Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1247

클라우드 저장장치 가상화 시스템을 위한 보안 요구사항 제안*

여 영 민,† 이 찬 우, 문 종 섭‡
고려대학교 정보보호대학원

Proposal of Security Requirements for the Cloud Storage Virtualization System*

Youngmin Yeo,† Chanwoo Lee, Jongsub Moon‡
Center for Information Security Technologies(CIST), Korea University

요 약

클라우드 저장장치 가상화 환경에서는 기존의 컴퓨터 시스템 환경과는 다른 형태의 새로운 보안 취약점들이 발생하고 있으며, 기존의 보안 시스템으로는 이러한 보안위협요소들에 대해 적절한 대응이 어려우므로 기술적 해결 방안의 수립이 시급하다. 이를 위해서는 먼저 클라우드 저장장치 가상화 기술들을 상세하게 분석하고, 클라우드 저장장치 서비스를 이용하는 다양한 이해관계자들의 보안 요구사항을 조사하여, 보안 요구사항의 기술적 가이드라인에 대한 연구가 선행되어야 한다. 이에 본 논문은 클라우드 저장장치 가상화의 보안 요구사항 정의하고, 사용자 역할별 보안 요구사항과 시스템 계층별 보안 요구사항을 각각 도출하여 계층 및 역할별 보안 요구사항을 제안한다. 제안된 보안 요구사항은 가상화 보안 솔루션을 개발할 수 있는 기초를 제공할 것으로 예상된다.

ABSTRACT

The security vulnerabilities of cloud storage virtualization environments are different from those of the existing computer system and are difficult to be protected in the existing computer system environment. Therefore we need some technical measures to address this issue. First of all, the technology used in cloud storage virtualization environment needs to be thoroughly analyzed, and also, we should understand those security requirements of various stakeholders in the view of cloud storage service and perform the research on security guidelines of the research security requirements. In this paper, we propose security requirements based on layers and roles of cloud storage virtualization. The proposed security requirements can be a basement for development of solution of cloud storage virtualization security.

Keywords: Virtualization, Storage Virtualization, Security Requirements, Standardization

I. 서 론

클라우드 컴퓨팅은 서로 다른 물리적 위치에 존재하는 컴퓨팅 자원을 가상화 기술을 사용하여 논리적으로 통합해 서비스를 제공하는 기술로, IT 자원을 서로 공유하고 유휴 자원을 효율적으로 이용해 궁극적으로는 전체적인 자원을 절감할 수 있다는 장점을 가지고 있다. 또한, 사용자는 IT 자원을 원하는 시점에 필요

접수일(2013년 11월 7일), 게재확정일(2013년 12월 4일)
* 본 연구는 미래과학창조부의 방송통신표준기술력향상사업인 "클라우드 서비스 시스템 보안 레이어 표준개발(과제번호: 2013-PK10-28)"의 연구결과로 수행되었음.
† 주저자, youngman1123@korea.ac.kr
‡ 교신저자, jsmoon@korea.ac.kr(Corresponding author)

한 만큼 빌려서 사용함으로써 비용을 절약한다[1]. 현재 클라우드 저장장치 서비스의 필요성에 대한 기업의 인식이 확산되고 있으나, 클라우드 저장장치 가상화 보안에 대한 우려와 가상화 기술에 대한 정확한 이해의 부재는 클라우드 서비스를 도입하는 데 있어 가장 큰 걸림돌로 작용하고 있다. 기존 컴퓨터 시스템 환경과 다른 클라우드 저장장치 가상화 환경에서의 새로운 보안 취약점들이 발견되고 있으며, 이러한 보안 취약점에 대하여 기존의 보안 시스템으로는 적절한 대응이 어려우므로 안전한 시스템의 보호를 위해서는 적절한 기술적 해결 방안이 제시되어야 한다. 이를 위해서 먼저 클라우드 저장장치 서비스를 이용하는 다양한 이해관계자들의 보안 요구사항을 조사하고, 이를 통하여 보안 솔루션 개발을 위한 요구사항이 기술적 가이드라인으로써 표준화가 선행되어야 하며, 특정 플랫폼의 독립적인 클라우드 저장장치 가상화 보안 솔루션 개발에 대한 연구가 진행되어야 한다. 이에 대하여 본 논문은 CCRA(Cloud Computing Reference Architecture)[2]에서 정의한 클라우드 서비스 시스템의 사용자 역할을 활용하고, 일반적인 클라우드 시스템 계층의 구조를 분석하여 구조에 따른 역할을 정의하고, 클라우드 저장장치 가상화에서 고려해야 하는 중요한 계층별 및 역할별 보안 요구사항을 도출한다. 또한, 이를 통하여 클라우드 컴퓨팅 환경에서의 다양한 클라우드 서비스 플랫폼과 보안 솔루션 간 상호 호환성을 보장하도록 다음과 같이 제안한다. 본 논문의 2장에서는 클라우드 저장장치 가상화 기술에 대한 이론적 배경을 상세하게 분석하고, 3장에서는 사용자 관점에서 본 클라우드 서비스 시스템, 클라우드 시스템 계층 구조, 그리고 컴퓨터 시스템에서의 보안 요구사항에 대한 정의와 이론적 배경을 분석하고, 4장에서는 클라우드 저장장치 가상화의 보안 요구사항을 제시하고, 사용자 역할별 보안 요구사항과 클라우드 시스템 계층별 보안 요구사항을 각각 종합하여 클라우드 저장장치 가상화 보안 기술 표준화를 위한 계층 및 역할별 보안 요구사항을 도출 및 제안하며, 5장에서는 본 논문의 결론을 제시하고, 향후 연구 계획을 소개한다.

II. 클라우드 저장장치 가상화 기술의 이론적 배경

2.1 저장장치 가상화

저장장치 가상화는 가상화 기능을 제공하는 소프트웨어 또는 별도의 하드웨어 장비를 통하여 물리적인 이기종 저장장치를 하나의 논리적인 가상화 저장장치 풀로 통합하여 관리하는 기술로 필요에 따라 저장장치를 할당하여 사용할 수 있도록 한다[3]. 이러한 저장장치 가상화 기술은 저장장치 자원에 대한 활용률을 높일 수 있으며 이로 인한 비용 절감을 가져 올 수 있다. 또한 저장장치의 손쉬운 확장과 가용성을 제공할 수 있다. 가상화된 저장장치는 실제 존재하지는 않지만 물리적인 저장장치와 동일한 특성을 갖기 때문에 가상화 저장장치를 접근하기 위해 애플리케이션을 변경할 필요는 없다.

저장장치 가상화를 통해 얻을 수 있는 장점은 다음과 같이 구분할 수 있다[4][5].

2.2 저장장치 가상화의 장점

2.2.1 저장장치 활용률 향상

데이터 센터의 저장장치 활용률은 50% 정도에 못 미치고 있다[6]. 따라서 저장장치 가상화를 통하여 필요에 따라 저장장치를 할당하고 관리함으로써 불필요한 저장장치 추가를 방지하여 기존의 저장장치의 활용률을 높일 수 있다.

2.2.2 I/O 성능 향상

높은 I/O 성능을 요구하는 애플리케이션을 위하여 저장장치 가상화에서는 여러 저장장치에 걸쳐서 데이터를 스트라이핑(striping)하여 저장하는 기술을 사용함으로써 데이터 입출력 성능을 향상시킬 수 있다[6].

2.2.3 가용성 제공

오류가 발생하더라도 서비스를 계속 제공할 수 있으며 데이터를 복구할 수 있어야 한다. 저장장치 가상화에서는 동일한 데이터를 미러링(mirroring)하거나 복제함으로서 저장장치 고장이 발생하더라도 데이터에 대한 손실을 막을 수 있도록 한다.

2.2.4 구매 비용 절감

저장장치 가상화를 통하여 분산된 저장장치를 통합하고, 사용되지 않은 저장장치를 필요한 곳에 재배치할 수 있도록 함으로써 저장장치 추가 등으로 인한 비

용을 절감할 수 있다.

2.2.5 관리 비용의 저렴

저장장치에 대한 관리 비용은 저장장치 구매 비용보다 더 많이 든다. 이러한 저장장치 관리 비용은 저장장치 가상화를 통해 줄일 수 있다. 저장장치 가상화는 개개의 많은 저장장치들을 하나의 가상화 저장장소로 통합함으로써 오류 복구 등과 같은 저장장치 관리에 용이하며 이를 위해 필요한 작업을 줄일 수 있다[6].

2.3 저장장치 가상화의 형태

2.3.1 디스크와 블록 저장장치 가상화

디스크 장치 가상화는 가장 많이 사용되는 가상화 형태로, 물리적인 디스크 장치의 펌웨어을 이용하여 구성된다. 블록 저장장치는 여러 디스크를 하나의 디스크처럼 사용하는 것으로, RAID(Redundant Array of Inexpensive Disk) 시스템, 볼륨 매니저 또는 네트워크 저장장치 어플라이언스로 구성된다. 따라서 블록 저장장치는 디스크를 사용하듯이 사용하게 된다.

2.3.2 파일시스템 가상화

사용자에게 원격 파일 시스템을 로컬 파일시스템처럼 사용할 수 있다. 또한 여러 파일 시스템을 하나의 파일 시스템으로 이용할 수 있는 가상화 형태로 파일 시스템의 저장장치를 이용할 수 있다[6]. NHN의 'N 드라이브'도 파일시스템 가상화의 예로 볼 수 있다[7].

2.3.3 테이프 라이브러리 가상화

테이프 라이브러리 가상화는 디스크 장치를 테이프 라이브러리 또는 테이프 드라이브로 가상화하여 기존의 테이프에 대한 백업 방법을 변경하지 않고도 사용할 수 있다. 테이프 대신 디스크를 사용하여 백업과 회복 성능을 향상시킬 수 있다[6].

2.3.4 서버 또는 호스트 기반 저장장치 가상화

호스트 기반 가상화는 호스트에 장착된 물리적인 저장장치들을 볼륨 매니저와 같은 소프트웨어를 통하여 논리적인 볼륨으로 가상화하여 관리하고 이러한 볼륨 매니저 외에 스냅샷(snapshot), 미러링, 복제 기능을 추가로 제공하기도 한다. 하지만 볼륨 매니저는 장착된 호스트에 제한 될 수 있다. 또한 일반적으로 호스트 운영체제에 종속적이기 때문에 호스트 플랫폼에 제한된다.

2.3.5 네트워크 기반 저장장치 가상화

저장장치 스위치에 연결된 저장장치를 가상화하여 사용하고, 가상화된 저장장치는 인-밴드(in-band)와 아웃-밴드(out-band)로 구현된다. 인-밴드는 클라이언트와 물리적인 저장장치 사이의 데이터 경로 상에 가상화 장치를 통하여 동작한다. 반면 아웃-밴드는 클라이언트와 물리적인 저장장치 사이의 데이터 경로와 가상화 장치를 별도의 경로로 분리했기 때문에 가상화는 다른 곳에서 이루어지고 클라이언트가 직접 저장장치에 접근한다[6].

2.3.6 클러스터 분산 파일시스템

네트워크상에 분산된 대량의 저장장치 서버를 하나의 클러스터 파일 시스템으로 가상화하여 대용량의 저장 공간과 빠른 입출력 성능을 제공함으로써, 확장성이 좋으며, 시스템 장애가 발생해도 여러 복제본이 있어 안전하게 서비스를 제공할 수 있는 신뢰성과 가용성을 보장할 수 있다. 일반적으로 클러스터 분산 파일 시스템은 비대칭 구조이며, 파일 메타데이터를 관리하는 전용 서버가 있다. 이때 메타데이터에 접근하는 경로와 데이터에 접근하는 경로를 분리한다. 그러나 메타데이터 서버에 부하가 집중될 경우 SPOF(Single Point Of Failure)가 발생하는 위험성이 있다. 이 클러스터 분산 파일 시스템은 클라우드 컴퓨팅에서 중요한 기술 분야로 구글의 GFS[8], 아파치 프로젝트인 하둡[9] 그리고 ETRI의 GLORY[10] 등이 있다.

Fig.1.은 SNIA(Storage Networking Industry Association)에서 저장장치 가상화 기술을 분류한 그림이다. 그림에서 'What is created'는 가상화 대상을 의미하고, 'Where it is done'은 가상화가 이루어지는 위치를, 그리고 'How it is implemented'는 가상화 기법을 나타낸다.

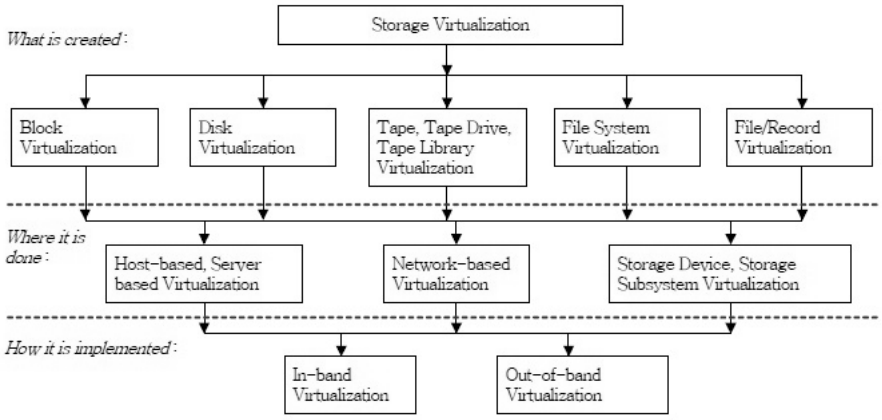

Fig.1. SNIA Storage Virtualization Taxonomy[11]

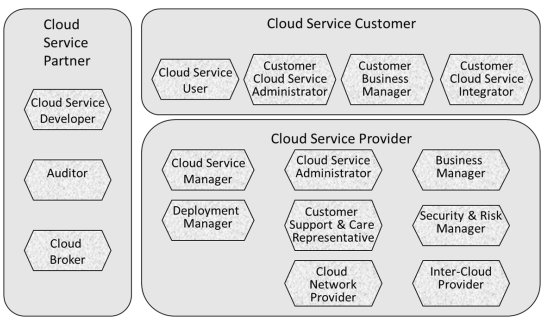

Fig.2. User Roles and Sub-Roles of CCRA

III. 클라우드 서비스 시스템 관점 제시

3.1 사용자 관점에서 본 클라우드 서비스 시스템

CCRA(Cloud Computing Reference Architecture)에서는 클라우드 시스템을 사용자 역할 입장에서 기술하였다. 클라우드 컴퓨팅 참조 구조는 ISO/IEC 17789의 초안 문서에서 제안되었으며, 이 초안은 ISO/IEC 17788(정보 기술-분산 응용 플랫폼 및 서비스-클라우드 컴퓨팅-개요 및 어휘)표준 문서와 ISO/IEC 10746-1:1998(정보 기술-개방형 분산 처리-참조모델: 개요)표준 문서를 참조하여 기술하였다. CCRA는 클라우드 컴퓨팅의 일반적인 개념과 구성요소 및 역할, 기능, 구성요소 간의 상호관계를 포함하는 문서이며, 클라우드 컴퓨팅 국제 표준을 지향하기 위해서 반드시 참조해야 하는 내용을 기술하였다. 이에 대하여 본 논문에서는 Fig.2.와 같이 CCRA 8장에 기술되어 있는 User View의 내용을 인용하여 클라우드 컴퓨팅 환경에서의 역할을 정의한다[2][12].

3.1.1 클라우드 서비스 고객(Cloud Service Customer)

클라우드 서비스 고객은 클라우드 서비스 제공자와 서비스 사용 목적을 위해 비즈니스 관계를 가진다. 클라우드 서비스 고객의 세부 역할은 클라우드 서비스 사용자, 고객 클라우드 서비스 관리자, 고객 비즈니스 매니저, 고객 클라우드 서비스 통합자 등으로 분류할 수 있다[13]. 클라우드 서비스 사용자는 어떤 작업을 수행하기 위해서 하나 이상의 클라우드 서비스를 사용하는 역할이다. 고객 클라우드 서비스 관리자는 고객의 클라우드 서비스 사용의 원활한 운영을 책임지고, 서비스 시도 및 테스트, 데이터 가용성 모니터링, 테넌시(tenancy) 관리 등의 활동을 통해 고객의 기존 ICT(Information & Communication Technology) 시스템과 응용 프로그램이 클라우드 환경에서 문제없이 실행되는 것을 보장한다. 고객 비즈니스 매니저는 고객이 비용 효율적인 방법으로 클라우드 서비스를 사용 하도록 비즈니스 목표를 달성하는 역할이다. 고객 클라우드 서비스 통합자는 응용 기능과 데이터를 포함한 고객의 ICT 시스템 기반의 기존 비클라우드 서비스와 함께 클라우드 서비스를 통합하는 역할이다.

3.1.2 클라우드 서비스 제공자(Cloud Service Provider)

클라우드 서비스 제공자는 클라우드 서비스 고객이 이용할 수 있도록 클라우드 서비스를 만드는 역할이다[14]. 클라우드 서비스 제공자의 세부 역할로는 클라

우드 서비스 관리자, 배포 매니저, 서비스 매니저, 비즈니스 매니저, 고객 보호 지원, 클라우드 간 연결 제공자, 보안 및 위험 매니저, 클라우드 네트워크 제공자 등으로 분류할 수 있다. 클라우드 서비스 관리자는 새로운 클라우드 서비스 구축을 위해 클라우드 서비스 제공자의 환경 시스템을 준비하는 역할이다. 배포 매니저는 환경과 프로세스를 정의하고, 매트릭스 과정을 정의하여 서비스 생산에서 서비스의 배포에 대한 책임과 권한을 갖는 역할이다. 서비스 매니저는 클라우드 서비스 고객이 서비스를 안전하게 사용함으로써 제공자의 서비스를 지속적으로 이용하도록 보장하는 역할이다. 비즈니스 매니저는 사업 계획 관리, 마케팅, 고객 관리, 금융 관리 등을 통하여 클라우드 서비스 고객에게 사업적인 측면으로 클라우드 서비스를 제공하는 역할이다. 고객 보호 지원 담당자는 고객의 만족을 유지하는 것을 목표로 고객 문제에 대해 신속하고 비용 효율적인 방법으로 대처하는 역할이다. 클라우드 간 연결 제공자는 클라우드 서비스 고객에게 서비스를 제공하기 위해서 하나 이상의 다른 클라우드 서비스 제공자를 필요로 하는 역할이다. 보안 및 위험 매니저는 클라우드 서비스 제공자가 서비스의 개발, 제공, 사용, 지원과 관련된 위험들을 적절하게 관리하는 역할이다. 클라우드 네트워크 제공자는 클라우드 서비스 고객, 클라우드 서비스 제공자 그리고 클라우드 서비스 파트너를 위해 네트워크 연결 및 네트워크 서비스를 제공하는 역할이다.

3.1.3 클라우드 서비스 파트너(Cloud Service Partner)

클라우드 서비스 파트너는 클라우드 서비스와 관련하여 서비스 고객이나 클라우드 서비스 제공자 중 하나에서 클라우드 활동의 지원에 관여한다. 클라우드 서비스 파트너의 세부 역할은 서비스 개발자, 클라우드 감시자, 클라우드 중개인 등으로 분류할 수 있다. 서비스 개발자는 서비스의 설계, 개발, 테스트 및 클라우드 서비스의 구현 유지에 대한 책임이 있는 역할이다. 클라우드 감시자는 클라우드 서비스의 제공과 사용에 대한 감사를 실시하고 결과를 보고하는 역할이다. 클라우드 중개인은 특정 목적을 위해 클라우드 서비스 제공자를 평가하고, 선택하는 클라우드 서비스 고객의 비즈니스와 관계된 서비스를 제공하는 역할이다.

3.2 클라우드 시스템 계층 구조

일반적인 클라우드 시스템 계층 구조는 Fig.3.과

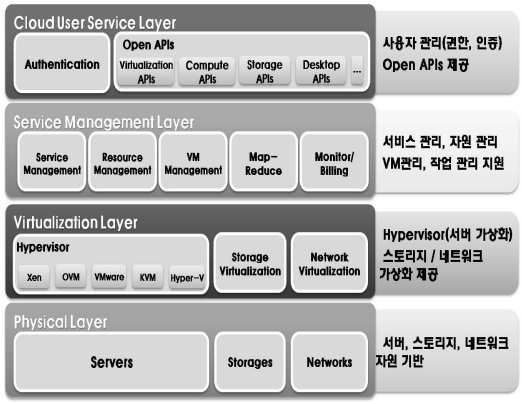

Fig.3. Architecture and Roles of Cloud System Layer

같이 나타낼 수 있다. 물리적 계층(physical layer)에는 서버(server), 스토리지(storage), 네트워크(network) 자원 기반이 있고, 가상화 계층(virtualization layer)에는 물리적 자원을 가상화 자원으로 통합 및 추상화하는 계층으로써 서버 가상화(hypervisor), 스토리지 가상화, 네트워크 가상화를 제공하고, 서비스 관리 계층(service management layer)에는 서비스 관리, 자원 관리, 가상 머신(VM, virtual machine)관리, 맵-리듀스(map-reduce) 관리, 모니터링 관리, 과금 관리 등을 제공하며, 클라우드 이용자 서비스 계층(cloud user service layer)에는 권한 및 인증에 관련된 사용자 관리, API(Open Application Programming Interface)를 제공하는 4계층 구조로 분류한다. 그에 따른 역할은 Fig.3. 의 세부 내역에 나타나 있다[15][16][17].

3.3 컴퓨터 시스템에서의 보안 요구사항

컴퓨터 시스템에서 고려해야 하는 보안 요구사항 6가지는 ITU-T X.ccsec에 발표한 자료[18]에 잘 나타 있으며, 이 요구사항은 컴퓨터 보안 시스템에 범용적으로 사용된다.

3.3.1 기밀성 및 데이터 암호화

정보를 오직 인가된 사람들에게만 공개하는 것을 말하며, 전송되는 데이터의 내용을 완벽하게 보호하여 사고가 발생하더라도 비인가자가 정보의 내용에 접근하는 것을 방지하도록 하는 보안 요구사항이 고려되어야 한다[19][20].

3.3.2 사용자 인증과 접근제어

주체는 객체 또는 객체 내의 데이터에 대한 접근을 요구하는 활동 개체이며, 객체는 정보를 가진 수동적 개체를 말한다. 접근 통제란 이러한 주체와 객체 사이의 정보의 흐름을 조절하는 것을 의미하며, 이에 대한 보안 요구사항이 고려되어야 한다[21][22].

3.3.3 데이터 무결성

정보가 훼손되지 않음을 의미한다. 이를 위하여, 훼손 여부를 검증하거나, 훼손 여부를 검증할 수 있는 정보를 제공하고, 관리하는 총체적인 기능을 의미한다[23].

3.3.4 가용성 및 복구

사용자의 요구 기능을 요구 시간동안 올바르게 수행할 수 있는 능력을 말하며, 서비스 제공 관점에서는 서비스가 중단되지 않고 성능을 유지하는 능력을 말하고, 망 운용자 관점에서는 언제든지 망에 대한 접근 및 접속을 가능하게 하는 능력을 말한다. 이에 대한 보안 요구사항이 고려되어야 한다[24].

3.3.5 가상화 보안

가상화는 컴퓨터 리소스의 물적인 특징을 추상화하며, 사용자에게 논리적 자원을 제공하고, 이를 통하여 다양한 기술적 또는 관리적 이점들을 제공하는 기술을 말한다. 또한 가상화는 사용자와 물리 리소스간의 가상화 계층 구현을 통하여, 컴퓨팅 리소스에 대한 접근 및 인프라 구조 관리를 간소화하는 것을 목적으로 이에 대한 보안이 고려되어야 한다[25].

3.3.6 네트워크 보안

네트워크는 공간적으로 분리되어, 다른 위치에 있는 컴퓨터와 상호 간에 정보 교환과 처리를 위한 데이터 통신망, 통신망 운영 체계, 통신망 데이터베이스 등을 의미하며 네트워크 보안은 네트워크를 통한 데이터간의 통신이 발생할 때, 기밀성과 무결성을 보장할 수 있는 보안을 의미한다[26].

IV. 보안 요구사항 제안

저장장치 가상화에 대한 보안은, 여러 사용자들이 물리적인 공간을 공용으로 사용하기 때문에, 저장 장치를 사용하는 사용자들에 대한 인증과, 다른 사용자들의 불법적인 데이터 접근에 대한 방어 그리고, 데이터 손실에 대한 방비와 데이터 복구 등이 포함된다[27][28][29][30].

4.1 클라우드 저장장치 가상화의 보안 요구사항 제안

4.1.1 기밀성 및 데이터 암호화

가상화된 저장장치는 일반적으로 다수 사용자들이 공용 환경에서 이용하기 때문에 인가되지 않은 개인, 단체, 프로세스 등으로부터 내용이 누출되는 것을 방지해야 한다. 따라서 민감한 데이터에 대한 기밀성 보장은 매우 중요하여 이러한 데이터의 유출을 막기 위한 안전한 암호 알고리즘, 기밀성을 보장하기 위한 암호화 알고리즘과 클라우드 특성상 대용량 데이터에 대한 암/복호화 시간에 대한 가용성, 그리고 시스템의 단계 및 환경을 고려한 암호화 방식 등이 고려되어야 한다.

4.1.2 사용자 인증과 접근 제어

다수의 사용자 데이터가 공존하는 저장장치에 접근하는 사용자에 대한 인증과 권한 관리를 위한 접근 제어 기법이 필요하다. 따라서 사용자와 적절한 권한을 가진 사용자의 접속을 보장하고 부적절한 행위를 모니터하기 위한 메커니즘, 계정을 관리하는 방법과 정보의 흐름을 통제하는 방법, 그리고 특정 정보에 접근할 수 있는 권한 설정 등이 고려되어야 한다.

4.1.3 데이터 무결성

클라우드 환경에서 서비스 사용자의 정보의 저장과 전달 시, 클라우드 서비스는 인가되지 않은 방식에 의한 정보 접근 및 변경이 이뤄지지 않도록 정확성과 안정성을 확보해야 한다. 따라서 무결성을 보장하기 위한 암호화 알고리즘 및 인증 방법 적용 시의 서비스의 가용성, 시스템 단계 및 환경을 고려한 암호기법 및 인증 기법, 그리고 바이러스 백신 및 프로그램 패치 정책 등이 고려되어야 한다.

Table 1. Relation between User Roles and Cloud Storage Virtualization Security Requirements

보안 요구사항	상세 요구사항	이용자	제공자	파트너
기밀성 및 데이터 암호화	데이터 암호화		○	○
	인증된 암호기술		○	
	키 관리		○	
	주기적인 키 변경	○		○
	알고리즘 및 키 길이		○	○
	다른 환경에 다른 키 사용		○	
사용자 인증과 접근 제어	계정관리		○	
	접근권한 배정		○	
	최소 권한 부여		○	
	휴대용 모바일 장치	○		
데이터 무결성	악성 코드 및 스팸 차단 기능	○		
	시스템 및 데이터 접근 제한	○		
	데이터 무결성 기술 제공		○	
	오류 처리		○	
가용성 및 복구	사고 모니터링		○	○
	데이터 백업		○	○
	데이터 복구		○	○

4.1.4 가용성 및 복구

클라우드 서비스는 인가된 사용자가 정보나 서비스를 요구할 때, 언제든지 즉시 사용 가능하도록 제공해야 하며, 사고로 인한 서비스 중단이나 데이터 손실을 막기 위해 사고 발생 시 서비스의 지속성을 확보해야 한다. 따라서 클라우드 컴퓨팅의 가용성을 보장할 수 있는 정책, 가용성 정책에 맞게 만들어진 계획 테스트와 검증, 사고 발생 시를 대비 할 수 있는 사고대응 정책, 그리고 사고에 대비한 백업시스템과 사고 발생 시 복구 절차 등이 고려되어야 한다.

4.2 역할별, 계층별 클라우드 저장장치 가상화 보안 요구사항의 연관성

클라우드 저장장치 가상화 시스템 이용에 관련하여 다양한 이해관계자가 존재하며, 이해관계자 별로 상이한 보안요구사항이 존재함으로서 클라우드 저장장치 환경에서 핵심적인 가상화 기술의 표준화 및 상호 호환성 확보의 어려움과 같은 문제가 지속적으로 발생하고 있다. 또한 클라우드 시스템 계층마다 특정한 보안 요구사항이 고려되어야 하며, 이에 대응해 각 계층에서 이해관계자의 역할과 보안 요구사항을 종합하고 클라우드 저장장치 가상화 시스템 환경에서의 계층 및 역할별 보안 요구사항을 도출하여 정의한다[31][32]. 이에 대하여 본 논문에서 제안하는 분석 방법은 다음과 같이 구성된다.

4.2.1 사용자 역할과 클라우드 저장장치 가상화 보안 요구사항의 연관성

본 장에서는 3.1에서 정의된 클라우드 서비스 시스템에서의 사용자 관점과 4.1에서 제시한 클라우드 저장장치 가상화의 보안 요구사항을 연계하여 사용자 관점별 세부적 보안 요구사항을 도출한다.

Table 1.에서 보듯이, 클라우드 저장장치 가상화의 보안 요구사항 측면에서 이용자 관점으로 고려해야 하는 세부적인 보안 요구사항은 기밀성 및 데이터 암호화에는 주기적인 키의 변경이 있고, 사용자 인증과 접근제어에는 휴대용 모바일 장치 사용, 그리고 데이터 무결성에는 악성코드 및 스팸 차단 기능, 시스템 및 데이터 접근 제한이 있다.

클라우드 저장장치 가상화의 보안 요구사항 측면에서 제공자 관점으로 고려해야 하는 세부적인 보안 요구사항은 기밀성 및 데이터 암호화에는 데이터 암호화, 인증된 암호기술, 키 관리 등이 있고, 사용자 인증과 접근 제어에는 계정관리, 접근권한 배정, 최소 권한 부여가 있고, 데이터 무결성에는 데이터 무결성 기술 제공, 오류 처리, 그리고 가용성 및 복구에는 사고 모니터링, 데이터 백업, 데이터 복구가 있다.

클라우드 저장장치 가상화의 보안 요구사항 측면에서 파트너 관점으로 고려해야 하는 세부적인 보안 요구사항은 기밀성 및 데이터 암호화에는 데이터 암호화, 주기적인 키 변경, 알고리즘 및 키 길이가 있고, 가용성 및 복구에는 사고 모니터링, 데이터 백업, 데

Table 2. Relation between Cloud System Layer Architecture and Cloud Storage Virtualization Security Requirements

보안 요구사항	상세 요구사항	서비스 계층	관리 계층	가상화 계층
기밀성 및 데이터 암호화	데이터 암호화	○	○	
	인증된 암호기술	○	○	
	키 관리	○	○	
	주기적인 키 변경	○	○	
	알고리즘 및 키 길이	○	○	
	다른 환경에 다른 키 사용	○	○	
사용자 인증과 접근 제어	계정관리	○	○	
	접근권한 배정	○	○	
	최소 권한 부여	○	○	
	휴대용 모바일 장치	○	○	
데이터 무결성	악성 코드 및 스팸 차단 기능	○	○	
	시스템 및 데이터 접근 제한	○	○	
	데이터 무결성 기술 제공	○	○	
	오류 처리	○	○	
가용성 및 복구	사고 모니터링	○	○	
	데이터 백업	○	○	
	데이터 복구	○	○	

이터 복구가 있다.

4.2.2 클라우드 시스템 계층 구조와 저장장치 가상화 보안 요구사항의 연관성

본 장에서는 3.2에서 정의된 클라우드 시스템 계층 구조에서 제시한 시스템 계층과 4.1에서 제시한 클라우드 저장장치 가상화의 보안 요구사항에서 제시한 보안 요구사항을 연계하여 Table 2.와 같은 계층별 역할과 보안 요구사항의 연관성이 도출된다.

서비스 계층은 기밀성 및 데이터 암호화, 사용자 인증 및 접근제어, 데이터 무결성, 가용성 및 복구 등 4개 영역의 모든 세부적인 보안 요구사항이 고려되어야 한다. 또한, 관리 계층도 기밀성 및 데이터 암호화, 사용자 인증 및 접근제어, 데이터 무결성, 가용성 및 복구 등 4개 영역의 모든 세부적인 보안 요구사항이 고려되어야 한다.

4.2.3 역할별, 계층별 클라우드 저장장치 가상화 보안 요구사항 도출

본 장에서는 4.2.1 사용자 역할과 클라우드 저장장치 가상화 보안 요구사항의 연관성에서 도출된 결과와 4.2.2 클라우드 시스템 계층 구조와 저장장치 가상화 보안 요구사항의 연관성에서 도출된 결과를 종합하여 Table 3.과 같은 결과를 제안한다.

계층별, 역할별 보안 요구사항의 도출 결과는 7가지의 경우로 분류할 수 있다. 서비스 계층에 보안과 관련된 역할에는 5개 영역이 있으며, (1) 이러한 서비스 계층에서 보안과 관련된 클라우드 서비스 이용자의 역할인 고객 클라우드 서비스 관리자가 고려해야하는 중요한 보안 요구사항으로 악성 코드 및 스팸 차단 기능, 시스템 및 데이터 접근 제한, 사고 모니터링 등을 들 수 있다. (2) 서비스 계층에서 보안과 관련된 클라우드 서비스 파트너의 역할인 클라우드 감시자가 고려해야 하는 중요한 보안 요구사항으로 악성 코드 및 스팸 차단 기능, 시스템 및 데이터 접근 제한, 데이터 무결성 기술 제공, 사고 모니터링 등을 들 수 있다. (3) 서비스 계층에서 보안과 관련된 클라우드 서비스 제공자의 역할인 클라우드 서비스 관리자가 고려해야 하는 중요한 보안 요구사항으로 악성 코드 및 스팸 차단 기능, 시스템 및 데이터 접근 제한, 데이터 무결성 기술 제공, 사고 모니터링 등을 들 수 있다. (4) 서비스 계층에서 보안과 관련된 클라우드 서비스 제공자의 역할인 클라우드 서비스 매니저가 고려해야 하는 중요한 보안 요구사항으로 사고 모니터링, 데이터 백업, 데이터 복구들 수 있다. (5) 서비스 계층에서 보안과 관련된 클라우드 서비스 제공자의 역할인 보안 및 위험 매니저가 고려해야 하는 중요한 보안 요구사항으로 기밀성 및 데이터 암호화, 사용자 인증 및 접근제어, 데이터 무결성, 가용성 및 복구의 모든 세부적인 보안 요구사항을 들 수 있다. (6) 관리 계층에 보안과 관련된 역할에는 1개 영역이 있으며, 이러한 관리영역에서 보

Table 3. Relation among User Roles, Cloud System Layer Architecture and Cloud Storage Virtualization Security Requirements

보안 요구사항	상세 요구사항	서비스 계층					관리 계층	가상화 계층
		고객 클라우드 서비스 관리자	클라우드 감시자	클라우드 서비스 관리자	클라우드 서비스 매니저	보안 및 위험 매니저	보안 및 위험 매니저	보안 및 위험 매니저
기밀성 및 데이터 암호화	데이터 암호화					○	○	
	인증된 암호기술					○	○	
	키 관리					○	○	
	주기적인 키 변경					○	○	
	알고리즘 및 키 길이					○	○	
	다른 환경에 다른 키 사용					○	○	
사용자 인증과 접근 제어	계정관리					○	○	
	접근권한 배정					○	○	
	최소 권한 부여					○	○	
	휴대용 모바일 장치					○	○	
데이터 무결성	악성 코드 및 스팸 차단 기능	○	○	○		○	○	
	시스템 및 데이터 접근 제한	○	○	○		○	○	
	데이터 무결성 기술 제공		○	○		○	○	
	오류 처리		○	○		○	○	
가용성 및 복구	사고 모니터링	○	○	○	○	○	○	
	데이터 백업	○	○		○	○	○	
	데이터 복구	○	○		○	○	○	

안과 관련된 클라우드 서비스 제공자의 역할인 보안 및 위험 매니저가 고려해야 하는 중요한 보안 요구사항으로 기밀성 및 데이터 암호화, 사용자 인증 및 접근제어, 데이터 무결성, 가용성 및 복구의 모든 세부적인 보안 요구사항을 들 수 있다. (7) 가상화 계층에 보안과 관련된 역할에는 1개 영역이 있으며, 이러한 가상화 계층에서 보안과 관련된 클라우드 서비스 제공자의 역할에는 보안 및 위험 매니저가 있다. 이 영역에서는 저장장치 가상화 보안 요구사항이 도출되지 않는다.

V. 결론 및 향후 계획

클라우드 저장장치 가상화 환경에서는 기존의 전통적인 네트워크 시스템 환경과는 다른 형태의 새로운 보안 취약점이 발생하기 때문에 기존의 보안 요구사항과는 다른 특징을 가지는 보안 요구사항의 연구가 필요하다. 따라서 본 논문에서는 보안 위협의 대상이 되는 클라우드 저장장치 가상화 환경을 가상화 기술 구현 형태별로 구분하여 상세하게 분석하고, 클라우드 저장장치 가상화 환경의 보안 요구사항을 도출하기 위해서 사용자 관점에서 본 클라우드 서비스 시스템과 클라우드 컴퓨팅 계층 구조를 각각 서술하고 기존에 연구된 클라우드 서비스 시스템 보안 요구사항을 활용하여 클라우드 저장장치 가상화 환경에서의 보안 요구사항을 도출 및 제안하였다. 이러한 연구 결과는 클라우드 저장장치 가상화 환경에 대해 공통적인 보안 요구사항을 식별함으로써 이기종의 클라우드 저장장치 가상화 보안 솔루션 간 참조해야 할 보안 요구사항에 대한 분석 자료로 활용되는 것에 본 연구의 의미가 있으며, 클라우드 서비스 사용자별 보안 요구사항을 조사하여 클라우드 저장장치 가상화 보안 기술 표준을 수립함에 있어 보안성과 편의성을 향상시킬 것으로 기대한다. 향후 본 논문에서 제안한 계층별 및 역할별 클라우드 저장장치 가상화 보안 요구사항을 활용하여 클라우드 가상화 환경에서 보안 기술에 대한 표준화를 진행하고, 이를 통하여 특정 가상화 시스템이나 서비스 플랫폼에 구현 독립적인 클라우드 저장장치 가상화 보안 솔루션에 대한 개발을 목표로 연구를 진행할 계획이다.

References

[1] Sung-jae Jung and Yu-mi Bae, "Trend analysis of Threats and Technologies for Cloud Security," Journal of Security Engineering, 10(2), pp. 119-212, Apr. 2013.

[2] L. Lindsay and O.L. Grand, "Cloud computing — Reference architecture," CT-CCA-o-022, Sep. 2013.

[3] Storage virtualization, http://en.wikipedia.org/wiki/Storage_virtualization

[4] P. Massiglia and F. Bunn, Virtual Storage Redefined: Technologies and Applications for storage Virtualization, VERITAS Software Corporation, pp. 1-5, Jan. 2003.

[5] Dong-wook Choi, Du-ho Kim, Jeong-ho Kang, Sung-woo Cho and Jong-min Park, Actual Cloud Virtualization Construction Technology, HanbitMedia, pp. 35-37, Sep. 2012.

[6] Yeong-cheol Kim, Myeong-hun Cha, Sang-min Lee and Yeong-gyun Kim, "Trends of Storage Virtualization Technologies on Cloud Computing," Electronics and Telecommunications Trends, 24(4), pp. 69-78, Aug. 2009.

[7] Ndrive, http://ndrive.naver.com/index.nhn

[8] S. Ghemawat, H. Gobioff and S. Leung, "The Google file system," In proc. of ACM Symp. on Operating sysytems principles, Aug. 2003.

[9] Hadoop, http://hadoop.apache.org/

[10] Young-su Min, Hong-yeon Kim and Young-gyun Kim, "Distributed File System Technology for Cloud Computing," Communications of KIISE, 27(5), pp. 86-94, May. 2009.

[11] F. Bunn, N. Simpson, R. Peglar and G. Nagle, "Storage Virtualization," The SNIA Technical Tutorial, Oct. 2003.

[12] E. Hibbard and M. Jeffrey, "Cloud Computing Overview & Vocabulary," CT-CCV-o-037, Oct. 2013.

[13] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger and D. Leaf, "Cloud Computing Reference Architecture," NIST SP 500-292, Sep. 2011.

[14] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," UCB/EECS-2009-28, UC Berkeley Reliable Adaptive Distributed Systems Laboratory, Feb. 2009.

[15] D. Chisnall, The Definitive Guide to the Xen Hypervisor, Prentice Hall, pp. 3-26, Nov. 2007.

[16] B. Sosinsky, Cloud Computing Bible, Wiley, pp. 45-64, Jan. 2011.

[17] Soon-ki Jeong, Man-hyun Chung, Jae-ik Cho, Tae-shik Shon and Jong-sub Moon, "A Research on Cloud Architecture and Funtion for Virtualization Security of Cloud Computing," Journal of Security Engineering, 8(5), pp. 627-643, Nov 2012.

[18] Z. Lin, H. Tian, "X.ccsec: Security framework for cloud computing," TD 0251 Rev.2, Apr. 2013.

[19] Data Confidentiality, http://msdn.microsoft.com/en-us/library/ff650720.as-px

[20] Data Encryption, http://msdn.micros-oft.com/en-us/library/dn149025(v=bts.80).aspx

[21] Data Origin Authentication, http://m-sdn.microsoft.com/en-us/library/ff648434.aspx

[22] Access Control, http://msdn.microsoft.com/en-us/library/windows/desktop/aa374860(v=vs.85).aspx

[23] Data Integrity, http://msdn.microsoft.com/en-us/library/aa291812(v=vs.71).aspx

[24] Availability, http://msdn.microsoft.com/en-us/library/aa292462(v=vs.71).aspx

〔25〕 In-hyuk Kim, Tae-hyoung Kim, Jung-han Kim, Byoung-hong Lim and Young-ik Eom, "Trends of Virtualization Technology Application for System Security," Review of KIISC, 19(2), pp. 26-34, Apr. 2009.
〔26〕 Network security, http://en.wikipedia.org/wiki/Network_security
〔27〕 T. Haeberlen and L. Dupre, "Cloud Computing Benefits, risks and recommendations for information security," Enisa, Dec. 2012.
〔28〕 W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST SP 800-144, Dec. 2011.
〔29〕 J.D Meier and P. Enfield, "Azure Security Notes Lessons Learned from Exploring Microsoft Azure and the Cloud Security Space," Microsoft, Nov. 2010.
〔30〕 A. Reed, C. Rezek and P. Simmonds, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0," CSA, Nov. 2011.
〔31〕 Chan-woo Lee, Sang-kon Kim, Youngmin Yeo and Jong-sub Moon, "Proposal of Security Requirements based on Layers and Roles for the Standardization of Cloud Computing Security Technology," Journal of Security Engineering, 10(4), pp. 473-488, Aug. 2013.
〔32〕 D. Merrill, "Security Controls Baseline v1.0," FedRAMP, Nov. 2010.

〈저자소개〉

여 영 민 (Youngmin Yeo) 학생회원
2013년 2월: 고려대학교 전자 및 정보공학과 학사 졸업
2013년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 클라우드 보안, 시스템 보안, 네트워크 보안

이 찬 우 (Chanwoo Lee) 학생회원
2008년 2월: 단국대학교 경제학과 졸업
2013년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보호, 클라우드 보안, 웹 보안, 네트워크 보안

문 종 섭 (Jongsub Moon) 종신회원
1981년 1월: 서울대학교 계산통계학과 졸업
1983년 1월: 서울대학교 대학원 계산통계학과 석사
1991년 5월: Illinois Institute of Technology 전산학 박사
2002년 3월~현재: 고려대학교 전자 및 정보공학과 교수
〈관심분야〉 정보보호, 인공지능, 패턴인식, 의공학, 클라우드 보안