한국컴퓨터정보학회 동계학술대회 논문집 제22권 제1호 (2014. 1)

클라우드 컴퓨팅 연구 동향과 보안

김만윤°, 윤희용*
°위덕대학교 정보통신공학
*성균관대학교 정보통신대학
e-mail: benimaru0609@naver.com°, youn@ece.skku.ac.kr*

The Research in Cloud Computing and Security

Man-Youn kim°, Hee-Young Youn*
°College of Information and Communication Engineering, Uiduk University
*College of Information and Communication Engineering, Sungkyunkwan University

● 요 약 ●

정보통신 기술의 발전과 함께 우리는 현재 수많은 정보의 홍수 속에서 살고 있다. 이 수많은 정보를 저장하는 기술로 과거엔 플로피디스크가 있었다. 최근에는 기가바이트 이상의 데이터를 저장하면서 크기도 작은 USB와 하드디스크를 사용하고 있다. 하지만 이것도 이젠 과거의 일이 되어버렸다. 유형의 장비가 아닌 언제 어디서든 인터넷이 가능한 곳이라면 웹상에 원하는 정보를 저장하고 다운로드할 수 있게 되었기 때문이다. 이러한 대용량의 정보를 웹상에 저장하는 핵심기술의 집약체가 바로 클라우드 컴퓨팅 시스템(Cloud Computing System)이다. 기업과 국가의 경쟁력이 된 클라우드 컴퓨팅에도 취약점은 있다. 바로 보안이다. 본 논문에서는 클라우드 컴퓨팅 시스템을 소개하고, 클라우드 컴퓨팅의 보안 취약점에 대한 분석과 대응방안을 제시한다.

키워드: 클라우드 컴퓨팅(Cloud Computing), 보안(Security)

I. 서 론

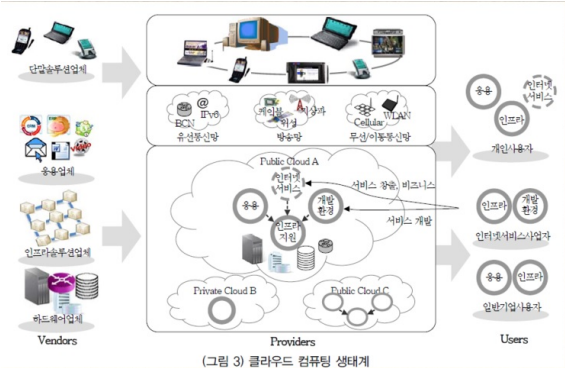
정보화의 급속한 발전과 함께 정보가 넘쳐나는 세상에 우리는 살고 있다. 이 수많은 정보를 저장하고 활용하는 방안의 연구가 활발히 진행 중이다. 1960년대 분산처리 시스템을 시작으로 병렬처리 시스템, 그리드 시스템, 클라우드 시스템이 바로 그것이다. 이 중 클라우드 컴퓨팅 시스템은 현재까지 꾸준히 연구, 개발하고 있는 대용량 컴퓨팅의 핵심기술이다.[1] 클라우드 컴퓨팅 시스템의 발전과 함께 보안 문제도 큰 이슈가 되고 있다. 사용자의 정보 유출과 데이터 보안 등 각종 보안 사고들이 발생하고 있다.

본 논문에서는 클라우드 컴퓨팅을 정의하고, 클라우드 컴퓨팅의 취약점인 보안 문제에 관하여 기술한다

II. 관련 연구

클라우드 컴퓨팅(Cloud Computing)이란 '웹 기반 애플리케이션을 활용하여 대용량 데이터베이스를 인터넷 가상 공간에서 분산처리하고 이 데이터를 데스트톱 PC, 휴대전화, PDA 등 다양한 단말기에서 불러오거나 가공할 수 있게 하는 환경'이라고 IBM은 정의한다.[3]

클라우드 컴퓨팅의 서비스는 크게 SaaS(Software as a Service), IaaS(Infrastructure as a Service), PaaS(Platform as a Service)로 나뉜다. SaaS는 개인과 기업을 대상으로 온라인으로 소프트웨어 서비스를 제공한다. IaaS는 서버, 스토리지, 네트워크 등을 인프라 서비스로 제공하는 것이며, PaaS는 운영체제를 빌려 쓰고 소프트웨어를 개발할 수 있는 환경을 제공한다.



(그림 3) 클라우드 컴퓨팅 생태계

그림 1. 클라우드 컴퓨팅
Fig. 1. Cloud Computing

클라우드 컴퓨팅의 기본 구성은 벤더(Vendors), 제공자(Providers), 사용자(Users)로 나뉜다. 벤더는 서버, 단말기기, 스토리지, 네트워크와

같은 하드웨어 장비들을 납품하는 업체와 SaaS의 응용 소프트웨어를 제공하는 업체, 클라우드 컴퓨팅 솔루션 제공하는 업체 등이 포함된다. 제공자는 벤더로부터 응용 소프트웨어, 솔루션 등을 구매하고 클라우드 컴퓨팅을 직접 운영하게 된다. 사용자는 제공자의 서비스를 사용하고 비용을 지급하여 수익을 내는 주체가 된다. [5]

II. 본 론

1. 클라우드 컴퓨팅 보안

클라우드 컴퓨팅 기술의 발달과 함께 대두되고 있는 여러 문제점 중 하나가 바로 보안이다. 한 번의 보안 사고로 발생하는 사용자의 손실은 막대하다. 클라우드 컴퓨팅의 보안이 그만큼 중요한 이유이다. 클라우드 컴퓨팅의 취약점인 보안 문제에 대응하는 방법에는 다음 사항이 있다.

1.1 데이터 암호화

그리고 데이터 암호화는 서버 내의 데이터 자체를 암호화하는 기술로 해커나 내부에서 어떤 방법으로든 방화벽, 접근 제어 등의 보안을 통과해서 데이터에 접근했다고 해도 암호화되어 있기 때문에 유출되는 위험이 적다.

1.2 악성코드 차단

클라우드 컴퓨팅은 기본적으로 웹 기반의 서비스이기 때문에 DDoS와 같은 악성코드의 공격을 받을 수 있다. 이에 침입을 차단하는 방화벽과 침입 행동을 실시간으로 감지, 제어, 추적할 수 있는 IDS와 같은 시스템을 적용한다.

1.3 다양한 단말의 접속과 데이터 무 결성 검사

스마트폰, 데스크톱 PC, 태블릿 PC 등 다양한 단말의 클라우드 서비스의 접속은 최고의 장점이다. 하지만 다양한 단말의 접속으로 보안의 취약점이 발생하기도 한다. 이에 데이터의 무 결성 검사는 필수이다.

1.4 허가되지 않은 접근에 필요한 인증

인증 방법에는 일반적으로 이름, 주소, 주민등록번호, 전화번호 등을 서비스 제공자에게 제공하여 인증하는 방법과 클라이언트의 IP를 검증하는 인증, 개인 단말기에 저장된 인증서와 키를 이용하는 스마트카드 인증, 전화/문자 인증 등 다양한 인증이 있다. 이에 보안 강화를 위해 이중 인증 시스템이 권장되고 있다.[4]

IV. 결 론

데이터의 크기가 커지고 다양한 빅 데이터 시대가 도래되면서 클라우드 컴퓨팅도 함께 이슈가 되고 있다. 클라우드 컴퓨팅의 기술 발전도 중요하지만 보안 취약점을 사전에 예방하는 것이 가장 중요하다.

ACKNOWLEDGEMENT

본 연구는 한국산학연협회(C0017380), BK21+사업, 한국연구재단 기초연구사업 (2013R1A1A2040257),
(2013R1A1A2060398), 미래부가 지원 한 2013 년 정보통신·방송 (ICT) 연구개발 사업 (1391105003)의 지원을 받아 수행되었음.

참고문헌

[1] Geon Woo Kim, Won Ju Lee, Chang Ho Jeon, “The Virtualization for Cloud Computing", The Korea Society of Computer & Information article18 no.1, 2010. 6

[2] Tae Sik Son, Jong Bin Go, “IoT(Internet of Things) Security Trends in Cloud Computing”, The Korea Institute of Information Security & Cryptology, 2012. 2

[3] Jae Hoon Sun, Kuinam J.Kim, “Cloud Computing in the Vulnerability Alalysis for Personal Information Security, The Journal of Information & Security 2010. 2 article10 no.4

[4] Naver Blog, “[Cloud Computing]Pros and Cons of Cloud Computing, Services and Income Structure”, 2013.11.13.