Journal of the Korea Convergence Society
Vol. 7. No. 1, pp. 1-8, 2016 http://dx.doi.org/10.15207/JKCS.2016.7.1.001

클라우드 융합을 위한 MAC 정책 기반 접근통제 메커니즘

최은복[1], 이상준[2*]
[1]전주대학교 스마트미디어학과, [2]전남대학교 경영학부

Access Control Mechanism based on MAC for Cloud Convergence

Eun-Bok Choi[1], Sang-Joon Lee[2*]
[1]Dept. of Smartmedia, Jeonju University
[2]School of Business Administration, Chonnam National University

요 약 클라우드 컴퓨팅 환경은 가상화 기술을 이용하여 네트워크에 기반한 컴퓨터 자원, 소프트웨어, 인프라 등을 서로 공유하는 기능을 제공한다. 가상화는 기업의 서버 운영효율과 비용절감을 위해 매우 유용한 기술이지만 보안을 고려하지 않고 수행할 경우 새로운 보안 위협의 대상이 될 수 있다. 본 논문에서는 클라우드 시스템 환경에서 발생할 수 있는 다양한 문제점을 해결하는 클라우드 융합을 위한 MAC 기반 접근통제 메커니즘을 제안한다. 이 메커니즘은 접근통제 시스템 모니터의 상태규칙 집합, 보안특성 그리고 알고리즘으로 구성된다. 본 논문에서는 제안된 접근통제 메커니즘을 갖는 제어 시스템과 초기 보안 상태가 안전한 시스템임을 증명하였다. 본 메커니즘은 정책 모듈을 통해 접근통제 시스템들 간의 통제된 자원들이 서로 안전하게 공유되며 유지 관리되어질 수 있는 장점을 제공한다.

• Key Words : 클라우드 컴퓨팅, 가상화 보안, 접근통제, 강제적 접근 통제 방식, 보안 정책

Abstract Cloud computing technology offers function that share each other computer resource, software and infra structure based on network. Virtualization is a very useful technology for operation efficiency of enterprise's server and reducing cost, but it can be target of new security threat when it is used without considering security. This paper proposes access control mechanism based on MAC(Mandatory Access Control) for cloud convergence that solve various problem that can occur in cloud environment. This mechanism is composed of set of state rules, security characteristics and algorithm. Also, we prove that the machine system with access control mechanism and an initial secure state is a secure system. This policy module of mechanism is expected to not only provide the maintenance but also provide secure resource sharing between virtual machines.

• Key Words : Cloud Computing, Virtualization Security, Access Control, MAC(Mandatory Access Control), Security Policy

*Corresponding Author : Sang-Joon Lee(s-lee@chonnam.ac.kr)
Received November 10, 2015 Revised December 23, 2015
Accepted February 20, 2016 Published February 29, 2016

1. 서론

오늘날 컴퓨터 기술은 이동성 보장을 위해 다양한 운영체제에 새로운 유형의 기기를 업무에 활용할 수 있는 클라우드 환경으로 빠르게 변화되고 있다. 클라우드 컴퓨팅은 네트워크에 기반한 컴퓨터 자원, 소프트웨어, 인프라 등을 서로 공유하는 서비스로서, 클라이언트 컴퓨터나 다른 장치들이 네트워크를 통해 클라우드가 제공하는 서비스를 이용할 수 있다. 클라우드 기술은 모바일, 빅데이터, 소셜 컴퓨팅 등 정보통신기술의 중심축으로서 다양한 정보기술의 진화를 이끌어 내는 역할을 수행하고 있다. 특히, 정보기술 기기와 기능의 융합, 산업과의 융합, 나아가 휴먼 융합 등 클라우드 기반의 융합 기술은 새로운 가치를 창조하는 창조경제의 핵심이 되고 있다. 국내외 산업에서의 클라우드 기반의 융합 서비스는 홈 오토메이션, 로봇, 교육, 금융, 자동차, 조선 등 다양한 분야에 걸쳐 수행되고 있으며, 기존 주력 산업과의 융합을 통해 산업간, 산업 내 기술, 서비스 등 전반적인 산업성장에 일조할 것으로 전망되고 있다[1].

가상화 기술은 1960년대부터 등장하였으나, 인터넷과 스마트 단말을 통한 클라우드 컴퓨팅이 확산되면서 클라우드의 핵심기술로 등장하였다. 가상화 기술을 통해 다중의 독립적인 컴퓨터 시스템을 하나의 하드웨어 컴퓨터 시스템으로 기능을 통합하는 것이 가능하다. 가상화 기술은 대기업뿐만 아니라 중소 중견기업의 조직의 효율성과 대응력을 강화할 수 있고, IT 비용을 절감할 수 있어서, 효과적인 컴퓨팅 환경으로 인식되고 있다[2].

전통적인 시스템 소프트웨어 시스템과 달리, 가상머신 시스템은 가상화된 시스템에서 운영체제와 하드웨어 사이에 가상머신시스템의 삽입이 가능하여 특화된 개별 운영체제로 운영되는 다중 가상머신을 동시에 운영할 수 있는 장점을 갖는다[3,4].

클라우드 컴퓨팅 환경에서는 다중 가상머신을 구성하는 하드웨어 및 응용 프로그램들 간에 많은 자원들이 서로 공유된다. 이런 환경에서는 연관된 가상머신 간에 자원을 안전하게 공유할 수 있는 접근통제 메커니즘이 요구된다. 또한, 보안성이 높은 데이터가 낮은 보안등급을 갖는 사용자에게 노출 및 변경되는 것을 방지하기 위해서는 클라우드 시스템 내・외부의 정보의 흐름을 통제하고 관리할 수 있는 메커니즘이 필요하다.

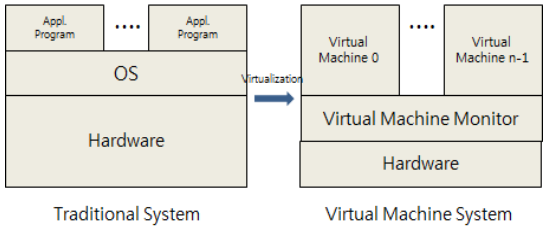
본 논문에서는 클라우드 환경에서의 보안 강화를 위해, 상태규칙집합과 보안특성으로 구성된 보안정책에 의해 접근통제하는 MAC(강제적 접근통제) 기반 가상머신 접근통제 메커니즘을 제안하였다.

2. 가상화

2.1 가상화 개념

가상화는 컴퓨터 자원의 물리적인 상태를 추상화하여 사용자들에게 논리적이고 가상적인 리소스를 분할 제공하여 기술적, 관리적, 경제적 이점을 제공하는 기술이다. 가상화 기술은 다중 가상머신들이 하나의 물리적 머신 내에서 독자적인 방법으로 운영될 수 있게 함으로서 컴퓨팅 자원을 효율적으로 활용하고 이에 대한 접근 및 관리에 대한 오버헤드를 최소화하는데 목적이 있다. 가상머신시스템은 독자적인 가상머신의 집합에서 다중의 협력 관계의 가상머신 그룹으로 진화되므로 그룹간의 적절한 접근통제 메커니즘과 하나의 그룹간 제한된 자원 공유가 제공되어야한다[5].

기존의 전통 시스템에서는 단일의 하드웨어에서 단일의 운영체제만이 수행되며 해당 운영체제가 하드웨어를 독점하여 운영되었다. 가상화 기술이 적용되면 [Fig. 1]과 같이 단일의 하드웨어 상에서 복수개의 논리적인 가상머신이 동시에 구동될 수 있으며, 각각의 가상머신에서는 서로 다른 종류의 운영체제가 독립적으로 수행될 수 있다.



[Fig. 1] Virtualization

가상화 시스템에서 가장 핵심적인 역할을 하는 소프트웨어 요소는 가상머신 모니터(하이퍼바이저)이다. 가상머신 모니터는 가상머신과 하드웨어 사이에 위치하여 다수의 가상머신들이 동작할 수 있게 해주는 가상화 계층을 제공한다. 이를 위해 각 게스트 운영체제(가상머신에서 동작되는 운영체제)가 구동될 수 있도록 논리적으로 독립된 가상머신 환경을 제공해주며, 이러한 게스트

운영체제의 CPU 및 메모리 등을 포함한 하드웨어 자원을 각 가상머신에 논리적으로 분할 할당하며, 이들의 스케줄링을 담당하는 역할을 수행한다[6].

2.2 가상화 보안

클라우드 핵심인 가상화 기술은 인터넷과 스마트 단말을 통한 클라우드 컴퓨팅이 확산되면서 핵심기술로서 중요성이 커지고 있다[2].

가상화는 기업의 서버 운영효율과 비용절감을 위해 매우 유용한 기술이지만, 보안을 고려하지 않고 수행할 경우 새로운 보안 위협의 대상이 될 수 있어 유의하여야 한다. 가상화 환경에서의 보안 문제는 기본적으로 기존 보안 솔루션들이 하나의 서버 내부가 아닌 서버 간의 트래픽을 모니터링 하도록 설계되었기 때문에 발생한다. 가상환경에서는 다양한 운영체제가 동작되고 있어 가상머신 간의 해킹 공격과 더불어 악성코드 감염에 가상머신이 감염될 경우 내부로 확산될 수 있는 가능성이 많다. 또한, 공격자가 가상 머신의 한 시스템을 점유하여 가상 네트워크를 통한 패킷 스니핑 공격기술을 수행하여 시스템 정보를 불법 유출시킬 우려가 있다. 가상화 환경에서는 정보의 분산 저장 및 처리로 인하여 기존의 정보 보호 기술을 기반으로 한 통제 정책으로는 한계가 있으며, 클라우드 서비스의 관리자가 갖는 권한 정도에 따라 고객의 정보를 조회할 수 있는 가능성에 대한 우려도 고려되어야한다[7,8].

가상화 환경에서 발생하는 대부분의 보안 위협은 보안 취약점이 존재하여 발생된다. 보안 위협은 사용자의 권한 남용 및 공격자의 권한 획득에서 비롯되며, 정보 유출 및 자원남용으로 인한 서비스 거부가 발생할 수 있다. 그러므로 다수의 사용자 데이터가 공존하는 가상화 기술에서 사용자에 대한 정확한 사용자 인증과 권한 관리를 위한 접근 제어 기법이 필요하다. 또한, 사용자 인증과 접근 제어를 위해 합법적인 권한을 가진 사용자의 접속 보장 메커니즘과 인증 및 접근 제어 정책 그리고 역할별 보안등급 부여 등 다양한 보안 요구사항을 고려하여야 한다. 서버 가상화 시스템을 사용 및 관리할 때 필요한 권한은 역할별로 다르므로 개발자, 관리자, 사용자 등과 같은 각각의 역할별로 필요로 하는 최소의 권한만 부여되어야 한다[1,9].

2.3 BIBA 모델

MAC(강제적 접근통제) 모델에서는 규칙기반 정책(Rule Based)과 관리기반(Administrative Based) 정책이 통제기법으로 이용된다. 규칙기반 정책은 군사 환경이나 매우 제한적인 환경에서 제한된 수의 보안 관리자들에 의해 일정한 규칙에 따라 사용자의 정보에 대한 접근을 통제하고 보안등급이 결정된다. 이와 반대로 임의적 접근 통제 모델은 정보의 소유자들이 임의적으로 접근권한을 다른 사용자에게 위임할 수 있으며, 신분기반 정책과 사용자기반 정책을 통제기법으로 이용하며, 접근을 요청한 주체가 객체에 대한 권한을 자율적으로 다른 주체에게 권한을 부여하거나 철회할 수 있다[10,11].

강제적 접근통제정책의 대표적인 모델은 BLP(Bell & LaPadula)와 BIBA 모델[12]을 들 수 있는데, BLP모델은 권한을 갖지 않는 사용자에게 정보가 흘러가는 것을 예방하는 비밀성에 기반을 둔 모델로서, 정보의 비밀성은 보장하지만 등급이 낮은 주체가 등급이 높은 객체의 정보를 변경할 수가 있어 정보의 무결성을 보장하지는 못한다. 이러한 단점을 보완하기 위해 무결성 보안정책에 의해 정책이 수행되는 BIBA 모델이 제안되었다. 이 무결성 보안정책은 크게 두가지로 분류한다. 하나는 Crucial(C), Very Important (VI), Important(I)로 구분되는 무결성 보안등급이고 다른 하나는 범주의 집합이다. 무결성 보안등급은 C>VI>I의 관계를 형성하며, 범주의 집합은 BLP모델과 마찬가지로 비계층 구조 관계를 갖는다. 만약, $C_1 \geq C_2$ 이고 $S_1 \supseteq S_2$의 관계를 가지면 무결성 보안등급 $L_1=(C_1,C_2)$는 $L_2=(C_2,S_2)$를 지배한다. 무결성 보안등급이 $L_1 \geq L_2$ 나 $L_2 \geq L_1$ 의 관계가 모두 아니면 이 두 등급은 비교가 가능하지 않다는 것을 의미한다[13,14,15].

BIBA 모델은 정보의 무결성을 보장하기 위해서 하나의 보안정책을 사용하지 않고, 해당 보안 환경에 맞는 여러 가지 보안 정책을 사용하는데 이중 일반적으로 이용되는 정책은 다음과 같다[5,16,17].

❒ 엄격한 무결성 정책(Strict integrity policy)

· Simple integrity : 주체의 무결성 등급이 객체의 무결성 등급에 지배된다면 주체는 객체에 Observe 오퍼레이션을 수행할 수 있다.

· Observe $\in$ M[s,o] $\Rightarrow$ $f_s(s) \leq f_o(o)$

· Invocation property : Invoke 오퍼레이션을 요청할 주체의 무결성 등급이 요청될 주체의 무결성 등급을 지배한다면 Invoke 오퍼레이션을 수행할 수 있다.

$$\cdot \text{Invoke } f_{s1}(s) \geq f_{s2}(s) \Rightarrow \text{Invoke}$$

❒ ☆(star) 무결성(integrity Star property)

· 주체의 무결성 등급이 객체의 무결성 등급을 지배한다면 주체는 객체에 Modify 오퍼레이션을 수행할 수 있다.

$$\cdot \text{Modify} \in M[s,o] \Rightarrow f_c(s) \geq f_o(o)$$

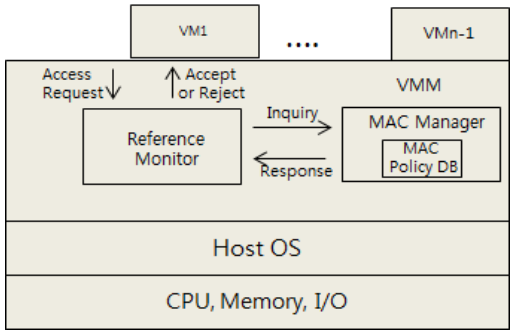
3. MAC 기반 접근통제 메커니즘

클라우드 컴퓨팅 환경의 가상머신시스템에서 가상머신모니터(VMM : Virtual Machine Monitor)와 다중 가상머신들의 하드웨어 및 응용 프로그램들 사이에 많은 자원들을 서로 공유하도록 하여, 연관된 가상머신들과 자원을 안전하게 공유할 수 있는 접근통제 메커니즘이 요구되어진다.

이러한 가상화 환경에서 보안성이 높은 데이터가 낮은 보안 단계의 사용자에게 노출 및 변경되는 것과 같은 정보의 불법 유출과 고의적인 자원 남용과 같은 심각한 보안위협요소를 사전에 예방하기 위해서는, 가상화 사용자에 대한 정확한 사용자 인증과 권한 관리를 위한 접근제어 기법이 필요하다. 개발자, 관리자, 사용자 등과 같은 각각의 역할별로 필요로 하는 최소의 권한만 부여되도록 유지관리 되어야 한다.

접근통제 메커니즘은 전형적으로 사용자가 자신이 소유하는 데이터에 대한 접근을 관리하는 임의적 접근통제 정책에 의존하고 있다. 그러나 이런 종류의 통제 정책은 증명된 약점을 갖고 있는데, 관리수준의 접근이 한 사용자에서 다른 사용자로 이전될 수 있어 네트워크 서비스에서 부당한 사용자로부터 접근정보가 취득되어지는 취약성을 갖는다.

본 논문에서는 클라우드 시스템 환경에서 발생할 수 있는 문제점을 보완하기 위해 [Fig. 2]와 같이 제3자에 의해 정의된 보안정책에 의거 접근을 통제하여 보안을 강화한 MAC 기반 가상머신 접근통제 구조를 제안하였다.



[Fig. 2] Architecture of Access Control based on MAC

가상머신들과 하드웨어 사이에 위치하는 가상머신모니터의 MAC정보 관리자에 탑재된 MAC정책 모듈을 통해, 가상머신 주체와 또 다른 가상머신의 객체의 접근 여부를 조회하여 참조모니터를 통해 요청여부를 통보하게 된다. 또한 정형적으로 기술되어지는 상태규칙 집합, 보안특성 그리고 알고리즘으로 구성된 접근통제 메커니즘을 통해 가상머신들이 안전한 방법으로 통제된 자원들을 서로 공유하며 자원들을 관리할 수 있다.

3.1 접근통제 정의

❒ 정의 1 :주체의 집합 $S = \{S_0,S_1,...,S_{n-1}\}$와 객체의 집합 $O=\{O_0,O_1,...,O_{n-1}\}$는 가상머신들로 구성되며, 가상머신중 S_0와 O_0는 신뢰주체와 신뢰객체를 갖는 관리자 가상머신을 나타내며, 나머지 $S`=\{S_1..S_{n-1}\}$과 $O`=\{O_1,...,O_{n-1}\}$은 사용자 가상머신들로 구성된다.

❒ 정의 2 : I(Integrity)는 무결성 보안등급의 집합으로 $I = \{(cr, vi, i)\}$를 갖으며 cr>vi>i의 관계를 갖는다. K는 범주의 집합이며, L는 무결성 보안등급의 집합으로 $L \in I \times K$로 $l_i=(i_i,k_i)$를 갖는다. $\propto$은 지배관계를 나타내는 기호로 만약 $i_i \geq i_j$ 이고 $k_i \supseteq k_j$이면 $l_i \propto l_j$로 표기하고 지배한다고 읽는다.

❒ 정의 3 : M은 접근모드의 집합으로 M ={c, d, r, a, w}에서 c는 생성(create)모드, d는 제거(delete)모드, r은 읽기(read)모드, a는 추가(append)모드, w는 쓰기(write)모드를 나타낸다.

❒ 정의 4: R은 접근 요청집합으로 R={R1 ,R2, R3}을 갖는데 R1은 가상머신들의 접근모드를 변경하기 위한 요청집합으로 R1 = S X O X M 로 구성되며, R2는 가상머신들을 생성하기 위한 요청집합으로 R2 = S_0 X O' X L 로 구성되며, R3는 가상머신들을 종료하기 위한 요청집합으로 R3 = S_0 X O'로 구성된다.

❒ 정의 5 : 시스템 상태 V = (b,M,f,H) 에서, b는 현재 접근 집합으로 b⊆(S×O×M)를 갖으며 b는 어떤 주체가 어떤 객체에 무슨 접근권한을 가지고 있는지를 나타낸다. M은 정의 3에 기술한 접근모드 집합이며, f={f_{si}(s), f_{oi}(o)}에서 f_{si}(s)는 무결성 주체 보안등급함수, f_{oi}(o)는 무결성 객체 보안등급함수을 의미한다. f_s(s)는 주체의 강화보안등급 함수, f_c(s)는 주체의 현재 강화보안등급 함수로 f_s(s) ∝ f_c(s)의 지배관계를 갖는다. H는 트리 구조를 갖는 현재 객체의 계층구조로 활성화 상태가 아니거나 접근할 수 없는 객체는 이 계층구조에 포함되지 않는다.

❒ 정의 6 : D는 결정집합으로 모든 요청 R에 대한 y(yes),n(no),er(error),?(잘못된 요청형식)을 갖는다.

R:(s,o,x)→D={y, n, er}은 주체 s가 객체 o에 대하여 x 접근모드를 요구하고, 주체 s가 x 모드를 갖는 객체 o를 부여받을 때 y(yes) 이고, 주체 s가 x 모드를 갖는 객체 o에 대해 거절될 때 n(no)이고 두 개 이상의 값이 공존할 때 er(error)이다.

3.2 접근통제 규칙

가상머신시스템에서는 가상머신 그룹들이 존재하며 다른 가상머신의 그룹 간에는 안전한 격리 상태가 유지되어야 한다. 본 논문에서는 이러한 가상머신시스템에서 가상머신을 생성, 종료하고 가상머신들의 접근속성을 조정하고 변경하는 등의 가상머신 접근통제 메커니즘을 구성하는 규칙을 기술한다. 가상머신시스템에서 관리자 가상머신은 새로운 사용자 가상머신을 생성하거나 운영중인 사용자 가상머신을 종료할 수 있도록 하기 위해서는 다음과 같은 보안 규칙이 보장되어야 한다.

❒ 규칙1(RULE1). 가상머신 생성(create)

시스템 상태 v ={b,M,f,H}에서 v'= (b, M, f',H'), f'={f_s, f'$_o$, f_c} H'= {H ∪ H(O_i)}

❒ 규칙 2(RULE2). 가상머신 종료(delete)

시스템 상태 v ={b,M,f,H}에서 v'= (b', M', f, H'), b'= b - {s_i,o_j,(r,a,w)} M'={M - M_{ij}} H'= {H - H(O_j)}

가상머신시스템에서 관리자 가상머신의 보안특성은 가상머신시스템의 활동주기 동안에 상태정보에 대한 정보관리가 보장되지만, 사용자 가상머신의 보안 특성은 가상머신간의 제한된 공유기능을 제공하기 위해서 정당한 요청에 따라 동적으로 할당되고 제거되어진다. 안전한 가상머신 시스템을 유지하기 위한 가상머신 S_i와 가상머신 O_j에 속한 데이터에 대한 읽기 (read), 쓰기(write), 추가(append) 보안 특성의 규칙은 다음과 같다.

❒ 규칙3(RULE3) 가상머신 읽기(read) 보안 특성

시스템 상태 v ={b,M,f,H}에서 v'={b ∪ {(S_i,O'$_j$,r), M, f, H}

❒ 규칙4(RULE4) 가상머신 추가(append) 보안 특성

시스템 상태 v ={b,M,f,H}에서 v'={b ∪ {(S_i,O'$_j$,a), M, f, H}

❒ 규칙 5(RULE5). 가상머신의 쓰기(write) 보안특성

시스템 상태 v ={b,M,f,H}에서 v'∪ {(S_i,O'$_j$,w), M, f, H}

3.3 접근통제 알고리즘

MAC기반 가상머신 접근통제 메커니즘의 의사결정 알고리즘은 다음과 같다. 먼저, 관리자 가상머신 S_0는 w나 a'접근모드를 갖는 o'$_i$에 대해 보안 등급의 지배구조가 다음 조건을 만족하는 경우 보안 등급 L_j를 갖는 새로운 가상머신 O'$_i$를 생성할 수 있으며 이를 정형적으로 정의하면 다음과 같다.

SWITCH(Ac_Rule_of_VM)
CASE CREATE:
IF [O'$_i$ ∈b(S_0,c(w,a))] AND [f_{oi}(o) ∝ f_{si}(s)] & [f_{ci}(o) ∝ f_{ci}(s)]
 THEN
{
v'(b, M, f',H'f'={f_s, f'$_o$, f_c} H'= {H ∪ H(O_i)}
reutrn R = [{create, S_0, O'$_i$, L_j} ∈ R2]는 Permit;

}
ELSE
return Deny;

관리자 가상머신이 기존의 사용자 가상머신을 종료시킬 경우, 관리자 가상머신과 사용자 가상머신이 다를 경우, 기존의 접근 집합과 접근행렬 그리고 계층구조에서 종료할 사용자 가상머신의 내용을 제거함으로서 종료되어지며 이를 정형적으로 정의하면 다음과 같다.

CASE DELETE:
IF {$O_j \neq O_0$}
THEN
{
v'= (b', M', f, H'), b'= b - {s_i,o_j,(r,a,w)} M'={M - M_{ij}} H'= {H - H(O_j)}
return R=[{delete, S_0, O_j} ∈ R3]는 Permit;
}
ELSE
return Deny;

가상머신시스템에서 관리자 가상머신의 보안특성은 가상머신시스템의 활동주기 동안에 상태정보에 대한 정보관리가 보장되지만, 사용자 가상머신의 보안 특성은 가상머신간의 제한된 공유기능을 제공하기 위해서 정당한 요청에 따라 동적으로 할당되고 제거되어진다. 안전한 가상머신 시스템을 유지하기 위해서 가상머신 S_i는 가상머신 O_j에 속한 데이터에 대한 읽기 (read), 쓰기 (write), 추가(append) 보안 특성의 규칙은 다음과 같다.

CASE READ:
IF [O'_j ∈b(S_i: r)] AND $f_{oi}(o) \propto f_{si}(s)$
THEN
{
v'={b ∪ {(S_i,O'_j,r), M, f, H}
return R =[{S_i,O'_j,r} ∈ R1]는 Permit;
}
ELSE
return Deny;

CASE APPEND:
IF [O'_j ∈b(S_i:a)] AND $f_{si}(s) \propto f_{oi}(o)$
THEN
{
v'={b ∪ {(S_i,O'_j,a), M, f, H}
return R =[{S_i,O'_j,a} ∈ R1]는 Permit;
}
ELSE
return Deny;

CASE WRITE:
IF [O'_j ∈b(S_i:w)] AND $f_{si}(s) = f_{oi}(o)$
THEN
{
v'={b ∪ {(S_i,O'_j,w), M, f, H}
return R =[{S_i,O'_j,w} ∈ R1]는 Permit;
}
ELSE
return Deny;

3.4 접근통제 규칙의 검증

가상머신 시스템 상태는 <b, M, f, H>의 4개의 튜플로 구성되어 v∈V로 표기되며 시스템 상태변화는 규칙 : R X V → D X V으로 기술된다. 규칙은 이전 시스템상태, 요청에 기반을 둔 새로운 시스템 상태 그리고 응답으로 정의할 수 있으며 만약 각각의 시스템 상태가 안전하다고 한다면 해당 전체 시스템은 안전하다고 정의할 수 있다.

❒ 공리 1 규칙 집합 W = {RULE1, RULE2,.., RULE5}는 안전한 상태유지 규칙들의 집합이다.

본 논문에서는 규칙 3(RULE3)을 기초로 하여 접근통제 규칙의 안전성을 검증하며 다른 규칙들은 같은 방법에 의해 검증되어질 수 있다. 규칙 3(RULE3)은 가상머신 읽기(read) 보안특성으로 시스템 상태 v ={b,M,f,H}에서 v'={b ∪ {(S_i,O'_j,r), M, f, H}을 특성을 정의되어진다. 규칙3에 의한 요청집합에 대한 결정집합 (D_m, v') = RULE3(R_k, v)에 의해 만약 v가 2.3절에 기술된 BIBA모델의 세가지 보안특성인 simple, invocation, integrity 보안특성을 만족한다면 v'도 당연히 BIBA모델의 보안특성을 만족할 것이다. 만약 규칙3에 존재하는 조건이 만족하지 않는다고 가정하면 v'와 v는 상태 변화가 없는 v'= v의 값을 가지므로 v'는 BIBA 모델의 보안특성을 역시 만족하게 된다. 상태집합 b에 (S_i,O_j,r)이 추가되는 b={b ∪(S_i,O_j,r)}상태를 가정하자. 이때 만약 (S_i,O_j,r)이 상태집합 b에 이미 존재하는 (S_i,O_j,r)∈b 라면 v'= v이고 v'는 세가지 보안특성을 만족하며, 만약 (S_i,O_j,r)이 상태집합 b에 이미 존재하지 않는 새로운 상태집합인 (S_i,O_j,r)∉b

라고 한다 하더라도, RULE3에 제시된 $f_{oi}(o) \propto f_{si}(s)$ 특성은 BIBA모델의 read(observe)연산에 해당하는 simple integrity 보안특성을 만족하게 되므로 결국 RULE3은 안전한 상태 유지 규칙이라고 볼 수 있다.

4. 결 론

클라우드 컴퓨팅은 네트워크에 기반한 컴퓨터 자원, 소프트웨어, 인프라 등을 서로 공유하는 서비스로서, 클라이언트 컴퓨터나 다른 장치들이 네트워크를 통해 클라우드가 제공하는 서비스를 이용할 수 있다. 클라우트 컴퓨팅 환경을 조성하는 가장 중요한 구성요소중 하나인 가상화 기술을 통해 다중의 독립적인 컴퓨터 시스템을 하나의 하드웨어 컴퓨터 시스템으로 기능을 통합하는 것이 가능해지고 있다. 가상화는 기업의 서버 운영효율과 비용절감을 위해 매우 유용한 기술이지만 보안을 고려하지 않고 수행할 경우 새로운 보안 위협의 대상이 될 수 있어 유의하여야 한다.

전 세계적인 클라우드의 활성화 추세에도 불구하고 기업이나 정부의 클라우드 도입에 있어 가장 걸림돌이 되고 있는 것은 가상화 환경에서 새롭게 발생하는 정보보호 취약성에 대한 우려 때문이다. 특히, 연관된 가상머신 간에 자원을 안전하게 공유할 수 있는 환경을 제공하기 위해서는 무엇보다 클라우드 시스템 내· 외부의 정보의 흐름을 통제하고 관리할 수 있는 접근통제 메커니즘이 절실히 요구된다.

정보의 분산 저장 및 처리로 인하여 기존의 정보 보호 기술을 기반으로 한 통제 정책으로는 한계가 있으며, 특히 다수의 사용자 데이터가 공존하는 가상화 기술에서 사용자에 대한 정확한 사용자 인증과 권한 관리를 위한 접근 제어 기법이 절실히 요구되어진다.

본 논문에서는 클라우드 시스템 환경에서 발생할 수 있는 다양한 문제점을 해결하는 MAC 기반 가상머신 접근통제 구조를 제안하였다. 가상머신모니터의 MAC정보관리자의 MAC정책 모듈을 통해 가상머신 주체와 또 다른 가상머신의 객체의 접근 여부를 조회하여 참조모니터를 통해 요청여부를 통보하게 되며 정형적으로 기술되어지는 상태규칙 집합, 보안특성 그리고 알고리즘으로 구성된 접근통제 메커니즘을 통해 통제된 자원들이 서로 공유되며 관리되어진다.

향후 연구방향으로는 비밀성, 무결성과 더불어 무책임한 자원공유 문제를 해결할 수 있는 정보의 활용성에 중점을 두는 가용성 측면의 연구를 병행할 예정이다.

REFERENCES

[1] ITU-T Y.CCDEF, “Information technology – Distributed application platforms and services – cloud computing — Overview and Vocabulary”, 2013.

[2] Security Requirements for Server Virutalization System, Telecommunications Technology Association, pp. 1-18, 2013.

[3] F. Sabani, “Virtualization-Level Security in Cloud Computing”, International Conference on Communication Software and Networks(ICCSN), pp. 250-254, 2011.

[4] M. Bishop, Computer Security : Art and Science, Addison Welsey, Vol. 200, 2012.

[5] H. Zhu, Y. Xue, Y. Zhang, X. Chen, H. Li, and X. Liu, “V-MLR : A Multilevel Security Model for Virtualization”, International Conference on Intelligent Networking and Collaborative Systems(ICINCS), pp. 9-16, 2013.

[6] G. Sala, D. Sgandurra, and F. Baiardi, “Security and Integrity of a Distribute File Storage in a Virtual Environment”, IEEE Security In Storage Workshop, pp. 58-69, 2007.

[7] F. Sabahi, “Cloud Computing Security Threats and Responses”, International Conference on Communication Software and Networks(ICCSN), pp. 245-249, 2011.

[8] M. Khan, K. Sakamura, “Context-Aware Access Control for Clinical Information Systems”, International Conference on Innovations in Information Technology, pp. 123-128, 2012.

[9] T. Y. Win, H. Tianfield, and Q. Mair, “Virtualization Security Combining Mandatory Access Control and Virtual Machine Introspection”, International Conference on Utility and Cloud Computing(ICUCC), pp. 1004-1009, 2014.

[10] G. Cheng, H. Jin, D. Zou, A. K. Ohoussou, and F. Zhao, “A Prioritized Chinese Wall Model for Managing the Covert Information Flows in Virtual Machine Systems”, International Conference for Young Computer Scientists(ICYCS), pp. 1481-1487, 2008.

[11] A. Corradi, R. Montanari, and D. Tibaldi, “Context-based Access Control for ubiquitous Service Provisioning”, Proceedings of the COMPSAC ’04, 2004.

[12] K. J. Biba, "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, 1975.

[13] D. Zou, L. Shi, H. Jin, “DYM-MAC: A Mandatory Access Control System in Distributed Virtual Computing Environment”, International Conference on Parallel and Distributed Systems(ICPDS), pp. 556-563, 2009.

[14] D. George, V. Nirmal, “SECCON:A Framework for Applying Access Control Policies in Context-Aware Wireless Networks”, World Congress on Computing and Communication Technologies, pp. 268-270, 2014.

[15] National Security Agency, Security-Enhanced Linux(SELinux). http://www.nsa.gov/selinux.

[16] S. Castano, DATABASE SECURITY, ADDISON-WESLEY. pp. 39-60.

[17] M. Blanc, J. Briffaut, J.-F., Lalande, C. Toinard, “Distributed Control Enabling Consistent MAC Policies and IDS based on a Meta-Policy approach”, IEEE POLICY’06, 2006.

저자소개

최 은 복(Eun-Bok Choi) [정회원]

- 1992년 2월 : 전남대학교 전산학과 (이학사)
- 1996년 2월 : 전남대학교 일반대학원 전산학과 (이학석사)
- 2000년 8월 : 전남대학교 일반대학원 전산학과 (이학박사)
- 2002년 ~ 현재 : 전주대학교 스마트미디어학과 교수

<관심분야> : 통신망관리, 접근통제, 가상화 보안, 홈 네트워크

이 상 준(Sang-Joon Lee) [정회원]

- 1991년 2월 : 전남대학교 전산통계학과 (이학사)
- 1993년 2월 : 전남대학교 일반대학원 전산통계학과 (이학석사)
- 1999년 8월 : 전남대학교 일반대학원 전산통계학과 (이학박사)
- 1995년 3월 ~ 2007년 2월 : 신경대학교 정보통신학과 조교수
- 2007년 2월 ~ 현재 : 전남대학교 경영학부 교수

<관심분야> : 경영정보시스템, 전자상거래, 지식서비스, 정보보호