클라우드 컴퓨팅 환경에서 정보유출 방지를 위한 명령어 감사시스템에 관한 연구

이동영*, 이을석**, 김진철***
*명지전문대 정보통신과
**(주)이너버스 기술연구소
***명지전문대 교양
e-mail:dylee@mjc.ac.kr*, uslee@innerbus.com**,jj9636@yahoo.co.kr***

A Study on the Command Auditing System for preventing the Information-leaking in Cloud Computing.

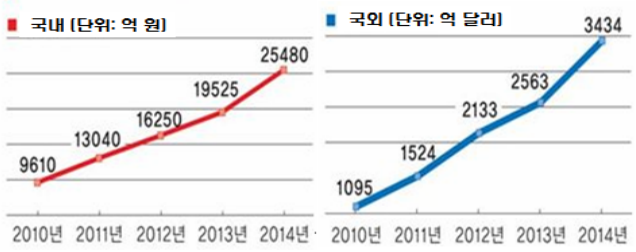
DongYooung Lee*, Eul-Suk Lee** ,Jin-Chul Kim***
*Dept of Information & Communication, MyongJi College
**Institute of Technology, Innerbus Company
***MyongJi College

요 약

최근 인터넷 기술을 활용하여 클라우드 서버에 저장된 IT 자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼의 비용을 지불하는 클라우드 컴퓨팅에 대한 수요가 증가하고 있다. 또한 클라우드 컴퓨팅의 개방성은 사용자에게 많은 편리함을 제공함과 동시에 클라우드 서버에 저장된 정보에 대한 유출은 시급히 해결해야할 문제이다. 이에 본 논문에서는 클라우드 환경에서 내부정보 유출 환경을 살펴보고 클라우트서버로부터의 사용자 명령어를 수집 및 로그(Log)파일로 생성하고 이를 분석하여 내부 정보 유출을 판단하고 이를 보호하기 위한 명령어 감사시스템 구조를 제안하고자 한다.

1. 서론

최근 세계적인 IT 리서치 업체인 가트너는 지난해 말 '2010년 주목할 만한 IT 성장 유망 업종'으로 클라우드 컴퓨팅(Cloud Computing) 시장의 성장을 예상했다. 기업이 활용하는 클라우드 시장의 성장이 두드러지고, 그 뒤에 개인용 클라우드 시장의 성장이 이어질 것이라고 예상했다. 가트너는 2013년에는 기업용과 개인용 클라우드가 서로 결합된 하이브리드형 클라우드 서비스가 시장을 주도해 나갈 것으로 예상했다[1]. [그림 1]은 클라우드 컴퓨팅 시장의 매출액 전망을 나타낸 것이다.



[그림 1]클라우드 컴퓨팅 시장의 매출액 전망

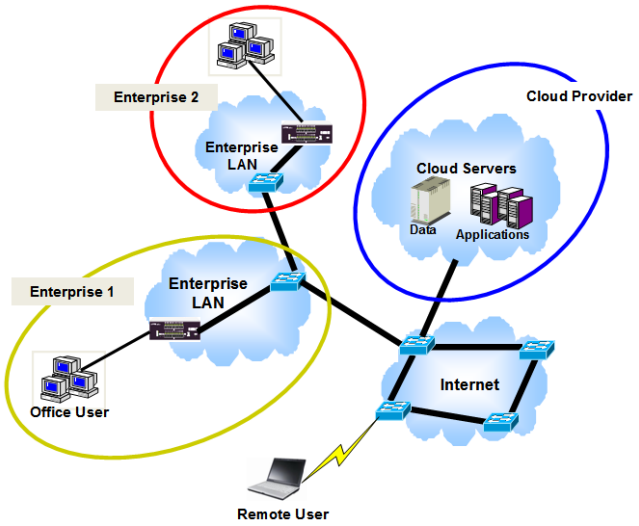
그러나 클라우드 컴퓨팅 서비스가 시장에서 오랫동안 살아남기 위해서는 해결해야 할 문제가 많다. 결정적인 약점으로 지적되고 있는 것이 바로 보안이다. 클라우드 서버는 누구에게나 문이 열려 있으며, 이와 같은 개방형 정책은 클라우드 컴퓨팅의 장점이자 단점이다. 누구나 서버에 접근해 정보를 열람할 수 있고 또 정보를 저장하거나 빼낼 수 있다. 이 경우 개인 정보 유출이나 사업 정보 유출 사고가 일어날 가능성이 높다. 2010년 IBM 비즈니스 가치 연구소(IBV)가 진행한 '2010 글로벌 리스크 서베이'에서 응답자의 77%는 클라우드 컴퓨팅 도입 후 개인 사생활 정보 보호가 더욱 어려워질 것이라고 답했다. 응답자들은 기업 IT 환경에 맞는 보안 시스템과 제도적 장치가 마련되어야 한다는 조언과 함께 내부정보 유출의 문제와 직결된다고 했다[2]. 이에 본 논문에서는 클라우드 환경에서 내부정보 유출 환경을 살펴보고 클라우트서버(유닉스/리눅스)로부터의 사용자 로그를 분석하여 정보 유출을 보호하기 위한 명령어 감사시스템 구조를 제안하고자 한다.

2. 연구 내용

2.1 클라우드 컴퓨팅과 내부정보유출

일반적으로 기업환경에서 서버관리는 조직에서는 내부 직원 및 외주업체, 침입자 등의 다양한 IT주체가 정의된 통제 정책에 따라 기밀성, 무결성, 가용성이 보장 된 상태로 운영될 수 있도록 여러 보안시스템들을 구축하여 관리를 하고 있다. 주요 정보를 관리하는 서버에 접근하기 위한 권한을 관리해주는 접근권한 통제 시스템이나 원격에서의 데이터 전송을 감사하거나 암호화 채널을 사용하는 등의 노력을 하고 있으나 많은 시스템 관리자 및 유지·보수에 많은 비용이 소요되고 있는 실정이다.

이에 클라우드 컴퓨팅의 경우 기업사용자는 자신이 소유하고 있는 IT자산을 클라우드 형태로 제공받기를 원하지만, 자신의 데이터가 타인과 공유됨으로 인한 정보유출은 클라우드 컴퓨팅을 도입하려는 기업에는 해결해야 할 중요한 선행과제이다[3-4]. (그림 2)는 기업-기업(Enterprise-to-Enterprise)간의 정보를 공유하는 클라우드 컴퓨팅 모델을 나타낸 것이다.

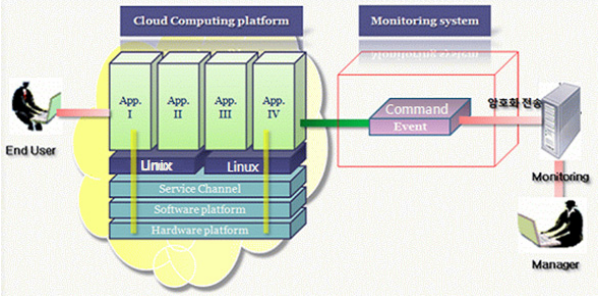


(그림 2) 클라우드 컴퓨팅모델(Enterprise to Enterprise)

2.2 클라우드 컴퓨팅에서 명령어 감사시스템 구조

클라우드 컴퓨팅 플랫폼에서 권한이 있는 사용자가 시스템에 접근하여 권한범위 안에서의 활동을 할 경우라도 그 내용이 보안에 위배되는 행위를 수행할 경우 이에 대한 수행내역을 감사 할 필요가 있다. 사용자가 시스템에서 실행 한 행위 중 가장 중요한 부분은 사용자가 입력한 명령어이며, 현재는 개별 시스템에 들어가서 history 등을 하나씩 개별 확인을 해야 가능한 형태로 구성되어 있다.

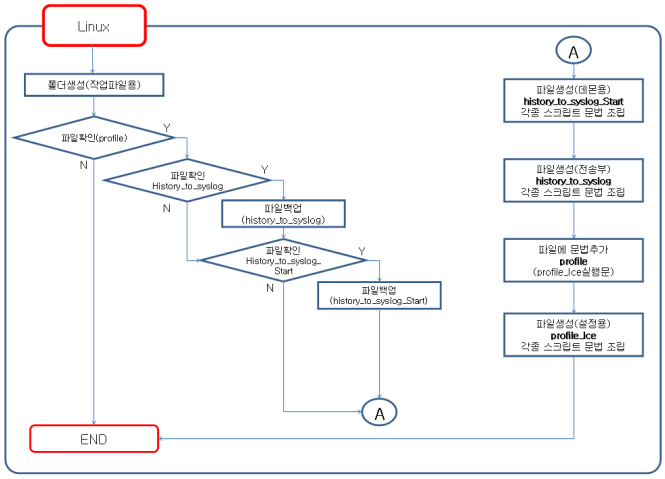
그리고 이에 대한 통합감사가 가능하도록 각 서버시스템에서 각 사용자의 실행 명령어를 에이전트시스템으로부터 수집하여 로그(Log) 형태로 발생시키고, 이를 중앙 서버로 전송하여 통합하는 것이 필요하다. (그림 3)은 클라우트컴퓨팅 플랫폼에서 명령어 감사시스템의 구조를 나타낸 것이다.



(그림 3) 클라우트컴퓨팅 명령어 감사시스템의 구조

2.3 명령어 감사시스템 동작 메커니즘

클라우드 컴퓨팅 플랫폼에 존재하는 유닉스/리눅스 서버에서 우선 본 논문에서는 오픈소스인 리눅스서버를 대상으로 프로토타입(prototype)으로 개발을 진행하고 있으며 (그림 4)는 리눅스서버로부터 에이전트(A)를 통해서 명령어 수집을 위한 환경설정 과정을 나타낸 것이다.



(그림 4) 명령어 수집을 위한 환경설정 과정

클라우드 컴퓨팅 플랫폼에 존재하는 리눅스 서버에 (그림 4)의 과정을 통하여 로그인시 명령어 수집을 위한 변수설정, trap규칙에 대한 명령문을 등록한다.

3. 연구 결과 및 향후 계획

클라우드 컴퓨팅의 개방성은 사용자에게 많은 편리함을 제공함과 동시에 클라우드 서버에 저장된 정보에 대한 유출은 시급히 해결해야할 문제이다. 이에 본 논문에서는 클라우드 환경에서 내부정보 유출 환경을 살펴보고 클라우트서버로부터의 사용자 명령어를 수집 및 로그(Log)파일로 생성하고 이를 분석하여 내부 정보 유출을 판단하고 이를 보호하기 위한 명령어 감사시스템 구조를 제안하였다. 현재 리눅스 서버를 대상으로 프로토타입(prototype)으로 구현을 진행하고 있다. 향후 계획으로는 프로토타입으로 개발된 시스템에 대한 성능 평가 및 다른 OS로의 확장이 요구된다.

참고문헌

[1] 김명준, “Korea’s Cloud Computing Strategy,” 2009년도 IT21 글로벌 컨퍼런스, 2009. 5.

[2] 정제호, “클라우드 컴퓨팅의 현재와 미래, 그리고 시장 전략,” 한국소프트웨어진흥원, 2008. 10.

[3] 은성경,조남수,김영호,최대선, “클라우드 컴퓨팅 보안기술” 전자통신동향분석 제24권 제4호, 2009. 8

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, Apr. 2009