클라우드 스토리지 보안을 위한 보안 아키텍처 설계 연구

배원일*, 이은지*, 곽진**
*아주대학교 컴퓨터공학과 정보보호응용및보증연구실
**아주대학교 사이버보안학과
e-mail:wibae.isaa@gmail.com*, ejlee.isaa@gmail.com*, security@ajou.ac.kr**

A Study on Security Architecture Design for Cloud Storage Security

Won-il Bae*, Eun-Ji Lee*, Jin Kwak**
*ISAA Lab., Department of Computer Engineering, Ajou University
**Department of Cyber Security, Ajou University

요 약

최근, 기업 및 사용자들은 클라우드 서비스의 필요성에 대한 인식이 확산되고 있다. 반면에 클라우드 보안 기술에 대한 관심의 부재는 클라우드 서비스를 도입하는데 어려움으로 작용하고 있다. 클라우드 컴퓨팅 환경에서는 기존의 컴퓨터 네트워크 환경과 다르게 서버 가상화, 네트워크 가상화, 스토리지 가상화와 같은 부분들이 가상화되어 서비스 및 자원을 공유하여 활용한다. 따라서 가상화 기반 취약점이 발생할 수 있으며 기존 보안장비의 한계점으로 인한 새로운 보안위협이 발생하고 있다. 특히, 방대한 양의 데이터를 클라우드 컴퓨팅 중 하나인 클라우드 스토리지를 통해 저장을 하게 되고 이러한 데이터를 겨냥한 공격이 이루어질 경우, 데이터 손실 및 유출 등 심각한 위험이 발생할 수 있다. 본 논문에서는 클라우드 스토리지 환경에서 문제점들에 대한 대응을 위해 ISO/IEC에서 제시한 스토리지 보안위협과 ITU-T, ENISA, CSA에서 제시한 클라우드 컴퓨팅 보안위협을 이용하여 클라우드 스토리지 관련 보안위협 유형 분석을 수행하고 이에 대응하는 보안 아키텍처를 설계하며 이에 대한 안전성 분석을 수행한다.

1. 서론

클라우드 스토리지는 서버와 스토리지들을 SAN(Storage Area Network)과 같은 전용 네트워크로 연결함으로써 다수의 서버와 스토리지를 공유할 수 있다. 또한 가상화를 가능하게 하는 소프트웨어 및 하드웨어 장비를 통해 물리 장치를 하나의 논리 장치로 통합할 수 있어, 자원에 대한 활용률 증가, 손쉬운 확장 및 가용성을 제공할 수 있다[1].

이러한 장점으로 인해, 클라우드 서비스 사용의 급격한 증가와 IoT, 스마트폰 보급으로 인해 방대한 데이터가 클라우드 스토리지에 저장되고 있다. 이에 따른 클라우드 스토리지에 대한 수요 증가로 인해 이를 활용한 구축 사례들이 늘어나고 있다[2].

스토리지 내에는 사용자에 대한 기밀 및 중요 정보가 저장될 수 있기 때문에 악의적인 공격자로 인한 데이터의 손실 및 유출 등 다양한 보안위협에 노출되어 있다[3].

하지만 클라우드 스토리지 보안 기술에 대한 연구가 미흡한 실정이며, 따라서 클라우드 스토리지 관련 보안위협에 대응하는 보안 기술을 확보하기 위해 클라우드 스토리지 보안 아키텍처가 필요하다.

본 논문의 구성은 다음과 같다. 2장에서는 스토리지 및 클라우드 컴퓨팅 보안위협과 클라우드 스토리지 보안요구사항에 대해 분석하고, 3장에서는 분석된 보안위협을 바탕으로, 클라우드 스토리지 관련 보안위협을 유형별로 분석한다. 이후, 이에 대응하는 보안 아키텍처를 제안하며 보안 아키텍처에 대한 안전성 분석을 수행하고, 4장에서 결론을 맺는다.

2. 관련연구

2.1 스토리지 보안위협

ISO/IEC(International Organization for Standardization /International Electrotechnical Commission) 27040문서의 「Information technology-Security techniques-Storage security」는 스토리지 보안에 대한 가이드라인을 제시하고 있으며 ISO/IEC 27040에서 제시하는 보안위협은 <표 1>과 같다[4].

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.R0126-16-1111, 클라우드 보안을 위한 위험기반 인증·접근제어 프레임워크 및 보안상태 점검기술 개발).

<표 1> ISO/IEC에서 제시한 스토리지 보안위협

No	스토리지 보안위협
1	데이터 유출
2	데이터 손실
3	임시 또는 영구적인 가용성 손실
4	법적 요구사항 불충족

2.2 클라우드 컴퓨팅 보안위협

클라우드 컴퓨팅 보안위협은 ITU-T X.1601의 「Security framework for cloud computing」, ENISA의 「Threat Landscape 2015」 및 CSA의 「Cloud Computing Top Threats in 2016」 문서에서 제시되어 있으며 <표 2>, <표 3>, <표 4>와 같다[5,6,7].

<표 2> ITU-T X.1601의 Security framework for cloud computing

No	클라우드 컴퓨팅 보안위협
1	데이터 손실과 유출
2	불안전한 서비스 접근
3	내부자 위협
4	비인가된 관리자 접근
5	책임의 모호성
6	신뢰의 손실
7	거버넌스 손실
8	프라이버시 손실
9	서비스 비가용성
10	클라우드 서비스 제공자 종속
11	지적재산권 남용
12	소프트웨어 무결성 손실
13	공유된 환경
14	보호 매커니즘의 충돌 및 불일치
15	관할 충돌
16	점진적 위험
17	부적절한 마이그레이션 및 통합
18	비즈니스 불연속성
19	클라우드 서비스 파트너 종속
20	공급 체인의 취약점
21	소프트웨어 종속성

<표 3> ENISA의 Threat Landscape 2015

No	클라우드 컴퓨팅 보안위협
1	악성코드
2	웹 기반 공격
3	웹 애플리케이션 공격
4	봇넷
5	서비스 비가용성
6	내부자 위협
7	데이터 유출
8	사이버 스파이
9	계정 도용
10	정보 유출

<표 4> CSA의 Cloud Computing Top Threats in 2016

No	클라우드 컴퓨팅 보안위협
1	데이터 유출
2	부적절한 신원
3	안전하지 않은 인터페이스 및 API
4	시스템 취약점
5	계정 도용
6	악의적인 내부자
7	지능형 지속 위협(APT)
8	데이터 손실
9	클라우드 서비스의 이해 부족
10	클라우드 서비스 남용
11	서비스 비가용성
12	공유기술의 취약점

2.3 클라우드 스토리지 보안요구사항

클라우드 스토리지에 대한 보안요구사항은 한국정보통신기술협회(TTA)에서 「저장장치 가상화 시스템 보안요구사항」 표준 문서에 정의되어 있으며 클라우드 스토리지를 제공하는 솔루션들과 보안 관리를 제공하는 솔루션들 간의 상호 호환성을 보장할 수 있도록 클라우드 스토리지 보안 관점에서의 기술적인 보안요구사항을 정의하고 있다[8].

• R1. 기밀성 및 데이터 암호화

클라우드 스토리지는 다수의 사용자들이 공용된 환경에서 이용하기 때문에 인가되지 않은 개인 및 단체로부터 내용이 유출되는 것을 방지해야 한다.

• R2. 사용자 인증과 접근제어

다수의 사용자가 가상화된 스토리지를 사용하는 환경에서 사용자에 대한 정확한 인증과 권한 관리를 위한 인증 및 접근제어 기술이 필요하다.

• R3. 데이터 무결성

클라우드 스토리지 환경에서 개인과 단체에 대한 중요한 데이터의 저장 및 전달 시 악의적인 공격자에 의한 데이터 접근 및 변경이 이루어지지 않게 안전성 및 보안성을 확보해야 한다.

• R4. 가용성 및 복구

가상화된 스토리지내의 보안사고 및 오류로 인한 데이터 손실을 최소화하기 위하여 사고 및 오류 발생 시, 스토리지 서비스의 지속성을 확보해야 한다.

3. 제안하는 보안 아키텍처

3.1 클라우드 스토리지 보안위협 유형 분석

본 절에서는 ISO/IEC 27040문서의 스토리지 보안위협과 ITU-T X.1601, ENISA, CSA에서 제시한 클라우드 보

<표 5> 클라우드 스토리지 보안위협 유형 분석

보안위협 유형	해당 기관	클라우드 스토리지 관련 보안위협
T1	ITU-T	데이터 손실과 유출, 신뢰의 손실, 프라이버시 손실
	ENISA	악성코드, 데이터 유출
	CSA	데이터 유출, 데이터 손실
T2	ITU-T	비인가된 관리자 접근, 불안전한 서비스 접근, 점진적 위험
	ENISA	악성코드, 계정 도용
	CSA	부적절한 신원, 계정 도용
T3	ITU-T	서비스 비가용성, 공유된 환경, 점진적 위험
	ENISA	서비스 비가용성
	CSA	서비스 비가용성
T4	ITU-T	서비스 비가용성, 점진적 위험, 비즈니스 불연속성
	ENISA	악성코드, 서비스 비가용성
	CSA	부적절한 신원, 서비스 비가용성

안위협 중에서 클라우드 스토리지 관련 보안위협을 분석하며 <표 5>와 같다.

• T1. 데이터 손실 및 유출

방대한 데이터를 저장 및 관리하는 클라우드 스토리지 환경에서 암호화, 정보 관리 등에 문제가 발생할 경우 데이터 손실 및 유출의 보안위협이 발생할 수 있다.

• T2. 비인가된 접근

분산된 클라우드 스토리지 자원에 대하여 비인가된 관리자 또는 사용자 접근에 의해 데이터, 계정 등의 정보를 임의로 추가 및 삭제할 수 있는 보안위협이 발생할 수 있다.

• T3. 공유된 환경

다수의 이용자들이 가상화 자원을 공유하기 때문에 스토리지에 무단 접근이 가능할 수 있다.

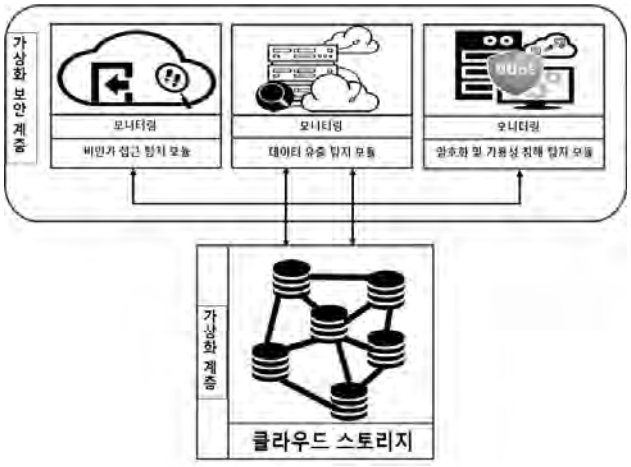
• T4. 서비스 비가용성

클라우드 스토리지 환경에서 서비스 가용성의 침해로 인해 스토리지 자원들을 사용할 수 없게 되면 비즈니스 불연속을 야기하는 추가적인 보안위협이 발생할 수 있다.

3.2 보안 아키텍처 설계

본 절에서는 앞서 새롭게 도출한 스토리지 보안위협을 방지 및 대응하기 위한 보안 아키텍처를 제안한다. 클라우드 스토리지가 포함되어 있는 가상화 계층과 모니터링 및 가상화 보안 계층으로 구성되며 (그림 1)과 같다.

가상화 계층은 클라우드에서 제공되는 가상 인프라 영역으로 기존 클라우드 컴퓨팅 인프라 구성과 동일하고, 가상화 보안 계층은 클라우드 스토리지를 대상으로 하며 새롭게 제안하는 계층으로써, 모니터링, 데이터 유출 탐지 모듈, 비인가 접근 탐지 모듈, 가용성 침해 탐지 모듈이 포함되어 있다.



(그림 1) 클라우드 스토리지 보안 아키텍처

• 모니터링

클라우드 스토리지 환경에 대한 모니터링을 수행하며 해당 환경에서 발생 가능한 의도치 않은 오류 및 악성행위를 탐지 및 분류하고 각각에 대한 정보를 수집하며, 데이터 유출 탐지 모듈, 비인가 접근 탐지 모듈, 데이터 암호화 모듈, 가용성 침해 탐지 모듈에 포함되어 있다.

• 비인가 접근 탐지 모듈

사용자 및 기업에 대한 계정 생성 및 폐기가 이루어져야 하며, 가상화된 스토리지에 접근하는 사용자, 서비스 제공자 및 관리자에 대한 역할별 상이한 권한을 부여한다. 또한 인가되지 않은 사용자의 접근을 방지하기 위한 인증 및 접근제어 프로토콜을 적용하여 비인가된 접근을 방지할 수 있다.

• 데이터 유출 탐지 모듈

모니터링을 통해 수집된 정보를 이용하여 데이터 유출을 발생시키는 악성코드 및 스팸 등 악성행위 분석을 통해 탐지하고 차단을 가능하게 한다.

• 암호화 및 가용성 침해 탐지 모듈

클라우드 스토리지에 저장되는 설정파일 및 중요 데이터를 표준으로 지정된 암호 알고리즘을 적용하여 암호화를 수행하며, 키의 유출을 대응하기 위하여 정해진 주기에 따라서 주기적으로 키를 변경한다. 또한 클라우드 스토리지 시스템의 기밀성을 보장하기 위해 적합한 키의 길이를 설정하여 적용한다.

또한 클라우드 스토리지 내의 대용량 데이터 암호화 시 가용성이 떨어질 수 있으므로, 블록, 스트림 공개키 등 적절한 암호 알고리즘을 사용하며 데이터에 대한 백업과 신속한 복구를 통해 클라우드 스토리지 환경에 대한 가용성을 보장한다.

3.3 안전성 분석

본 절에서는 한국정보통신기술협회의 「저장장치 가상화 시스템 보안요구사항」 표준 문서에 정의되어 있는 보안요구사항에 따라서 앞서 제안한 보안 아키텍처에 대한 안전성을 분석하며 <표 6>과 같다.

• R1. 기밀성 및 데이터 암호화

데이터 유출 탐지 모듈에서 악성코드 및 스팸 등 악성 행위에 대한 탐지와 차단을 수행하여 중요 정보에 대한 기밀성을 보장할 수 있으며 암호화 및 가용성 침해 탐지 모듈의 데이터 암호화 기능을 통해 데이터 암호화 요구사항을 만족시킬 수 있다.

• R2. 사용자 인증과 접근제어

비인가 접근 탐지 모듈은 서비스를 이용하는 제공자 및 관리자별로 상이한 접근권한을 부여하며 인증 및 접근제어 프로토콜을 적용하여 인가되지 않은 사용자의 접근을 탐지하고 차단할 수 있으므로 사용자 인증과 접근제어 보안요구사항을 만족시킬 수 있다.

• R3. 데이터 무결성

데이터 유출 탐지 모듈에서 악성코드로 인한 데이터의 무결성을 방지할 수 있으며 비인가된 접근 탐지 모듈에서 악의적인 공격자에 의한 데이터 접근을 방지할 수 있다.

또한 암호화 및 가용성 침해 탐지 모듈에서 데이터에 대한 변경이 이루어지지 않도록 암호화를 수행하기 때문에 데이터 무결성 보안요구사항을 만족시킬 수 있다.

• R4. 가용성 및 복구

암호화 및 가용성 침해 탐지 모듈에서 부적합한 암호화 방식을 통한 서비스 비가용성을 방지하기 위해 적절한 암호 알고리즘을 적용하고 데이터에 대한 백업과 복구를 수행하기 때문에 가용성에 대한 보안요구사항을 만족시킬 수 있다.

<표 6> 보안 아키텍처 안전성 분석

보안요구사항 / 모듈	R1	R2	R3	R4
데이터 유출 탐지 모듈	✓		✓	
비인가 접근 탐지 모듈		✓	✓	
암호화 및 가용성 침해 탐지 모듈	✓		✓	✓

4. 결론

클라우드 스토리지 환경에서 스토리지에는 사용자의 중요 정보를 저장될 수 있기 때문에 다양한 보안위협에 노출되어 있다. 하지만 클라우드 스토리지 보안 기술에 대해 미흡하므로 이에 대응하는 보안기술을 확보하기 위해 보안 아키텍처를 설계하였다.

따라서 설계한 보안 아키텍처가 보안 솔루션 개발에 활용될 수 있으며, 향후에는 설계한 보안 아키텍처의 각 모듈에 대해서 구체화하고 구현을 통해 검증해보고자 한다.

참고문헌

[1] 김영철, 차명훈, 이상민, 김영균, “클라우드 컴퓨팅에서 스토리지 가상화 기술 동향”, 전자통신동향분석 제24권 제 4호 2009.08.

[2] 박정숙, 이상민, 김홍연, 김영균,“클라우드 스토리지 기술 동향”, ETRI, 2016.08.

[3] Jungho Ju, Seungyoung Ma, Jongsub Moon, “Proposal of Security Requirements for Storage Virtualization System against Cloud Computing Security Threats”, Journal of Security Engineering, 2014.12.

[4] ISO/IEC 27040, “Information technology-security techniques-Storage security”, 2015.01.15.

[5] ITU-T X.1601, “Security Framework for Cloud Computing”, 2014.01.

[6] ENISA, “A Threat Landscape 2015”, 2016.01.

[7] CSA, “Cloud Computing Top Threats in 2016”, 2016.02.

[8] 한국정보통신기술협회, “저장장치 가상화 시스템 보안요구사항”, 2013.09.