ISSN 2586-1816
Journal of Convergence for Information Technology
e-ISSN 2586-4440
Vol. 8. No. 5, pp. 69-75, 2018
DOI : https://doi.org/10.22156/CS4SMB.2018.8.5.069

클라우드 컴퓨팅 환경에서 가상화 관리 융합접근제어 모델

최은복
전주대학교 스마트미디어학과 교수

A Virtualization Management Convergence Access Control Model for Cloud Computing Environments

Eun-Bok Choi
Professor, Department of Smartmedia, Jenoju University

요 약 접근제어 목적은 컴퓨팅 자원을 불법적인 사용자로부터 유출, 수정, 파괴와 같은 비합법적인 행위로부터 원천적으로 차단하고 보호하는데 있다. 클라우드 컴퓨팅 환경이 가상화 기술을 활용한 자원공유 서비스로 확장됨에 따라 동적이고 안전한 클라우드 기반 서비스를 제공하기 위해서는 새로운 보안 모델과 접근제어 기법이 요구되어진다. 본 가상화 관리 융합접근제어 모델은 역할기반 접근제어 기법에 동적 권한 배정 기능을 적용하여 유연한 사용자 권한 부여 기능을 제공하였다. 또한 보안등급과 규칙에 의거한 접근제어 기법을 적용함으로써 공유개념의 가상머신 시스템에서 권한충돌 문제 해결과 물리적 자원의 안전성을 보장토록 하였다. 본 모델은 안전하고 효율적인 클라우드 기반의 가상화 관리 시스템을 구축하는데 도움이 될 것이며 향후 다단계 특성을 반영한 메카니즘으로 확장될 필요성이 있다.

주제어 : 클라우드 서비스, 가상화, 망관리, 접근제어, 융합

Abstract The purpose of access control is to prevent computing resources from illegal behavior such as leakage, modification, and destruction by unauthorized users. As the cloud computing environment is expanded to resource sharing services using virtualization technology, a new security model and access control technique are required to provide dynamic and secure cloud-based computing services. The virtualization management convergence access control model provides a flexible user authorization function by applying the dynamic privilege assignment function to the role based access control mechanism. In addition, by applying access control mechanism based on security level and rules, we solve the conflict problem in virtual machine system and guarantee the safeness of physical resources. This model will help to build a secure and efficient cloud-based virtualization management system and will be expanded to a mechanism that reflects the multi-level characteristics

Key Words : Cloud Services, Virtualizaion, Network Management, Access Control, Convergence

1. 서론

최종 사용자가 한곳에서 하나의 기기로 사용하여 업무를 처리하였던 클라이언트 서버 컴퓨팅 환경에서 장소나 운영환경에 구애받지 않는 모바일 클라우드 컴퓨팅 환경으로 급속히 변화하고 있으며 탄력적이고 신축적인 정보시스템 구조를 구현한 최신기술의 클라우드 서비스로 확장되는 추세에 있다[1].

클라우드 컴퓨팅은 다양한 사용자들이 물리적 자원, 응용 소프트웨어, 디바이스 등을 네트워크를 통해 서로 공유하는 서비스로서, 모바일 플랫폼, 빅데이터, 인공지능, SNS 등 정보통신기술을 구현하고 다양한 정보기술

*Corresponding Author : Eun-Bok Choi(ebchoi@jj.ac.kr)
Received July 10, 2018
Revised August 1, 2018
Accepted October 20, 2018
Published October 31, 2018

로의 진화를 이끌어내는 주요 기술중 하나로 자리잡고 있으며 디바이스, 산업 및 휴먼 융합기술을 통해 가정자동화, 로봇, 핀테크, 자율자동차 등 다양한 산업분야로 확장함으로써 기업에 새로운 가치를 창조하는 핵심으로 부상하고 있다[2].

인터넷과 스마트 기기의 등장으로 출현한 클라우드 컴퓨팅은 가상화 기술을 이용하여 다중의 독립적인 시스템을 하나의 논리적인 하드웨어 시스템으로 통합함으로써 기업 조직의 효율성을 강화함과 동시에 정보기술 구축비용을 줄일 수 있으며 특화된 개별 운영체제로 운영되는 다중 가상머신을 동시에 운영할 수 있는 장점을 갖는다. 하지만 전체적인 컴퓨팅환경이 개방성을 갖는 클라우드 환경으로 급변함에 따라 지능화되는 사이버위협에 효과적으로 대비하는 보안 기능을 갖춘 안전한 클라우드 기술이 구축될 필요성이 대두되었다[3].

다수의 사용자들이 무선 단말기를 통한 원격 접속으로 구성되는 클라우드 서비스 환경에서는 가상화 기술, 정보의 위임, 사용자나 가상머신간의 자원의 공유, 그리고 이용되는 단말의 다양성등 다중 특성으로 인한 보안 위협에 다양하게 노출되므로 데이터의 기밀성, 무결성, 가용성을 제공하는 융통성있는 보안 기법이 요구되어진다.

클라우드 기반에서 효율성을 갖추면서 비용 절감을 극대화하는 시스템을 구축하기 위해서는 여러개의 가상머신 간의 적정한 접근통제 기능과 더불어 제한된 자원 공유가 필요하다. 이러한 공유개념의 가상머신에서 안전성을 보장하면서 보안정책에 근거하여 과업 협업이 원활하게 이루어지기 위해서는 권한 충돌을 방지하는 능동적인 권한배정 규칙과 권한 등급에 의한 접근제어 정책이 선결되어야 한다.

2. 관련연구

2.1 가상화

가상화란 Fig. 1과 같이 클라이언트, 서버 그리고 이와 연관된 운영체제와 저장장치, 응용프로그램과 같은 IT 자원들의 물리적인 특징을 추상화하여 응용프로그래머나 사용자에게 가상적이고 논리적인 자원을 제공하는 기술로, 하나의 물리적인 호스트나 단일서버에 여러 개의 운영체제를 갖는 가상머신이 적재되어 실행되도록 함으로써 무분별한 인프라 확장으로 인한 구축비용을 줄일 수 있으며 궁극적으로 정보기술 관리와 유지보수 간소화를 꾀할 수 있는 장점을 갖는다[4].

하지만 정보기술의 효율성 향상과 더불어 비용 절감 효과를 달성하기 위해서는 서로 통신 관계를 형성하는 여러개의 가상머신 간의 적정한 접근통제 메카니즘과 제한된 자원 공유가 제공되어야한다.

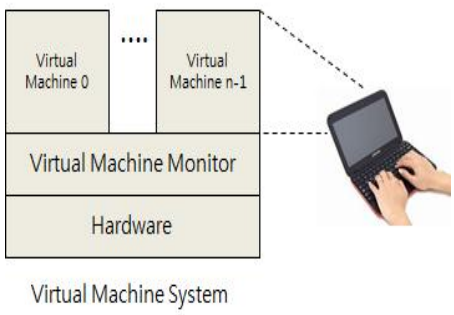

Fig. 1. Virtualization

가상화 기술의 유형은 하드웨어 자원을 기반으로 다음과 같이 3가지로 분류할 수 있다[5].

- 서버 가상화 : 단일서버를 논리적으로 구분하여 서로 다른 운영체제를 탑재한 다수의 가상머신들을 운용하도록 지원하는 기술로서, 시스템의 이용자들은 하이퍼바이저를 통해 서버 가상화 시스템의 독립된 영역을 할당받고 해당된 서비스를 이용할 수 있는 기술을 말한다.
- 스토리지 가상화 : 개인용 컴퓨터 환경은 단말기와 운영체제 그리고 애플리케이션 설치 및 물리적인 저장 공간을 가상으로 할당하여 사용자별로 개별 운용배정되며 프로토콜을 통해 동기화된 동일한 자료를 언제 어디에서나 사용할 수 있는 특징을 갖는다.
- 네트워크 가상화 : 하나의 물리적 네트워크 인프라를 서로 다른 프로토콜로 운영되는 논리적 공존 네트워크처럼 네트워크 링크와 노드를 포함한 네트워크 내 모든 자원을 가상화하여 독립적인 가상 네트워크를 구성하여 운영하는 기술이다.

2.2 클라우드 기반 접근제어

클라우드 컴퓨팅 환경은 가상화 기술을 통한 자원 공유 서비스로 인해 기존 클라이언트 서버 환경과는 달리 서비스를 제공하는 서버 입장과 서비스를 사용하는 사용

자 입장 모두 특정한 보안 요건을 갖는 정보 보안 통제 기법이 요구된다. 자원 공유 기능을 제공하는 클라우드 컴퓨팅 환경은 가상계층의 도입으로 인해 전통 기반의 컴퓨팅 환경보다 더 많은 공격에 노출되어 보안 위협이 커지고 있으며 동적이고 유연성을 갖는 가상머신의 특성으로 인해 보안정책에 대한 일관성 유지와 정책 집행의 보장성을 확보하는데 어려움을 주고 있다[6]. 뿐만 아니라 물리적 서버간의 가상머신 이전, 복제 및 배분에 의해 발생되는 정보 유출과 불법전파 그리고 권한남용등의 심각한 보안 문제는 클라우드 컴퓨팅 서비스의 정책 관리를 어렵게하는 한 요인으로 작용하며 다수의 사용자와의 과업 수행을 위한 협업은 접근제어 정책과 집행 메카니즘을 복잡하게 만들어 시스템 관리에 지장을 초래한다[7,17].

클라우드 컴퓨팅에서 보안은 기업으로부터 중요한 이슈중에 하나로써, VMware, 아마존, 마이크로소프트, 레트햇과 같은 기업들은 가상자원을 안전하게 운용하고 관리하기 위한 접근제어 메카니즘을 제공한다. 아마존은 EC2와 S3라는 주요 클라우드 컴퓨팅을 결합한 제품을 통해 접근제어를 제공하는데, EC2[8] 제품은 ID와 문맥기반 접근제어 기법을 통해 안전하게 가상머신과 가상네트워크를 관리하도록 설계되었고 S3[9]는 객체 등급 접근제어 기법으로 객체 사용자에게 자신의 모든 데이터에 대한 권한을 제어할 있도록 자신의 소유한 접근제어 리스트를 작성하도록 허가하는 정책을 사용한다. VMWare의 주력제품인 VirtualCenter[10]은 주어진 과업이 사용자에 의해 결정되는 역할기반 접근제어기법에 기반한 과업기반 권한 관리 시스템을 제공한다. 마이크로 소프트사의 가상 플랫폼인 Hyper-V[11]도 사용자에게 역할과 권한을 배정하여 지정된 권한 집합내에서 가상머신을 관리하도록 하는 역할기반 접근제어 메카니즘에 기반하여 구현되었다. 레드햇의 oVirt[12]는 Kerberos/LDAP를 통해 가상머신과 가상 저장장치의 기본 권한 서비스를 제공하며 사용자에게 SSO(SingleSignOn) 기능을 갖도록 제공한다.

클라우드 컴퓨팅 환경에서 역할기반 접근제어 기술을 적용할 경우 사용자 계정 권한을 설정하고 역할과 책임을 동반하는 직무기반의 최소 권한 규칙이 준수되어야 한다. 또한 다양한 사용자에 의해 이용되는 클라우드 특성상 사용자들의 세션과 데이터별 접근을 세분화하여 데이터와 세션 접근을 위한 인증절차 및 관리기능 그리고 위임된 권한에 대한 권한 철회 등을 통해 전반적인 권한의 진행절차 및 클라우드 컴퓨팅 제반 규정이 준수되어야 한다. 또한 제3자에 의한 다수 사용자 점유 구조하에서 세션과 데이터 접근 세분화, 서비스 대 서비스 애플리케이션, 데이터와 세션 접근을 위한 인증, 정보처리 상호운용이 관리되어야 하며 권한 철회 등을 통해 계정 자격증명 라이프 사이클 관리등과 함께 클라우드 컴퓨팅의 법, 규칙 및 규정을 준수해야 한다[13].

2.3 역할기반 접근제어 모델

정보시스템에서 계층이나 등급기반 격자개념은 주체와 객체, 이들간의 요소 값 등의 배열과 연관성을 기술하고자 할 때 자주 사용되는 용어이다. 특히, 대부분의 접근제어 시스템에서 사용자들은 책무와 적정성에 기반하여 보안 등급이나 역할 등과 같은 클래스로 구성된 계층 개념으로 구성된다. 계층에는 책무나 적정성에 따라 계층간의 서로다른 권한부여와 책임이 뒤따르는데, 대규모의 정보시스템을 관리하는 역할기반접근제어 모델(Role-Based Access Control : RBAC)의 경우 다른 시스템보다 더 복잡한 계층구조를 가지며 계층구조를 기술한 역할계층(RH)이 권한과 책무를 조직에 반영하기 위한 자연스러운 방법으로 사용된다[14].

역할기반 접근제어 모델은 여러 명의 사용자는 역할이라고 하는 클래스들로 그룹화하고 객체 또는 데이터를 관련된 카테고리로 구분하여 배정한다. 역할은 어떤 조직의 사용자들이 갖고 있는 책무를 여러 개의 영역으로 구분해 놓은 것으로서 조직체에서 사용자의 활동 위치에 따라 결정되며 역할 이름과 카테고리에 접근할 수 있는 권한으로 구성된다[15]. 이 접근제어모델은 역할에 사용자를 할당하는 과정과 객체에 대한 권한을 부여하는 두 단계로 세분함으로써 효율성있는 권한부여가 가능하고 하나의 트랜잭션을 여러 역할이 분할하여 수행되도록 하는 임무분리 정책을 통해 정보의 무결성을 보장받을 수 있다[16,18].

3. 가상화 관리 융합접근제어 모델

Fig. 2와 같이 가상화 관리 융합접근제어(NMCAC: Network Manangement Convergence Access Control) 모델은 프로세스와 같은 능동적 주체 그리고 파일이나

저장공간, 장치와 같은 피동적 객체에 대한 접근 권한 관계로 구별하여 운영한다. 접근권한을 저장하고 관리하는데 이용되는 접근행렬 방법은 주체나 객체를 저장해야 할 행렬의 값이 광범위하기 때문에 현실적이지 못하다는 단점을 갖는데, 본 모델에서는 서로 유사한 주체와 객체를 연관된 가상머신(VM)들과 역할들로 그룹핑하여 연관관계의 수량을 제한하여 현실화하였다. 연관된 가상머신들은 신뢰를 기반으로 협동해야하는 활동적인 주체들의 집합 그리고 역할은 유사한 보안 특성 관점을 갖는 객체들의 집합으로 각각 구성된다. 임의적 접근제어 방식으로 운영되는 전통적인 접근제어 모델에서 이용자는 다른 주체나 이용자에게 자신의 객체에 대한 권리를 부여하는 위임 결정 권한을 갖는 반면 본 모델에서는 보안 정책 관리자의 참조모니터(Reference Monitor)와 접근제어 디시전 메이커를 통해 최소 권한배정 원칙에 의거하여 객체 권한을 수정할 권리를 갖도록 하는 강제적 접근제어 기능을 제공한다. 또한, 사용자의 서비스 제약사항 요청/응답에 따른 인스턴스를 갖는 읽기 권한, 쓰기 권한으로 구성된 규칙에 의거한 역할로 정의하고 세부항목을 설계하여 제공함으로서 공유개념의 가상머신에서 안전성을 보장받을 수 있다.

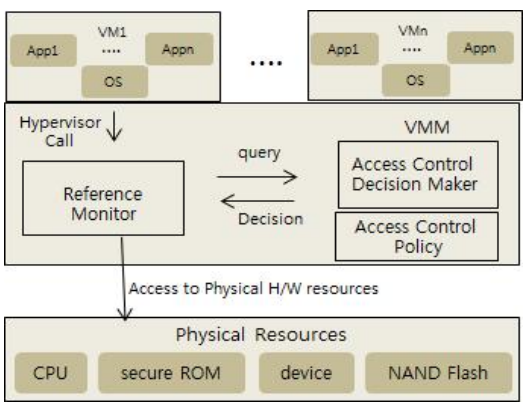

Fig. 2. Architecture of NMCAC

3.1 시스템 집합 정의

본 제안 시스템에서는 주체들의 집합 S, 객체들의 집합 O, 가상머신 레이블 집합 V, 역할 레이블 집합 R, 권한집합 P, 역할 계층 RHi ⊆ R X R, 가상머신-주체 배정 관계 VS ⊆ V X S, 주체-역할 배정 관계 SR ⊆ S X R, 역할-객체 배정 관계 RO ⊆ R X O, 가상머신-역할 권한 매트릭스 VRPM와 가상머신-가상머신 권한 매트릭스 VVPM을 정의하고 있다. 이 모델에서는 VVPM(v,r) ⊆ P 이며 VVPM(v,v) ⊆ P, v ∈ V, r ⊆ R 의 관계를 갖는다.

본 논문에서 가상머신은 특별한 개체 타입으로 주체나 객체중 하나의 특성을 갖는데, 역할-가상머신의 경우 가상머신은 객체로서 기능을 수행하는 가상머신으로서, 주어진 가상머신에 대한 역할들에 대해 서로다른 각각의 고유 권한을 갖는다. 예를 들어 시스템 메니저 역할은 가상머신의 create, acquire, view, start, stop 기능을 갖는데 비해 운영자 역할은 단지 가상머신의 view 연산만을 소유하도록 한다. 또한, 가상머신-자원 경우 가상머신은 주체로서 기능을 수행하는 가상머신으로 자신들의 보안레이블 유형인 보안타입과 권한 매트릭스인 TTPM에 의해 결정된 객체의 권한으로 구성되는 주체 기반 가상머신이며 가상머신들은 사용자에 의해 동적으로 빈번하게 생성되고 삭제될 수가 있으므로 각 가상머신에 대해 보안타입을 배정하며 가상머신이 소유한 권한을 P_{vm} = TTPM(tv, tr)로 표기한다.

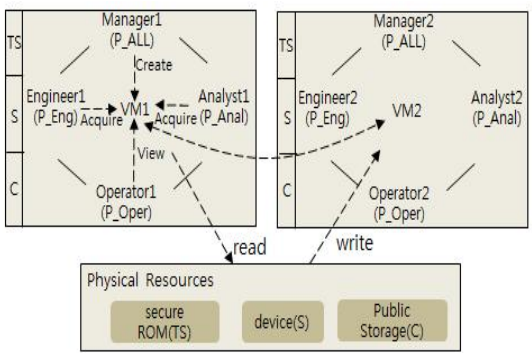

Fig. 3. A Process of NMCAC

Fig. 3은 클라우드 컴퓨팅 환경에서 가상화 관리 융합 접근제어 모델의 프로세스 흐름을 도식화한것이다. 가상화 관리 융합시스템에는 연관된 4개의 역할 타입인 매니저(Manager)역할, 엔지니어(Engineer)역할, 분석가(Analyst)역할, 운영가(Operator)역할로 구성되며 NM1(Manager1, Engineer1, Analyst1, Operator1)과 NM2(Manager2, Engineer2, Analyst2, Operator2)로 구성된다.

NM1과 NM2 가상머신은 서로 독립적으로 운영되지만 물리적 장비, 저장공간 및 네트워크 환경을 서로 공유한다. 이 예제에서 VM1과 VM2는 물리적 자원을 가상머신들이 공유하여 사용하는 가상디스크(vDisk)를 접근제

어 배정정책에 의거한 등급비교에 의해 read와 write 연산을 하도록 설정하여 서로 읽고 쓸 수 있도록 공유되었다. 또한, NM1과 NM2 가상머신들은 오류 디버깅 기능을 통해 상호 호환과 협력기능을 수행한다.

3.2 접근제어 정책

가상머신(NM_n)의 Manager는 보안등급 TS(Top Secret), Engineer와 Analyst는 보안등급 S(Secret), Operator는 보안등급 C(Crucial)를 가진다. 초기에 매니저 역할은 모든 권한인 P_{all}의 권한집합을, 엔지니어와 분석가 역할은 P_{eng}, P_{anl}의 권한집합을, 운영자 역할은 P_{oper}라는 권한집합을 각각 배정 받게 된다. 초기 권한집합과 보안등급이 배정되면 역할 계층이 자연적으로 형성된다. 정해진 역할들은 초기에 구성된 권한집합과 보안등급으로 구성되는데, 예를 들어, 같은 보안등급인 S 등급을 갖는 Engineer1, Analyst1은 VM1을 operate할 수 있는데, Engineer1, Analyst1에 의해 acquired 되어진 VM1은 Engineer1, Analyst1로부터 보안타입을 상속받아 엔지니어, 분석가 역할이 갖는 권한집합을 취득하게 된다.

본 시스템에서 적용되는 가상머신 VM_i와 객체에 대한 O_j에 속한 자원에 대한 읽기(read), 쓰기(write)의 시스템 상태와 보안 특성은 다음과 같다.

□ 가상머신의 읽기(read) 시스템 상태와 보안특성

시스템 상태 v ={b,P,f,H}에서 v={b ∪ {(VM_i, O_j, r), P, f, H}로 구성되며 보안특성으로는 가상머신의 보안등급이 객체의 보안등급에 지배된다면 가상머신은 객체에 read 연산을 수행할 수 있으며 $P[VM_i,o_j] \Rightarrow f(VM_i) \leq f(o_j)$와 같이 기술한다.

□ 가상머신의 쓰기(write) 시스템 상태와 보안특성

시스템 상태 v ={b,P,f,H}에서 v={b ∪ {(VM_i, O_j, w), P, f, H}로 구성되며 보안특성으로는 가상머신의 보안등급이 객체의 보안등급을 지배한다면 가상머신은 객체에 write 연산을 수행할 수 있으며 $P[VM_i,o_j] \Rightarrow f(VM_i) \geq f(o_j)$와 같이 기술한다.

여기에서 b는 현재 접근권한 집합으로 b⊆(VM×O×P)을 갖으며 객체의 주체에 관한 접근권한을 표현한다. P는 접근권한 집합이며, f={f(VM_i), f(o_j)} f(VM_i)는 가상머신 보안등급함수, f(o_j)는 객체 보안등급함수을 의미한다. H는 현재 객체의 계층구조로 트리 구조를 갖으며 활성화 상태이거나 접근가능한 객체만이 이 계층구조에 포함된다.

본 접근제어 모델에서 관제객체에 적용되는 연산과 속성값에 적용되는 연산으로 구분하는데, 전반적인 관제객체에 적용되는 연산에는 관제객체를 실행하기 위한 가상머신의 실행과 종료를 담당하는 start, stop 연산과 관제객체의 인스턴스를 생성하고 삭제하는 create, destory 연산이 있다. 그리고 속성값에 적용되는 연산에는 가상머신의 역할을 지정받는 acquire 연산, 속성값을 읽는 read 연산, 속성값을 쓰는 write 연산이 있다.

3.3 동적 권한 전이 배정

가상머신을 운영할 역할은 권한에 맞는 보안타입을 가지며 이 역할에 배정될 권한은 현재 문맥과 연관되어 동적으로 배정된다. 동적 권한 배정 규칙은 △ = (A, E, ∂, M)와 같이 유한 상태 머신으로 정의하였다. 여기에서 A는 동적 권한 상태의 유한 집합으로 공집합을 포함하며 가상머신이 소유한 권한상태는 보안 등급에 의해 결정된다. 또한 E는 동적 권한이 발생되는 이벤트 집합이며, 권한 A는 가상머신이 생성되고 삭제되는 creation과 deletion이 발생될 때 동적 권한이 배정되고 철회되며 권한 배정과 철회는 ∅ ⇒ A와 A ⇒ ∅로 표기한다.

클라우드에서 과업 협업이 가능하기위해서 가상머신은 다수의 사용자와 역할들에 의해 공유되어지며 다양한 역할을 통하여 객체 자원에 접근하게 되는데 이때 권한 충돌 현상이 발생할 수 있다. 이러한 충돌 현상을 해결하기위해 본 모델에서는 $\partial \subseteq S \times E \times S$를 정의하여 보안타입에 의한 등급비교를 통하여 어떤 한 시점에서 하나의 가상머신은 단지 하나의 역할에만 점유되도록 함으로써 최소권한배정원칙을 준수하는 역할등급 비교 기능을 갖도록 하였다. 예를 들어, 보안타입 T_A를 갖는 역할 r_1이 배정된 가상머신 VM이 있을 경우, r_1은 보안타입 T_B인 r_2와 VM을 share(E: Event)하고자 한다. 여기에서 share는 vm의 동적 권한 배정을 발생시키는 이벤트로 $P_{TA}^{r1}(S) \Rightarrow P_{TB}^{r2}(S')$로 표기한다. 여기에서 P_{TA}^{r1}는 동적 권한배정 전 단계의 가상머신의 권한을 표기한 것이고 P_{TB}^{r2}는 동적권한배정후 단계의 가상머신의 권한을 표기한 것이다. M은 동적권한배정 ∂에 대한 허가와 거부를 결정할 참조 모니터이다. 동적권한배정은 참조모니터 M의 명시된 접근정책에 따라 제어되는데, 예를 들어, 보안타입 T_A를 갖는 역할 r_1이 보안 타입 T_B를 갖는 역할 r_2

와 가상머신 VM을 공유하고자 할 경우 참조모니터 M은 공유를 위한 동적권한배정 ∂를 허용하기 전에 먼저 M은 보안타입 T_A를 갖는 역할 r_1이 가상머신을 공유할 수 있는 권한을 가졌는지 점검하고, 다음으로 M은 만약 역할 r_2가 보안 타입 T_A, T_B와 권한 메트릭스에 의거해 VM을 점유할 권한을 가졌는지 조사할 것이다. 만약 2가지 모두 결과가 참이다면 전이 ∂는 허락된다.

3.4 비교 분석

모든 기업에서는 전략적인 가치향상과 안전성 보장을 담보로 하는 자사의 비지니스 성장을 위해 가상 데이터센터를 일관되게 관리하고 자동화하는 데 많은 노력을 기울이고 있다. 아마존, VMware 그리고 마이크로소프트와 같은 기업에서는 가상자원을 안전하게 접근하고 관리하기 위한 클라우드 컴퓨팅 기반의 접근제어 메카니즘 제품을 제공하고 있다. 아마존 제품은 ID와 문맥 기반 접근제어 기법을 통해 안전하게 가상머신과 가상네트워크를 관리하도록 설계되었고 S3는 객체 등급 접근제어 기법으로 객체 사용자에게 자신의 모든 데이터에 대한 권한을 제어할 있도록 자신의 소유한 접근제어 리스트를 작성하도록 허가하는 정책을 사용한다. VMWare 제품은 주어진 과업이 사용자에 의해 결정되는 역할기반 접근제어기법에 기반한 과업기반 권한 관리 시스템을 제공하며 마이크로 소프트사 제품은 사용자에게 역할과 권한을 배정하여 지정된 권한 집합내에서 가상머신을 관리하도록 하는 역할기반 접근제어 메카니즘에 기반하여 구현되었다.

접근제어리스트나 접근제어행렬에 등록되어 있는 주체에게만 객체의 정보를 제공하는 자율적 접근제어 정책 모델은 객체에 관한 권한을 자율적으로 다른 주체에게 재공하거나 회수할 수 있어 악의적인 목적에 이용될 수 있는 보안상 취약점을 내포한다.

데이터 또는 객체를 몇 개의 범주로 나누고 사용자들의 임무를 여러 개의 영역으로 분할해 놓은 역할에 기반하여 접근권한을 부여하는 역할기반 접근제어 정책 모델은 상업적인 측면의 보안정책을 강화시킬수 있는 정책으로 환경에 따라 역할이 자연스럽게 재구성되고 생성될 수 있는 확장성을 갖는다. 하지만 이 모델은 역할에 의해 접근되는 객체의 중요도 등급이 기술되어 있지 않아 해당 역할을 수행할 수 있는 모든 사용자들이 모든 객체를 사용하거나 변경할 수 있어 정보의 비밀성과 무결성을 침해할 우려가 있다.

본 모델은 주체가 해당 객체를 부당하게 유출, 변경하는 것을 방지하기 위해 가상머신의 보안등급과 사용자의 서비스 제약사항 요청/응답에 따른 인스턴스를 갖는 읽기 권한, 쓰기 권한으로 구성된 규칙에 기반한 역할로 정의하고 세부정책에 의해 접근권한을 제공함으로서 유연한 사용자 권한 부여 기능과 공유개념의 가상머신에서의 안전성을 보장받을 수 있다.

4. 결론

클라우드 컴퓨팅 환경은 모바일 플랫폼, 빅데이터, 인공지능 등 정보통신기술을 구현하고 다양한 정보기술로의 진화를 이끌어내는 주요 기술중 하나로 자리잡고 있으며 디바이스, 산업 및 휴먼 융합기술을 통해 가정자동화, 로봇, 핀테크, 자율자동차 등 다양한 산업분야로 확장함으로써 기업에 새로운 가치를 창조하는 핵심으로 부상하고 있다. 클라우드 기술은 네트워크에 기반한 컴퓨터 자원, 소프트웨어, 인프라 등을 서로 공유하는 서비스로서 가상화 기술을 통한 자원 공유 서비스로 인해 서비스를 제공하고 이용하는 서버와 클라이언트 모두 특정한 보안 요건을 갖는 정보 보안 통제 요건이 요구된다.

클라우드 컴퓨팅 환경에서는 동적이고 유연성을 갖는 가상계층의 도입으로 인해 자원 정보 유출과 불법전파 그리고 권한남용 등 보안 관리에 대한 일관성 유지와 정책 집행의 보장에 어려움을 초래하며 다수의 사용자와의 과업 수행을 위한 협업으로 접근제어 정책과 집행 메카니즘을 복잡하게 만들어 시스템 관리에 지장을 발생시킨다.

본 가상화 관리 융합 접근제어 모델은 역할기반 접근제어 기법에 등급과 동적기능을 적용하여 유연한 사용자 권한 부여 기능을 갖으며 임대 정책 등의 서비스 수준에 따른 요소 조건을 기준으로 다양한 권한을 설정할 수 있으며 서로 유사한 객체를 연관된 가상머신 역할로 그룹핑하여 사용자의 역할을 조합한 정책을 바탕으로 접근통제를 수행한다. 그리고 사용자의 서비스 제약사항 요청/응답에 따른 인스턴스를 갖는 읽기 권한, 쓰기 권한으로 구성된 규칙에 기반한 역할로 정의하고 세부항목을 설계하여 제공함으로서 공유개념의 가상머신에서 안전성을 보장받을 수 있다. 또한, 규칙에 기반한 세부적인 속성값이 명명된 역할을 클라우드 이용자에게 제공하고 관리하도록 함으로써 추후적인 서비스 확장시 부여된 역할이 동적으로 변경 가능한 장점을 제공한다.

REFERENCES

[1] R. Aluvalu & L. Muddana. (2016). A Dynamic attribute-based risk aware access control model(DA-RAAC) for cloud computing. *IEEE International Conference on Computational Intelligence and Computing Research.*
DOI : 10.1109/iccic.2016.7919618

[2] D. Zou, L. Shi & H. Jin. (2009). DVM_MAC:A Mandatory Access Control System in Distributed Virtual Computing Enviroment, *IEEE 15th Internaltional Conference on Parallel and Distributed Systems*, 556-563, DOI : 10.1109/ICPADS.2009.128

[3] W. Li, H. Wan, X. Ren & S. Li. (2012). A Refined RBAC Model for Cloud Computing, *IEEE/ACIS International Conference on Computer and Information Science*, 43-48
DOI : 10.1109/icis.2012.13

[4] C. Weng, Y. Luo, M. Li & X. Lu. (2008). A BLP-based Access Control Mechanism for the Virtual Machine System, *IEEE 9th International Conference for Young Computer Scientists*, 2278-2282.
DOI : 10.1109/ICYCS.2008.503

[5] H. Zhu, Y. Xue, Y. Zhang, X. Chen, H. Li & X. Liu. (2013). V-MLR:A Multilevel Security Model for Virtualization, *IEEE 5th International Conference on Intelligent Networking and Collaborative Systems*, 9-16.
DOI : 10.1109/INCoS.2013.12

[6] L. Kerr & J. Alves-Foss. (2016). Combining Mandatory and Attribute-bsed Access Control, *IEEE 49th Hawaii International Conference o System Sciences*, 2616-2623.
DOI : 10.1109/HICSS.2016.328

[7] S. M. Lee, S. B. Suh, B. D Jeong & S. D. Mo. (2008). A Multi-Layer Mandatory Access Control Mechanism for Mobile Devices Based on Virtualization, *IEEE Communications Society,* 251-256
DOI : 10.1109/ccnc08.2007.63

[8] *Amazon Elastic Compute Cloud(EC2).* (2009). http://aws.amazon.com/ec2.

[9] *Amazon Simple Storage Service(S3)* (2009). http://aws.amazon.com/s3.

[10] *VMware vCenter Server.* (2011). http://aws.vmware.com/products/vcenter-server.

[11] *Windows Server 2008 Virtualization with Hyper-V.* (2009).http://www.microsoft.com/windowsserver2008/en/us/hyperv-main.aspx.

[12] Ovirt. (2011). http://www.ovirt.org/.

[13] British Standards. (2013). *ISO/IEC 27001:2013(E) (Information technlolgy-Security techniques-A Information security management systems-Rquirements)*

[14] Y. Zhu, C. J. Hu, & X. Wang. (2015). From RBAC to ABAC:Constructing Flexible Data Access Control for Cloud Storage Services, *IEEE Transactions on Services Computing, 8(4)*, 601-616.
DOI : 10.1109/TSC.2014.2363474

[15] C. Pengrui, W. LingDa, Y. Chao & Y. Ronghuan. (2016). A Hierachical Access Control Model of Software Repository Based on RBAC, *IEEE*, 761-765
DOI : 10.1109/icsess.2016.7883179

[16] R. S. Sandhu, E. J. Coyne, H. L. Feinstein & C. E. Youman. (1996) Role-Based Access Control Models, *COMPUTER SOCIETY, IEEE*, 38-47

[17] E. B. Choi & S. J. Lee. (2016). Acces Control Mechanism based on MAC for Cloud Convergence, *Jouunal of the Korea Convergence Society,* 1-8
DOI : 10.15207/jkcs.2016.7.1.001

[18] M. Benedetti & M. Mori. (2018). Parametric RBAC Maintenance via Max-SAT. *ACM on Symposium on Access Control Models and Technologies,* 15-25.
DOI : 10.1145/3205977.3205987

최 은 복(Choi, Eun Bok) [정회원]

- 1992년 2월 : 전남대학교 전산학과(이학사)
- 1996년 2월 : 전남대학교 대학원 전산학과(이학석사)
- 2000년 8월 : 전남대학교 대학원 전산학과(이학박사)
- 2002년 3월 ~ 현재 : 전주대학교 교수
- 관심분야 : 통신망관리, 접근제어, 가상화보안
- E-Mail : ebchoi@jj.ac.kr