Journal of The Korea Society of Computer and Information
Vol. 23 No. 12, pp. 81-87, December 2018
www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.12.081

The Security Architecture for Secure Cloud Computing Environment

Sang-Yong Choi*, Kimoon Jeong**

Abstract

Cloud computing is a computing environment in which users borrow as many IT resources as they need to, and use them over the network at any point in time. This is the concept of leasing and using as many IT resources as needed to lower IT resource usage costs and increase efficiency. Recently, cloud computing is emerging to provide stable service and volume of data along with major technological developments such as the Internet of Things, artificial intelligence and big data. However, for a more secure cloud environment, the importance of perimeter security such as shared resources and resulting secure data storage and access control is growing. This paper analyzes security threats in cloud computing environments and proposes a security architecture for effective response.

▸Keyword: Cloud computing, Access Control, Security Architecture, Security Threats, Cloud Security.

I. Introduction

클라우드 컴퓨팅은 IT자원을 사용자가 공유하는 시스템으로 사용자가 필요한 만큼 대여하여 원하는 시점에 네트워크를 통해 사용하는 컴퓨팅 환경이다. 즉, 기존의 컴퓨팅 환경이 IT자원을 조직 내에서 고정적으로 설치하는 사용하는 개념 이었다면, 클라우드 컴퓨팅 환경은 자원 운영비용을 낮추고 자원 사용에 대한 효율성을 증대시키기 위해 필요한 시점에 필요한 만큼의 IT자원을 임대해서 사용하는 개념이다. 최근 사물인터넷, 인공지능, 빅데이터 등 주요 기술의 발전과 함께 폭증하는 데이터의 처리와 서비스에 대한 안정적인 제공을 위해 클라우드 컴퓨팅이 활성화 되고 있다[1].

클라우드 컴퓨팅은 퍼블릭 클라우드(Public Cloud), 사설클라우드(Private Cloud), 하이브리드 클라우드(Hybrid Cloud), 커뮤니티 클라우드(Community Cloud)와 같은 배치모델(Deployment Model)과 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)와 같은 서비스 모델(Service Model)로 구분할 수 있다[2-3].

이러한 서비스는 구글[4], 아마존[5], KT[6], Naver[7]등 국내외 다양한 기업에서 상용서비스를 제공하는 형태로 이루어지고 있으며, 서비스 제공자들 입장에서 보안 서비스를 포함하여 제공하고 있다.

하지만, 클라우드 컴퓨팅 환경에서는 기존의 IT서비스 환경에서 나타나는 보안 위협뿐만 아니라, 클라우드 환경의 특성에 따른 새로운 보안 위협이 등장하고 있으며[8-11], 이러한 위협에 대한 효과적인 대응방안이 고려되지 않는다면 고객으로부터 클라우드 컴퓨팅 서비스 제공자들은 보안 신뢰도를 확보하지 못할 것이다.

본 연구에서는 보다 안전한 클라우드 컴퓨팅 서비스를 제공하기 위해 클라우드 컴퓨팅 환경의 위협을 분석하고, 기존 서비스 제공자들이 제공하는 보안 환경에 대한 분석을 통해 안전한 클라우드 서비스 보안을 위한 아키텍처를 다양한 측면에서 제안한다. 이를 위해 2장에서는 클라우드 환경과 클라우드 환경의 보안 이슈 및 알려진 클라우드 서비스 제공자의 보안환경을 분석한다. 3장에서는 분석된 결과를 통해 클라우드 서비스에서 고려해야 할 보안의 주요 요소를 식별한다. 4장에서는 고려해야 할 보안요소를 기초로 하여 다양한 각도에서 보안 아키텍처를 제안하고 5장에서 결론을 맺는다.

본 연구는 실제 서비스하는 대형 클라우드 서비스에 실제 적용된 보안 기술을 바탕으로 공통적으로 활용할 수 있는 보안 아키텍처를 도출하였다는 점에서 기존 연구와 차별성이 있다.

• First Author: Sang-Yong Choi, Corresponding Author: Kimoon Jeong
*Sang-Yong Choi (csyong95@gmail.com), Cyber Security Research Center, Korea Advanced Institute of Science and Technology
**Kimoon Jeong (kmjeong@kisti.re.kr), HPC Cloud Center, Korea Institute of Science and Technology Information
• Received: 2018. 10. 11, Revised: 2018. 11. 12, Accepted: 2018. 11. 16.
• This work was supported by major project of KISTI(Korea Institute of Science and Technology Information) in 2018

II. Preliminaries

1. Related works

1.1 Cloud computing model

클라우드 컴퓨팅은 배치모델과 서비스 모델로 구분할 수 있다[2-3].

배치모델은 퍼블릭 클라우드(Public Cloud), 사설클라우드(Private Cloud), 하이브리드 클라우드(Hybrid Cloud), 커뮤니티 클라우드(Community Cloud)로 나누는 방법이고 서비스 모델은 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service) 등으로 분류가 가능하다. 각 서비스 모델에 대한 주요 특징은 Table 1.과 같다.

1.2 Security threats for cloud computing

CSA(Cloud Security Alliance)에서는 산업분야에서의 12가지 클라우드 보안 위협을 발표하였다[8][11]. CSA에서 발표한 12가지의 위협은 데이터 유출(침해), 불충분한 신분(접근) 관리, 불완전한 API, 시스템 취약점, 계정탈취, 악의적인 내부자, APT, 데이터 유실, 불충분한 실사, 불손한 사용, 서비스 거부, 공유기술 취약점 등과 같이 기술적인 위협과 관리적인 위협이 혼재되어 있다. 또한 다른 여러 연구에서도 클라우드 환경의 보안 위협을 다루고 있으며[9-10][12] 이러한 위협은 크게 기술적 위협과 기술외적 위협으로 나눌 수 있다. 또한 기술적 위협은 기존 IT환경에서와 동일한 위협과 클라우드 환경의 특성, 즉 가상화 환경에 따른 위협으로 나눌 수 있다. 기술외적 위협은 관리측면의 문제와 법제도의 문제로 분류할 수 있다. 이와 같은 위협요소를 정리하면 다음 Table 2와 같이 분류가 가능하다.

이와 같은 클라우드 컴퓨팅에 대한 보안이슈가 발생되는 근본원인은 클라우드 컴퓨팅의 특징인 “공유자원” 문제라 말 할 수 있다. 클라우드의 특성상 저장된 데이터의 정확한 위치를 알아내기 어렵고, 산재되어 있다는 점이 보안 우려의 주요인이다. 특히, Public 클라우드를 사용할 때 외부공간에 민감한 데이터를 클라우드 상에 저장하는 것에 대한 신뢰성과 안정성이 이슈가 될 수 있다. 이 관계를 살펴보기 위해 클라우드와 기존 시스템간의 자원공유 범위를 살펴보면, Public 클라우드의 경우 기업이 소유한 컴퓨터의 자원 없이 서비스 제공자가 보유 및 제공하는 자원을 나누어 사용하는 형태이며, 사용량에 따라 과금된다. 따라서 Public클라우드는 기업 간에 컴퓨팅 자원을 상호 공유하는 형태이다. 반면 Private클라우드의 경우에는 데이터센터 내에 가상화 기술을 적용을 하는 것을 기술적인 측면에서는 Public클라우드와 유사하지만 기업별로 소한 자원을 기업 내에서 공유한다는 것이 Public클라우드와 차이점이다. 따라서 Private클라우드는 기업마다 전용 컴퓨팅 자원을 보유하고 있어 자원 공유가 Public클라우드에 비해 적다고 볼 수 있다. 자원공유를 좀 더 자세히 살펴보면 클라우드 컴퓨팅의 핵심 기술

Table 1. Characteristics by Cloud Service Type

Model		Characteristics
Deployment Model	Public Cloud	A form of billing to an end user or company based on usage Infrastructure is owned by a vendor selling services
	Private Cloud	Services that are managed to provide a cloud computing-enabled environment within a particular organization and are implemented closed
	Hybrid Cloud	A mix of public and private clouds ensures that critical materials are kept in private clouds and partly operated using public clouds
	Community Cloud	Services designed for common use by agencies and organizations in similar circumstances Sharing distributed relationships (purpose, policy, security requirements, agreements, etc.)
Service Model	IaaS	Services that make infrastructure such as servers, processors, networks, storage a virtualized environment, enabling you to use infrastructure resources as needed
	PaaS	A service that provides an integrated platform for users to develop and test applications. Users develop new applications through PaaS and provide other SaaS services.
	SaaS	A service to rent and use various software such as calendar, address book, programs for CRM, and office programs via the web

Table 2. Security Threats on Cloud Computing

Threats		Contents
technical field	Traditional security threats	Wiretapping and tampering with network traffic Loss of data leakage due to authentication and access authority Denial of Service (DoS, DDoS) attacks Error in system design
	New Threats	Hypervisor Infection Intra-VM attack and this makes intrusion detection difficult Security issues with mobility of virtual machines
untechnical field	managerial field	Internal design/management mistakes User Account Information Leak Provide a variety of hackers with a source of hacking the spread of damage Data center Building Management Physical damage to the data center and loss of data due to disasters such as fire and earthquake
	field of legal system	Policy and resource control issues with geographically dispersed infrastructure, depending on country-specific legal systems

이 가상화 기술과 단일 응용소프트웨어를 여러 고객이 공유하여 사용하게 해주는 멀티 태넌시(Multi-Tenancy)기술 두 가지이지만, 이 기술들은 공통적으로 OS와 S/W를 공유하고, 저장소를 공유한다는 특징이 있다. 따라서 클라우드 컴퓨팅에서의 가장 큰 문제는 공유자원으로 인해 보안의 경계가 겹치는 것에서 기인한다.

종합적으로 클라우드 환경의 보안 위협은 클라우드 공유자원의 문제에 기인하는 클라우드 환경만의 위협인 VM호핑, 이미지 변조, 하이퍼 바이저 기반 룻트킷 등의 가상화 문제, Multi-Tenancy로 인한 보안경계의 중첩이 가져오는 중복된 신뢰경계와 같은 클라우드 환경에서만의 위협과 네트워크 트래픽 도청, 악의적인 중간자 공격과 같은 네트워크 침입공격, 서비스 왜곡, 래핑, 스캐닝 등과 같은 서비스 공격, 접근권한의 위변조, 식별자 관리, 익명화와 같은 권한 탈취, DoS, DDoS, 가상머신이 급격한 생성과 같은 서비스 거부 공격, 설계 결함 등을 취약점을 악용하는 구현오류와 같은 기존과 동일(유사)한 보안문제 등으로 정리할 수 있다.

2. Commercial Cloud Services Security

2.1 Amazon Web Service

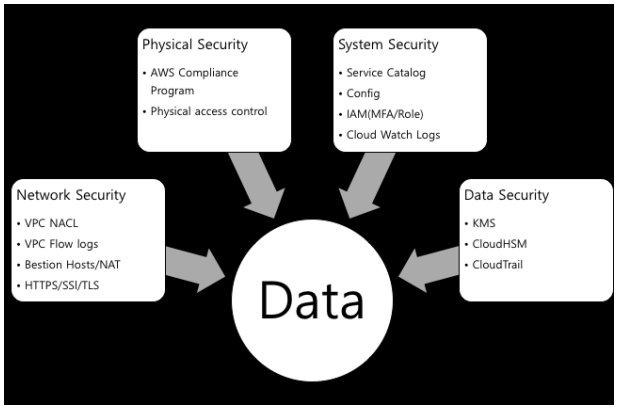

Fig. 1. AWS Security Function

대표적인 클라우드 서비스로 아마존社에서 제공하는 AWS(Amazon Web Service)가 있다[5]. AWS는 클라우드에 최적화된 보안을 제공한다는 모토를 가지고 기존의 보안솔루션과의 연계, 인증, 인가, 로깅 등의 보안기술을 제공하고 있다. AWS는 데이터 보안, 어플리케이션 보안, 운영체제 보안에 대해서는 기존에 고객이 수행하던 방식과 유사하게 적용할 수 있도록 다양한 기능을 제공하고 있으며, 하이퍼바이저 보안, 서비스 보안, 관리자보안, 네트워크 보안에 대해서는 API를 이용하여 제공하고 있다. 이 모델을 AWS에서는 “책임 공유 모델”이라 한다. 책임공유 모델에 따른 AWS의 보안기능은 Fig. 1과 같이 4가지 영역으로 나누어진다. 물리적 보안에 대해서는 물리적으로 위치한 장소에 대해 AWS에서 전적으로 책임진다. 네트워크 보안에 대해서는 NACL(Network ACL), Flow Logs, NAT, HTTPS/SSL과 같은 암호통신, 접근통제, 감사로그 등의 기능을 제공하며, 시스템 보안에 대해서는 설정, 식별 및 접근통제, 클라우드 시스템 감사로그 등의 기능을 제공하나, 데이터 보안에 대해서는 암호화와 감사로그를 통해 보안을 제공한다.

AWS CloudWatch(가시성) : AWS CloudWatch는 AWS리소스와 AWS기반 애플리케이션에 대한 모니터링 서비스를 제공하는 기능이다. AWS CloudWatch는 클라우드를 구성하는 각종 요소들에 대한 데이터를 취합하고 경보를 설정할 수 있으며, 그래프와 통계를 조회할 수 있는 서비스를 제공한다.

AWS Inspector(보안수준진단) : AWS Inspector는 애플리케이션 보안 수준진단을 하는 서비스로, 보안진단결과와 조치를 위한 가이드를 제공한다. 또한 이 기능은 API를 사용하여 자동화하여 구현할 수 있도록 해준다. AWS Inspector는 CVE의 수천 개의 항목과 Network security best practices, Authentication best practices, Operation system security best practices, Application security best practices, PCI DSS 3.2 readiness 등 다양한 분야에 대한 보안 진단이 가능하다.

AWS에서 제공하는 암호화 기능은 전송 중 암호화와 저장 시 암호화로 나누어진다. 전송 중 암호화는 HTTPS, SSH, SSL/TLS, VPN등의 대부분의 전송암호 프로토콜을 지원하며, 저장 시 암호화는 Database, Object, Filesystem, Disk 등에 대한 암호화를 지원한다. 또한 암호화에 사용되는 키를 생성/보관/관리해주는 서비스인 AWS KMS가 있다. 이는 암호화키를 안전하게 생성/보관/관리해주는 관리형 서비스로 중앙 집중화 키관리이다.

AWS Identity and Access Management(IAM, 식별 및 접근통제) : AWS IAM은 서비스와 리소스에 대한 접근통제를 지원하는 기능이다. 사용자이름, 사용자, 그룹 등에 대해 어떤 계정에서 어떠한 작업이 가능한지를 사용자의 롤과 권한에 따라 통제하는 중앙집중식 식별 및 접근통제를 지원한다.

2.2 Google Cloud

Fig. 2. Google Security Layers

Google社의 보안서비스는 운영보안, 인터넷 통신 보안, 스토리지 보안, 사용자 식별, 서비스 배포, 하드웨어 인프라 보안

등 6가지 레이어로 구성된다[4]. 운영보안에서는 침입탐지, 내부위험 감소, 안전한 직원 단말기 사용, 안전한 소프트웨어 배포 등이 있으며, 인터넷 통신보안 레이어 에서는 DoS방지와 암호통신을 다룬다. 스토리지 보안에서는 암호화와 데이터 삭제 부분을 다루고 있으며, 사용자 식별은 인증과 로그인 도용을 방지하기 위한 기술을 다룬다. 서비스 배포 보안에서는 최종사용자 데이터에 대한 접근관리, 내부통신에 대한 암호화, 내부 서비스에 대한 접근통제, 서비스 식별, 무결성, 격리 등이 포함되며, 하드웨어 인프라 보안에서는 안전한 부팅스택과 기계식별, 하드웨어 디자인 및 물리적인 보안을 다룬다. Google의 보안 서비스와 4.1 AWS와의 차이점은 AWS의 경우 사용자에게 인프라를 임대하는 클라우드 서비스인 반면, Google Cloud는 클라이언트에게 서비스를 제공하는 SaaS이다. 따라서 보안을 바라보는 관점에서 큰 차이를 보이고 있으며, 가장 핵심적인 차이는 AWS가 인프라를 보호하기 위한 접근통제, 암호화, 방화벽, 침입탐지 등의 솔루션 기반이 보안서비스를 제공하는데 비해, Google Cloud는 사용자 계정, 서비스에 대한 접근권한, 운영관리 등에 대한 보안서비스가 중심이다.

2.3 KT & Naver

한국에서 클라우드 서비스를 제공하는 기업은 대표적으로 KT[6]와 Naver[7]가 있다. KT는 기업전용 클라우드와 공공전용 클라우드를 별도로 서비스하고 있다. 하지만 정보보안의 측면에서는 대동소이한 서비스를 제공하고 있으며, KT 클라우드의 보안서비스는 웹방화벽, 관리보안, 심층보안, 웹쉘 모니터, 암호화, 사용자 시스템 보안, 취약성 보고 및 침투 테스트 등과 함께 부하 테스트 및 관제서비스를 제공하고 있다. 서비스 제공의 항목 측면에서는 AWS와 유사한 서비스를 제공하고 있으며, 인프라 보안에 대해서는 AWS와 일부 상이한 측면이 있다.

KT클라우드의 특징은 이와 같이 제공되는 각종 보안 솔루션을 서비스 등급별로(과금의 크기)에 따라 달리 적용하고 있으며, 고객이 일정부분 컨설팅을 통해 필요한 서비스를 선택할 수 있도록 하는 것이다. 이를 Managed Security 서비스라 하고 있다. 또한 Agent설치가 필요하지 않은 WAF와 같은 네트워크 보안서비스는 고객사에서 직접 운영하는 웹서비스에 대해 트래픽우회(DNS를 이용한)와 같은 방법으로 네트워크를 우회시켜 보안서비스를 제공할 수 있도록 하고 있다. 즉, KT의 보안서비스는 기존의 다양한 보안장비를 활용하여 보안 서비스 자체를 클라우드로 제공하고 있다.

네이버 클라우드의 보안서비스는 서비스 보호, 데이터 보호, 보안환경구축, 보안 예방, 보안인증 등의 타입으로 제공하고 있다. 서비스 보호에서는 Basic Security, Security Monitoring, Site Safer, App Safer, File Safer등과 같은 서비스를 제공한다. Security Monitoring은 IDS, Anti-DDoS, Anti-virus, IPS, WAF와 같은 보안시스템을 이용하여 제공하는 보안서비스이며, Site Safer는 고객이 개발한 웹사이트가 해킹 또는 다른 문제로 인해 악성코드를 배포하는지 여부를 검사해주는 서비스이다. App Safer는 고객의 앱이 모바일에서 실행될 때, 루팅/탈옥, 악성 앱 설치, 앱변조, 메모리변조 등이 보안 위협 여부를 실시간으로 탐지하는 서비스이며, File Safer는 고객의 서비스에서 제공하는 파일과 아웃링크 URL의 악성 감염 여부를 해시기반으로 빠르게 검사하는 서비스이다.

데이터 보호에서는 KMS, Secure zone,서비스가 있으며, KMS는 고객데이터의 암복호화에 사용되는 키를 안전하게 보호하는 서비스이다. Secure Zone은 개인정보와 같이 중요한 정보를 보다 안전하게 보호하기 위한 별도의 존을 제공하는 서비스이다.

보안환경구축은 SSLVPN, vFirewall, vWAF, ACG와 같은 서비스를 포함하고 있다. 이 중 vFirewall과, vWAF는 가상 환경에 특화된 방화벽과 웹방화벽 서비스로 고객에게 할당된 클라우드 인프라를 잘 보호할 수 있도록 설계되어 있다.

보안예방은 Web Security Checker, App Security Checker, System Security Checker등 웹과 모바일 애플리케이션, 운영체제 및 WAS의 보안상 문제점과 취약점을 점검하고 가이드를 제공하는 서비스이다.

보안인증이 경우에는 클라우드 서비스를 사용하는 고객이 보안인증을 준비하고 있을 때, 네이버 클라우드 플랫폼이 보유한 인증서를 제공하여 보아 인증수준에 부합하는 서비스 제공을 보장하는 서비스이다.

이 외에도 클라우드 인프라에 대한 기본운영 보안 항목인 백업 등과 같은 서비스를 제공한다. 네이버 클라우드의 분야별 보안 서비스는 Fig. 3과 같다.

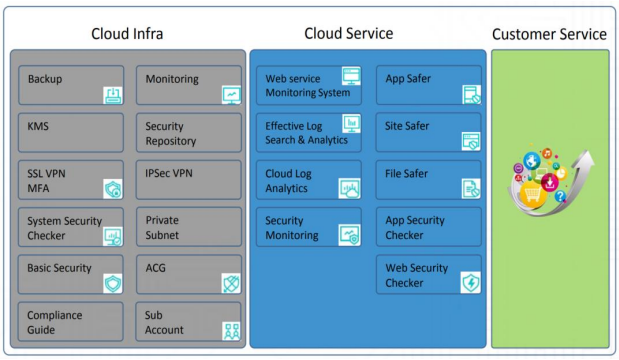

Fig. 3. Naver Cloud Security Service

III. Proposals for Cloud Security Architecture

클라우드 서비스의 구성은 클라우드 환경 외부의 외부구간, 외부와 클라우드 환경이 만나는 접점구간, 클라우드 인프라가 포함되어 있는 내부-공통구간, 그리고 내부에서 사용자별로 할당된 자원이 존재하는 내부-전용구간으로 나눌 수 있다. 각 구

간에 대해 외부구간의 경우에는 네트워크를 통해 유입되는 위협을 적절히 통제해야 하고, 경계구간에서는 외부에서 유입되는 위협과 내부에서 외부로의 인가되지 않은 접근 및 정보유출 등을 방지해야 한다. 내부-공통구간에서는 가상화 환경을 지원하기 위하 인프라 측면에서 보안기술이 적용되어야 한다. 이는 가상 환경 내의 가상머신과 가상머신 사이에서 발생 또는 확산 가능한 위협에 대한 대응 기술이 필요하며, 가상 환경 전체를 보호할 수 있어야 한다. 내부-전용구간은 실제로 고객에게 할당된 고객의 공유자원이다. 이 구간에서는 가상 환경 내에서 발생 가능한 위협과 다른 가상 환경에서 유입되는 위협을 고객 서비스의 관점에서 보호하여야 한다. 이와 같은 4가지 클라우드 영역에 대한 보안의 책임은 클라우드 서비스 제공자 또는 사용자에게 전적으로 부가되는 것이 아니라 구간과 서비스의 목표에 따라 제공자와 사용자에게 적절하게 책임이 부과되어야 한다. 기본적으로 서비스 제공자는 4가지 모든 영역에 대한 보안책임이 있으며, 서비스 사용자는 내부-전용 구간에 대한 보안책임, 즉 사용자가 설정하는 환경과, 소프트웨어, 데이터에 대한 보안책임이 있다고 말할 수 있다. 이러한 측면에서 클라우드 보안을 위해 고려되어야 할 보안의 기능을 먼저 정의해 보면 Table 3과 같이 정의가 가능하다. 각각의 기능을 구현하는 보안 시스템은 다양한 방면으로 구축할 수 있지만, 고객에게 보안 아키텍처를 배치하기 위해 클라우드 서비스 제공자 측면에서 검토해야할 것이라 할 수 있다. 표에서 필수여부는 기본적인 보안 서비스를 제공하기 위해 반드시 필요한 기능에 대한 설명으로 “필수(Essential)”는 고객과 서비스제공자와의 이해관계에 관계없이 컴플라이언스 측면 또는 기본적인 보안속성으

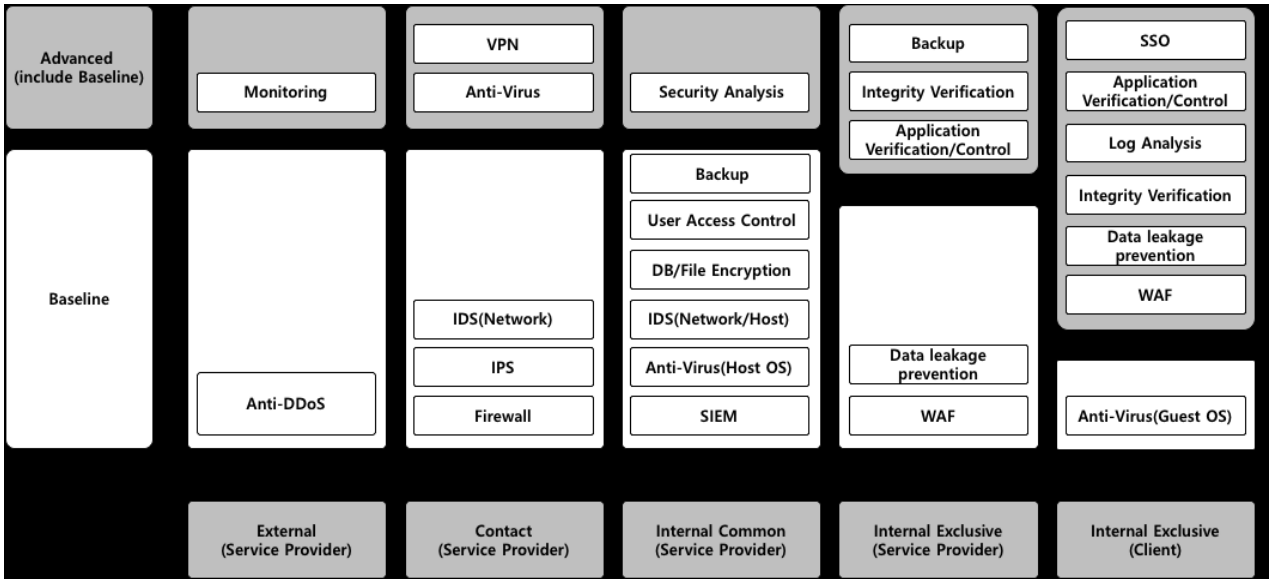

Fig. 4. Cloud Security Architecture

Table 3. Security Function for Cloud Computing

Owner	Zone	Security Function	Condition
Service Provider	External	Block denial-of-service attacks	Essential
	Contact	Network access control	Essential
		Intrusion detection	Essential
		Secure Communication	Options
		Block entry of malicious code	Options
	Internal (Common)	intrusion detection	Essential
		Block entry of malicious code	Essential
		Response of APT and Log Analysis	Essential
		Encryption	Essential
		Certification	Essential
	Internal (exclusive)	Web security	Essential
		Backup	Options
		Data leakage prevention	Essential
		Integrity verification	Options
		Application Verification/Control	Options
Service Client	Internal (exclusive)	Web security	Options
		Data security	Options
		Malicious code infection prevention	Essential
		Integrity verification	Options
		Log Analysis	Options
		Application Verification/Control	Options
		SSO	Options

로 반드시 필요한 기능이며, “선택(Options)”은 서비스의 특성 및 고객 데이터의 특성에 따라 선택이 가능한 기능이다. 필수와 선택의 여부는 클라우드 서비스를 구축하고자 하는 필요성에 따라 달라질 수 있는 상대적인 기준이다.

이러한 보안기능들을 기반으로 효과적인 클라우드 서비스 구축을 위해 활용대상, 인증요구사항, 클라우드 아키텍처 기반 클라우드 환경에서 고려해야 할 사항들과 보안솔루션을 배치하는 방법에 대한 전체적인 클라우드 보안 아키텍처는 Fig. 4와 같다.

클라우드 보안 아키텍처를 설계함에 있어 가장 최적의 보안 환경을 제공하기 위해 고려한 사항은 첫 째, 해당 보안서비스가 반드시 필요한 것인가 여부 즉, 컴플라이언스 측면에서 반드시 필요한 보안서비스와 컴플라이언스가 아니라 할지라도 일반적인 보안의 목적 달성을 위해 꼭 필요한 것인가와 꼭 필요하지 않은 것인가와 같이 기본적인 보안 기능인지 부가기능인지 여부, 둘 째, 클라우드 환경의 구조, 즉, 클라우드 서비스를 구성하는 가상 인프라와 가상 환경, 그리고 각 환경에 따른 보안의 기본적인 책임여부 등의 환경적인 요인이 될 수 있다.

Fig. 4 보안 아키텍처에서 Baseline은 클라우드 서비스를 제공하기 위한 제공자와 클라우드 서비스를 사용하기 위한 사용자가 최소한으로 지켜야 할 보안요구 사항이며, Advanced의 경우에는 Baseline을 포함하고, 보다 안전한 클라우드 환경을 운영하기 위해 추가적으로 검토되어야 할 보안기능이라 할 수 있다. 하단에 있는 제공자와 사용자는 해당 보안기능에 대해 책임이 있는 영역이라 할 수 있다. 일반적으로 클라우드 서비스 제공자의 경우에는 공통 네트워크 인프라와 클라우드를 위한 가상화 플랫폼에 대한 보안책임이 있고, 서비스 사용자는 사용하는 가상 환경에 보안책임이 부여될 수 있다.

물론, Advanced에 포함된 기능 – Baseline을 제외한 – 에 대해서는 컴플라이언스 측면에서는 필수기능으로 포함될 수 도 있다.

IV. Conclusions

본 연구에서는 안전한 클라우드 컴퓨팅 서비스 환경 구축을 위한 클라우드 보안 아키텍처에 대해 살펴보았다. 안전한 보안 아키텍처 설계를 위해 먼저, 클라우드 환경의 특성과 이에 따른 보안 기능을 분석하였고, 아마존, 구글, 네이버, KT등 국내외 클라우드 서비스를 제공하는 기업의 상용 서비스에 대한 보안 기능을 분석하였다. 또한, 클라우드 컴퓨팅의 특성에 따라 클라우드 컴퓨팅 구간을 4개의 구간으로 분리하여 서비스 구간별 요구되는 최소한의 보안 기능을 분석 하였으며, 이를 기반으로 하여 클라우드 컴퓨팅 보안 아키텍처를 제안하였다.

제안하는 보안 아키텍처는 클라우드 서비스 제공자와 클라우드 서비스 사용자에게 보안의 책임을 적절하게 분배하였으며, 이러한 개념은 보안이 어느 한 영역의 소관이 아니라 비용을 받고 서비스를 제공하는 제공자와 비용을 지불하고 서비스를 제공받는 사용자가 모두 보안에 대한 책임이 있다는 것을 반영하였다는데 에 큰 의미가 있다고 볼 수 있다. 또한, 클라우드 환경의 특성에 따라 기본 보안 아키텍처와 고급 보안 아키텍처를 분리하여 보안환경을 구축하고자 하는 자가 선택할 수 있도록 기본 프레임을 제공한다는데 의미가 있다.

제안하는 보안 아키텍처는 향후 클라우드 서비스를 제공하고자 하는 자나 클라우드 서비스를 사용하고자 하는 자가 공통적으로 활용할 수 있을 것으로 기대한다.

본 연구의 한계점으로는 제안하는 보안 아키텍처는 현재의 기술, 서비스와 환경을 기반으로 설계한 아키텍처로써 향후 새로운 기술과 서비스의 등장에 따라 지속적으로 개선하고 확장해 나가야 할 필요가 있다. 특히, 오픈소스를 활용한 클라우드 서비스의 확산이 예상됨에 따라, 오픈소스를 사용할 때의 보안 이슈 및 취약점 관리 방안, 위협 대응 방안을 포함한 오픈소스 기반 클라우드 서비스의 보안강화 방안에 대한 연구가 지속적으로 필요하다.

또한, 본 논문에서 제안한 클라우드 보안 아키텍처를 검증하기 위해 오픈소스를 기반으로 하는 클라우드 서비스 환경을 구축하여, 알려진 오픈소스 보안 소프트웨어를 활용하여 제안한 아키텍처의 활용성 및 안전성에 대한 실험을 수행함으로 개선해야 할 사항을 발굴하고 보다 완전한 아키텍처를 설계하는 연구를 향후 수행할 예정이다.

REFERENCES

[1] DEMPSEY, David; KELLIHER, Felicity. Industry Trends in Cloud Computing. 2018.

[2] JOSHI, N.; SHAH, S. A Comprehensive Survey of Services Provided by Prevalent Cloud Computing Environments. In: Smart Intelligent Computing and Applications. Springer, Singapore 2019, pp. 413-424, 2018.

[3] VARGHESE, Blesson; BUYYA, Rajkumar. Next generation cloud computing: New trends and research directions. Future Generation Computer Systems, pp. 849-861, 2018.

[4] https://cloud.google.com/security/security-design/

[5] https://aws.amazon.com/security/

[6] https://gov.ucloudbiz.olleh.com/portal/ktcloudportal.epc.productintro.waf.html

[7] https://cloud.naver.com

[8] Cloud Security Alliance, “The Treacherous 12 CloudComputing Top Threats in 2016,” Security, no. February, pp. 1-34, 2016.

[9] M. Kazim and S. Zhu, “A Survey on Security Threats

in CloudComputing Technology," Int. J. Res., vol. 1, no. 8, pp. 1071-1081, 2015.
[10] G. Aswini and R. Mervin, "A Survey on Cloud Security Issuesand Techniques," Int. J. Comput. Sci. Appl., vol. 4, no. 1, pp.125-132, 2016.
[11] https://cloudsecurityalliance.org/download/top-threats-cloud-computing-plus-industry-insights/
[12] PARK, Jae-Kyung; LEE, Won Joo; LEE, Kang-Ho. A Study on the Isolated Cloud Security Using Next Generation Network. Journal of The Korea Society of Computer and Information, Vol. 22, No. 11, pp. 9-16, 2017.

Authors

Sang-Yong Choi received his B.S. degree in Mathematics and M.S. degree in Computer Science, both from Hannam University in 2000 and 2003, and Ph.d degree in Interdisciplinary of Information Security from Chonnam National University in 2014, Korea. Dr. Choi is a Research associate professor at the Cyber Security Research Center in Korea Advanced Institute of Science and Technology (KAIST). His research interests are in web security, network security and cloud computing security,

Kimoon Jeong received the B.S. and M.S. degrees in Computer Science, and Ph.D. degree in Interdisciplinary of Information Security from Chonnam National University. Korea. in 1999, 2001 and 2009, respectively Dr. Jeong is a Senior researcher at the HPC Cloud Center in Korea Institute of Science and Technology Information (KISTI). His research interests are in cloud computing security, network security and big data security.