사용자 관점의 클라우드 컴퓨팅 보안 연구

황수연*, 남보원*, 박민우**, 이준호**, 정태명*
*성균관대학교 정보통신공학부
**성균관대학교 전자전기통신공학과
e-mail: l_need@naver.com, genien1@dreamwiz.com,
{mwpark, jhlee83}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

A Study of Cloud Computing Security on User's View

Sue-Yeon Hwang*, Bo-won Nam*, Min-Woo Park**, Jun-Ho Lee**, and Tai-Myoung Chung*
*School of Information Communication Engineering, Sungkyunkwan Univ
**Dept of Electrical and Computer Engineering, Sungkyunkwan Univ

요 약

클라우드 컴퓨팅 시스템은 방대한 정보와 자료를 가진 컴퓨팅 시스템으로 해커의 공격 대상이 되기 쉽다. 또한 복잡한 구조를 가지기 때문에 취약점이 발생하기 쉬워 체계적인 보안 분석이 필요하다. 현재 클라우드 컴퓨팅 보안 요구사항 분석이나 권고 사항 연구를 위해 많은 국제 협의기구가 활발히 활동 중이다. 하지만 협의기구들의 연구 활동은 서비스 유형에 따라 사업자 기준에서 보안 분석이 이루어지고 있다. 클라우드 컴퓨팅 서비스가 보다 활발히 발달하기 위해서는 클라우드 컴퓨팅 서비스를 이용하는 사용자들을 세분화하고 그들에 맞는 보안 서비스가 제공되어야 한다. 본 논문에서는 기존의 보안 분석들과 다르게 사용자 기준에서 분석한 클라우드 컴퓨팅 서비스의 보안 분류를 제시한다.

1. 서론

클라우드 컴퓨팅이란 정보가 인터넷 상의 서버에 영구적으로 저장되고 데스크탑이나 타블릿 컴퓨터, 노트북, 벽걸이 컴퓨터, 휴대용 기기 등과 같은 클라이언트에는 일시적으로 보관되는 패러다임[1]이다. 클라우드 컴퓨팅은 기업들의 IT 인프라 구축에 대한 부담과 비용 경감에 대한 요구로 인해 각광받고 있다. 또한 노트북과 태블릿 PC와 같은 개인용 컴퓨터, 스마트폰과 같은 휴대기기의 대중화로 인해 시간과 장소에 제약받지 않고 인터넷을 사용할 수 있게 되면서, 무제한에 가까운 클라우드 컴퓨팅 능력에 대한 관심이 커지고 있다. 세계 클라우드 컴퓨팅 시장은 2009년에는 795억 달러, 2010년 1,095억 달러로 증가 추이를 보이고 있고, 2012년엔 이 두 배인 2,133억 달러, 2014년엔 세 배인 3,434억 달러로 계속 증가할 전망이다[1]. 클라우드 컴퓨팅 시장의 활성화는 이전보다 더 다양한 성격의 사용자와 제공자가 시장에 참여하게 하여 서비스의 다양화를 촉진시키고 있다.

클라우드 컴퓨팅 시스템은 서버와 클라이언트 간의 관계를 바탕으로 각종 기술들이 복합적으로 사용된다. 또한 네트워크를 기반으로 하므로 보안 문제를 필연적으로 가지게 된다. 2009년 3월에 발생한 Google Docs의 보안 사고는 기업 간 문서 공유 과정에서 접근 권한 제어가 제대로 이루어지지 않아 발생했다. 이러한 유형의 사고가 발생하는 이유는, 해당 서비스를 이용하는 사용자의 속성을 등한시하고 서비스 자체만을 고려하여 보안 시스템을 구현했기 때문이다. 실제로 <표 1>의 통계에 따르면 클라우드 컴퓨팅 서비스 제공자들은 사용자들에게 보안상의 신뢰를 얻지 못하고 있다[2]. 기존의 클라우드 컴퓨팅은 서비스를 중심으로 서비스 제공자의 관점에서 보안 이슈에 접근하고 있으며, 이는 사용자의 요구 사항을 충족시키기에 부족하다. 제공자 중심의 서비스 문제점을 해결하기 위하여, 본 논문에서는 사용자 관점의 클라우드 컴퓨팅 보안 분류 방법을 제시하고자 한다.

<표 1> 클라우드 서비스에 대한 사용자들의 태도

항 목 \ 우려도	매우 그렇다	다소 그렇다	거의 그렇지 않다	전혀 아니다
다른 사람에게 자신의 파일을 판매하는 것	90%	5%	2%	3%
마케팅에 자신의 정보를 이용하는 것	80%	10%	3%	6%
자신의 정보를 분석하고 어떤 데이터를 가지고 있는지 광고하는 것	68%	19%	6%	7%
자신의 파일을 삭제했어도 복사본을 가지고 있는 것	63%	20%	8%	8%
자신의 파일을 사법당국의 요청에 따라 전달하는 것	49%	15%	11%	22%

1) IEEE(Institute of Electrical and Electronics Engineers)의 클라우드 컴퓨팅에 대한 정의

2. 기존 클라우드 컴퓨팅 서비스의 분류

2.1 기존의 클라우드 컴퓨팅 분류

클라우드 컴퓨팅은 서비스의 성격에 따라 SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service)의 세 가지로 분류된다. SaaS는 각각의 컴퓨터마다 설치해야했던 응용 소프트웨어가 인터넷을 이용하여 서비스 사용자를 대상으로 제공되는 서비스 형태로, 사용자는 단말기로 원격 접속하여 해당 소프트웨어를 활용한다. PaaS는 소프트웨어가 동작하는 플랫폼이나 사용자가 소프트웨어를 개발할 수 있는 환경을 제공해 주는 서비스이다. 사용자는 플랫폼 상에서 제공되는 자원을 활용해 새로운 소프트웨어를 만들 수 있다. IaaS는 컴퓨터 저장 공간과 처리능력과 같은 하드웨어 자원을 서비스 사용자에게 서비스하는 형태이다.

위의 분류 모델 외에, 인프라 배치(Deployment)에 따라 Private cloud, Community cloud, Public cloud, Hybrid cloud의 네 가지로 분류하는 모델이 있다. Private cloud는, 클라우드 컴퓨팅 인프라가 특정 사용자 또는 조직을 위해 운용되는 형태로, 인프라를 조직 내에서 직접 운영하거나 제 3자에 의해서 제공받는다. Community cloud는 인프라를 관리하는 하나의 Community를 두고 여러 조직으로 하위 인프라를 분산시킨다. Public cloud는 공공이나 대기업에서 주로 사용하는 클라우드 서비스로 인프라가 서비스를 제공하는 조직에 소유된다. Hybrid cloud는 위에서 언급한 3가지 형태 중 2가지 이상이 혼재된 형태이다[2][3].

2.2 기존의 클라우드 컴퓨팅 보안 이슈

CPNI(Centre for the Protection of National Infrastructure)에서는 클라우드 위협 요소(Cloud Threats)를 요소의 성격에 따라 <표 2>와 같이 분류한다.

<표 2> 클라우드 위협 요소

성격	세부 요소
기밀성 (Confidentiality)	내부 사용자 외부 사용자 정보 유출
무결성 (Integrity)	정보 격리 사용자 접근 정보의 질
가용성 (Availability)	정보 변경 관리 서비스 접근 거부 물리적인 어려움 취약점 복구 절차 개발

또한 CPNI에서는 치명적인 클라우드 보안 위협 요소(Security risk)로 다음의 5가지를 제시하고 있다. 첫 번째는 허가된 사용자 접근(Privileged user access)으로, 권한이 없는 사용자가 데이터에 접근하는 것을 막는다. 두 번째는 데이터 저장 위치 및 격리(Data location and segregation)로, 데이터의 물리적, 혹은 가상적인 저장 위치가 보안 상 안전하게 설계되어야 한다. 세 번째는 데이터 처분(Data disposal)으로, 폐기 데이터가(백업 데이터를 포함하여)본래의 저장 공간에서 물리적, 전자적으로 완전히 파기되어야 한다. 네 번째는 온라인 접근 및 방어 모니터링(e-Investigations and Protective monitoring)으로, 클라우드 컴퓨팅의 속성 상 네트워크 기반 서비스를 제공하므로 이 분야에서의 보안이 보장되어야함을 의미한다. 마지막으로 클라우드 보안 보증(Assuring cloud security)으로, 위에서 제시한 4가지 성격의 위협 요소들에 대해 안전성을 보장하여 사용자들에게 보안을 보증하여야 한다[4].

2.3 기존 모델의 문제점

2.1에서 언급한 기존의 클라우드 컴퓨팅 분류는 여러 문제점을 가지고 있다. 서비스의 성격에 따른 분류 방법은 클라우드 컴퓨팅 서비스 제공자의 관점에서 해석된 분류 방법이다. 이러한 분류의 방법은 사용자의 요구 사항 반영에 취약하고, 사용자의 성향을 반영한 세부적인 보안을 제공하기 어렵다. 인프라 배치에 따른 분류 방법에서는 사용자의 조직 유형에 따라 분류하였다. 인프라 위치가 분류에 따라 명확하게 제시되므로 이를 기준으로 한 보안 시스템 설계에 용이하다. 그러나 서비스를 사용하는 개인 및 단체가 가지고 있는 세부적인 보안 요구 사항을 파악하기 힘들다.

3. 사용자 관점에서의 접근

앞에서 언급한 바와 같이, 기존의 클라우드 컴퓨팅 분류 기준으로는 사용자의 성향을 고려한 보안 시스템 구축에 어려움이 있다. 따라서 클라우드 컴퓨팅 사용자의 특성을 분석하는 과정이 필요하고, 이를 기초로 보안 요소들을 분류하고 보안 시스템을 구축해야 할 것이다. 본 절에서는 사용자를 개인 사용자와 기업 사용자의 두 가지 유형으로 분류하고 각각의 성향을 분석하였다. 또한 각 유형의 성향을 기준으로 중점적으로 고려되어야 할 보안 요소들을 제시한다[5].

3.1 개인 사용자

개인 사용자는 개별적으로 클라우드를 이용하며, 그룹 구성원 성격을 지니지 않은 사용자를 지칭한다. 주이용 서비스 형태는 개인 자료 저장, 어플리케이션, 소셜 커뮤니케이션(블로그, 동호회, 이메일)등이다. 서비스 이용 목적이 비영리적이며, 무료 서비스를 선호하는 경향이 있다. 개인 사용자들을 서비스 유형에 따른 분류에 적용하면 SaaS형의 서비스 사용자에 가깝다. 또한 주 사용자 계층은 아니나 개발을 목적으로 클라우드에서 개인적으로 플랫폼을 이용하는 PaaS형의 서비스 사용자도 개인 사용자

에 포함된다. 개인 사용자를 대상으로 하는 클라우드 컴퓨팅 서비스의 보안은 다음과 같은 사항을 중점적으로 고려해야 한다.

3.1.1 허가된 사용자 접근

개인 사용자는 자신의 클라우드의 자원에 대하여 선택적인 대상에게만 공유를 허가하는 경향이 있다. 여기서의 선택적인 대상에 대한 허가란 개인 사용자의 자원에 접근하여 사용하고자 하는 사용자 집단 A그룹과 B그룹이 있다고 가정할 때, A그룹에 대해서는 허가하고 B그룹에 대해서는 불허하는 형태를 의미한다. 대표적인 예로 블로그와 같은 개인 홈페이지를 운영하는 개인 사용자는 방문자들의 일부에게 접근 권한을 부여함으로써 원치 않는 방문자의 자료 열람을 제한한다. 이를 위해 클라우드 컴퓨팅 시스템에서는 허가되지 않은 사용자의 접근을 차단하여야 한다. 또한 시스템에서 개인 사용자에게 허가된 접근자들과 비허가된 접근자들을 선택할 수 있도록 관련 서비스를 제공하여야 한다.

3.1.2 허가된 자원 접근

개인 사용자는 자신의 클라우드 자원에 대하여 선택적인 공유를 허가하는 경향이 있다. 선택적인 공유의 허가란 개인 사용자의 자원 중 a자원과 b자원이 있다고 가정할 때, a자원에 대해서는 접근을 허가하고 b자원에 대해서는 접근을 불허하는 형태를 의미한다. 개인 사용자가 웹하드 서비스 등에서 파일 공유를 허용할 경우, 자신이 공유하는 파일 중 일부에만 공유를 허용하는 형태가 그 예이다. 이를 위해 시스템에서는 선택적인 자원에 대한 공유 여부 설정 서비스를 제공할 필요가 있다. 또한 접근이 허가되지 않은 자원들에 대하여 정보가 누출되지 않도록 스토리지 보안 기술을 적용해야 한다.

3.1.3 개인 정보 유출

개인 사용자는 서비스 제공자에게 본인의 식별 수단으로 개인 정보를 제공하는 것이 일반적이다. 개인 정보는 유출 시 치명적인 보안 사고로 이어질 수 있기 때문에 서비스 제공자는 개인 정보가 누출되지 않도록 이를 보관하는 저장 공간에 데이터베이스 보안 기술을 적용해야 한다. 또한 개인 정보가 사용자 식별 이외의 용도로 사용되지 않음을 개인 사용자에게 보증하여, 개인 정보 보안에 대한 신뢰도를 높여야 한다.

3.1.4 정보의 질

개인 사용자는 자신의 자원에 대하여 상업적인 이해관계 외에 정보 공유 자체를 목적으로 불특정 다수의 사용자에게 접근을 허용하기도 한다. 웹하드와 같은 서비스가 가장 대표적인 예이다. 이러한 불특정 다수와 개인 간의 정보 공유에서는 본래 공유하려는 정보 외에 바이러스나 악성 코드 등이 함께 공유될 수 있다. 따라서 서비스 제공자는 사용자가 공유하는 정보의 바이러스나 악성 코드 감염 여부를 시스템에서 점검하여 공유되는 정보의 안전성을 보장해야 한다. 이러한 보안 점검 서비스는 개인 사용자에게 클라우드 컴퓨팅 서비스 제공자의 보안 의식이 높음을 보일 수 있으며, 보안 사고를 사전에 차단할 수 있는 방법이다.

3.2 기업 사용자

기업 사용자는 같은 목적을 가진 그룹 내의 일원으로서 클라우드를 이용하는 사용자를 의미한다. 주이용 서비스로는 기업 내에서 공유되는 자료 저장, 작업 환경(OA, 회계, 연구 및 개발) 공유, 협력 기업 간 또는 본사와 지사 간 정보 공유 등이 있으며, 대개 영리 활동을 목적으로 사용된다. 이러한 특성으로 인하여 이해관계와 서비스의 질에 따라 유료로 클라우드 컴퓨팅 서비스를 이용하기도 한다. 이용하는 서비스의 성격을 기준으로 이들을 분류하면 IaaS, PaaS형의 서비스 사용자로 분류할 수 있다.

기업 사용자를 대상으로 하는 클라우드 컴퓨팅 서비스의 보안은 다음과 같은 사항을 중점적으로 고려해야 한다.

3.2.1 허가된 사용자 및 자원 접근

기업은 기업의 클라우드 자원의 공유에 대해 그룹 내부적으로는 허용하나 외부로부터의 접근은 불허한다. 접근이 허가된 기업 사용자들은 동일한 자원에 대해 다시 차등적으로 접근 제한을 받는다. 차등적인 접근 제한이란 자원 A, B, C가 있다고 가정할 때, a사원은 A자원을, b사원은 A, B자원을, c사원은 A, B, C자원을 접근하는 권한을 가지는 형태를 의미한다. 가장 대표적인 예로 직급별로 이용 가능한 자원의 한계가 다른 형태를 들 수 있다. 이러한 형태에서는 대개 높은 직급일수록 더 많은 자원에 접근할 수 있다. 차등적인 접근 제한과 동시에 사용될 수 있는 접근 제한 방법으로 그룹별 접근 제한이 있다. 그룹별 접근 제한이란, 기업 내의 기업 사용자들을 그룹별로 분류하고 그룹별로 자원 접근에 제한을 두는 형태이다. 이러한 형태를 적용한 예시로, 기업의 부서별로 주로 이용하는 자원 이외에는 접근을 제한하는 것을 들 수 있다. 이러한 기업 사용자의 특성을 반영한 클라우드 컴퓨팅 시스템을 구현하기 위해 서비스 제공자는 사용자 접근 보안에 관하여 3가지 요소를 고려해야 한다. 첫 번째는 외부 접근 제한, 두 번째는 차등적 접근 제한, 세 번째는 그룹별 접근 제한이다. 서비스 제공자는 보안 설계 시, 3가지 요소에서 첫 번째 요소를 기본으로 사용자 요구에 따라 나머지 2가지 요소를 선택적으로 적용할 수 있다. 각 요소들을 구현하기 위해 접근 제어 기술, 네트워크 보안 기술, 단말 보안 기술 등이 사용될 수 있다[6].

3.2.2 정보 변경 관리

기업 사용자는 그룹원의 성격을 가지므로, 동일 그룹

내에서 동시에 동일 자원에 접근하여 이용하는 경우가 발생한다. 동시 접근의 경우, 클라우드는 접근한 사용자들에 대한 각기 권한 여부 확인 및 보안이 보장된 자원 할당이 필요하다.

3.2.3 정보 유출

기업의 자원은 영리적인 성격을 띄는 경우가 많다. 또한 개인이 아닌 단체의 성격을 가지기 때문에 정보 누출 시 개인의 정보 누출 사고에 비해 그 위험성이나 심각성이 매우 크다. 따라서, 서비스 제공자는 스토리지 보안 기술 도입을 통해 클라우드 컴퓨팅 시스템상의 보안을 강화해야 한다.

3.2.4 보안 보증

클라우드 사업자는 사업자 본인이 서비스를 이용하는 기업 사용자의 자원에 접근할 수 없도록 조치하고 이를 명시해야 한다. 이는 클라우드 서비스도 영리를 목적으로 하는 기업의 성격을 가지기 때문이다. 이러한 보안 보증의 적용 형태로, 서비스 사업자는 클라우드 컴퓨팅 시스템 운영상에서 규정하고 있는 보안 보증 내용과 보안 사고 발생 시의 대응 및 복구 절차를 기업 사용자에게 패키지 형태로 제공하여 보안상의 신뢰를 얻는 방법을 제안한다.

3.2.5 서비스 접근 거부 및 취약점 복구 절차 개발

클라우드 컴퓨팅 서비스 제공자는 시스템이 서비스 접근 거부 상태에 빠졌을 경우를 대비한 복구 정책을 수립하여야 한다. 또한 데이터 손상 사고에 대한 대응 체계 역시 마련해야 한다. 이를 위한 대응 기술로는 데이터 백업이나 스토리지 분산 기술 등이 있다[7].

4. 결론

본 논문에서는 클라우드 컴퓨팅의 보안 이슈를 개인 사용자와 기업 사용자의 성격에 따라 분류하고 이에 다른 보안 요소를 제시했다. 사용자 관점에서의 클라우드 컴퓨팅 보안 접근 방식은 기존의 관점과 다른 시각을 서비스 사용자와 제공자에게 제시한다. 사용자 관점에서의 접근을 통해, 서비스 사용자는 보안에 대한 이해와 신뢰성을 높일 수 있고, 서비스 제공자는 클라우드 컴퓨팅 시스템의 보안 설계와 구축에 있어서 사용자에 성향을 고려한 보안 요소를 제공할 수 있게 될 것으로 기대한다. 본론에서 제안한 관점을 보안 시스템에 적용하기 위하여 각 특징에서 제시한 보안 요소들에 대한 지속적인 연구가 필요할 것이다. 향후 연구 계획으로, 본 논문에서 제안한 사용자 성향에 따른 분류 외에 사용자 관점에서 접근할 수 있는 추가적인 분석을 통해 연구하도록 한다.

참고문헌

[1] 이주영 “클라우드 컴퓨팅의 특징 및 사업자별 제공 서비스현황” 정보통신정책연구원

[2] CSA(Cloud Security Alliance) “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”, Dec, 2009.

[3] 김현승, 박춘식 “클라우드 컴퓨팅과 개인 인증 서비스” 정보보호학회지, Apr, 2010.

[4] CPNI(Centre for the Protection of National Infrastructure) “Information Security Briefing 01/2010 CLOUD COMPUTING″, Mar, 2010.

[5] 은성경, 조남수, 김영호, 최대선 “클라우드 컴퓨팅 보안 기술” 전자통신동향분석 제24권 제3호, Aug, 2009.

[6] 임철수 “클라우드 컴퓨팅 보안 기술”정보보호학회지 제19권 제3호, Jun, 2009.

[7] Cong Wang, Qian Wang, Kui Ren “Ensuring Data Storage Security in Cloud Computing″