 자리 잡아 가고 있다. 이러한 가운데 스마트 기기(smart device)의 보급은 정보의 신속함과 편리함 등 다양한 클라우드 서비스를 확산시키는데 전파 매체로서 매우 큰 역할을 수행하고 있다고 해도 과언이 아니다. 이러한 스마트 기기들 중 높은 보급률을 갖고 있는 스마트폰의 경우, 클라우드 컴퓨팅의 장점인 편의성과 신속성, 이동성, 호환성 등 서비스 확산에 필요한 조건들을 모두 만족시키고 있어 보다 넓은 사용자층을 확보하며, 매우 큰 전파매체로서의 역할을 수행하고 있다. 그러나 클라우드 서비스의 보급과 확산에 걸림돌이 되었던 보안 문제는 아직까지 미흡한 상태로 지속적인 보완을 필요로 하고 있다. 이러한 보안 문제는 공격자들에게 새로운 서비스의 등장이 새로운 취약점들을 제공하는 요인이 되고 있으며, 서비스의 개발과 함께 공격기법과 기술도 함께 진화하고 있음을 반영해 준다. 특히 클라우드 서비스는 복잡한 구조와 처리, 가변적인 연결 상태 등 여러 부분에서 기존 네트워크 기술과 차이를 갖고 있으며, 이러한 차이는 기존의 보안 기술만으로 대응을 어렵게 할 뿐만 아니라, 가상화 서비스(virtualization service)로 인해 법용적인 대응 기술 개발을 어렵게 하는 요인이 되고 있다. 이와 같은 요인들 중, 몇몇 글로벌 기업들은 클라우드 기술 개발을 주도하고 있어, 특정기업의 보안 기술 독점화에 대한 우려와 다양한 보안기술 개발에 걸림돌이 되고 있다. 이러한 가운데 현재 사용되고 있는 클라우드 서비스의 개인 프라이버시(privacy) 문제는 가장 큰 문제로 대두되고 있으며, 이에 대한 대응방안 마련이 시급한 실정이다.

따라서 본 논문은 클라우드 컴퓨팅의 프라이버시 침해 요인에 대한 분석을 통해, 향후, 클라우드 컴퓨팅의 보안 체계에 필요한 자료로 활용될 수 있을 것으로 기대한다. 연구내용에 대한 논리적 근거를 위해서, 논문의 2장은 클라우드 컴퓨팅 서비스와 보안 동향에 대해 알아보고, 3장은 클라우드 서비스의 프라이버시 침해 요인들을 분석한다. 그리고 4장은 클라우드 서비스의 침해 요인들에 대한 대응 기술들에 대해 알아보고, 5장의 결론 부분으로 이글을 마치도록 한다.

2. 관련 연구

2.1 클라우드 서비스 동향

클라우드 컴퓨팅 서비스는 표1과 같이 기본 유형에서 다양한 유형으로의 이뤄지고 있다. 기존의 클라우드 서비스는 IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service)로 분류되고, 운영 형태에 따라, 퍼블릭(public)과 프라이빗(private), 하이브리드(hybrid) 클라우드로 구분되고 있다[1]. 그러나 최근의 클라우드 서비스는 활용범위의 확장과 새로운 기술 및 서비스의 개발로 유형 및 분류의 범위를 확장해 가고 있으며, 클라우드의 주요 기술인 가상화(virtualization)와 공유 (share)및 임대(tenancy) 기술들은 각종 기기에 최적화된 서비스 형태로 다양한 서비스와 콘텐츠의 개발로 이어지고 있다.

<표 1> 클라우드 컴퓨팅 서비스[1]

구분		주요개념
서비스유형	IaaS(Infrastructure as a Servi ce)	하드웨어 자원 임대·제공
	PaaS(Platform as a Service)	플랫폼 임대·제공
	SaaS(Software as a Service)	소프트웨어 임대·제공
서비스운용형태	Public Cloud	불특정 다수 대상
	Private Cloud	기업 및 기관 내부
	Hybrid Cloud	결합형태

이에 대해 최근 비즈니스 측면에서 가장 매력적으로 다가오고 있는 클라우드 컴퓨팅의 주요 특성들로 [2]는 다음과 같이 요약하고 있다.

① 클라우드는 IT 서비스 중심의 접근성으로 사용자는 네트워크나 시스템 기타 환경 등에 신경을 쓰지 않고도 서비스를 즉시 사용할 수 있

으며, 간단하게 접근이 가능하다.

이러한 점은 신속한 서비스의 사용은 이를 지향하는 사용자들에게 있어, 편의성과 신속성을 제공해 주며, 다양한 서비스를 쉽게 접근할 수 있도록 하는 장점을 갖고 있다.

② 주문형 셀프 서비스 기반의 사용은 사용자들에게 서비스 제공자들로부터 자원을 제공받아 그들의 비즈니스 서비스에 대한 업로드, 구축, 적용, 스케줄, 관리 등에 대한 설정만으로 가능하다.

이와 같은 클라이드 서비스는 제공자가 사용자의 취향과 사용 목적을 명확히 분석한 맞춤형 서비스를 제공함으로써, 사용자들은 단순 조작만으로도 쉽고, 간단히 사용할 수 있도록 하는 장점을 갖고 있다.

③ 소비기반의 청구 및 측정 서비스를 통해 서비스 제공자는 소비자가 요청하는 서비스에 대해 모든 것을 제공하며, 이에 대한 청구와 서비스만 제공하면 되도록 단순화 되어 있다.

클라우드 사용자는 다양한 서비스를 사용하며, 이에 대한 청구와 결재를 손쉽게 할 수 있도록 함으로써, 제공자 및 사용자의 편의성과 신속함, 정확성을 제공하는 장점을 갖고 있다.

④ 리소스 풀링 및 광범위한 네트워크 접근성으로 사용자는 브라우저만을 가지고 간단한 접근이 가능하다.

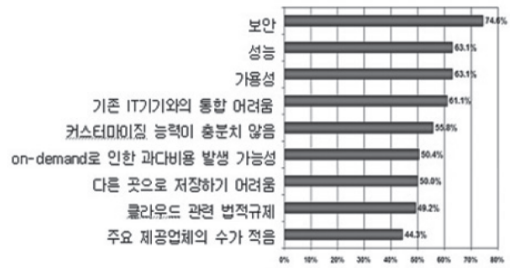
사용자는 브라우저의 간단한 조작만으로 다양한 서비스를 선택 및 사용할 수 있도록 함으로써, 사용자의 서비스 복잡한 사용방법에 대한 두려움을 없애고 시도의지를 이끌어내는 장점을 갖고 있으며, 간편한 조작을 유도하고 있다.

⑤ 빠른 확장성은 가장 중요한 요소 중에 하나로써 단순성과 스피드로 서비스의 향상성을 꾀할 수 있다.

이러한 특성들은 클라우드 서비스의 다양한 콘텐츠나 서비스를 단순한 방법으로 접근성을 높이고, 이에 따른 서비스 이용 빈도를 높일 수 있는 장점을 포함하고 있다. 이와 같은 클라우드의 주요 특성들은 향후, 클라우드 서비스를 응용한 비즈니스 모델 구축과 다양한 서비스의 개선, 관련 기술의 동반 성장 등이 전망되고 있다.

2.2 클라우드의 보안 동향

클라우드 보안에 관련해서는 다양한 취약 요인들과 이에 따른 보안 대응에 대해 CSA(cloud security alliance)를 비롯한 여러 연구단체와 전 세계 글로벌 기업들은 대응과 보완을 통해 지속적인 관심을 갖고 있다.



(그림 1) 클라우드 컴퓨팅 사용으로 발생가능한 문제점[3]

이에 대해 [3]은 그림1과 같이 클라우드 컴퓨팅 사용으로 인한 발생가능한 문제점들에 대해 2008년 IDC 자료를 인용하고 있는데 이를 살펴보면, 보안 위험성이 가장 큰 비중을 차지하고 있음을 알 수 있다. 또한 [3]은 이와 함께 클라우드 컴퓨팅의 보안위협에 대해 7가지로 축약해 다음의 표2와 같이 기술하고 있다.

<표 2> 클라우드 컴퓨팅 서비스의 보안위협[3]

- 클라우드 컴퓨팅 서비스의 남용과 불손한 사용
- 안전하지 않은 인터페이스와 API
- 악의적인 내부자들
- 기술문제의 공유
- 데이터 손실
- 계정이나 서비스의 트래픽 하이재킹
- 공개되지 않은 위협

이와 함께 2012년 CSA는 추가적으로 다음 표3과 같은 위험들을 경감해 갈 것을 권고하였다.

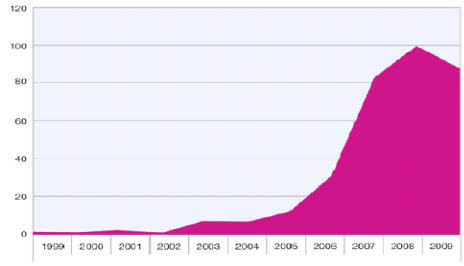
〈표 3〉 CSA 권고사항[3]

- 해당 로그와 데이터의 공개
- 인프라 세부 정보의 공개(패치 수준이나 방화벽)
- 모니터링 및 경고의 보강

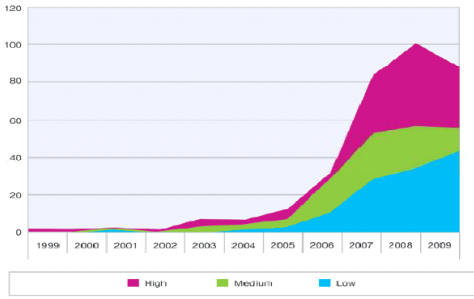
이러한 클라우드 컴퓨팅의 보안 위협과 위험들로 인해 표준화의 필요성이 높아지면서 제공업체 및 국가들은 다음과 같은 표준화 기구들을 구성하게 되었다. 이러한 클라우드 컴퓨팅의 표준화 기구들에는 OCC(open cloud consortium)와 OGF(open grid forum), CCIF(cloud computing interoperability forum), CSA(cloud security alliance), DMTF (distributed management task force), SGCC(study group cloud computing) 등이 있으며, 이러한 기구들에서는 각종 클라우드 컴퓨팅에 관련한 서비스 기술 개발, 표준모델의 제시, 보안, 각종 보안 위협에 대해 경고 및 대응 방안들을 마련하고 있다[3]. 그러나 클라우드 컴퓨팅은 기존 보안 기술의 가상화 환경 적용 시, 한계점으로 인해 새로운 문제에 직면하게 되면서, [4]는 이에 대해 가상화 환경에서의 주요 보안 이슈로 다음 3가지를 지적하고 있다.

- 첫째, 가상화 시스템 내부 영역은 기존 방화벽과 IPS, 안티바이러스 등 기존 보안기술로 보안 탐지를 할 수 없다.
- 둘째, 가상화 시스템 내부 영역에서는 다중 임대의 특성을 가진 서로 다른 이용자 그룹들의 가상머신들이 상호 연결되어 다양한 해킹, 악성코드 전파 등 공격경로 발생이 가능하다.
- 셋째, 가상 머신의 동적인 라이프 사이클로 인해 보안 관리가 복잡해진다.

그리고 [5]는 그림2와 3과 같이 클라우드 컴퓨팅의 가상화와 시스템 취약성의 증가추세를 언급한 것으로 1999년부터 2009년까지의 가상화 취약성 발견건수를 나타내고 있어, 가상화에 따른 보안문제의 심각성을 뒷받침해주고 있다.



(그림 2) 가상화 취약성 노출 동향[5]



(그림 3) 가상화 시스템 취약성[5]

최근 가상화 환경에 부합되는 보안시스템 개발이 활발히 진행되고 있으나, 정형화되거나 표준화가 필요한 상황에서 몇몇 글로벌 기업들에 의한 주도적이며, 의존적인 개발로 전 세계 시장을 점유해나가고 있다. 이는 특정 기업의 독점화와 서비스 및 보안기술의 표준화를 저해하는 요인이 되고 있으며, 나아가 대응기술 개발에 걸림돌로 작용할 수 있어 클라우드 서비스의 표준화가 필요함을 알 수 있다.

3. 프라이버시의 침해요인 분석

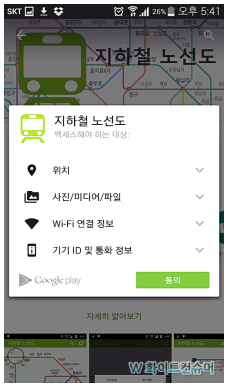
최근 클라우드 서비스는 몇몇 글로벌 기업들에 의해 주도되고 있는 것이 사실이다. 이러한 글로벌 기업들은 자체 독자적인 서비스의 개발뿐만 아니라, 유사 서비스들을 제공하고 있지만, 이에 따른 보안체계도 서로 달리 개발 및 적용하고 있다. 국내 클라우드 서비스 또한 대형 통신사들을 비롯한 포털 서비스 기업들을 주축으로 자체 개발된 서비스와 보안체계로 운용하고 있다. 이러한 상황에서 클라우드 서비스 기업들의 가상화에 따

른 보안 문제를 평가 및 언급하기에는 다소 어려움이 있다. 따라서 클라우드 서비스의 공통적이며 보편적인 사용자 프라이버시 침해요인들에 대해 분석한다.

3.1 고객정보의 수집방법에 따른 요인

국내의 경우, 클라우드 서비스 사용자 확보를 위해 기존 사용자들에게 새로운 클라우드 서비스로 전환을 요청 및 강제하는 형태로 이뤄지고 있다. 대표적인 고객정보 수집방법으로는 웹과 스마트 기기를 이용한 수집 방법을 예로 볼 수 있으며, 대부분 기존 가입자에게 서비스 종료에 따른 전환 또는 로그인 방식의 통합 등을 이유로 클라우드 서비스의 사용을 강제하도록 유도하고 있다. 이와 같은 서비스 강제에 의한 고객확보 방법은 클라우드 서비스에 대한 보안 문제와 고객정보의 안전성 문제에 대한 사용자의 서비스 사용 선택권을 침해하는 부분이 되며, 사용자는 클라우드 서비스에 대한 안전성 판단 기회를 박탈당함으로써, 1차적인 개인정보 대응을 어렵게 하는 요인이 되고 있다.

3.2 수집 정보의 일방적 동의에 따른 요인



(그림 4) 정보[7]

(그림 5) 정보[8]

국·내외 클라우드 서비스는 앱을 활용한 서비스제공을 하고 있으며, 서비스 사용을 위해 그림4, 5와 같이 제공자가 요구하는 수집정보에 대해 동의를 해야만 서비스를 사용할 수 있도록 하고 있다[7][8]. 수집정보는 무선 단말기기의 각종 정보 및 위치정보, 사용자의 프라이버시 관련 정보, 사진 및 동영상, 파일, 전화통화 상태, ID 등을 포함하고 있으며, 서비스에 따라 요청 정보는 차이를 갖는다. 그러나 이와 같은 수집정보에 대한 제공자의 동의 거부 시, 서비스를 사용할 수 없도록 하고 있어, 사용자의 일방적인 선택이 불가피한 상태이다. 그리고 이러한 사용자 정보 수집은 무료 유용한 앱(app)이나, 게임 등을 이용해 수집되고 있다. 이는 제공자의 불필요한 정보수집요구임에도 불구하고, 사용자는 무조건 동의를 해야 하며, 사고발생시 사용자에게 책임을 전가하려는 의도로 해석해 볼 수 있으며, 나아가 고의적으로 제공자가 수집하고자 할 경우에는 사용자의 대응이 매우 어려운 상황이 된다. 이와 같은 정보수집방법은 사용자에 의한 1차 대응을 저해하는 침해 요인이 되고 있다.

3.3 수집정보의 공유에 따른 요인

클라우드 서비스 제공자는 사용자에게 어느 정도의 신뢰성을 제공하느냐에 따라 시장 주도에 있어 중요한 요인으로 작용하기 때문에 고객 정보의 관리는 매우 중요하다. [6]은 글로벌 제공업체를 사례로 개인정보의 저장 위치와 정부기관의 의한 누출 문제를 다루면서 수집된 개인정보의 저장위치 및 취급자에 따른 유출 문제와 중요성에 대해 법률적인 관점에서 접근하고 있다. 여기서 수집정보에 따른 국내 클라우드 서비스의 취약 요인들을 살펴보면, 기존 서비스 제공자와 클라우드 서비스 제공자가 다를 경우, 고객정보의 공유로 인한 고객정보의 유출문제는 불가피하다. 또한 최근 앱들은 클라우드 서비스 제공기업의 로그인 정보를 이용한 인증방법을 사용함으로써, 로그인 정보의 공유하고, 스마트기기 상에 저장하도록 하는 방식을 사용자가 선택하도록 하고 있는데 이와 같은 방식은 인증정보를 악용한 공격이 예상되며, 침해 요인이 되고 있음을 알 수 있다. 따라서 제공자는 애플과 구글의 사례에서와 같이 서비스 업그레이드로 인한 고객정보의 관리 및 서비스 통합에 따른 인증정보의 공유문제에

대해 침해 요인의 분석을 통한 새로운 인증기술의 개발 및 도입이 요구되는 상황이다.

3.4 서비스 및 시스템 관리에 따른 요인

클라우드 서비스는 원활한 서비스와 가입 사용자의 수에 따라 스토리지(storage) 및 고성능 시스템으로의 업그레이드, 망의 설계 변경 등의 예기치 못한 여러 변경 상황들을 예상해 볼 수 있다. 그리고 시스템 업그레이드 및 망 변경, 서비스 추가 등의 부득이한 유지보수 작업이 요구될 수 있어, 외부업체의 참여로 인한 공개 및 공유 등의 업무협조로 인해 사용자 정보의 접근 대상이 확대됨에 따라 유출 위험을 높이는 요인이 되고 있다. 따라서 이러한 침해 대응을 위해서는 클라우드의 가상화 환경에 부합되는 보안 시스템 개발 등은 현실성을 고려하여 개발되어야 한다.

3.5 무선 취약성에 따른 요인

클라우드 서비스는 유무선 통신망에서 모두 제공되고 있으나 대부분 스마트기기를 통해 사용되고 있다. 특히 스마트폰은 클라우드 서비스의 대표적인 활성화 기기이다. 스마트기기는 편의성과 이동성, 신속성을 모두 제공할 수 있으며, 간단한 앱의 설치만으로 사용자는 서비스를 간편하고, 신속하게 설치 및 사용할 수 있다. 그러나 이미 알려진 무선 보안의 취약점 및 공격사례들로 인해 클라우드 서비스는 이미 공격에 노출되어 있으며, 실제 정보유출 사고가 증가하고 있다[9][10]. 따라서 클라우드 서비스는 무선 보안 취약성에 대한 대응기술 개발과 사용자의 프라이버시 침해에 대한 대응 방안이 함께 고려되어야 한다[11].

3.6 보안시스템에 따른 요인

클라우드 서비스 환경은 가상화와 공유, 임대 서비스뿐만 아니라, 시스템 자원의 공유형태 등 기존 유선망과의 차이를 갖고 있다. 그리고 몇몇 글로벌 기업들에 의해 서비스 및 보안 기술 개발이 주도되고 있어, 기술의존성(dependency)에 따른 독과점이 매우 높다. 이로 인해 클라우드 서비스에 관련한 호환성 및 이식성이 매우 미흡하며, 다양한 공격에 대응하기 위해서는 클라우드 서비스와 보안기술의 표준화가 절실히 필요한 상황이다. 따라서 프라이버시 보호를 위한 보안시스템의 개발이 미흡한 현실을 고려해 볼 때, 보안시스템은 개인정보의 중요한 유출요인이 되고 있음을 알 수 있다.

4. 프라이버시 침해대응

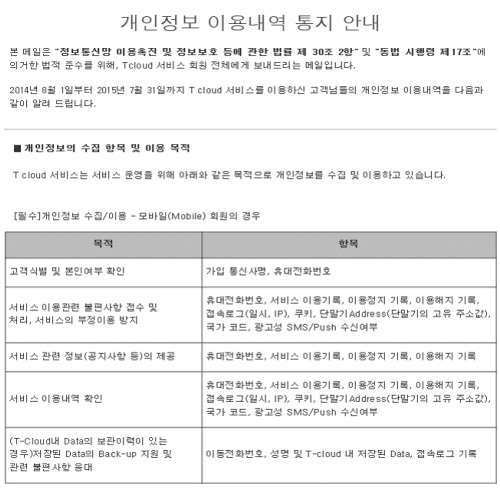
<표 4> 한국인터넷진흥원 IaaS 환경 점검 리스트[12]

보안취약성	모바일 웹	· 어플리케이션 변조
		· 입력값 검증
		· 암호화 통신 여부 확인
		· 개인정보취급방침 게시 및 수집 동의 구현
		· 비정상(탈옥, 루팅)단말기의 실행제한
		· 중요정보 평문저장
	웹	· 명령어 삽입 가능성
		· Cross Site Scripting
		· SQL Injection
		· 쿠키 스니핑/조작 가능성
		· 디렉터리 인덱싱
		· 관리자 페이지 접근
		· 백업파일
		· 디폴트 페이지
		· 파일 업로드
		· 파일 다운로드
		· 인증우회
		· 히든필드 점검
		· 취약한 계정/패스워드
		· 에러처리 미흡
		· 사용자 개인정보 노출 취약점
		· 기타 취약점
	어플리케이션	· 어플리케이션 변조
		· 입력 값 검증
	공통	· 중요정보 노출
		· 인증 처리

최근 클라우드 컴퓨팅은 제공자와 사용자 모두에게 있어, 신뢰가 보장되어야한다. 그러나 클라우드 컴퓨팅 서비스의 다양한 보안 취약성들이 알려지면서, [12]는 표 4와 같이 모바일과 웹, 어플리케이션 등에 따라 점검 리스트를 작성하고, 체계적이며 지속적인 관리의 필요성을 강조하고 있다. 이에 대해 3장에서는 클라우드 컴퓨팅 서비스에 따른 프라이버시 침해 요인들을 분석해 보았는데, 표2의 내용과 비교해 볼 때, 모바일 웹 부분의 '개인정보취급방침 게시 및 수집동의 구현'은 클라우드 서비스에 대한 침해요인으로 점검 리스트에 포함되어 있음을 확인해 볼 수 있다. 본 장에서는 클라우드 서비스에 대한 여러 침해 요인들 중 수집정보의 방법 및 취급 및 관리 수집내용 등에 대한 구체적인 분석과 대응 방안들에 대해 알아본다.

4.1 수집정보의 선별적 동의

국내 클라우드 서비스는 사용자가 서비스를 사용을 하고자 한다면, 사전 제공자의 동의 항목에 동의를 해야만 사용이 가능하며, 그림4, 5와 같이 앱에 따라 동의 요구에 따라 항목들이 다를 수 있다. 그러나 그림5와 같이 제공자는 '개인정보'라는 항목으로 동의를 요구하며, 사용자에게 충분한 개인정보의 용도 및 정보의 사용범위 등에 대해 명확히 설명되고 있지 못하고 있음을 알 수 있다. 이는 국내 은행의 대출계약서나 웹에서의 신규가입 등에서는 개인정보 수집 시, 수집정보에 대한 사용목적, 보유기간, 파기 등 세부적인 설명과 함께 법적 책임도 명시하며, 이에 대한 동의를 받고 있는 점과는 달리, 앱은 사용자가 원하지 않는 항목이 있음에도 불구하고 제공자의 일방적인 정보수집에 무조건적인 동의를 해야만 하는 상황이 된다. 만약 악의적인 제공자가 의도적으로 불필요한 정보의 수집을 요구할 경우, 사용자는 동의를 해야 하기 때문에 정보유출의 1차적인 사용자 대응이 불가하다. 알 수 있다. 특히 무선기기 상에서의 프라이버시 침해 위험에 대해 인식이 부족한 사용자에게는 매우 위험한 요인이라 할 수 있다. 또한 이러한 점은 제공자가 일방적으로 사용자 개인에게 책임을 전가할 수 있는 부분으로 사용자에 대한 선별적 동의는 반드시 필요한 부분이라 할 수 있다.



개인정보 이용내역 통지 안내

본 메일은 "정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 30조 2항" 및 "동법 시행령 제17조"에 의거한 법적 준수를 위해, Tcloud 서비스 회원 전체에게 보내드리는 메일입니다.

2014년 8월 1일부터 2015년 7월 31일까지 T cloud 서비스를 이용하신 고객님들의 개인정보 이용내역을 다음과 같이 알려 드립니다.

■ 개인정보의 수집 항목 및 이용 목적

T cloud 서비스는 서비스 운영을 위해 아래와 같은 목적으로 개인정보를 수집 및 이용하고 있습니다.

[필수]개인정보 수집/이용 - 모바일(Mobile) 회원의 경우

목적	항목
고객식별 및 본인여부 확인	가입 통신사명, 휴대전화번호
서비스 이용관련 불편사항 접수 및 처리, 서비스의 부정이용 방지	휴대전화번호, 서비스 이용기록, 이용정지 기록, 이용해지 기록, 접속로그(일시, IP), 쿠키, 단말기Address(단말기의 고유 주소값), 국가 코드, 광고성 SMS/Push 수신여부
서비스 관련 정보(공지사항 등)의 제공	휴대전화번호, 서비스 이용기록, 이용정지 기록, 이용해지 기록
서비스 이용내역 확인	휴대전화번호, 서비스 이용기록, 이용정지 기록, 이용해지 기록, 접속로그(일시, IP), 쿠키, 단말기Address(단말기의 고유 주소값), 국가 코드, 광고성 SMS/Push 수신여부
(T-Cloud내 Data의 보관이력이 있는 경우)저장된 Data의 Back-up 지원 및 관련 불편사항 응대	이동전화번호, 성명 및 T-cloud 내 저장된 Data, 접속로그 기록

(그림 6) 클라우드 서비스 개인정보 이용내역 통지내역[14]

최근 클라우드 서비스 제공자는 개인정보의 사용내역에 대해 그림6과 같이 메일로 전송하여 고지하고는 있으나, 사용자 의지와는 무관하게 수집 후, 공지는 클라우드 서비스의 위험 요인을 경감시키기 보다는 제공자에 대한 서비스의 활성화와 신속성, 편의성만을 고려하였다고 볼 수밖에 없다. 하루에도 수많은 앱들이 개발되고, 업로드(upload)되고 있다는 현실을 고려해 볼 때, 클라우드 서비스와 관련한 악성 앱의 설치로 개인정보 유출의 시도는 계속되고 있으며, 이러한 침해요인은 또 다른 공격시도를 야기 시키는 원인이 된다. 따라서 제공자는 사용자에게 수집 정보의 선별기회를 부여함으로써, 기존 동의방식보다 개인정보의 침해 위험으로부터 불필요한 정보의 수집을 차단할 수 있도록 사전 선별 절차를 통한 대응이 있어야 한다.

4.2 수집정보의 관리 대응

대표적인 클라우드 컴퓨팅 서비스 업체인 애플과 구글은 각각 '아이 클라우드'와 '구글 플러스'를 운영하고 있다. 이들 업체의 대표되는 서비스로는 사진 및 동영상, 문서, 음악 파일 등의 공유가 있는데 이에 대한 해킹사고가 발생한 사례들을 갖고 있다. '아이 클라우드'와 '구글 플러스'의 경우, 인증정보의 유출로 인한 사용자 데이터의 해킹사례로 최근 인증체계에 대해 '해외 로그인 및 타 지역 로그인', '새로운 기기 로그

인', '일회용 로그인' 등의 시스템 구축으로 보완하였다[13]. 이러한 사례들을 살펴볼 때, 가상화 환경에 따른 직접적인 내부 해킹 공격은 아직까지 알려지지 않고 있지만, 가상화에 최적화된 공격시도에 대해 대비하고 있다. 애플과 구글의 공격 사례를 통해 수집정보의 저장 및 관리체계와 인증 정보의 유출에 대한 침해 요인의 분석과 보유정보에 대한 관리상의 대응방안의 마련이 필요함을 알 수 있다. 최근 인증정보의 유출을 대비해 이중 인증방식으로 대응하고 있지만, 무엇보다도 수집된 정보의 관리 및 접근, 취급 등에 대한 관리체계의 보안을 통한 침해 대응이 요구된다.

4.3 가상화 환경의 보안시스템 개발

클라우드 컴퓨팅은 기존 기술과 달리 가상화 환경을 통해 운영되고 있어, 현재 공격 또한 클라우드 서비스의 직접적인 내부 정보의 유출 공격사례는 아직까지 알려지고 있지 않다. 그러나 클라우드 환경은 기존 보안 시스템만으로 기술적 대응이 불가한 상황이며, 복잡한 가상화 환경은 오히려 다양한 공격들이 가능할 것으로 예상되고 있는 만큼 가상화 환경에 적합한 보안 기술의 개발이 시급한 실정이다. 그리고 글로벌 기업들의 기술선도화로 인해 국내 보안 기술이 무용지물이 될 수 있어, 국내 클라우드 보안기술은 대형 기업들의 클라우드 보안기술의 동향과 가상화 환경을 함께 고려한 연구 및 개발이 지속되어야 한다. 또한 국내 대부분의 클라우드 서비스는 국내 사용자를 위한 서비스에 비중을 두고 있어, 추후 글로벌 기업과의 호환 및 이식성이 높은 비중 있는 기술개발이 이뤄져야 한다. 오히려 국내 기업들의 자체 보안 기술개발은 향후 클라우드 서비스의 위험성을 높일 수 있는 점을 고려해 글로벌 서비스에 대한 가상화 환경 연구와 보안 기술 개발을 통한 대응은 계속되어야 한다.

5. 결 론

최근 클라우드 서비스는 몇몇 글로벌 기업들에 의해 주도되어 전 세계적인 서비스로 자리 잡아 가고 있다. 특히 스마트 기기의 보급의 급증은 클라우드 서비스의 이용 확산과 보급에 큰 매개 역할을 수행하고 있다고 해도 과언이 아니다. 이중 스마트 폰은 다양한 연령층의 사용자를 갖고 있으며, 이동성과 호환성이 뛰어나 서비스의 활용을 더욱 가속화 하고 있다. 이러한 가운데 클라우드 서비스는 각종 프라이버시 정보들을 요청하고 있으며, 이에 따른 보안 취약성의 증가와 이를 이용한 공격으로 물리적, 경제적 피해뿐만 아니라 개인의 사생활 침해에 따른 정신적 피해까지 발생하고 있다. 그리고 클라우드 서비스를 이용한 빅데이터(big data)의 수집은 무분별한 개인 정보 및 기기 정보의 수집으로 여러 위협들에 노출된 상태로 철저한 보안 관리가 요구되고 있다. 또한 클라우드 컴퓨팅 서비스의 보안적 관점에서 살펴보면, 프라이버시 수집과 관리, 사용에 관한 취약성 및 위협들에 대한 연구를 통해 이에 대한 대응방안마련 및 기술 개발이 시급함을 알 수 있다. 따라서 본 논문은 다양한 클라우드 컴퓨팅 서비스에서 요구되고 있는 프라이버시 침해 가능성이 높은 취약성 및 위협들에 대해 분석하고, 이에 따른 요인들을 알아보았다. 이와 같은 결과는 향후, 클라우드 컴퓨팅 서비스의 보안을 위한 기술 개발 및 대응에 유용한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후, 국내 클라우드 컴퓨팅 서비스의 프라이버시 보안을 위해서는 다양한 공격기술의 분석과 함께 글로벌 클라우드 서비스별, 기기별 취약점 연구와 클라우드 컴퓨팅 기술의 표준화에 따른 체계적이고, 지속적인 연구가 병행되어야 할 것으로 사료되며, 보다 안정된 글로벌 서비스 제공에 초점을 맞춘 연구가 요구된다.

참고문헌

[1] 강원영, "최근 클라우드컴퓨팅 서비스동향," KISA, NETTerm No. 3, pp. 20-24, 2011.

[2] Anupama Prasanth, Monika Bajpei, Vertika Shrivastava, Raj Gaurav Mishra "A Survey of Associated Service," HCTL Open India, chapter3, 2015.

[3] 양희동, 황세운, "클라우드 컴퓨팅 보안 위협요소 소개와 창조경제 실현을 위한 방향성 제안," KISA, Internet & Security Focus, pp. 66-83, 2013.12.

[4] 신영상, "클라우드 환경에서의 하이퍼바이저 기반 가상화 보안 기술 동향," KISA, Internet & Securi

ty Focus, pp. 55-75, 2014.8.
[5] 전정훈, “클라우드 컴퓨팅 서비스의 취약성과 대응 기술 동향에 관한 연구” 한국융합보안학회, Vol. 13, No. 6, pp. 1239-1246, 2013.4.
[6] 박완규, “클라우드 컴퓨팅 환경에서의 개인정보의 미국 이전에 따른 문제점 및 대응방안 연구,” 경북대학교 법학연구원, pp. 456-478, 2012.2.
[7] http://i1.daumcdn.net/thumb/R750x0/?fname=http%3A%2F%2Fcfile30.uf.tistory.com%2Fimage%2F253E094F54D33F3F1B610A
[8] http://blog.naver.com/PostView.nhn?blogId=zzxcvgh&logNo=30126611476&categoryNo=28&viewDate=&currentPage=1&listtype=0, "SKT Tstore 설치 방법"
[9] 박진호, 이재휘, “클라우드 컴퓨팅 서비스 침해사례 분석 및 정보보안 기술 동향,” 경북대학교, pp. 3-14, 2013.7.
[10] 유우영, 임종인, “클라우드 컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구,” 한국정보보호학회, pp. 337-346, Vol. 22, No. 2, 2012.4.
[11] 장은영 외4명, “모바일 클라우드 서비스의 보안 위협 대응 방안 연구,” 한국정보보호학회, pp.177-186, vol.21, no.1, 2011.2.
[12] 한국인터넷진흥원 “국내 클라우드 서비스 보안 취약점 점검,” 2012.8.
[13] Christian Moss, “Integrating Cloud Computing and Mobile Application,” JCC, 2014.
[14] T Cloud 서비스 “https://www.tcloud.co.kr/main.do,” 통지안내메일, 2015.8.27.

[저 자 소 개]

전 정 훈 (Jeong-hoon Jeon)

2000년 8월 숭실대학교 일반대학원 컴퓨터학과 공학석사
2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교 컴퓨터학과 교수

email : nerdrandy@dongduk.ac.kr