클라우드 보안 기술과 취약점 분석

김아용* · 이성옥** · 류승한** · 정회경***

*배재대학교

Cloud Security Technology and Vulnerability Assessment

A-Yong Kim* · Sung-Ock Lee** · Seung-Han Ryu** · Hoe-Kyung Jung***

*Paichai University

E-mail : janlssary@pcu.ac.kr, jesuissarah@hotmail.com, mrryu93@hanmail.net, hkjung@pcu.ac.kr

요 약

빅데이터 시대를 맞이하여 주목 받는 기술 중 하나인 클라우드는 인터넷 기반인 컴퓨팅 기술이다. 클라우드는 여러 대의 물리 서버를 하나의 가상 서버로 통합하여 필요할 때 마다 인터넷 상에서 가져와 사용하는 기술이며 현재 미국 IT 선두 기업인 아마존, IBM, 구글, MS와 국내 기업인 삼성, SK, KT, NHN 같은 대기업들이 클라우드에 투자하여 현재 상용화하고 있으며 앞으로 클라우드 시장은 국내외로 계속 성장할 것이다. 클라우드 도입에 주요한 이유는 운영 비용의 절감이며 가장 문제점으로 보이는 것은 개인 정보 유출이다. 본 논문에서는 클라우드 보안 기술과 취약점을 분석하고 보안을 향상시키는 방법을 제안한다.

ABSTRACT

Cloud computing is an Internet-based technology, one of the Big Data era aspiring technology. Bring on the internet whenever you need to use multiple physical servers into one virtual server, cloud Cloud technology and large companies, such as leading U.S. IT company, Amazon, IBM, Google, Microsoft and the domestic firm Samsung, SK, KT, NHN the cloud market at home and abroad, and commercialization by investing in the future to continue to grow. The main reason for the introduction of the cloud and reduced operating costs, and to see the most problems is the leakage of personal information. In this paper, we propose a method to improve the security and vulnerability analysis of security technologies and cloud.

키워드

클라우드, 보안, 취약점, 가상화

Ⅰ. 서 론

기업들은 IT 자원을 효율적으로 사용하면서 비용 절감 효과도 가져오고 환경 보호에도 도움이 되는 클라우드라는 기술을 주목하고 있다. 전문 리서치 회사인 Gartner에서 발표한 2013 IT Trend에 Hybrid IT & Cloud Computing이 포함되어 있다[1]. 이것은 전 세계의 이목을 집중 받고 있는 차기 주력 비즈니스라는 것을 증명한다. 클라우드는 사용자들이 전문 지식과 기술 없이도 자신이 필요한 IT 자원을 네트워크를 통하여 서비스를 받을 수 있으며 사용한 만큼만 과금하는 종량제 개념을 가신 IT 서비스이다. 이러한 서비스는 초기 투자비용과 유지 보수를 요구하지 않아 클라우드 사용은 점차 증가하고 있다. 하지만 네트워크 기반으로 서비스를 공급하기 때문에 보안 부분에서는 문제점이 발생하고 이러한 문제점들은 클라우드 도입에 큰 장애요소로 남게 된다.

이에 본 논문 구성은 다음과 같다. 2장에서는 클라우드 특징과 분류, 가상화를 살펴보고, 3장에서는 클라우드에 사용되는 보안 기술을 분석한다. 4장에서는 클라우드 보안 취약점을 설명하며, 마지막 5장에서는 결론 및 향후 연구과제에 대해 기술한다.

Ⅱ. 관련 연구

2.1 클라우드 특징과 분류

클라우드를 사용하는 사용자는 자원을 무한대로 확장할 수 있거나 필요한 만큼의 수준으로 마음대로 줄일 수 있다[2]. 사용한 자원은 모니터링되어 과금 및 자원 부족에 따른 자원 추가 요청 작업을 할 수 있으며, 다 사용한 자원은 자동으로 반환된다. 클라우드 사용자는 서비스 제공자의 개입 없이 사용할 수 있으며 다양한 기기들로 서비스 받을 수 있다. 클라우드 서비스의 가장 대표적인 서비스는 SaaS, PaaS, IaaS로 분류한다. SaaS(Software as a Service)는 서비스 제공자가 소프트웨어를 네트워크 기반으로 사용자에게 제공하는 모델이다. 클라우드 최상위 계층에 해당하며 다른 서비스에 비해 인지도가 높다. PaaS(Platform as a Service)는 서비스 제공자가 소프트웨어를 개발할 수 있는 환경을 제공해주는 서비스로 사용자는 일반 사용자가 아니라 개발자를 타겟팅하는 모델이다. 대표적인 예는 Google의 AppEngine이 있다. 마지막으로 IaaS(Infrastructure as a Service)는 서비스 제공자가 서버 인프라를 서비스하는 모델로서 사용자는 IT장비를 구매하지 않고 서버나 스토리지 능력을 사용할 수 있게 해준다. 대표적인 예로는 아마존의 S3 및 EC2가 있다.

2.2 클라우드 가상화

클라우드에서 가상화는 자원 가상화를 의미하며 자원 가상화는 스토리지, 네임 스페이스, 네트워크 자원 등과 같은 구체적인 리소스에 대한 가상화를 의미한다[3]. 가상화는 프로세스, 서버, 네트워크, 스토리지로 분류할 수 있다[4]. 가상화 시스템은 반가상화와 전가상화로 분류되며, 게스트 운영체제와 호스트 운영체제 간 자원 공유할 수 있는 기능은 하이퍼바이저 소프트웨어가 담당한다. 따라서 가상 환경에서의 안전한 실행과 관리는 하이퍼바이저에 의해 제공되기 때문에 중요한 부분이다.

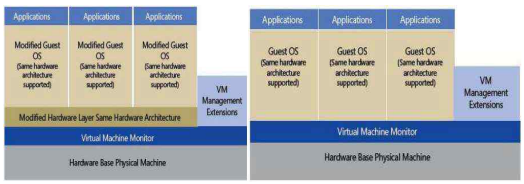

그림 1. 클라우드 가상화 전체 구성도

Ⅲ. 클라우드 보안

3.1 클라우드 보안 기술

•기밀성과 데이터 암호화 : 개인 및 기업 데이터에 대한 기밀성 보호를 위해서는 기본적으로 암호화 기술이 제공되어야 하며 대용량 데이터의 암호화시 전체 시스템의 가용성이 떨어질 수 있다는점을 고려하여 적합한 암호화를 해야 한다[6].

•사용자 인증과 접근제어 : 공용 환경에서 다수의 사용자에게 서비스를 지원하는 것을 고려하여 사용자의 인증과 권한 관리가 필요하다.

•데이터 무결성 : 2008년 7월 AWS S3 서비스 다운 사례는 무결성 검사 루틴이 없었던 데서 기인하였으며, 이 사례로 확인할 수 있듯이 클라우드에서 저장되는 데이터와 교환 메시지에 대한 오류 검사가 매우 중요하다.

•가용성 및 복구 : 서비스 중단 및 데이터 손실을 방지하기 위해서 고장 감내성 및 데이터 복구 기법이 필요하다.

•네트워크 보안 및 웹 보안 : 네트워크 기반으로 서비스를 하고 있기 때문에 기존 네트워크 보안 기술을 활용하여 효율적으로 적용해야 한다.

3.2 가상환경 보안

클라우드 서비스를 가능하게 하는 가장 핵심적인 개념은 가상화(Virtualization)이며 가상 환경에서의 보안은 하이퍼바이저 및 가상 머신에 대한 정기적인 취약점 패치 수행과 물리적 환경에서 적용했던 보안 방식을 가상 환경에서 적용하면 된다.

Ⅳ. 클라우드 보안 취약점

클라우드는 네트워크 기반으로 서비스를 하고 다양한 IT 기기들을 지원하기 때문에 이러한 것은 장점으로 부각되지만 보안 분야에서는 단점으로 부각된다. 특히 가상화는 클라우드에게 많은 이점을 주지만 새로운 공격 시나리오의 출현을 가능하게 했다. 가상환경에서 중요한 역할을 하는 하이퍼바이저는 자체 취약점으로 인해 위협이 노출될 수 있고 악성코드를 사용하여 가상 머신을 감염시킬 수 있다.

Ⅴ. 결론 및 향후연구과제

본 논문에서는 클라우드가 가지고 있는 특징 및 보안 기술, 가상화를 살펴보고 클라우드에서 가장 시급히 해결해야 할 보안 기술 및 취약점을 분석하였다. 클라우드 보안을 향상 시키려면 각 계층마다 보안 체계를 확실히 하고, 모의 해킹 테스트로 취약점을 분석하여 취약 부분을 보완해야 한다. 보안체계 뿐만 아니라 사용자와 관리자에게도 보안 교육을 실시하여 사회공학 위협을 줄여야 한다.

향후 연구 방향은 상용 제품이 아닌 오픈 소스로 보안을 구성하여 효율적인 보안이 되는지를 알아보는 연구 과제이다.

참고문헌

[1] Gartner, http://www.gartner.com
[2] 김형준, 조준호, 안성화, 김병준, “클라우드 컴퓨팅 구현 기술”, 2012년 5월 25일
[3] 김학범, 전은정, 김성준, “클라우드 컴퓨팅 환경에서의 보안관리에 관한 연구” 경영컨설팅 리뷰 제 2권 제 1호, 2011년 2월, pp.127-144
[4] Studnia, Ivan, et al. "Survey of Security Problems in Cloud Computing Virtual Machines." Proceedings of Computer and Electronics Security Applications Rendez-vous (C&ESAR 2012) (2012): 61-74.
[5] 금융부분 클라우드 보안 가이드, 금융보안연구원, 2010.12
[6] 최재규, 노봉남, “클라우드 컴퓨팅 환경에서의 보안 평가 요소”, 보안공학연구논문지 제 8권 제 3호 2011년 6월