# 클라우드 컴퓨팅 환경에서 비정상 사용자 추적을 통한 효율적 침입 탐지 방안 연구

이준호*, 박민우*, 강동민*, 정태명**
*성균관대학교 전자전기통신공학과
**성균관대학교 정보통신공학부
{jhlee83, mwpark, dmkang}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

# An Efficient Intrusion Detection Method by Tracing Anormal User in Cloud Computing

Jun-Ho Lee*, Min-Woo Park*, Dong-Min Kang*,
and Tai-Myoung Chung**
*School of Information Communication Engineering, Sungkyunkwan Univ
**Dept of Electrical and Computer Engineering, Sungkyunkwan Univ

요 약

클라우드 컴퓨팅 환경에서 가상머신에 침입 탐지 시스템을 사용하는 것은 중대한 트레이드-오프를 갖는다. 강력한 보안 서비스를 적용할 경우 시스템의 성능이 저하될 수 있으며, 시스템 성능을 위해 보안 서비스의 수준을 낮출 경우 시스템이 안전하지 못할 수 있다. 또한, 클라우드 컴퓨팅 시스템의 경우 짧은 시간 동안 엄청난 양의 보안 로그가 쌓이기 때문에 무작정 보안 로그를 작성하는 것은 비효율적이다. 본 논문에서는 사용자 행위를 기준으로 비정상 정도를 판단하고 이를 바탕으로 멀티-레벨의 보안 서비스를 제공할 수 있는 방안을 제안한다.

## 1. 서론

기업들은 세계경제위기를 맞아 원가절감을 위한 방안으로 고가의 IT 기기 비용을 축소하는 방안을 모색하고 있다. 또한, 최근 그린IT가 각광을 받기 시작하면서 클라우드 컴퓨팅이 빠르게 성장하고 있다. 클라우드 컴퓨팅이란 인터넷 기술을 활용하여 여러 고객들에게 확장성을 가진 IT 자원들을 제공하는 컴퓨팅 서비스이다. 클라우드 컴퓨팅 환경을 사용하는 고객은 자신에게 필요한 만큼의 자원만을 할당받아 사용이 가능하다. 현재 클라우드 컴퓨팅 서비스는 그 유형에 따라 IaaS(Infrastructure as a Service), PaaS(Platform as a service), SaaS(Software as a Service) 등 다양하다. 이러한 다양성과 인터넷이 사용 가능한 장소면 어디서나 서비스를 받을 수 있는 편리성에 의해 많은 사람들로부터 관심을 받고 있다.

하지만 클라우드 컴퓨팅은 동일한 도메인에 많은 사용자의 데이터가 존재한다는 점에서 해커들의 공격대상이 되기 쉽다. 또한 고객과 시스템 관리자 역시 잠재적으로 클라우드 컴퓨팅을 공격할 수 있는 위협요소로 분류할 수 있다[1]. 이러한 클라우드 컴퓨팅 환경에서의 보안은 기존의 컴퓨팅 보안 기술과 모델을 그대로 적용시키는 것은 적합하지 않다. 따라서 본 논문에서는 클라우드 컴퓨팅 환경에 적합한 침입 탐지 시스템 구축 방안을 제시한다.

본 논문은 다음과 같이 구성되었다. 2장에서는 기존의 클라우드 컴퓨팅과 IDS의 특성과 문제점에 대해서 살펴보고, 3장에서는 본 논문에서 제안하는 클라우드 컴퓨팅의 IDS 구조와 구성에 대해 소개하며, 4장에서는 본 논문의 결론에 대해 제시하였다.

## 2. 관련연구

### 2-1. 클라우드 컴퓨팅

클라우드 컴퓨팅은 경제성과 유용성, 무한한 확장성으로 인하여 향후 세계 IT기술을 선도할 전략산업으로 성장될 것으로 기대되고 있다[2]. 기존의 컴퓨팅 시스템은 각 기업이 서버와 데이터센터를 구축하고, 필요시 추가적으로 장치를 증설하는 작업을 수행하였다. 이러한 방식은 인터넷 사용인구의 증가와 정보의 생산량이 기하급수적으로 늘어남에 따라 기업들에게 IT자원의 증설부담과 비효율적인 자원 운영 및 관리를 초래하였다. 따라서 기업들은 필요한 만큼의 자원을 손쉽게 증설하고 관리할 수 있는 클라우드 컴퓨팅에 대해 관심을 갖게 되었다.

클라우드 컴퓨팅은 새롭게 등장한 기술이 아니라 기존의 여러 첨단 기술들이 융합된 형태의 새로운 패러다임이다. 분산된 자원들을 공유하여 강력한 컴퓨팅 능력을 제공하는 그리드 컴퓨팅, 자원 사용량에 따라 과금하는 유틸리티 컴퓨팅, 서버에 응용프로그램, 데이터 등을 저장해 두고 사용자가 필요시 서버에 접속해서 서버의 자원으로 처리하는 방식의 서버 기반 컴퓨팅(Server Based Computing, SBC), SBC와 동일하게 서버에 응용프로그램과 데이터를 저장하지만 이용자의 자원으로 처리하는 방식의 네트워크 컴퓨팅, 1대의 컴퓨터에 여러 개의 운영체제를 동작시킬 수 있는 가상

화 등이 융합된 기술이다[3]. 특히 가상화를 실현시키는 기술인 하이퍼바이저는 여러 개의 운영체제를 동작시키기 위한 가상 플랫폼으로써, 실제 물리적인 자원을 여러 운영체제를 관리하는 호스트 OS와 사용자가 이용하는 게스트 OS에게 논리적으로 제공한다.

여러 가지 기술이 복합적으로 작용하는 클라우드 컴퓨팅의 보안은 기존의 접근방법으로는 충분한 안전성을 제공하지 못한다. 특히 클라우드 컴퓨팅 환경에서 사용될 수 있는 공격 기법, 악성코드 등에 대응하기 위해서는 클라우드 컴퓨팅의 환경을 이해하고, 공격 방식의 특성을 파악해야 한다.

## 2-2. IDS

IDS란 시스템에 대해 정당한 사용자가 원치 않는 조작을 탐지하는 시스템이다. IDS는 설치 위치에 따라 특정 호스트의 컴퓨터에 설치되는 호스트 기반 IDS(Host-based IDS), 네트워크 트래픽을 감시하는 네트워크 기반 IDS(Network-based IDS)로 분류할 수 있다. 또한 탐지 방법에 따라 알려진 공격 행위로부터 시그니처를 추출하여 룰 셋에 저장하고 분석 대상에 공격 시그니처가 있는지 비교하는 오용탐지(Misused Detection)방식과 기존의 네트워크 사용 상황을 기반으로 정상적인 행위 범위를 설정해두고 이 외의 모든 행위를 비정상행위로 간주하는 비정상행위 탐지(Anomaly Detection)방식이 있다[4].

호스트 기반 IDS는 각 호스트에 설치되어 정밀한 점검이 가능하지만 모든 호스트에 H-IDS를 설치하기 위해서는 경제적 부담이 크기 때문에 하나의 네트워크에 하나의 IDS만 설치하여 운용하는 네트워크 기반 IDS방식이 선호되고 있다. 오용탐지 기법의 경우 알려진 공격 행위는 정확하게 탐지할 수 있지만, 새로 등장하거나 알려지지 않은 공격 기법의 경우 탐지하기가 힘들다는 단점 때문에 알려지지 않은 공격도 탐지하는 비정상행위 탐지 방식이 각광을 받고 있다. 하지만, 공격이 아닌 경우에도 공격으로 인식하는 경우가 많기 때문에 많은 양의 로그를 발생시킨다는 단점이 존재한다. 그럼에도 불구하고 비정상행위 탐지 방식은 알려지지 않은 패턴의 공격 행위를 탐지할 수 있다는 장점 때문에 많은 연구가 진행되고 있다.

## 3. 제안방식

본 논문에서는 클라우드 컴퓨팅에서의 효율적인 침입 탐지를 위하여 네트워크 기반 방식에서 게스트 OS들의 비정상적인 행동패턴의 평가기준을 제시한다. Multi-level로 이루어진 비정상행위 탐지시스템(Anomaly-based IDS, A-IDS)은 호스트 OS에 설치되어 평가기준에 명시된 비정상 행동에 대해 정의된 위협수준을 적용한다. 위협수준은 게스트OS에게 적절한 탐지 강도를 제공할 수 있도록 한다.

## 3-1. 비정상 행동패턴 평가

A-IDS는 클라우드 컴퓨팅 서비스 사용자들의 행동 패턴에 대한 평가를 수행하며, 각 행동 패턴에 따른 비정상 정도를 점수로 판단한다. 사용자는 트래픽을 발생시킬 때마다 A-IDS로부터 행동을 평가받으며, 사용자가 로그오프할 때까지 점수가 유지된다. 또한, A-IDS는 사용자의 행동 패턴에 대한 점수를 누적하여 평가한다. 비정상적인 사용자의 행동을 평가하는 기준은 <표 1>과 같다.

<표 1> 비정상 행동패턴 평가 기준

| 비정상적인 행동패턴 | 위협 수준 |
|---|---|
| 업무시간외 서비스 관리자 계정으로의 로그인 또는 시도 | 5 |
| 단일 게스트OS의 트래픽이 평상시보다 500% 이상인 경우 | 4.5 |
| 관리자가 다수의 호스트OS에 접근하는 행위 | 4 |
| 사용자가 클라우드 서비스 이용 중에 원격 단말기의 IP주소가 바뀌었을 경우 | 3.5 |
| 단일 게스트 OS의 트래픽이 평상시보다 300% 이상인 경우 | 3 |
| 관리자가 특정 호스트 OS에 접근하려는 행위 | 3 |
| 게스트 OS가 할당되지 않은 메모리 영역에 접근하려는 행위 | 2 |
| 사용자가 로그인 과정 중 자격증명이 5번 이상 틀린 경우 | 1.5 |
| 동일한 호스트 OS에서 동작하는 게스트 OS간에 세션이 설정된 경우 | 1.5 |
| 동일한 호스트 OS에서 다수의 게스트 OS가 동작 중일 때 게스트OS들의 트랜잭션 발생이 저조한 경우 | 1 |
| 단일 게스트 OS의 트래픽이 평상시보다 150% 이상인 경우 | 1 |
| 사용자가 개인정보를 변경하는 경우 | 1 |

위협수준은 비정상적인 행동패턴이 실제 공격으로 이어질 경우 예상 되는 피해 규모를 바탕으로 도출하였다. 단일 게스트 OS의 트래픽 증가는 악성코드 또는 해킹에 의해 트래픽을 발생시켜 과금시키는 공격(Economical Denial of Service, EDOS)을 염두에 둔 행동패턴이다. 다수의 게스트 OS가 미미한 트랜잭션을 발생 시키는 경우, A-IDS는 호스트 OS내의 게스트 OS가 정상적이지 않은 상태라고 판단한다. 클라우드 컴퓨팅 환경에서는 서비스 관리자 역시 잠재적인 공격자가 될 수 있으므로 서비스 관리 인터페이스도 가상화 되어야하며, 관리자에 의한 공격은 클라우드 컴퓨팅 환경에서는 치명적인 결과를 초래하므로, 관리자의 행동 패턴은 A-IDS에 의해 감시된다.

## 3-2. Multi-level IDS

사용자에게 할당되는 게스트 OS는 호스트 OS에서 동작하는 IDS를 통해 보호 받는다. 이때, 호스트 OS에서 동작하는 A-IDS의 탐지율을 높이기 위해서는 다양한 시그니처를 이용하여 탐지과정을 수행하기 때문에 전체 시스템의 효율이 떨어진다. 이를 보완하기 위한 방안으로 각각의 호스트 OS에는 각기 다른 탐지율의 A-IDS가 동작한

다. 그리고 사용자가 가상머신을 할당 받기 원하는 시점에서 사용자의 비정상 정도를 확인하여 비정상 정도가 높은 사용자는 보다 높은 탐지율이 적용된 호스트OS에 할당하고 비정상 정도가 낮은 사용자는 비교적 탐지율이 낮은 호스트OS에 할당해 준다. 본 논문에서는 탐지 정도에 따라 3종류의 A-IDS로 분류하였으며, <표 2>와 같다.

<표 2> 게스트OS의 호스트OS 배치기준

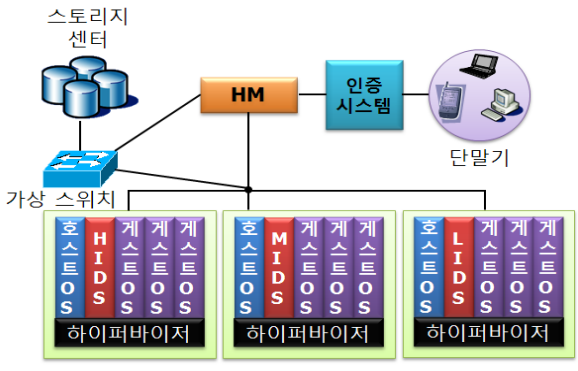
| 침입 탐지 수준 | 행동평가기준 |
|---|---|
| 높음 | 3.5이상 |
| 중간 | 2~3.9 |
| 낮음 | 0~1.9 |

높은 수준의 A-IDS는 업데이트된 모든 룰 셋을 이용하여 공격이라고 의심될 만한 행동을 탐지한다. 중간 수준의 A-IDS는 중요한 공격 패턴과 시스템에 크게 영향을 줄 수 있는 룰 셋을 이용하여 침입을 탐지한다. 낮은 수준의 A-IDS는 중요한 공격 패턴과 시스템에 영향을 줄 수 있는 룰 셋만을 이용하여 침입을 탐지하게 된다.

IDS는 하나의 게스트 OS에서 발생하는 비정상적인 행동들에 대한 위협수준을 합산하여 결정한다. 게스트 OS들에 대한 평가 결과가 결정되면 게스트 OS들은 위협 수준에 적합한 호스트 OS를 할당 받는다. 하나 또는 여러 위협이 발생하여 기존의 침입 탐지 수준을 변경해야 할 경우 게스트OS를 다른 침입 탐지 수준을 유지하고 있는 호스트OS로 이동시킨다.

### 3-3. 비정상 사용자 추적을 통한 침입 탐지 모델

본 절에서는 제안한 비정상 행동패턴 평가와 Multi-level IDS가 구성되기 위한 침입 탐지 모델을 (그림 1)에 나타내었다.




(그림 1) 제안하는 클라우드 컴퓨팅 침입 탐지 모델

하이퍼바이저 매니저(Hypervisor Manager, HM)는 하이퍼바이저들의 상태를 주기적으로 관리하고, 사용자에게 호스트 OS를 할당 및 회수하며, 사용자가 로그아웃할 때의 위협 수준 정보를 저장하는 등의 작업을 수행한다. 사용자가 클라우드 컴퓨팅 서비스를 이용하기 위해 인증절차를 통과하면, HM은 사용자의 저장되어 있는 위협 수준을 확인한다. HM은 위협 수준에 적절한 IDS를 운영하고 있는 호스트 OS들의 자원 가용량을 확인하고, 사용자 정보에 인증키를 추가하여 게스트 OS 할당을 요청한다. 요청을 받은 호스트 OS는 사용자에게 게스트 OS를 할당하고, 사용자 정보와 인증키를 하이퍼바이저에게 전달한다. 사용자 정보와 인증키를 받은 하이퍼바이저는 이 정보를 이용하여 가상 스위치에게 사용자의 데이터를 요청한다. 가상 스위치는 사용자 정보와 인증키가 정당한지 HM에게 확인 후 스토리지 센터에 존재하는 사용자의 데이터를 하이퍼바이저에게 논리적인 링크시킨다.

게스트 OS와 호스트 OS가 주고받는 트랜잭션과 트래픽 정보들은 A-IDS에게 포워딩된다. (그림 1)에서의 HIDS는 높은 수준의 A-IDS, MIDS는 중간 수준의 A-IDS, LIDS는 낮은 수준의 A-IDS를 의미한다. 게스트 OS의 위협수준이 변경되면, 적절한 IDS 배치를 위해 가상머신 마이그레이션(Virtual Machine Migration) 기법을 이용하여 호스트 OS를 변경한다[5].

호스트 OS들이 동일한 수준의 능력을 가진다고 가정하였을 때, LIDS는 MIDS나 HIDS보다 호스트 OS의 자원 사용량이 적으므로 더 많은 게스트 OS를 할당할 수 있어 클라우드 컴퓨팅 환경에 적합한 자원 운용을 할 수 있다. 또한 사용자의 비정상적인 행동을 A-IDS로 추적하고, 신뢰성 있는 사용자에게는 더 유연한 보안 정책을 설정함으로써 기존의 IDS들의 False Positive 로그를 줄일 수 있다.

## 5. 결론

클라우드 컴퓨팅은 사용자에게 경제적이고 무한한 컴퓨팅 파워를 가져다 줄 수 있지만, 다수의 사용자의 민감한 데이터들이 저장된다는 점에서 매력적인 공격 대상이다. 따라서 클라우드 컴퓨팅의 보안을 강화해야 하지만, 기존의 IDS는 클라우드 컴퓨팅 환경을 고려하지 않았기 때문에 자원의 사용이 크고, 동시다발적으로 생산되는 엄청난 양의 로그는 관리자로 하여금 분석이 불가능하게 한다.

본 논문에서는 클라우드 컴퓨팅 환경에서 게스트 OS의 이상행위 수준에 따라 다른 수준의 IDS의 감시 하에 동작하게 함으로써 로그를 감소시키고 효율적으로 자원을 관리할 수 있는 방안을 제시하였다.

## 참고문헌

[1] enisa, "Cloud Computing Risk Assessment", Nov. 2009
[2] Gartner inc, "The Top 10 Strategic Technogies for 2010", Gartner Symposium/ITxpo, Oct. 2009
[3] 이주영, "클라우드 컴퓨팅의 특징 및 사업자별 제공 서비스 현황", 정책통신연구원, Apr. 2010
[4] 양대일, "정보 보안 개론", 2008, 한빛미디어
[5] Kento S, Hitoshi S, Satoshi M, "A Model-based Algorithm for Optimizing I/O Intensive Applications in Clouds using VM-Based Migration", 9th IEEE/ACM International Symposium, Cluster Computing and Grid, 2009