클라우드 컴퓨팅 : 관리적 측면에서의 보안 취약점 분석

최창호* · 이영실** · 이훈재***

*동서대학교 컴퓨터공학과

**동서대학교 일반대학원 유비쿼터스 IT 학과

***동서대학교 컴퓨터정보공학부

Cloud Computing : An Analysis of Security Vulnerabilities in managerial aspect

Chang-Ho Choi* · Young Sil Lee** · Hoon Jae Lee***

*Dept. of Computer engineering Dongseo University

**Dept. of Ubiquitous IT, Dongseo University Graduate School

***Dept. of Computer Information Engineering, Dongseo University

E-mail : ckdgh4832@naver.com, youngsill.lee0113@gmail.com, hjlee@dongseo.ac.kr

요 약

최근 많은 기업들이 빅데이터를 활용할 수 있는 환경을 구축하면서 클라우드 컴퓨팅 기술에 대한 관심이 높아지고 있다. 클라우드 환경은 기존 가상화 환경에서 발전했으나 그 과정에서 관리, 가상머신, 하이퍼바이저, 하드웨어 등 다양한 영역에서 보안적으로 취약점을 들어내고 있다. 이 중 클라우드 환경의 관리적 측면에서의 보안 기법은 보안 위협을 식별 및 통제함으로써 안전하게 데이터를 저장할 수 있는 환경을 제공한다. 본 논문에서는 먼저, 클라우드 서비스를 제공하는 기업과 제공되는 서비스의 종류를 조사하고, 클라우드 환경의 관리적 측면에서 존재하는 보안 위협 요소에 대해서 분석한다. 더불어 최근 발생한 보안 사건·사고들의 사례들을 조사하여 이를 통해 앞으로의 개선 방향을 제시한다.

ABSTRACT

By building an environment that can utilize big data, many companies are interested in the cloud computing technology that has increased its popularity recently. By developing cloud environments from existing virtual environments, in the process, we discovered a variety of security vulnerabilities such as management, virtual machines, hypervisors, hardware etc. The security techniques from administrative aspects in the cloud environment provide the environment which can securely store data by the identification and control of security threats. In this paper, we investigate a list of companies which supports the cloud services and the types of services, and analyze the security threats according to the administrative aspects in the cloud environment. In addition, we suggest the direction for future improvements by investigating accidents or incidents which occurred recently.

키워드

클라우드 컴퓨팅, 빅데이터, 클라우드 보안, 관리적 기법

Ⅰ. 서 론

클라우드 환경이 국내에 활성화됨에 따라 데이터의 보유량이 많은 기업과 공공기관에서 빅데이터를 구축하고 이용하고 있으며, 이를 일반 사용자들에게 공유하고 이용하게 함으로써 다양한 데이터를 모을 수 있는 환경이 갖추어졌다. 이렇게 수집된 데이터는 각각의 서버에 저장되어 최종적으로 대용량 가상화 서버로 이동되고, 이를 분석하여 사용자들에게 다시 서비스를 제공한다. 이렇

게 만들어진 클라우드 환경은 관리적 측면, 가상머신, 하이퍼바이저, 하드웨어 등 다양한 영역에 존재하는 보안 위협 요소들을 가지며, 특히 관리적 측면에서 발생하는 클라우드 서비스 제공자에 의한 보안사건·사고들이 다른 영역에서의 위협 요소들보다 치명적이고, 사건·사고를 파악하는데 있어 어려움을 가진다.

이에 본 논문에서는 클라우드 환경에서 발생하는 보안 취약점들(데이터 관리적 부분, 책임소재를 판별하기 위한 기준이 불확실한 부분, 인가되지 않은 사용자가 임의로 서비스의 사용을 확장 등)을 방지하고 그에 따른 보안사건·사고 사례를 분석하여, 이를 통해 앞으로의 개선 방향을 제시한다.

본 논문의 구성은 다음과 같다. 먼저, 클라우드 환경의 정의 및 현재 제공되고 있는 서비스의 사례들을 2 장에서 서술한다. 또한 3 장에서는 클라우드 환경의 관리적 측면에서의 보안 취약점들에 대해서 기술하고, 4 장에서는 관리 부주의로 인한 사건·사고 사례들에 대해서 나타내었으며, 마지막 5 장에서 결론을 맺도록 한다.

Ⅱ. 관련연구

클라우드 컴퓨팅이란 인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅으로 정의한다.

이러한 환경은 우리가 인터넷 통신, 미디어, 포털 등 다양한 매체를 통해 데이터들을 서버에 저장하고 분석하여 사용자들에게 유선통신망, 방송망, 무선/이동통신망을 이용하여 서비스를 제공한다. 그 특징은 서비스를 받는 사용자들이 자신이 원하는 만큼 서비스 제공자로부터 IT자원을 빌리고 그에 대한 비용을 지급하는 것이다.

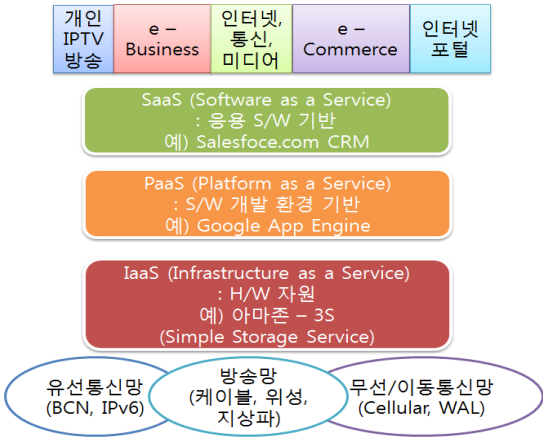

그림 1. 클라우드 컴퓨팅 환경[1]

이러한 클라우드 컴퓨팅 환경은 그림 1과 같이 크게 3가지로 분류할 수 있다. 먼저, IaaS는 H/W 자원을 가상화하여 여러 사용자에게 서비스를 제공하며, PaaS는 H/W 자원을 추상화한 공간 위에 S/W 개발 환경을 서비스로 제공한다. 마지막으로 SaaS는 응용 소프트웨어를 서비스로 제공한다. 먼저 사용자는 일반적인 사용자와 IT 구매자(클라우드 환경)로 분류하였으며, 이에 따라 이용서비스의 종류가 나뉘게 된다.

Ⅲ. 클라우드 환경의 관리적 측면에서 보안 취약점과 보안적인 대처 방법

클라우드 환경에서 관리적 측면은 보안에서 핵심을 나타내고, 위협을 식별 및 통제함으로써 안전한 데이터 저장을 제공할 수 있으며, 이를 통해 클라우드 환경에 적합한 관리 체계를 만드는 것을 말한다.

아래의 표 1은 클라우드 컴퓨팅 환경의 관리적 측면의 취약점[1]을 분류한 표로, 관리적 측면에서 크게 데이터 보안, 관리적 보안으로 취약점을 나눌 수 있다. 이 중 제공자에 의한 관리적 보안 위협으로 발생 원인으로는 클라우드 제공자의 무책임, 관리 미흡, 증거 은닉 등이 있으며, 이러한 요소들로 인해 내부 직원의 권한 남용으로 인한 데이터 유출, 개인과 기업의 사적정보 유출, 관리자에 의한 시스템 잘못된 사용 등 다양한 사고 요인이 되어 보안사건·사고들이 발생한다.

이러한 보안사건·사고들은 사용자들로 하여금 서비스를 이용하는데 있어 많은 불안감을 심어주고 신뢰성을 떨어뜨리게 되므로 다른 보안 위협보다 더욱 치명적이라고 볼 수 있다.

Ⅳ. 관리 부주의로 인한 사건사고 사례들

최근 관리 부주의로 인해 발생한 대표적인 보안사건·사고 사례들을 표 2에서 나타내고 있으며, 이 외에 악의적인 제삼자에 의한 해킹, 서비스 장애, 천재지변 등 다양한 외부적 요인에 의한 사건·사고들이 많이 발생하고 있다. 그러나 내부적 요인(내부 직원들에 의한 데이터 유출, 관리 소홀 등)에 의한 보안사건·사고들은 더욱 피해가 심각하고 사건·사고를 파악하기도 어려워 큰 피해를 불러올 수 있다.

표 1. 클라우드 환경의 관리적 측면에서의 보안 취약점[2]

위협 대상	위협 분류	발생원인	사고 요인
클라우드 위탁/ 제공	데이터 보안	클라우드 제공자의 내부 관리 미흡에 의한 사고	-제공자의 인수, 합병, 폐업 -내부직원의 권한 남용으로 인한 데이터 유출 -개인과 기업의 사적정보 유출 -서버의 잔존데이터
	관리적 보안	클라우드 제공자의 무책임, 관리 미흡, 증거 은닉에 의한 사고	-클라우드 환경 및 협업 클라우드 환경에서 사고발생시 클라우드 제공자와 협력사 간에 책임자를 찾기 힘듬 -클라우드 제공자의 보안 사고에 대한 소극적 대응 가능성 -책임을 판별하기 위한 제공자의 보안통제 관련증거의 은닉 사고 추적을 위한 정보의 접근이 제한 -클라우드 환경 및 협업 클라우드 환경에서의 제한된 보안 정책 적용 -온라인 자동화 셀프 환경에서 사용자 신분 도용 -관리자에 의한 시스템 잘못된 사용. -내부직원의 권한 남용으로 인한 데이터 유출 -개인과 기업의 사적정보 유출

표 2. 관리 부주의로 인한 사건・사고

일시	유형	회사	주요 내용
2008.7	데이터 손실	미디어 맥스	스토리지 업체 미디어 맥스의 폐업으로 데이터 유실 : 약 2만 명의 유료 회원의 데이터가 유실됨[4]
2009.9.24	서비스 장애	구글	2시간 장애 발생(9월 중 2번째 서비스 중단 사태) : 라우터 에러 부터 서버 유지 보수 문제 등 다양한 원인으로 추정[4]
2010.10.12	데이터 유출	MS	BPOS 서비스 환경설정 오류로 인해 기업정보가 유출[3]
2011.2.28	데이터 손실	구글	50만 명의 이용자가 Gmail 메시지 및 주소록이 사라지는 사고 발생 : 기존의 백업데이터로 24시간내 복구되었으나 자세한 원인 밝혀지지 않음[4]
2011.4.21 ~ 4.24	서비스 장애	아마존 EC2	미국 버지니아 북부데이터센터 장애로 11시간 동안 서비스 중단 : 포스퀘어, 레드딧 등 EC2를 통해 서비스하던 고객사들의 서비스가 다수 중단됨[4]
2012.6.20	데이터 손실	First Server	고객 웹 사이트 다운 : 피해 고객 건수는 5698건에 달하며, 모든 백업 삭제, 전원 복구 불가능[4]
2013.2	데이터 유출	메리츠 화재	내부 직원이 분석목적으로 받은 163,925명의 고객 Data를 2013년 2월 유출
2013.5	데이터 유출	RentPath	프리미디어 네트워크에 접속할 수 있는 독립 계약자 한명이 직원과 전직원, 구직자 5만 6000여 명의 정보가 든 하드웨어 분실
2013.5	데이터 유출	Adventist Health System/ Sunbelt	내부 직원으로 인한 정보유출 : 2009 ~ 2011년까지 서비스를 이용한 환자의 기록을 판매
2013.12.11.	데이터 유출	씨티 은행 및 SC은행 등 16개의 금융 회사	내부 직원이 부실한 보안 관리의 허점을 악용 : 고객 정보를 USB 또는 프린트 인쇄물로 제작하여 제 3자에게 전달 (피해 건수 약 13.7건)
2014.1.8.	데이터 유출	국민, 농협, 롯데 카드	고객 인정 사항 정보를 불법 수집하고 그중 일부를 유출한 외부 직원에 의한 사고 (피해 건수 약 1억 400만 건)

Ⅴ. 결론

본 논문에서는 클라우드 컴퓨팅 환경을 위협하는 요소들(적용기술에 의한 위협, 자원 공유에 의한 위협, 데이터 센터의 위치로 인한 위협, 위탁 및 서비스 제공에 의한 위협들)중 관리적 측면에서의 보안 위협에 대하여 논의하였다.

이러한 보안 위협 요소에 대한 대응 방법들을 두 가지로 나눌 수 있는데 첫 번째로는 서비스를 이용하는 사용자의 데이터를 보호하는 영역이다. 유・무형 자산에 대해 소유자, 중요도 식별, 책임, 분류, 취급방법, 라벨링 등을 다루는 표준화된 규정인 ISO 27001의 자산관리 영역과 유사하나 클라우드 서비스에서는 제공자에게 위탁된 이용자의 데이터 자산을 대상으로 한다는 것이다.

두 번째로는 조직의 정보보호 및 운영에 대한 기본 정책을 수립하고 업무 추진 시 체계적인 정보보호 활동을 수행하는 것이다. 이에 해당하는 표준화된 규정은 ISO 27001의 인적보안, 정보보호 정책, 정보보호조직, 준거성, 물리적/환경적 보안 영역을 들 수 있다[3].

현재까지 보안사건・사고에 대한 정책들이 세워지고 그에 따른 관리적 측면에서의 보안 대책은 잘 세워져있지만, 아직까지 서비스를 제공하는 회사들이 지침에 따라 준수를 하는 것을 확인하고 그를 관리하는 대책이 미흡한 실정이다.

이러한 클라우드 컴퓨팅 환경에서, 보안성을 향상시키기 위해 클라우드 서비스에 최적화된 보안 기술을 적용하거나, 전문적인 장비(Spam Filtering, SSL VPN, Viruswall, Spyware Protection, IPS, Firewall 등)의 적절한 사용도 중요하지만, 그에 앞서 서비스 제공 기업 내 담당자들에게 정기적인 보안교육을 실시함과 더불어 서비스 사용자들을 대상으로 보안 교육을 실시하는 등 간단한 기본 인식 제고만으로도 담당자의 관리 소홀 등 관리적 측면에서 발생하는 다양한 보안사건・사고들을 예방할 수 있을 것이라 사료된다.

이를 위해 먼저 서비스 제공 기업은 두 달에 한 번 관리자들의 업무태도 평가 및 한 달에 한 번 관리자들에게 보안 교육 및 인성 교육 실시하고 또한 서비스 사용자들의 데이터에 대한 관리 지침서를 공지하고 보안사건・사고가 발생했을 때, 즉시 문자로 공지하는 서비스를 제공하는 등의 다양한 정책을 수립하는 것도 관리적 측면에서 보안성을 높일 수 있는 여러 가지 방법 중 한 가지 방법일 것이다.

Acknowledgement

이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었으며(과제번호:2013-071188) 또한, 부산광역시에서 지원하는 BB21 과제에서 지원받았음.

참고문헌

[1] 김학범, 전은정, 김성준, “클라우드 컴퓨팅 환경에서의 보안 관리에 관한 연구,” 경영컨설팅 리뷰, 제 2권 제1호, pp.127-144, 2011년 2월.

[2] 은성경, “클라우드 컴퓨팅 보안 기술 동향,” 한국정보보호학회, Vol.20 No.2, 2010년.

[3] 신경아, 이상진 “클라우드 컴퓨팅 서비스에 관한 정보보호관리체계,” 한국정보보호학회, 제 22권 제 1호, 2012년 2월.

[4] 박춘식, “클라우드 보안이 왜 이슈로 대두 되는가?,” CLOUDSE Conference, 2013년 4월.

[5] 정성재, 배유미, “클라우드 보안 위협요소와 기술 동향 분석,” 보안 공학 연구 논문지, 제 10권 제 2호, 2013년 4월.

[6] 박형근, “클라우드 컴퓨팅 보안 동향과 통찰,” Code Conference, 2013년 10월.

[7] 전정훈, “클라우드 컴퓨팅 보안의 취약성에 관한 연구,” Journal of The Korea Institute of Information Secutiry & Cryptology , vol.23, no.6, December. 2013.

[8] 미래창조과학부, 한국인터넷진흥원, “정보보호 관리체계(ISMS) 인증제도 안내서,” 미래창조과학부, 2013년 3월.