안전한 클라우드 데이터센터 구축을 위한 보안요구사항 분석

변연상*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : ysbyun@sch.ac.kr, jkwak@sch.ac.kr

Security Requirements Analysis for construction of Secure Cloud Data Center

Yun-Sang Byun*, Jin Kwak**
*ISAA Lab, Dept. of Information Security Engineering, Soonchunhyang University
**Dept. of Information Security Engineering, Soonchunhyang University

요 약

IT기술 및 인터넷의 발전으로 시·공간의 제약 없이 다양한 서비스를 제공받을 수 있는 클라우드 컴퓨팅 기술이 등장하게 되었다. 이로 인해 기존 데이터센터를 가상화 및 클라우드 컴퓨팅 기술과 융합한 클라우드 데이터센터로 전환하여 개인용 클라우드 서비스(Private Cloud Service)나 외부 기업 등에게 아웃소싱 하여 공개형 클라우드 서비스(Public Cloud Service)를 제공하고 있다. 그러나 클라우드 환경은 기존의 IT환경에서 발생한 악성코드를 이용한 데이터 해킹 및 유출과 같은 보안 위협이 존재하며, 새로운 보안 위협들이 발생하고 있다. 따라서 본 논문에서는 안전한 클라우드 데이터센터 구축을 위한 보안요구사항에 대해서 분석한다.

1. 서론

IT기술 및 인터넷의 발전으로 시·공간의 제약 없이 다양한 서비스를 간편하게 제공받을 수 있는 클라우드 컴퓨팅 기술이 등장하였다. 일부 대기업 같은 경우 클라우드 컴퓨팅 기술을 도입하여 사용자들에게 다양한 서비스를 제공하고 있지만 실제 수많은 기업들은 보안 및 가용성, 구축비용과 같은 이유로 도입하지 않고 있다. 이로 인해 기존 데이터센터를 가상화 및 클라우드 컴퓨팅 기반의 클라우드 데이터센터로 전환하고 있으며, 개인용 클라우드 서비스(Private Cloud Service)나 외부기업에 아웃소싱 하여 공개형 클라우드 서비스(Public Cloud Service)를 제공하고 있다. 그러나 클라우드 환경은 수많은 서버와 스토리지 등으로 구성되어 있어 기존의 IT환경에서 발생한 악성코드유포, 데이터 해킹 및 유출과 같은 보안 위협이 존재한다[1][2].

최근 방어 시스템을 우회하는 지능형 공격 형태가 발생하고 있으며, 클라우드 컴퓨팅 환경은 다양한 경로에서 접속이 가능하기 때문에 악성코드에 감염될 경우 클라우드 데이터센터의 스토리지 또는 데이터베이스에 저장된 데이터가 유출될 가능성이 높다. 또한 특정 환경에 악성코드를 감염시켜 서비스를 제공받는 사용자들이 사용자 모르게 많은 양의 개인정보를 유출시킬 가능성도 존재한다.

클라우드 데이터센터의 경우 수많은 서버와 데이터베이스 등으로 구성되어 있기 때문에 다양한 보안 취약점이 있으며, 악성코드에 감염될 경우 연관된 다른 구성요소들이 취급하는 내부 데이터의 유출 등과 같은 추가적인 피해가 발생할 수 있다[1]. 따라서 본 논문에서는 안전한 클라우드 데이터센터 구축을 위한 보안요구사항에 대해서 분석한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구로 클라우드 컴퓨팅 기술과 클라우드 데이터 센터 보안 위협에 대해서 분석한다. 3장에서는 보안요구사항을 분석하고 끝으로 4장에서 결론으로 끝을 맺는다.

2. 관련연구

2.1 클라우드 컴퓨팅 기술

클라우드 컴퓨팅은 언제 어디서나 소프트웨어나 스토리지 등 사용자가 사용가능한 대부분의 컴퓨팅 자원을 필요한 만큼 제공받아 사용하고 일정 비용을 지불하는 방식이라고 Cloud Security Alliance(CSA)에서 정의하였다. 클라우드 컴퓨팅의 경우 크게 세 가지 유형의 모델로 분류할 수 있으며 각각의 특징을 가지고 있다[3][4].

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임. (2012-010886)

❒ SaaS

SaaS(Software as a Service)는 사용자가 플랫폼 또는 하드웨어 인프라에 관계없이 클라우드 환경에서 동작 가능한 애플리케이션을 서비스 제공자로부터 제공받아 소비하는 형태이다. 사용자가 서비스를 이용할 수 있는 환경을 구축하고 있다면 쉽게 서비스 이용이 가능하다. 또한 간단한 계약절차를 통해 서비스 이용이 가능하다.

인프라부터 애플리케이션의 업데이트, 보안패치 등과 관련된 사항을 서비스 제공자가 일괄 처리하기 때문에 사용자는 편리하게 사용하기만 하면 된다. 하지만 사용자는 서비스 제공자가 제공하는 서비스만 이용가능하고 관리규정을 따라야 한다[1][4].

❒ PaaS

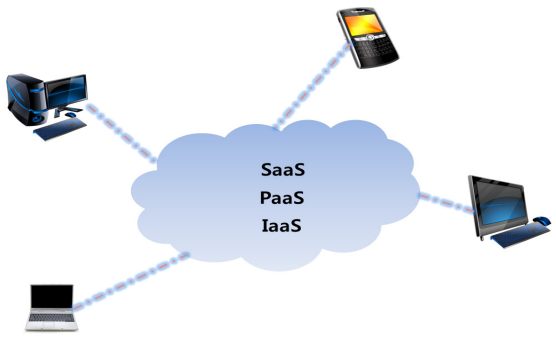
PaaS(Platform as a Service)는 사용자가 자신이 사용하는 애플리케이션부터 애플리케이션을 구동시킬 수 있는 환경까지 제공하는 서비스이다. PaaS는 SaaS의 개념을 플랫폼영역까지 확장한 방식으로 사용자가 개발을 위해 필요한 플랫폼을 구축하지 않고 개발에 필요한 요소들을 클라우드 서비스를 통해 제공받아 사용할 수 있는 방식이다.

또한 서비스 제공자가 확장성 확보를 수행하기 때문에 애플리케이션을 작성하여 플랫폼에 적용만 시키면 PaaS의 기능을 활용할 수 있다. 또한 PaaS는 플랫폼에서 구동되는 애플리케이션을 제어가능하다[2][3].

❒ IaaS

IaaS(Infrastructure as a Service)는 서비스 제공자가 연산 프로세스, 하드웨어, 네트워킹 서버 등을 제공하는 서비스이다. 네트워크부터 스토리지를 서비스 제공자를 통해 이용하는 경우, 별도의 인프라를 구축해야 하는 시간, 비용이 필요하지 않으며 네트워크 기능만 있다면 바로 이용이 가능하다.

주로 서비스 제공자가 인프라의 정비 및 관리를 담당하기 때문에 사용자가 직접적으로 정비, 관리를 하는 것보다 확장성 확보가 쉽고, 가용성이 높다[4].



(그림 1) 일반적인 클라우드 서비스

2.2 클라우드 데이터센터 보안 위협

클라우드 데이터센터의 보안 위협으로는 대표적으로 관리자에 의한 보안 위협, 네트워크 전송간의 보안 위협 , 비 인가된 사용자의 접근으로 인한 접근통제, 프라이버시 보호 등이 있다.

❒ 관리자에 의한 보안 위협

관리자에 의한 보안 위협은 데이터센터의 관리자에 의 기밀 데이터나 중요 자료의 복사 또는 유출과 같은 보안 위협을 나타낸다.

사용자의 기밀 데이터는 클라우드 데이터센터 내에 존재하기 때문에 하이퍼바이저, 또는 관리자에 의한 정보 유출이나 위·변조와 같은 보안위협이 존재한다.

데이터를 외부로 노출시키지 않고 별도로 격리시키는 방법이 안전하지만 격리되었을지라도 서비스 제공자 또는 하이퍼바이저는 데이터 접근에 용이하기 때문에 관리자에 의한 유출 또는 위·변조 등 보안 위협에 노출되어 있다.

❒ 네트워크

클라우드 데이터센터를 이용하기 위해서는 네트워크를 기본적으로 사용할 수 있어야 하는 서비스이다. 만약 사용자와 데이터센터 사이에 네트워크가 불안전하거나, 데이터 전송중 끊어지게 될 경우 서비스 이용이 힘들 뿐만 아니라 데이터의 훼손이 발생할 수도 있다. 추가적으로 서비스 접근을 통해 위·변조 공격이 발생하여 데이터센터 접근을 방해하거나 악용하는 사례가 발생할 가능성이 있으며, 사용자의 개인정보를 탈취하여 사용할 가능성도 존재한다.

❒ 접근통제

클라우드 데이터센터는 수많은 사용자들이 이용하는 서비스로 각 사용자마다 권한부여 및 정책에 맞는 관리가 필요하다. 만약 비 인가된 사용자의 접근으로 인하여 데이터센터내에 악성코드가 유포되거나 자료가 유출될 경우 막대한 피해가 발생하게 된다. 또한 클라우드 데이터센터와 같은 경우 데이터를 서버에 저장하고 수많은 사용자들이 접근하여 사용하기 때문에 보안에 취약하게 된다.

❒ 프라이버시 훼손

기존의 데이터센터와 다르게 클라우드 데이터센터는 서비스제공자가 사용자의 개인정보를 저장 및 관리하는 경우 개인정보를 취급하는 것에 대한 기술적인 측면이나 법률적인 측면을 생각하고 관리를 해야 한다. 클라우드 데이터센터를 이용하는 사용자의 경우 막대한 양의 데이터를 다중으로 이용하는 경우가 많기 때문에 개인정보 저장 및 관리, 개인정보를 취급하는 것에 대한 기술적인 측면이나 법률적인 측면을 고려하지 않는다면 유출과 같은 보안 위협에 노출되게 된다.

3. 보안요구사항

3.1 인증

클라우드 데이터센터는 사용자가 서비스제공자와 계약을 통해 클라우드 데이터센터를 이용할 때마다 인증과정이 필요하다. 인증과정이 완료된 사용자만 클라우드 데이터센터를 이용할 수 있다. 자주 데이터를 열람 및 접근해야 하는 사용자의 경우 인증의 빈도와 횟수에 관련된 문제가 발생할 수 있다. 만약 데이터의 열람횟수가 잦은 사용자가 매번 인증과정을 새롭게 진행하게 된다면 편리하게 사용하기 힘들 것이다. 또한 사용자의 인증정보의 입력 횟수가 증가하게 됨에 따라 유출과 같은 사고가 발생할 수 있다. 이와 같은 문제점은 SSO(Single Sign-On)기능이나, 물리적 보안토큰을 이용하여 해결 가능하다.

또한 기업 상호 신뢰관계를 기반으로 SAML(Security Assertion Markup Language) 등을 연합하여 사용하는 개인정보 관리 방식, 인증과 개인정보의 관리과정에서 인증 시스템의 선택과 정보시스템 간 개인정보의 흐름을 개인정보 소유자가 통제 가능한 사용자 중심의 개인정보 관리 방식 등이 있다[4].

3.2 프라이버시 보호

클라우드 데이터센터는 기존의 데이터센터와는 다르게 가상화 기술을 이용하여 다양한 서비스를 제공하는 기술이다. 데이터센터를 이용하기 위해서는 사용자의 직접적인 관리권에 제약이 발생하며, 데이터의 관리권을 서비스 제공자에게 양도한다는 계약이 필요하다.

클라우드 데이터센터의 사용자는 막대한 데이터에서 다양한 데이터를 다중 이용하는 경우가 많기 때문에 서비스 제공자는 데이터센터에 저장된 데이터 안전성 및 관리 방법에 대해 고려하고 대책을 강구해야 한다. 즉, 중요 데이터의 저장 및 관리하는 서비스 제공자는 기술적인 측면이나 법률적인 측면 등 다양한 방법을 고려해야 한다[3].

3.3 네트워크 보안

클라우드 데이터센터는 네트워크 기능을 필요로 하는 서비스이다. 서비스 제공자와 사용자 사이에 네트워크가 불안하거나, 연결이 끊어지게 될 경우 서비스에 대한 이용이 불가능해지고, 이로 인해 가용성에 문제가 발생하게 된다. 또한 서비스 접근 간 변조공격으로 데이터센터의 이용 및 접근을 방해하거나 악용하여 악의적인 제 3자가 사용자의 서비스를 이용하거나 계정정보를 절취하여 이용할 경우 프라이버시 관련 문제가 발생하게 된다[4].

따라서 서비스 제공자는 DOS공격 등 서비스 거부에 대한 대책 및 사용자 및 디바이스 인증에 대한 대책 등 네트워크에 대한 보안이 필요하다.

4. 결론

본 논문에서는 안전한 클라우드 데이터센터 구축을 위해 보안위협과 보안요구사항에 대해서 분석하였다. 클라우드 데이터센터는 수많은 사용자가 서비스 제공자에게 자신의 정보를 저장하고, 업무를 수행한다. 따라서 데이터센터에 저장된 정보를 안전하게 보관하는 것이 목적이다. 따라서 서비스 제공자를 위한 데이터 관리 지침이나 관련 법규가 필요하다. 또한 향후 발생 가능한 보안위협에 대해서 안전한 클라우드 데이터센터 구축을 위한 보안 기술 및 데이터 관리 기법 등과 같은 구체적인 기술 개발 및 연구가 필요하다.

참고문헌

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

[2] NIST SP 800-144, “Guidelines on Security and Privacy in Public Cloud Computing”, 2011.

[3] 김태형, 김인혁, 민창우, 엄영익, “클라우드 컴퓨팅 보안기술 동향”, 정보과학회지, 2012.

[4] 이형효, IT기획시리즈 - 클라우드 컴퓨팅 보안 연구 동향, 2011.

[5] 김태형, 김인혁, 김정한, 민창우, 김지홍, 엄영익, 클라우드 컴퓨팅 환경에서 보안성 향상을 위한 로컬 프로세스 실행 기술, 정보보호학회논문지, 제20권, 제5호, 2010,

[6] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, March, 2010.

[7] “방통위, 클라우드 개인정보보호수칙(안) 마련,” 방송통신위원회, 2011.