클라우드 컴퓨팅 가상화 보안을 위한 아키텍처 구성 및 기능 분석 연구

정순기[1], 정만현[2], 조재익[3], 손태식[4], 문종섭[5]

A Research on Cloud Architecture and Function for Virtualization Security of Cloud Computing

Soonki Jeong[1], Manhyun Chung[2], Jaeik Cho[3], Taeshik Shon[4], Jongsub Moon[5]

요 약

클라우드 컴퓨팅 시스템은 기존의 시스템과 달리 서버, 네트워크, 스토리지와 같은 부분들이 가상화되어 자원 및 서비스를 공동화하여 활용한다. 클라우드 서비스 기업들은 이러한 서비스를 위해 서비스 기업별로 각기 다른 구성의 컴퓨팅 아키텍처를 사용하고 있다. 다양한 구성의 컴퓨팅 구조에서는, 보안 침해 문제가 발생하면 신속한 대처가 어렵고, 각각의 아키텍처별에 대해, 각기 다른 대응 방법을 사용해야 한다. 또한, 서로 다른 아키텍처에 맞춰 각기 다른 보안요소를 적용하는 방법은 클라우드 컴퓨팅 아키텍처에서 중요 기술인 가상화 기술에 대한 구체적인 보안 요구사항 적용이 어렵고, 상호 호환성에 대한 문제점이 발생 할 수도 있다. 따라서 본 논문에서는 이러한 문제점 해결을 위해 클라우드 컴퓨팅 가상화 보안요소 및 정보보호 요구사항을 분석하고 새로운 구조를 제안한다. 이때 가상화와 관련되어 역할 및 기능별 발생 가능한 위협, 그리고 이에 대응하기 위한 보안요소와 정보보호 요구사항을 도출하여 정의한다. 이러한 방법을 통해 클라우드 컴퓨팅에 대한 위협 요인을 미리 예방하고, 동시에 효율적이고 체계적인 운영 및 관리에 적용 할 수 있다.

핵심어: 클라우드 컴퓨팅 서비스, 클라우드 컴퓨팅 아키텍처, 가상화 보안 레이어, 정보보호 요구사항

Abstract

Unlike a classic client-server model, Cloud Computing System shares resources and services through the

접수일(2011년08월11일), 심사의뢰일(2011년08월12일), 심사완료일(1차:2011년08월20일, 2차:2011년09월17일)
게재일(2011년10월31일)

[1]136-701 서울시 성북구 안암동 5가, 고려대학교 정보보호대학원 석사과정
email: soonki32@korea.ac.kr
[2]136-701 서울시 성북구 안암동 5가, 고려대학교 정보보호대학원 박사과정
email: manhuyn4@korea.ac.kr
[3]136-701 서울시 성북구 안암동 5가, 고려대학교 정보보호대학원 박사과정
email: chojaeik@korea.ac.kr
[4]136-701 경기도 수원시 영동구 원천동 산 5, 아주대학교 정보컴퓨터공학부 부교수
email: tsshon@ajou.ac.kr
[5](교신저자)136-701 서울시 성북구 안암동 5가, 고려대학교 정보보호대학원 교수
email: jsmoon@korea.ac.kr

*본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 육성지원 사업의 연구결과로 수행되었음"(NIPA-2011-C1090-1101-0004)

virtualization of server, network and storage. Cloud Service providers offer a variety of cloud services based on different types of cloud computing architectures. Different architectures make swift response to security breaches difficult. Each architecture requires different solutions. In addition, applying different security elements to each architecture makes it hard to require specified security elements for virtualization technology, the core technology of Cloud Computing. It can cause compatibility issues as well. Recognizing the need to solve the issues stated above, this study analyzes security elements required for Cloud Computing virtualizatoin and information protection-related requirements and presents new architectures. We also identify possible threats that may occur depending on different functions and roles concerning virtualiztion and define security elements and information protection related requirements to deal with those issues. From this study, we aim to prevent any possible threat to Cloud Computing and provide more efficient and systemic way of managing and operating Cloud Computing system.

Keywords: Cloud Computing Services, Cloud Computing Architecture, Virtualization Security Layer, Information Security Requirement.

1. 서론

클라우드 컴퓨팅 서비스는 규모의 경제에 입각한 대규모 분산 컴퓨팅 패러다임으로서 스토리지, 플랫폼, 서비스 등과 같은 거대한 IT 자원들을 가상화와 동적 확장이 가능한 체제로, 사용자가 필요한 만큼을 인터넷을 통하여 사용하는 컴퓨팅 서비스 환경이다. 현재 클라우드 컴퓨팅 시장은 초기 도입기를 거치고 있으며, 웹메일, 블로그, 웹하드 서비스, 웹호스팅 서비스 등이 이미 사용되고 있다. 그러나 본격적인 성장단계로 진입하기 위해서는 사용자의 요구수준에 맞는 애플리케이션과 서비스 발굴, 기존 시스템과의 연동성 확대, 보안에 대한 우려 불식 등과 같은 문제들이 선결되어야 한다. 국제 시장 조사 기관인 IDC에서 IT 임원을 대상한 조사 결과 클라우드 컴퓨팅 서비스를 사용을 위해 선결되어야 할 과제가 보안이라고 응답하였다. [2] 이러한 이유로 현재 클라우드 컴퓨팅 기술 및 보안에 대한 연구가 활발히 진행되고 있으나, 기업별 각기 다른 클라우드 아키텍처로 인해 보안요소 연구 및 구체적인 대응 방법 연구에 대한 문제가 발생하였다. 또한, 상호 호환성 및 연동성 문제와 클라우드 컴퓨팅의 주요 기능인 가상화에 대한 보안요소를 도출하여 적용하는데 어렵다는 단점이 존재한다. 이러한 문제점에 대한 효과적인 보완을 위해서는 각 벤더 및 기관의 아키텍처의 공통적인 기능이 반영된 아키텍처를 구성하여, 가상화 보안 레이어 역할 및 이와 관련된 기능에 대한 분석과 그에 따라 발생 가능한 위협 및 대응방안에 대한 연구가 필요하다.

본 논문에서는 공통적 개념의 클라우드 컴퓨팅 아키텍처를 구성하여 가상화 관련 역할 및 기능별 발생 가능한 위협, 그리고 이에 대응하여 가상화 환경의 보안성 향상을 위한 대응방법 및 정보보호 요구사항을 제안한다. 논문의 구성은 다음과 같다. 2장에서는 기존의 클라우드 컴퓨팅 서비스 및 아키텍처 보안관련 연구에 대해 살펴보고, 3장에서는 제안 방법으로 공통적 개념의 클라우드 컴퓨팅 아키텍처를 제안하고, 이를 바탕으로 클라우드 컴퓨팅 '가상화 보안 레이어'의 위협요소를 도출하여, 이에 대한 대응방법 및 정보보호 요구사항을 제시한다. 그리고 클라우드 컴퓨팅 아키텍처 가상화 보안 레이어 비교 및 활용 방법에 대해 서술한다. 마지막으로 4장에서는 본 논문의 결론을 기술한다.

2. 클라우드 컴퓨팅 서비스 및 아키텍처 보안 관련 연구

2.1 클라우드 컴퓨팅 아키텍처 모델 분석

클라우드 컴퓨팅 표준화 측면에서는 각 벤더별로 자사 플랫폼 의존적인 보안 솔루션 제공으로 인한 다양한 클라우드 컴퓨팅 플랫폼의 벤더 종속성은 시스템간 상호 호환성, 이식성, 보안성 등에 대한 적용 어려움이 있다. 기존의 시스템이나 공용 소프트웨어가 제공되는 한정 자원의 경우 패치, 또는 충분한 보안 정책으로 시스템의 안정성이 유지 될 수 있었다. 그러나 자원의 통합 및 가상화 기술을 사용하는 클라우드 환경의 경우 기존의 패치나 보안 정책만으로는 한계가 있다. 따라서 전체 시스템의 안정성이 우선되어야 하기 때문에 클라우드 컴퓨팅의 핵심 기술인 가상화 특성 및 관계가 구체적으로 반영된 공통의 가상화 레이어 구성 및 기능에 대한 분석이 필요하다.

이 장에서는 효율적인 보안요소 분석을 위해 클라우드 컴퓨팅 구축에 많이 사용되는 클라우드 컴퓨팅 가상화 오픈소스 운영체제인 Xen [4] 과 대표적인 클라우드 서비스 기업 IBM, Microsoft, Redhat, 그리고 국제 클라우드 관련 기관에서 제시한 아키텍처의 각 레이어별 역할과 기능들을 비교, 분석하여 공통적인 각 레이어별 특징을 파악하였다. 각 벤더 및 기관이 제시한 아키텍처의 구성을 표 1, 2와 같이 1단계부터 6단계로 구분하여, 아키텍처 레이어별 기능 및 역할에 따라서 분류하였다. 표 1에서 공통적인 개념으로 1단계는 물리적인 장비 및 시설, 2단계는 서버, 스토리지, 네트워크와 같은 물리적인 자원을 가상화 하는 단계, 3단계는 통합 및 가상화된 자원들을 제공 및 관리하는 단계, 4단계는 할당된 자원을 이용하여 어플리케이션, 미들웨어 등을 추가하여 서비스를 제공하는 단계로 분류 하였다. 추가적으로 CSA에서 제시한 클라우드 서비스 형태에 따른 아키텍처의 5단계와 6단계는 표 2에서 보듯이 각 각 PaaS와 SaaS를 제공하기 위한 추가적인 미들웨어 또는 어플리케이션 구성을 위한 단계로 분류 하였다. [5, 6]

(1) 표 1.의 Xen, IBM, MS, Redhat의 클라우드 컴퓨팅 아키텍처 분석을 통한 레이어별 기능 및 분류

1단계, 클라우드 컴퓨팅의 인프라스트럭처로서 데이터 처리를 위한 서버, 네트워크 내/외부 통신을 위한 네트워크, 데이터 저장을 위한 스토리지와 같은 기반 시설로서 물리적인 자원으로 구성되어 있다.

2단계, 서버, 스토리지, 네트워크와 같은 물리적인 자원을 통합 및 추상화하여 캡슐화된 자원으로 가공하는 가상화 단계이다.

3단계, 가상화된 자원을 상위 계층이나 종단 사용자들에게 가상기계(VM)/클러스터, 논리적 파일 시스템, 데이터베이스 시스템등과 같은 통합된 자원을 제공한다.

4단계, 할당받은 서비스 자원을 이용하여 특화된 도구, 어플리케이션 등을 통합된 자원 위에 추가하여 개발 및 배치 플랫폼으로 사용자들에게 서비스로 제공한다.

[표 1] Xen, IBM, MS, RedHat 클라우드 아키텍처 레이어 분류

[Table 1] Xen, IBM, MS, RedHat Cloud Computing Architecture Classification

구 분	Xen	IBM	MS	Redhat	공통적 개념
1단계	Physical Host hardware	System Resources	Servers Storages Networks	Physical Hardware (Servers, Storage, Networking)	물리적 시설 (서버, 스토리지, 네트워크 등)
2단계	Xen Hypervisor	Virtualized Infrastructure	Virtualization	RHEV (Virtual servers /storage/networks, Virtualclients/Apps, middleware)	가상화 자원으로 가공
3단계	dom0 (Host Domain) domU (Guest Domain)	Virtualized Application	Virtualized Infra Mgmt, Cloud Service Platform, Infrastructure Service Platform	JBoss, Websphere Windows, RHEL	가상화 자원 제공 및 관리
4단계		Service Management	Cloud Service Presentation	Thousands of Certified Applications	할당 자원을 이용하여 도구 및 어플리케이션 추가하여 제공

[표 2] CSA, IETF, DMTF 클라우드 컴퓨팅 아키텍처 레이어 분류

[Table 2] CSA, IETF, DMTF Cloud Computing Architecture Classification

<table>
<tr><th rowspan="2">구 분</th><th colspan="3">CSA (Cloud Security Alliance)</th><th rowspan="2">IETF (Cloud Reference Framework)</th><th rowspan="2">DMTF (Cloud Service Reference Architecture)</th><th rowspan="2">공통적 개념</th></tr>
<tr><th>IaaS</th><th>PaaS</th><th>SaaS</th></tr>
<tr><td rowspan="2">1단계</td><td>Facilities</td><td>Facilities</td><td>Facilities</td><td rowspan="2">Physical Resource Layer</td><td rowspan="2">Firmware, Hardware</td><td rowspan="2">물리적 시설 (서버,스토리지, 네트워크 등)</td></tr>
<tr><td>Hardware</td><td>Hardware</td><td>Hardware</td></tr>
<tr><td>2단계</td><td>Abstraction</td><td>Abstraction</td><td>Abstraction</td><td>Resource Abstract & Virtualization Layer</td><td>Software Kernel (OS, VM Manager)</td><td>가상화 자원으로 가공</td></tr>
<tr><td>3단계</td><td>Core Connectivity &Delivery</td><td>Core Connectivity &Delivery</td><td>Core Connectivity &Delivery</td><td>Resource Control Layer</td><td>Virtualized Resources, Virtual image</td><td>가상화 자원 제공 및 관리</td></tr>
<tr><td>4단계</td><td>APIs</td><td>APIs</td><td>APIs</td><td>Application/ Service Layer</td><td>Cloud Applications</td><td>할당 자원을 이용하여 도구 및 어플리케이션 추가하여 제공</td></tr>
<tr><td>5단계</td><td rowspan="5"></td><td>Integration& Middleware</td><td>Integration& Middleware</td><td rowspan="5"></td><td>SaaS, PaaS, IaaS</td><td>PaaS를 위한 자원통합 및 미들웨어 제공</td></tr>
<tr><td rowspan="4">6단계</td><td rowspan="4"></td><td>Data, Metadatas, Content</td><td rowspan="4"></td><td rowspan="4">SaaS를 위한 콘텐츠, 어플리케이션 제공</td></tr>
<tr><td>Applications</td></tr>
<tr><td>APIs</td></tr>
<tr><td>Presentation Modality, Presentation Platform</td></tr>
</table>

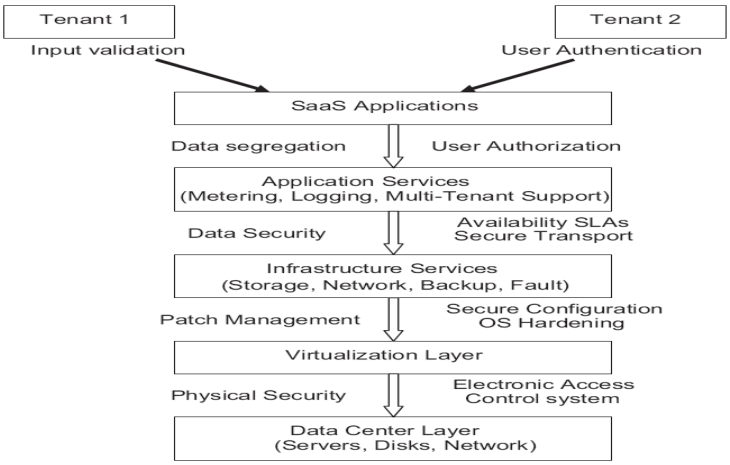
(2) 표 2.의 CSA, IETF, DMTF의 클라우드 컴퓨팅 아키텍처를 분석하여 각 레이어별 기능 및 분류 1, 2, 3, 그리고 4단계: 표 1과 동일하다.

5단계, 애플리케이션 개발 프레임워크, 프로그래밍 언어, 툴 기능(PaaS 서비스) 제공을 위한 자원 통합 및 미들웨어를 제공한다.

6단계, IaaS와 PaaS 스택위에 구축되며, 컨텐츠를 제시하는 방식을 포함하여 전체 사용자 환경을 전달하기 위해 사용되는 독립형 운영 환경을 제공한다.

2.2 클라우드 컴퓨팅 아키텍처 보안 관련 연구

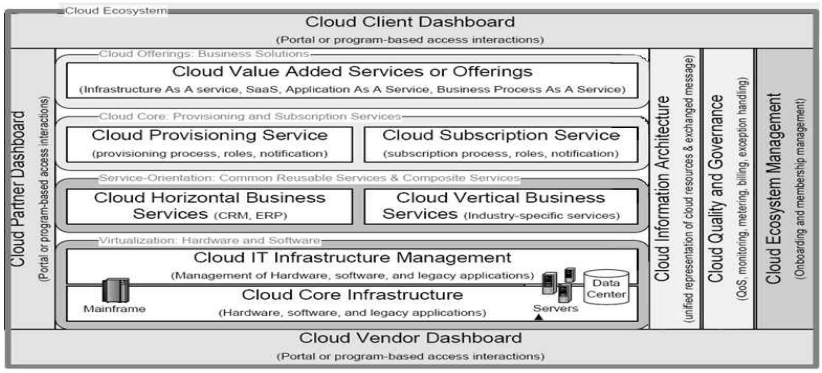
S. Subashini [7] 는 클리우드 컴퓨팅 환경에서의 데이터 프라이버시와 데이터 보호를 위한 보안 이슈들과 이를 위한 대응방법을 제안하였다. 클라우드 컴퓨팅에서의 데이터 보안을 위해 SaaS, PaaS, IaaS 각 서비스별 특성을 분석하고, 취약점이나 발생 가능 공격에 대해 조사 및 분석 하였다. 그림 1은 S. Subashini가 제안한 보안을 위한 SaaS 스택으로, 기본적인 SaaS 클라우드 서비스 제공을 위해 자원 생성부터 사용, 그리고 관리에 대한 구성 단계를 보여준다. 이러한 단계 및 절차에서 데이터 보호를 위해 고려되어야 할 보안 요소로 데이터 보안(Data security), 네트워크 보안(Network security), 데이터 무결성(Data integrity), 데이터 접근(Data access), 인증 및 권한부여(Authentication and Authorization), 웹 어플리케이션 보안(Web application security), 가상화 취약점(Vulnerability in virtualization), 가용성(Availability), 백업(Backup), 인증관리 및 접근절차(Identity management and sign-on process)로 나누어 정의하였다. 이밖에도 플랫폼 서비스 자원을 제공하는 PaaS와 인프라 서비스를 제공하는 IaaS에서는 SaaS의 조건과 다르게 자원 사용의 확장과 권한범위의 증가에 대한 차이점을 고려하여 각 서비스의 환경 및 추가적인 보안요소가 연구 되었다. 그러나 해당 논문에서 SaaS, PaaS, 그리고 IaaS 데이터 관리에 대한 보안 요소로 데이터 보안, 무결성, 접근, 권한과 인증 등과 같이 데이터 처리에 대한 보안요소는 적절히 고려가 되었지만, 서비스 종류에 따라 구성된 아키텍처에 적용 가능한 보안요소에 대해 중복되거나, 제외되는 단점이 존재한다. 또한 SaaS, PaaS, 그리고 IaaS 각 서비스의 특징만을 중심으로 보안 이슈를 적용한 방법은 클라우드 컴퓨팅 시스템의 핵심 기술인 가상화 단계에서 컴퓨팅, 스토리지, 네트워킹 자원들의 가상화와 이를 관리 위한 모니터링, 미터링, 레포팅 등과 같은 가상화 관련 기술 및 운영에 대한 세부적인 보안요소 연구가 부족하다.



[그림 1] Security for the SaaS stack [7]

[Fig. 1] Security for the SaaS stack [7]

Liang-Jie Zhang [8] 가 제안한 클라우드 컴퓨팅 오픈 아키텍처는 클라우드 컴퓨팅의 유연성, 확장성 그리고 재사용성에 대한 특징을 반영하여 클라우드 아키텍처 개념과 아키텍처 모듈 기반의 Cloud Computing Open Architecture(CCOA)를 제안 하였다. 또한, 비즈니스 서비스 또는 자사의 기업 소비자인 사용자에 따른 클라우드 서비스 제공에 대한 통합적인 접근 제공과 클라우드 컴퓨팅 기반으로 확장 가능한 IT 인프라스트럭처 및 관리시스템의 비즈니스적인 가치를 고려하여 아키텍처의 기능 및 역할을 분류 하였다. 이러한 주요 연구 내용을 바탕으로 물리적인 인프라 자원 공유 및 비즈니스 측면을 고려하여 그림 2 와 같이 7가지 개념을 정의하여 CCOA에 반영하였다.



[그림 2] 클라우드 컴퓨팅 오픈 아키텍처 개요 도표 [8]

[Fig. 2] Cloud Computing Open Architecture Overview Diagram [8]

이와 같이 SOA(Service Oriented Architecture)와 클라우드 컴퓨팅의 비즈니스 가치의 개념을 적용하여 아키텍처 레이어를 분류, 정의하였다. 그러나 각 레이어에 운영 및 역할에 대한 정의가 단

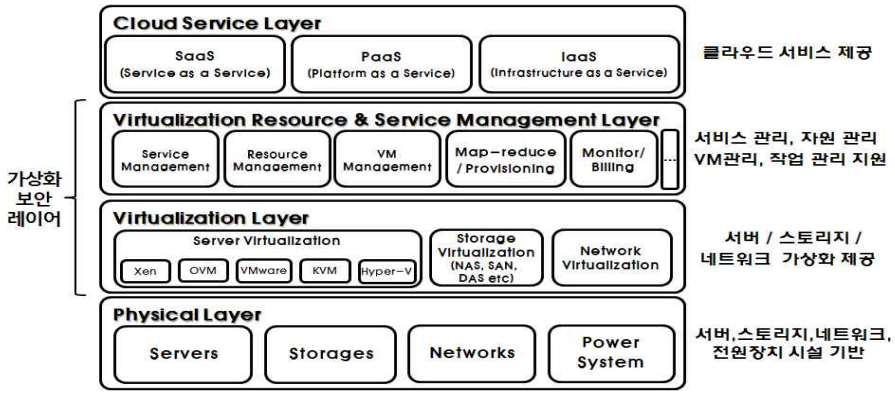
편적으로 이루어졌으나. 레이어별 세부 기능 정의와 아키텍처 레이어별 요구되어지는 보안적 요소들에 대한 연구가 고려되어지지 않았다. 또한 클라우드 컴퓨팅의 주요 기능인 가상화에 대한 분석과 이에 요구되는 보안 요소 연구가 부족하다.

3. 제안 방법

클라우드 컴퓨팅 분야는 최근 개념 정립과 동시에 서비스 및 제품 출시가 이루어지고 있기 때문에 클라우드 컴퓨팅에서 중요 기술인 가상화 기술에 대한 보안 및 상호 호환성에 대한 문제가 야기 될 수 있다. 이러한 문제 개선을 위해 본 논문에서는 클라우드 컴퓨팅 가상화 관련 기술 및 역할을 분석하고, 새로운 구조를 제안한다. 이때 가상화 환경에서 발생 가능한 위협과 이에 대응하기 위한 보안요소와 정보보호 요구사항을 도출하여 정의한다. 본 논문에서 제안하는 방법은 다음과 같이 구성된다. (1) 클라우드 기업 및 기관 아키텍처 분석을 바탕으로 공통적 개념의 아키텍처를 구성한다. (2) 클라우드 컴퓨팅 가상화 환경의 기능 및 역할 분석을 통해 '가상화 보안 레이어'를 정의하고, '가상화 레이어'와 '가상화 자원 및 서비스 관리 레이어'로 구분하여 세부 기능을 제안한다. (3) '가상화 보안 레이어'에서의 기능 및 역할에 따라 발생 가능한 위협 및 보안 요소를 정의하고 정보보호 요구사항을 제시한다. (4) 본 논문에서 제시한 공통적 개념의 아키텍처와 가상화 보안 레이어 특징과 장점에 대해 서술한다. (5) 클라우드 가상화 환경에서 발생 가능한 위협에 직접 적용한다. 이러한 방법을 통해서 클라우드 컴퓨팅 가상화 기능 및 역할에 따라 발생가능한 문제점에 대한 예방 및 대응방법을 제시한다.

3.1 클라우드 컴퓨팅 공통개념의 아키텍처

본 장에서는 2.1 '클라우드 컴퓨팅 아키텍처 모델 분석' 내용을 바탕으로 공통적 개념의 클라우드 컴퓨팅 아키텍처를 분류하여 제안한다. 1단계는 서버, 스토리지, 네트워크 그리고 전원장치와 같은 물리적인 장비를 의미하는 Physical Layer(물리적 단계), 2단계 물리적 자원을 가상화 자원으로 통합 및 추상화하는 Virtualization Layer(가상화 단계), 3단계 가공된 가상화 자원과 서비스를 할당, 수거, 모니터링, VM 관리 등의 역할을 수행하는 Virtualization Resource & Service Management Layer(가상화 자원 및 서비스 관리 단계), 마지막으로 4, 5, 6 단계는 SaaS, PaaS, IaaS 서비스 제공을 위해 필요한 APIs, 미들웨어, 어플리케이션 등을 제공하는 Cloud Service Layer(클라우드 서비스 단계)로 그림 3 과 같이 4개 레이어로 구성한다. 또한 가상화 레이어(Virtualization Layer)와 가상화 자원 및 서비스 관리 레이어(Virtualization Resource & Service Management Layer)를 클라우드 컴퓨팅 가상화 보호를 위한 '가상화 보안 레이어'로 정의한다.



[그림 3] 본 논문에서 제안하는 공통적인 개념의 클라우드 컴퓨팅 아키텍처

[Fig. 3] Common concept of colud computing architecture suggested on this paper

3.2 가상화 보안 레이어 분류 및 기능 분석

3.2.1 가상화 레이어(Virtualizationl Layer)

가상화 레이어(Virtualization Layer)는 컴퓨팅 자원 최적화를 지원하고, 사용자에게 동일한 환경을 제공하는 기술이다. 이를 위해 가상화 계층에서는 하부단의 물리적인 자원들을 통합, 가상화하는 기능을 제공하며 서버 가상화(Server Virtualization), 스토리지 가상화(Storage Virtualization), 네트워크 가상화(Network Virtualization)로 구분된다. [5, 9, 15]

- 서버 가상화는 프로세서나 메모리와 같은 다양한 컴퓨터 자원에 서로 다른 각종 운영체제(OS)의 접근 방법을 통제하고, 다수의 운영체제(OS)를 하나의 컴퓨터 시스템에서 가동할 수 있게 하는 소프트웨어로 중앙장치(CPU)와 운영체제(OS) 사이에 일종의 미들웨어로 사용된다.
- 스토리지 가상화는 가상화 기능을 제공하는 소프트웨어 또는 별도의 하드웨어 장비를 통하여 물리적인 이기종 스토리지 장치를 하나의 논리적인 가상화 스토리지 풀로 통합하여 관리하는 기술로, 필요에 따라 스토리지를 할당 한다. 이러한 스토리지 가상화 기술은 스토리지 자원에 대한 활용률을 높일 수 있으며 스토리지의 손쉬운 확장과 가용성을 제공한다.
- 네트워크 가상화는 사용자 또는 IT 인프라 자원들 간의 연결을 가상화 하여 지원하는 네트워크를 의미한다. 링크 가상화, 호스트 가상화, 라우팅 가상화, 가상머신 마이그레이션 그리고 가상 네트워크 아키텍처 등의 가상화 기술이 사용되고 있다. 클라우드 컴퓨팅 환경에서 네트워크 역할 수행을 위해 분리되어 있는 네트워크 자원을 합치거나 논리적으로 하나의 네트워크를 여러 개로 분리하여 하나의 네트워크를 전혀 다른 네트워크처럼 사용하게 지원한다.

3.2.2 가상화 자원 및 서비스 관리 레이어(Virtualization Resource & Service Management Layer)

가상화 자원 및 서비스 관리 레이어(Virtualization Resource & Service Management Layer)에서는 사용자에게 제공되는 서비스와 자원에 대한 관리를 한다. 구성 요소로는 서비스관리(Service Management), 자원관리(Resource Management), 가상머신 관리(VM Management), 맵리듀스(Map-Reduce), 프로비져닝(Provision-ing), 모니터링(Monitoring), 과금관리(Billing)로 구성된다. [5,9,15]

- 서비스관리(Service Management)는 클라우드 컴퓨팅 서비스 가입자/사용자 또는 운용자와 관련된 정보의 통제나 서비스의 적절한 운용을 지원하기 활동으로 서비스 개발, 서비스 제공, 서비스 제어, 요금 및 서비스 감시와 같은 절차를 지원한다.
- 자원관리(Resource Management)는 분산된 자원들을 동적으로 할당할 수 있는 병렬/분산형태를 띄면서 각 도메인별로 관리 정책에 따라 자원이 관리된다. 서비스 제공자와 사용자 간의 협상을 통해 정해진 SLAs 기반으로 통합된 컴퓨팅 자원으로서 제공되는 내부 가상머신 간의 연결과 가상화된 컴퓨터의 집합으로 구성된 형태를 가지고 있다. 이를 바탕으로 요청된 서비스에 대한 수용여부를 결정하게 되고, 수용이 결정된 서비스 수행을 위한 자원의 선정 / 할당 / 스케쥴링을 관리한다.
- 가상머신 관리(VM Management)에서는 작업을 위해 필요한 독립된 가상머신 환경을 생성하여 제공하고 관리한다. 미리 정의된 환경을 제공하기 위해 작업별 기본 가상머신을 생성하고, 작업 실행 관리자는 지속적으로 작업을 모니터링하고 가상머신의 상태를 확인한다. 사용자에 요청으로 할당된 가상머신은 차후 사용이 끝나고 가상머신 관리(VM Management)에 의해 회수되고 관리된다.
- 맵 리듀스(Map-reduce)는 구성된 컴퓨팅 자원들을 효율적 사용을 위해 데이터를 적당한 크기로 분리한 다음 각각의 컴퓨팅 자원에 효율적으로 분배하여 처리한다. 맵 리듀스(Map-reduce)의 작업은 Map 과 Reduce 두 가지 단계로 하여, Map 단계는 어플리케이션에 사용되는 데이터를 Reduce단계에서 처리하기 전에 미리 데이터를 제련하는 단계로 입력된 데이터를 확인하여 비정상적인 데이터는 배제 시킨다. Reduce 단계에서는 Map 단계에서 생성된 데이터를 이용해서 처리하는 단계로 사용자가 정의한 작업을 실행한다.
- 프로비져닝(Provisioning)은 클라우드 컴퓨팅 자원 및 서비스 운영/관리를 위한 단계로서 사용자의 요구사항을 받아들이고 이를 분석하여 알맞게 할당, 배치, 배포 하여 시스템을 효율적으로 사용할 수 있도록 지원하기 위한 일련의 행위를 주도하는 단계이다.
- 모니터링(Monitoring)은 클라우드 컴퓨팅 기술에서 자원에 대한 모니터링은 필수적인 요소이다. 데이터베이스, 네트워크 통신, 어플리케이션 사용, 트랜잭션 응답시간, 호스트 및 게스트 OS의 상태&성능, 통계정보 관리, 프로세스 레벨 등의 여러 요소에 대한 모니터링 및 관리가

필요하다. 또한 수백에서 수천대의 호스트 머신 및 가상머신을 모니터링 하기 위해서는 부하를 감안해야 한다.

- 과금관리(Billing)는 클라우드 서비스 사용량을 측정하고 이를 바탕으로 비용을 지불하는 기능을 제공한다. 이를 위해서 사용자에게 어떤 사양의 머신을 제공하는지, 저장 공간 및 어느 정도의 트래픽을 발생 했는지 등의 사용과 소비량을 미터링을 하여 과금 기준에 따라 측정 및 평가한다.

3.3 클라우드 컴퓨팅 가상화 보안 레이어 보호

클라우드 컴퓨팅에 사용되는 인프라 시설과 서비스 제공 및 접근을 위한 웹과 네트워크에 사용되는 기술들은 기존의 시스템 환경과 큰 차이가 없다. 이처럼 클라우드 컴퓨팅 기술은 모두 새로운 것이 아니기 때문에 공통적 개념의 클라우드 컴퓨팅 아키텍처에서 1단계 물리적 단계와 4단계 클라우드 서비스 계층 에 대한 보안 기술은 기존의 IT 보안 기술들을 고려하여 적용할 수 있다. [11, 12, 13]

[표 3] 클라우드 컴퓨팅 아키텍처 가상화 레이어 보안 요소
[Table 3] Security elements of cloud computing architecture virtualization layer

구분	레이어 세부 기능	위 협	정보보호 요구사항	대응방안
가상화 레이어	◦서버 가상화 ◦스토리지 가상화 ◦네트워크 가상화	◦불필요한 권한 부여 ◦가상머신 정보 유출 및 변조 ◦하이퍼바이저 보안 위협 ◦불법적인 통신포트 접근 ◦가상머신 우회채널 공격 ◦알려지지 않은 가상화 위협 ◦Malwares 공격	◦기밀성 ◦가용성 ◦사용자 인증 및 접근제어	◦최신 가상화 보안 패치 적용 ◦가상머신 백신 설치 및 관리 ◦가상머신 모니터링 및 로깅 ◦가상 네트워크, CPU, 디스크, 메모리 사용 데이터 관리 ◦불법 통신포트 차단/통신 암호화 ◦가상머신간 격리 및 경계 설정 ◦하이퍼바이져 위협 분석 및 예방 ◦시스템 인증 및 세션 관리 ◦이미지 백업 및 관리 ◦가상화 자원 및 관리 정보 암호화 ◦Host 및 Guest OS에 대한 최신 패치 적용
가상화 자원 및 서비스 관리 레이어	◦서비스/자원관리 ◦가상머신관리 ◦맵리듀스 ◦프로비져닝 ◦모니터링 ◦과금관리	◦권한부여 및 접근제어 위협 ◦서비스 및 자원 불법사용 ◦사용량 변조 및 삭제 ◦가상머신 불법적인 사용 ◦비인가/불법적 접근 ◦관리자 권한 남용/관리 위협 ◦모니터링 정보 변조 ◦불법적인 서비스 접근/사용 ◦가상화 계층 서비스 거부 공격 및 과부화	◦기밀성 ◦무결성 ◦가용성 ◦사용자 인증 및 접근제어	◦사용자/관리자 접근제어 관리 ◦최신 보안 패치 적용 ◦서비스 및 자원 흐름 통제 ◦환경을 고려한 암호기법 적용 ◦사용자인증 권한 관리 ◦서비스 및 자원 모니터링/로깅 ◦가상머신 스케쥴링 관리 ◦불법 통신포트 차단/통신 암호화 ◦입력 값 유효성 검증 ◦적절한 에러 처리, 관리 ◦서비스별 관리 보안 정책수립 ◦SLA 준수 확립

그러나 컴퓨팅 자원의 효율적 사용을 위해 가상화 기술이 적용된 2 단계 가상화 단계, 3 단계 가상화 자원 및 서비스 관리 단계에서는 기존의 IT 환경과 다른 클라우드 컴퓨팅 가상화 기능 및 환경의 특성을 분석하여 물리적 자원 가상화, 하이퍼바이저, VM 운영/관리, 가상화 자원 모니터링, 가상화 네트워크 통신 등과 같이 활용된 기술에 대한 보안요소들이 추가적으로 고려되어야 한다. 따라서 본 논문에서 이러한 클라우드 컴퓨팅 가상화에 대한 특징과 기능을 분석하여 '가상화 보안 레이어'에서 발생 될 위협과 그에 따른 정보보호 요구사항과 대응방안을 표 3, 4 와같이 정의하였다. [17, 20, 22]

[표 4] 클라우드 컴퓨팅 가상화 보호를 위한 정보보호 요구사항 및 고려사항

[Table 4] The information security requirments and considerations for cloud computing virtualization protection

구 분	내 용	고려사항
기밀성	클라우드 서비스 환경은 일반적으로 다수 사용자들이 공용 환경에서 서비스를 이용하기 때문에 개인 및 기업 데이터에 대한 기밀성과 데이터 암호화가 필요	◦과금 및 자원에 관련 정보 ◦사용자 계정 및 권한정보 ◦데이터 유출 방지를 위한 안전한 암호 알고리즘 ◦클라우드 특성인 대용량 데이터에 대한 암/복호화 시간고려 ◦유/무선 환경 등의 다양한 접근 방법고려 ◦개발, 테스트, 운영 등의 다른 환경에서 서로 다른 암호키 사용
무결성	저장되는 데이터와 교환되는 메시지에 대한 오류 및 변조 여부확인을 위한 데이터 무결성이 요구	◦데이터 정확성, 완전성 보증 방안 ◦암호화 알고리즘 및 인증방법 적용 ◦시스템 단계 및 환경을 고려한 암호기법 ◦사용자 특성에 따른 데이터 성질을 고려한 데이터 처리 ◦입력 값에 대한 유효성 검증
가용성	사고로 인한 서비스 중단이나 데이터 손실을 막기 위해 사고 발생 시 서비스의 지속성을 위한 가용성 및 복구가 요구	◦주기적인 가상머신 및 시스템 모니터링 규정 및 방법 ◦Host OS에 대한 최신 패치 적용 ◦가상머신들의 자원 사용량 제한 ◦자원관리 및 지속적인 취약점 모니터링 ◦하이퍼바이저 보안 위협 분석 및 예방 ◦사고에 대비한 백업 시스템과 복구 절차 ◦사고 발생 시를 대비한 사고대응 정책 ◦보안장비의 이중화(로드밸런싱)
사용자 인증 및 접근제어	다수 사용자의 데이터가 혼재되어 있는 클라우드 환경에서의 사용자에 대한 인증과 권한 관리를 위한 사용자 인증 및 접근제어가 필요	◦시스템에 접근하는 방법에 대한 정책과 절차 ◦계정 관리 방법 및 정보 흐름 통제 ◦유/무선 장비에 대한 사용 주체에 대한 방법 ◦시스템 상의 인증 및 세션 관리 ◦승인 받지 않은 사용자 권한 관리 및 접근통제 ◦Host OS와 Guest OS간의 통신포트 확인 ◦네트워크 및 웹 취약점 보안 ◦운영서버와 가상머신간의 분리

3.4 클라우드 컴퓨팅 아키텍처 및 가상화 보안 레이어 비교

본 논문에서 현재 사용 클라우드 서비스 기업 및 기관의 아키텍처를 분석하여 공통적 개념의 클라우드 컴퓨팅 아키텍처를 제안하였다. 이를 바탕으로 관련연구에서 제시된 클라우드 서비스 및 역할 기준의 아키텍처 보안연구에서 부족한 클라우드 가상화 환경에서의 위협 및 보안요소 분석과 정보보호 요구사항을 도출 하여 정의하였다. 또한 클라우드 컴퓨팅 가상화 보안을 위핸 관리 되어

야 할 레이어를 가상화 보안 레이어로 구분하고, 각각의 기능에 따라 요구되는 정보보호 요구사항 및 대응방안을 제안한 연구 방법은 표 5와 같은 특징을 갖는다. 또한 이를 통해 아래와 같은 장점이 있다.

[표 5] 클라우드 컴퓨팅 아키텍처 연구 비교 분석
[Table 5] Comparing analysis of cloud computing architecture

구 분	S. Subashini [7] 클라우드 아키텍처 연구	Liang Jie Zhang [8] 클라우드 아키텍처 연구	본 논문의 공통적 개념의 클라우드 아키텍처 연구
아키텍처 구성 기준	◦SaaS, PaaS, IaaS ◦서비스 형태를 바탕으로 데이터 및 자원 흐름	◦서비스 제공을 위한 역할 및 단계별 기능	◦아키텍처 단계별 기능 및 세부 역할 기준
아키텍처 구성	◦Data Center Layer ◦Virtualization Layer ◦Infrastructure Services ◦Application Services ◦SaaS / PaaS / IaaS Applications	◦Virtualization: HW & SW ◦Service-Orientation: Common Reusable Services&Composite Services ◦Cloud Core: Provisioning and Subscription Services ◦Cloud Offerings: Business Solutions(Cloud Value Added Services or Offerings)	◦Physical Layer ◦Virtualization Layer ◦Service Resource & ◦Service Management ◦Layer ◦Cloud Service Layer
가상화 기능 및 역할 분석 여부	세부적인 가상화 기능 및 역할에 대한 분석이 어려움	Hardware & Software Virtualization 으로 분류하여 단순 기능 분석	가상화 보안 레이어(가상화 레이어, 가상화 자원 및 서비스 관리 레이어)로 구성, 세부 기능 분류
레이어별 위협 및 취약점 분석	◦데이터에 대한 위협 및 취약점 분석 가능 ◦가상화에 대한 분석 부족함	◦위협 및 취약점 분석이 부족함.	◦각 레이어별 역할 및 세부 기능에 따라 분석 가능
보안요소 적용	◦서비스 형태별 스택에 따른 단순 보안요소 적용 ◦중복 및 제외된 보안요소 존재	◦아키텍처 레이어별 보안요소 고려 어려움	◦단계별 기능 및 역할을 고려한 보안요소 적용 ◦아키텍처 레이어별 기밀성,무결성, 가용성, 인증 및 접근통제 적용

- 클라우드 컴퓨팅 기능 및 역할에 대한 보안요소는 추상화 및 통합된 자원의 생성, 전송, 처리하는 상황에 맞게 적용함으로써, 클라우드 가상화를 보호하고, 사고발생을 감소시킴으로써 안정적 운영과 관리에 기여한다.
- 클라우드 컴퓨팅 서비스의 중요 역할인 서비스 사용 관리 및 운영에 대한 데이터 변조 및 삭제, 부정 거래 등의 위협에 대한 보안을 고려함으로서 보다 정확하고 안정된 서비스 제공할 수 있다.
- 현재 초기 단계의 클라우드 컴퓨팅은 새로운 서비스 모델에 따라 새로운 위협이 지속적으로

발생할 것이다. 이러한 문제에 대해 각 기능에 따른 보안요소 분류와 위협 및 이를 예방하기 위한 암호화, 모니터링, 로깅 요소 도출 등의 대응방안을 제시함으로서 피해가능 대상 예측이 가능하고 이를 신속히 예방할 수 있다. 또한, 효율적인 클라우드 정보보호 관리체계 수립의 기본 자료로 활용 할 수 있다.

3.5 클라우드 컴퓨팅 아키텍처 가상화 보안 레이어 적용

기존에 연구된 클라우드 컴퓨팅 환경에서의 가상화 악성코드 논문 [18] 에서 클라우드 컴퓨팅 가상화 환경에서 발생 가능한 6 가지 위협에 대해 표 6과 같이 분류 하였다. 게스트 OS간의 영향으로 인한 위협, 게스트 OS에서 호스트 / 가상화 관리 모듈 / 하드웨어로의 위협, 게스트 OS 자신으로의 위협, 외부로부터 호스트 / 가상화 관리 모듈 / 하드웨어로의 위협, 가상화 관리 모듈에서 전체시스템으로의 위협, 하드웨어에서 가상환경 관리 모듈로의 위협으로 총 6가지 상황의 위협과 각 취약점에 대한 대응 및 예방을 위한 방법으로 본 논문에서 제시한 가상화 보안요소 및 고려사항을 적용 가능하다.

[표 6] 클라우드 컴퓨팅 가상화 환경의 위협에 대한 가상화 보안 요소 / 고려사항 적용
[Table 6] Security elements and considerations for the threat of cloud computing virtual environments

가상화 환경에서의 주요 위협 [15, 18]	취약점	가상화 보안 레이어 (가상화 레이어 & 가상화 자원 및 서비스 관리 레이어)	
		보안요소	대응방안
게스트 OS 간의 영향으로 인한 위협	◦게스트 OS간 악성코드전달 ◦소프트웨어 취약점 악용 ◦자원의 독점으로 인한 위협	◦가상머신 백신 설치, 관리 ◦가상머신 모니터링 및 로깅 ◦불법 통신포트 차단/통신 암호화 ◦가상머신간 격리, 경계설정 ◦가상 이미지 백업 및 관리	◦안전한 암호 알고리즘 적용 ◦대용량 데이터에 대한 암/복호화 ◦시스템 단계 및 환경을 고려한 암호기법 ◦입력값에 대한 유효성 검증 ◦가상머신 및 시스템 모니터링 규정 및 방법 ◦가상머신들의 자원 사용량 제한 ◦사고에 대비한 백업 시스템과 복구절차 ◦보안장비의 이중화
게스트 OS에서 호스트/ 가상화 관리 모듈 /하드웨어로의 위협	◦게스트 OS에서의 취약점 악용 ◦자원의 남용	◦가상머신 백신 설치, 관리 ◦가상머신 모니터링 및 로깅 ◦불법 통신포트 차단/통신 암호화 ◦가상머신간 격리, 경계설정 ◦가상 이미지 백업 및 관리 ◦서비스 및 자원 흐름 통제 ◦가상머신 스케쥴링 관리 ◦적절한 에러 처리, 관리	◦사용자 계정 및 권한정보 ◦대용량 데이터에 대한 암/복호화 ◦개발, 테스트, 운영 등의 다른 환경에서 서로 다른 암호키 사용 ◦데이터 정확성, 완전성 보증 방안 ◦시스템 단계 및 환경을 고려한 암호기법 ◦입력값에 대한 유효성 검증 ◦가상머신 및 시스템 모니터링 규정 및 방법 ◦하이퍼바이저 보안 위협 분석 및 예방 ◦가상머신들의 자원 사용량 제한 ◦사고에 대비한 백업 시스템과 복구절차 ◦보안장비의 이중화 ◦시스템상의 인증 및 세션 관리 ◦운영서버와 가상머신간의 분리

게스트 OS 자신으로의 위협	◦가상화 이전의 단일 호스트 상의 문제가 가상환경의 게스트 OS 내에서 발생	◦가상머신 백신 설치, 관리 ◦가상머신 모니터링 및 로깅 ◦가상머신간 격리, 경계설정 ◦가상 이미지 백업 및 관리	◦대용량 데이터에 대한 암/복호화 고려 ◦데이터 정확성, 완전성 보증 방안 ◦시스템 단계 및 환경을 고려한 암호기법 ◦입력 값에 대한 유효성 검증 ◦가상머신 및 시스템 모니터링 규정 및 방법 ◦사고에 대비한 백업 시스템과 복구절차 ◦보안장비의 이중화
외부로부터 호스트 /가상화/ 관리모듈/ 하드웨어로의 위협	◦가상머신 환경의 취약점을 악용 ◦외부에서 오는 모든 트래픽 및 사용자 요구들이 위협으로 인식	◦가상머신 백신 설치, 관리 ◦가상머신 모니터링 및 로깅 ◦불법 통신포트 차단/통신 암호화 ◦가상 머신간 격리, 경계설정 ◦가상 이미지 백업 및 관리 ◦적절한 에러 처리, 관리 ◦서비스별 관리 보안 정책 수립 ◦입력 값 유효성 확인, 검증	◦사용자 계정 및 권한정보 ◦안전한 암호 알고리즘 적용 ◦대용량 데이터에 대한 암/복호화 고려 ◦데이터 정확성, 완전성 보증 방안 ◦시스템 단계 및 환경을 고려한 암호기법 ◦입력 값에 대한 유효성 검증 ◦가상머신 및 시스템 모니터링 규정 및 방법 ◦하이퍼바이저 보안 위협 분석 및 예방 ◦가상머신들의 자원 사용량 제한 ◦사고에 대비한 백업 시스템과 복구절차 ◦보안장비의 이중화 ◦시스템에 접근방법에 대한 정책과 절차 ◦시스템상의 인증 및 세션 관리 ◦운영서버와 가상머신간의 분리
가상화 관리 모듈에서 전체 시스템으로의 위협	◦가상화 관리 모듈은 게스트 OS의 모든 관리를 수행하여 가상화 관리 모듈에서 악성코드 실행시 게스트 OS와 전체 하드웨어에 전달	◦최신 가상화 보안 패치 적용 ◦가상머신 백신 설치, 관리 ◦가상머신 모니터링, 로깅 관리 ◦사용자/관리자 접근제어 관리 ◦서비스 및 자원 흐름통제 ◦환경을 고려한 암호기법 적용 ◦사용자 인증 권한 관리 ◦서비스 및 자원 모니터링/로깅 ◦불법 통신포트 차단/통신 암호화 ◦입력값 유효성 검증 ◦적절한 에러 처리, 관리 ◦SLA 준수 확립	◦가상머신 및 시스템 모니터링 규정 및 방법 ◦Host OS에 대한 최신 패치 적용 ◦가상머신들의 자원 사용량 제한 ◦자원 관리 및 지속적인 취약점 모니터링 ◦하이퍼바이저 보안 위협 분석 및 예방 ◦사고에 대한 백업 시스템과 복구 절차 ◦사고 발생 시를 대비한 사고 대응 정책 ◦보안장비의 이중화 ◦입력 값에 대한 유효성 검증 ◦시스템에 접근 방법에 대한 정책과 절차 ◦시스템 상의 인증 및 세션 관리 규정 ◦Host OS 와 Guest OS간 통신포트확인
하드웨어에서 가상환경 관리모듈로의 위협	◦하드웨어적인 문제가 각 게스트 OS에 영향	◦가상 이미지 백업 및 관리 ◦사용자/관리자 접근제어 관리 ◦사용자 인증 권한 관리 ◦서비스별 관리 보안 정책 수립 ◦SLA 준수 확립	◦가상머신 및 시스템 모니터링 규정 및 방법 ◦Host OS에 대한 최신 패치 적용 ◦하이퍼바이저 보안 위협 분석 및 예방 ◦사고에 대비한 백업 시스템과 복구 절차 ◦사고 발생 시를 대비한 사고대응 정책 ◦보안장비의 이중화

4. 결론

클라우드 서비스에서는 필연적으로 가상화 환경에 대한 보안 문제가 제기되고, 반드시 보안 체

계가 확립되어야 한다. 따라서 본 논문에서는 클라우드 컴퓨팅 가상화 환경 보호를 위해 공통적 개념의 아키텍처를 구성하여 가상화 보안 레이어에 대한 보안요소 및 정보보호 요구사항을 정의하였다. 또한, 제시한 보안 요소와 정보보호 요구사항을 활용하여 클라우드 컴퓨팅 가상화 환경의 위협 및 취약점에 대한 대응방법으로 적용이 가능함을 보였다. 그리고 본 논문의 연구 내용을 바탕으로 한국 클라우드 서비스 협회에서 구축하여 운영되는 클라우드 컴퓨팅 테스트 베드 구축에 참여하여 보안요소 및 정보보호 요구사항을 적용하여 활용성 및 보안성을 확인하였다.

이러한 연구 결과는 현재 각기 다른 클라우드 기업 및 기관별 차이가 있는 아키텍처에 대해 공통적으로 사용이 가능한 가상화 보안 레이어 구성 및 기능들을 분석한 자료를 제공함으로써, 기존의 SaaS, PaaS, IaaS와 같은 서비스 형태별, 역할별 아키텍처에서의 보안 연구에서 부족한 가상화 환경에 대한 세부적이고 효율적인 보안성 향상 방법을 제시하였다. 향후 클라우드 서비스 수요가 증가와 동시에 클라우드 컴퓨팅 가상화에 대한 새로운 취약점과 다양한 공격 방법이 발생할 것이다. 또한 다양화되는 클라우드 서비스별 다른 특징을 가지는 가상화 및 관련 아키텍처 단계에 대한 보안성 문제도 예상된다. 따라서 지속적인 클라우드 컴퓨팅 가상화 환경의 취약점 및 악성코드에 대한 대응 방법 및 보호 대책 연구가 진행되어야 할 것이다.

참고문헌

[1] 민옥기, 김학연, 남궁한, “클라우드 컴퓨팅 기술 동향”, 전자통신동향분석 제24권 제4호, Aug. 2009

[2] Asia Pacific End-User Cloud Computing Servey, IDC, Sep. 2009

[3] "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", Cloud Security Alliance, December 2009.

[4] David E. Williams, Juan Garcia, "Virtualization with Xen : including XenEnterprise, XenServer, and XenExpress", 2007

[5] "Cloud Architecture Reference Models: A Survey", NIST CCRATWG 004 v2, Jan. 2011.

[6] 김태형, 김인혁, 김정한, 민창우, 김지홍, 엄영익, “클라우드 컴퓨팅 환경에서 보안성 향상을 위한 로컬 프로세스 실행 기술”, 한국정보보호학회 논문지, pp.69-79, Oct. 2010

[7] S. Subashini, V. Kavitha, "A servey on security issues in service delivery models of cloud computing", Elsevier : Journal of Network and Computer Application, pp.1-11. 2010

[8] Liang-Jie Zhang, Qun Zhou, CCOA : Cloud Computing Open Architecture, 2009 IEEE International Conference on Web Services, pp.607-616, 2009.

[9] "Guide to Security for Full Virtualization Technologies", NIST, Special Publication 800-125

[10] 박춘식, 김형종, “클라우드 컴퓨팅 보안 동향”, 정보통신산업진흥원 주간기술 동향, 통권1432호, 2010

[11] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, Ivona Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Elsevier : Future Generation Computer Systems, Dec. 2008.

[12] "Secure Cloud Architecture",WP-7083-0809, NetApp, Aug. 2009.

[13] "Security Whitepaper Google Apps Messaging and Collaboration Products", 2010

[14] "Amazon Web Services: Overview of Security Processes", Amazon, 2008.

[15] "Above the Clouds : A Berkeley View of Cloud Computing", Electronic Engineering and Computer Sciences University of California at Berkeley, Technical Report No. UCB/EECS-2009-28, Feb. 2009.

[16] Daniel Nurmi, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff, Dmitrii Zagorodnov,“ The Eucalyptus Open-source Cloud-computing System”, the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, 2009.

[17] "Guidelines on Security and Privacy in Public cloud Computing", NIST, Draft Special Publication 800-144, Jan. 2011

[18] 김형종, 박춘식, “클라우드 컴퓨팅 환경에서의 가상화 악성코드”, 한국정보보호학회 논문지, pp.44-50 2010. 4.

[19] Paul Mason, Dan Kusnetzky, "Server Provisioning, Virtualization, and the On-demand Model of Computing: Addressing Market cofusion," IDC, Jun. 2003.

[20] "Top Threat of Cloud Computing V 1.0", Cloud Security Alliance, Mar. 2010.

[21] "Cloud Computing use cases white paper version 4.0", Cloud Computing Use Cases Discussion Group, 2. July 2010.

[22] "Assessing the Security Risks of Cloud Computing", Gartner Report, Jun. 2008.

저자 소개

정순기 (Soonki Jeong)

2005년 3월 : 한국외국어대학교 컴퓨터공학과 졸업
2009년 9월 ~ 현재: 고려대학교 정보보호대학원 석사
관심분야 : 클라우드 컴퓨팅 보안, 네트워크 보안, 시스템 보안

정만현 (Manhyun Chung)

2006년 2월: 동국대학교 컴퓨터학과 학사 졸업
2009년 2월: 고려대학교 정보경영공학전문대학원 석사
20010년 9월~현재: 고려대학교 정보보호대학원 박사과정
관심분야 : 네트워크 보안, 패턴인식, 시스템 보안

조재익 (Jaeik Cho)

2005년 2월: 동국대학교 컴퓨터학과 학사 졸업
2008년 2월: 고려대학교 정보경영공학전문대학원 석사
2008년 3월~현재: 고려대학교 정보보호대학원 박사과정
관심분야 : 네트워크 모델링, 패턴인식

손태식 (Taeshik Shon)

2000년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월: 아주대학교 컴퓨터 공학 석사
2005년 8월: 고려대학교 정보보호대학원 박사
2007년 ~ 2011년: 삼성전자 DMC 연구소 책임연구원
2011년 ~현재: 아주대학교 정보컴퓨터공학부 부교수
관심분야 : 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지

문종섭 (Jongsub Moon)

1981년 2월 ~ 1985년: 금성 통신 연구소 연구원
1991년: Illinois Institute of technology 졸업(전산학 박사)
1993년 ~현재: 고려대학교 정보보호대학원 교수
관심분야 : 생체인식, 침입탐지, 운영체제