중소기업융합학회 논문지 제5권 제1호 pp. 31-35, 2015 ISSN 2234-4438

클라우드 컴퓨팅 보안 대책 연구

이상호[1]
[1]충북대학교 정보보호경영학과

Cloud computing Issues and Security measure

Sang Ho Lee[1]
[1]Department of Information Security Management, Chungbuk National University

요 약 클라우드 컴퓨팅은 인터넷 기반 컴퓨팅 기술이다.인터넷을 중심으로 서비스를 주고받는 형태이다. 비용이 절약되고, 쉬운 사용이 가능하기 때문에 많은 기업들이 이용하고 있는 추세이다. 클라우드의 형태로는 public cloud,private cloud,hybrid cloud가 있다.서비스 모델에는 SaaS,PaaS,IaaS가 있다.클라우드 컴퓨팅은 쉬운 사용이 가능한 만큼 보안 취약점을 가지고 있다. 특히 가상화와 정보집중화에 따른 취약점이 있다.이를 극복하기 위해서는 새로운 보안 기술이 개발되어야한다.또 다른 극복 방법은 보안 책임을 분명히 해야하고, 정책을 통일화 해야 한다.

주제어 : 클라우드 컴퓨팅, 클라우드 컴퓨팅 보안, 클라우드 서비스,가상화,공공 클라우드,사설 클라우드

Abstract Cloud computing is internet-based computing technology.This is a form for exchanging service focused on the Internet.Because Cost is saved and use is easy there's a tendency that many companies are using.Cloud is in the form of a public cloud and private cloud and hybrid cloud.The service model is SaaS, PaaS, IaaS.Cloud computing use is simple but it has a security vulnerability.In particular, there is a vulnerability in virtualization and centralized information..In order to overcome this new security technology is to be developed.In particular, network security technology and authentication technology should be developed.Another way to overcome security responsibilities must be clearly and policies should be unified.

Key Words : cloud computing, cloud computing measure, cloud service, virtualization, public cloud, private cloud

1. 서론

컴퓨팅 자원을 관리할 수 있도록 특화된, 제 3자가 제공하는 인프라를 저렴하고 쉽게 사용할 수 있도록 서비스를 제공하는 클라우드 컴퓨팅(cloud computing)은 말뿐만이 아닌 현실로 우리 앞에 다가오고 있다.

실제로 많은 기업들의 클라우드 활용이 점점 높아지고 있으며 구글, 아마존 등의 1세대 글로벌 기업들은 자체적인 클라우드 컴퓨팅을 구현했고, 페이스북, 트위터 등의 2세대 기업들은 구글이 오픈한 클라우드 기술을 활용해 클라우드 컴퓨팅을 구현했다.

또 2015년 3월 클라우드 컴퓨팅 발전법이 국회를 통과하며 국내 클라우드 컴퓨팅 산업을 발전시키기 위해 금전적 지원, 전문 인력 양성 등의 기반이 조성되고 있다.

그러나 클라우드 컴퓨팅(cloud computing)은 자원의 효율적 관리를 기반으로 발전되어 왔고, 모든 정보가 가

Received 2015-01-06 Revised 2015-01-24 Accepted 2015-02-20
*Corresponding Author : Sang Ho Lee(shlee@chungbuk.ac.kr)

상화된 인터넷상의 서버에 저장되기 때문에 그 내부영역의 보안에 대한 취약점을 안고 있다.

그 취약점에 대해 연구하고 보안대책을 연구해 보고자 이 보고서를 작성하였으며, 본 연구보고서는 2장에서 클라우드 컴퓨팅에 대한 설명과 클라우드 컴퓨팅 서비스 모델에 대한 설명 등등에 대해 기술하였고, 3장에서는 보안 취약점과 보안대책을 기술하였으며 마지막으로 4장에서는 결론을 기술하였다.

2. 클라우드 컴퓨팅(cloud computing)

2.1 클라우드 컴퓨팅(cloud computing)

클라우드 컴퓨팅은 개인이 가진 단말기를 통해서는 주로 입력,출력의 작업만 이루어지고, 정보 분석 및 처리, 저장, 관리, 유통 등의 작업은 '클라우드'라고 불리는 네트워크 공간에서 이루어지는 컴퓨팅 시스템 형태라고 할 수 있다.[1]

이 형태를 통해 우리는 필요한 정보나 정보의 관리를 원하는 시간에 내가 필요한 양만큼 사용할 수 있으며,따로 소프트웨어를 구축하지 않아도 되기 때문에 비용절감과 관리가 용이하다.

Fig. 1. 클라우드 컴퓨팅의 간략도

Fig. 1은 클라우드 컴퓨팅 정의에 대한 간략도를 나타낸 것이며 구름처럼 가상의 인터넷을 중심으로 많은 단말기들이 여러 가지 형태의 서비스를 주고 받는 모습이다.

2.2 서비스 유형에 따른 클라우드 컴퓨팅

클라우드의 형태는 공공 형태인 public cloud와 사설 형태인 private cloud와 이 두 가지의 혼합형태인 hybrid cloud로 나뉜다.

public cloud는 모든 사용자를 위한 공개된 클라우드 서비스로 'external cloud'라고도 불린다.

외부 데이터센터를 사용하는 유틸리티 컴퓨팅 형태로, 주로 중소기업에서 이용하며 원하는 양에 비례하여 비용을 지불하므로 비용 절약 효과가 뛰어나며 모든 사용자를 위해 제공됐지만 자원이 사용자별로 권한이 관리 되어 있으므로 사용자들 사이에서는 전혀 문제가 없으나 전문적인 서비스 제공이 어렵다는 단점이 있다.

예로 네이버의 N드라이브, 다음의 다음 클라우드 등이 있다.

private cloud는 자원이 데이터센터 내의 서비스로 제공되기 때문에 데이터 보안이 public cloud보다 뛰어나나 비용의 부담이 커 주로 대기업에서 사용하는 형태이다.

마지막으로 hybrid cloud 형태는 퍼블릭 형태의 비용절감 효과와 프라이빗 형태의 보안성을 결합한 장점만 모은 형태로 보안이 강조되는 서비스나 시스템은 private cloud를 사용하고 그렇지 않은 서비스나 시스템에서는 public cloud를 쓰는 방식으로 관련 업계에서 뜨거운 호응을 얻고 있다.

2.3 운용형태에 따른 클라우드 컴퓨팅

클라우드 컴퓨팅 서비스 종류는 가상화를 이용할 수 있는 가능 단계에 따라 크게 Saas, PaaS, IaaS 세가지로 나뉜다.

2.3.1SaaS(Software-as-a-Service)

SaaS는 사용자가 네트워크로 접속해 메일, 워드 프로세스 등과 같은 애플리케이션을 사용할 수 있는 서비스이다.

또 공급자 또는 서비스 제공자에 의해 관리되거나 고객들이 일반적으로 인터넷인 네트워크를 걸쳐 사용이 가능한 소프트웨어 배포 모델로 사용한 만큼의 지불하는 모델(pay-as-ypu-go model)이다.

SaaS는 비즈니스 소프트웨어 기능을 기업 고객들에게 낮은 가격에 제공하기 위해 가장 많이 구현되었고 고객들이 설치하지 않아도 되면서 관리, 지원, 허가 그리고 높은 초기비용과 같은 복잡함 없이 내부적으로 운영된

소프트웨어와 똑같은 혜택을 받을 수 있게 하였다. [2]

소프트웨어를 서비스 형태로 제공한다는 의미로 SaaS라고 불린다.

대표적으로는 salesforce.com의 CRM SFA, Net Suite의 ERP CRM e커머스 등이 있다.

2.3.2 PaaS는(Platform-as-a-Service)

PaaS는 SaaS 애플리케이션 전달모델의 파생물로 서비스가 실행되는 환경을 제공해 개발자나 it관리자 또는 최종사용자가 소프트웨어를 다운로드 하거나 설치하지 않아도 전적으로 인터넷으로부터 가능하도록 서비스한다.

대표적으로는 Google의 Google App Engine이 있다.

2.3.3 IaaS(Infrastructure-as-a-Service)

IaaS는 서버, 스토리지, 네트워크같은 인프라를 가상화 환경으로 만들어서 필요에 따라 자원을 사용할 수 있게 해주는 서비스로 기업에서 많이 사용한다. 서버의 확장이 자유롭게 가능하고,Window와 Linux모두를 지원한다. 대표적으로는 Amazon의 EC2,C3 와 Gabia에서 서비스하는 클라우드 호스팅이 있다.[3]

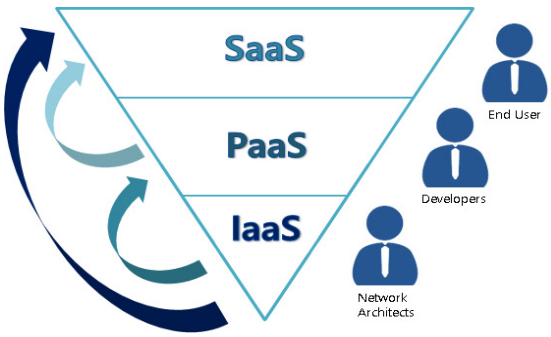

Fig. 2. Types of Service

2.4 가상화

가상화 기술은 클라우드 컴퓨팅을 구축하기 위해 필요한 핵심 기술로 서버 및 스토리지, 하드웨어 등을 분리된 시스템이 아닌 하나의 자원으로 구성되는 영역으로 간주하며 자원을 사용자들의 필요에 따라 할당 할 수 있다.[4]

따라서 유연성과 효율성을 가지며 비용절감이라는 장점을 가지고 있다.

목적은 컴퓨팅 리소스에 대한 접근 및 인프라관리 간소화하는 것을 목적으로 한다.[5]

가상화 기술의 분류는 다음 표와 같다.

Table 1. Types of Virtualization

가상화	인프라(자원) 가상화	시스템 서버 가상화
		스토리지 가상화
		네트워크 가상화
	정보 가상화	파일 가상화
		데이터 가상화
	워크로드 가상화	트랜잭션 가상화
		태스크 가상화
		프레젠테이션 가상화

특히 인프라 가상화에서 서버 가상화는 크게 하이퍼바이저(Hypervisor)형과 호스트(Hosted)형으로 나눌 수 있다.

하이퍼바이저형은 어떻게 가상화하느냐에 따라 가상화가 지원되는 하드웨어의 사용에 따라 전가상화(Full-Virtualization)과 반가상화(Para-Virtualization)로 나뉜다.

전가상화는 하드웨어를 모두 가상화한 것을 말한다. 그렇기 때문에 아무런 수정 없이 다양한 os를 사용할 수 있다. 그러나 cpu의 가상화 기술을 이용해야 하기 때문에 성능의 저하를 가져온다. 반가상화는 전가상화와 다르게 모두 가상화하지 않았기 때문에 하이퍼바이저를 통해 제어가 가능하다.

따라서 게스트os가 하드웨어를 제어 할 수 없다.

호스트형은 버츄얼 머신 모니터(VMM)이라는 소프트웨어를 호스트 운영체제가 위에 설치되며, 그것을 통해서 사용자들은 다양한 운영체제를 실행할 수 있다.

3. 보안

3.1 보안 위협요인

클라우드 도입을 위한 보안 가이드 라인을 제시하는 CSA(Cloud Security Alliance)는 보안위협을 요인들을 table2와 같이 7가지로 정의하고 있다.[6]

Table 2. Seven Threats

보안위협	• 클라우드 컴퓨팅 남용 및 불손한 사용 • 안전하지 않은 애플리케이션 프로그래밍 인터페이스 • 악의를 가지고 있는 내부 관계자 • 공유 기술의 취약점 • 데이터 유실 및 유출 • 계정,서비스 및 트래픽 하이재킹 • 공개되지 않은 위협 프로파일

위와 같이 위험요소들이 기술적인 부분이 아니라 사람과 관련이 있는데, 이에 대해 HP의 보안전략 최고 책임자인 Chris Whitener는 클라우드 컴퓨팅의 보안의 문제점은 기술이 아닌 사람의 문제라고 지적했다.[6]

가트너(Gatrner) 보고서는 위협요인들을 table3과 같이 정의 했는데, 위의 보안위협보다 더 기술적인 위협에 대해 정의하고 있다.[7]

Table 3. Gartner's Threat

보안위협	• 권한 관리자의 접근 • 정책 • 데이터의 저장 위치 • 조사 자원 • 데이터의 분리 • 복구 • 장기적 생존 가능성

또 한국인터넷진흥원(KISA)은 table4와 같이 클라우드 서비스의 보안 위협들을 정의하고 있다.

클라우드 컴퓨팅의 핵심 기술인 가상화의 취약점과 법규 및 규제의 문제에 대해 정의하고 있다.[7]

여러 보안 위협 요인들의 표로 보아 위협 요인들이 굉장히 다양한 것을 알 수 있고, 보안위협들에 대한 보안 대책의 필요성을 알 수 있다.

3.2 보안위협 (가상화 취약성)

앞에 소개한 하이퍼바이저(가상화 기술)을 통해 이용자들의 가상머신이 상호 연결되어 다양한 공격이 존재하며 다른 가상머신 및 하이퍼바이저로 해킹이나 악성코드 등의 전파가 용이해진다.

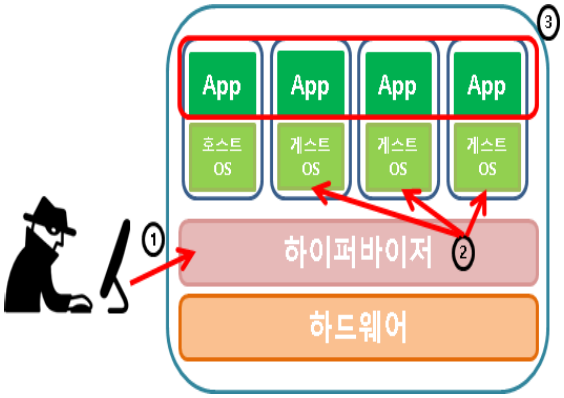

Fig. 3. Hypervizer Hacking's Attack

fig3은 하이퍼바이저 해킹으로 인해 통제권을 상실하게 되는 과정을 그림으로 나타낸 것으로 첫 번째로 해커가 하이퍼바이저를 해킹한다.

두 번째로 하이퍼바이저가 관리하는 모든 게스트 OS 기능을 통제하며 동일 하이퍼바이저 상 모든 사용자의 가상머신이 해커에 의해 노출된다. 세 번째로 서버에 저장되어 있는 모든 사용자의 데이터가 유출되거나 손실된다.

공격자는 해커가 아닌 악성코드가 될 수 있으며 악성코드에 감염 되었을 때는 1차로 호스트OS에서 게스트OS로 감염이 되고, 2차로 게스트OS에서 다른 게스트OS로 감염이 되며, 마지막 3차 감염으로는 하이퍼바이저 감염으로 확산돼 모든 가상머신이 감염된다.[8]

3.3 보안위협 (정보 집중화로 인한 피해)

클라우드 서버 하나에 사용자들의 데이터가 집중되어 저장되기 때문에 해커들에 의한 공격이나 DDOS공격에 당하기 쉽고, 공격 발생시 전 사용자에게 서비스가 연쇄 중단이 되고, 대규모 피해를 일으킨다.

실제 11년 4월 아마존 사이트가 11시간 동안의 장애로 190개 서비스가 동시마비 되었으며 서비스 장애 발생시, 서비스 제공자에게 의존하기 때문에 서비스 제공자가 복구나 패치를 하기 전 이용이 불가하고, 사용자는 원인을 빠르게 파악할 수가 없다.[8]

Fig. 4. Information centralization phenomenon

3.4 클라우드 컴퓨팅 보안 대책

보안 대책으로는 기존의 IT환경에서 사용되었던 사항들이나 클라우드 컴퓨팅의 특성에 맞게 재구성이 필요한

것으로 보인다.[9]

1) SSO(Single-Sign On)에 대한 취약점인지

SSO는 인증 기술의 하나로 한번의 시스템 인증으로 여러 관련 사이트에 재인증 없이 접근할 수 있어 사용자로 하여금 편리함을 제공하는 기술로 최근 클라우드 인증에서 사용되는 기술이다.

그러나 가상화와 보안 보장 생성 언어(AML)의 적용에 따른 문제가 발생해 효율성이 저하되고 하나의 보안만 뚫으면 모든 보안이 뚫리기 때문에 이를 인지하고 새로운 인증 기술 대책을 마련해야한다.[7]

2) 네트워크 보안 신기술 개발

기존의 IT에서 사용되는 보안 기술인 SSL(Secure Socket Layer), Ipsec(IP Security protocol), Ips(침입 방지 서비스)를 클라우드 보안으로 사용하고 있으나 단순히 데이터를 전송하는데 있어서 보안기능이 아닌 가상화와 공유화에 적용되는 보안 기술을 새로 개발,진행 해야 한다.[10]

3) 보안 책임소재 분명 및 정책통일

서비스 모델에 따라 자원의 관리나 책임이 상이하여 보안 책임의 분할이 어렵다고 한다.

서비스 다양한 접속 환경이나 다양한 단말기들 등이 있어 책임 소재를 명확히 규정하는게 어렵다고 하니 책임소재를 분명화하고 정책에 대한 통일화가 필요하다.[8]

4. 결론

클라우드 컴퓨팅은 자원관리의 효율성과 관리비용의 절약이 뛰어나 차세대 컴퓨팅 기술로 주목받고 있지만 더 나아가기 위해서는 보안의 취약성에 대한 문제를 해결해야 할 것으로 보인다.

가상화에 대한 보안 취약점이 존재하며 정보 집중화 현상으로 서버 하나가 공격 당하면 모든 서비스가 중단되는 큰 위기에 빠진다.

이러한 문제를 해결하기 위해 기존 IT환경의 존재했던 보안 기술을 클라우드 컴퓨팅의 핵심기술인 가상화와 공유화를 적용해 새로 보안 기술을 개발하고 악성코드에 감염되거나 DDOS공격에 대비해 단말기의 성능이나 보안을 항상 업데이트 시키는 것이 중요하다.[10]

REFERENCES

[1] Rongxing et al, —Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing, ASIACCS'10, Beijing, China

[2] R. La'Quata Sumter, —Cloud Computing: Security Risk Classification ACMSE 2010, Oxford, USA

[3] Mladen A. Vouch, —Cloud Computing Issues, Research and Implementations, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235 - 246

[4] Wenchaoet al, —Towards a Data-centric View of Cloud Security, CloudDB 2010, Toronto, Canada

[5] Soren Bleikertz et al, —Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds, CCSW 2010, Chicago, USA.

[6] Flavio Lombardi& Roberto Di Pietro, —Transparent Security for Cloud, SAC'10 March 22-26, 2010, Sierre, Switzerland.

[7] Wayne A. Jansen, —Cloud Hooks: Security and Privacy Issues in Cloud Computing, 44th Hawaii International Conference on System Sciesnces 2011.

[8] Jinpeng et al, —Managing Security of Virtual Machine Images in a Cloud Environment, CCSW, 2009, Chicago, USA

[9] Miranda & Siani, —A Client-Based Privacy Manager for Cloud Computing, COMSWARE'09, 2009, Dublin, Ireland

[10] Dan Lin & Anna Squicciarini, —Data Protection Models for Service Provisioning in the Cloud, SACMAT'10, 2010, Pittsburgh, Pennsylvania, USA

저 자 소 개

이 상 호(Sang Ho Lee) [정회원]

▪ 1981년 3월 ~ 현재 : 충북대학교 전자정보대학 소프트웨어학과 교수

<관심분야> : 네트워크 보안, 개인정보보호, 데이터베이스 보안