클라우드 스토리지 보안성 평가를 위한 프로세스 설계 방법론

김지윤, 박기웅†
대전대학교 해킹보안학과 시스템보안연구실
e-mail:eoddl460@naver.com, woongbak@dju.kr

Design Methodology for Security Assessment of Cloud Storage System

Ji-Youn Kim, Ki-Woong Park
Dept of Computer Hacking and Information Security, Deajeon University

요 약

최근 모바일 컴퓨팅 환경이 발전함에 따라 모바일 디바이스 이용자들에게 다양한 서비스를 제공하기 위한 방법으로 클라우드 스토리지 서비스가 주목받고 있으며, 여러 장치의 데이터 동기화를 지원해준다. 이러한 편리성을 제공하고 있지만, 개인과 기업의 핵심 자료 유출에 따른 보안 이슈가 중요한 문제로 대두되고 있기 때문에, 클라우드 스토리지 보안 검증의 중요성도 증대되었다. 이처럼 클라우드 스토리지 서비스는 보안 검증 과정을 거친다. 본 논문에서는 기존의 클라우드 스토리지 보안 평가 가이드라인의 문제점을 분석하여 다형성, 종속성, 병렬성, 중복성 등을 고려해 효율적인 클라우드 스토리지 보안 평가를 위한 새로운 방법론을 제시 하였다. 제시한 방법론을 이용해 클라우드 스토리지 보안 검증 프로세스를 설계하였다.

1. 서론

클라우드 스토리지 서비스는 사용자들의 개인 데이터를 인터넷 상에 존재하는 클라우드 서비스 사업자의 스토리지에 저장시켜, 인터넷에 연결된 다양한 단말을 통해 개인 데이터에 대한 접근 및 보관을 제공하는 서비스이다. 최근 모바일 컴퓨팅 환경이 발전함에 따라 모바일 디바이스 이용자들에게 다양한 서비스를 제공하기 위한 방법으로 클라우드 스토리지 서비스가 더욱 주목받고 있다.

현재 상용화된 클라우드 스토리지 서비스로는 Dropbox[1], Ubuntu One[2], Mozy[3], CrashPlan[4], CloudMe[5], Wuala[6] 등이 있으며, 이와 같은 클라우드 스토리지 서비스를 이용하는 일반 사용자들이 늘어나고 있다. 지난해 2013년 한국미디어 패널조사에서 4,386가구 내 약 10,464명(6세 이상)에 대한 클라우드 스토리지 서비스 이용현황에 대한 설문을 실시하였다. 문항으로 “클라우드 스토리지 서비스를 이용하고 있다.”에 응답한 사람의 비율이 2012년도에서 2013년도사이 2.6% 포인트 가량 증가하였다[7].

이처럼 이용자 수와 클라우드 스토리지 업체가 증가되면서 가장 큰 화두로 등장한 것이 클라우드 스토리지 보안이다[8]. 2012년 1월 클라우드 기반 스토리지 서비스 업체인 Dropbox의 직원 계정이 해킹되어 사용자들의 개인정보가 유출되고 스팸 메일이 보내지는 사건이 발생하였다[9]. 클라우드 기반 웹 호스팅 서비스 업체인 DreamHost에서는 클라우드 데이터베이스에 대한 해킹 공격이 탐지되는 사건이 발생하였다[10]. 국내에서는 국가정보원이 2012 년 정부부처와 산하기관에 클라우드 서비스 이용에 따른 정부 자료 유출과 DDos 공격의 위험성을 제기하며 클라우드 서비스의 사용 중단을 요청하였다[11].

클라우드 스토리지 보안에 대한 중요성이 증대되면서, 클라우드 스토리지 보안에 대한 검증 과정을 거치고 있다. 기존의 클라우드 서비스 보안 검증 과정으로 2012년도에 발표된 모델이 두 가지가 있는데, 한국인터넷진흥원(KISA)에서 발표한 클라우드 보안 평가 가이드라인[12]과 보안 정보 기술(SIT)에서 제공하는 클라우드 스토리지 보안에 대한 자료[13]가 그것이다. KISA의 보안 평가 가이드라인은 국내 클라우드 서비스 사업자들의 자발적인 보안성 강화가 목적이고, SIT에서 발표한 클라우드 스토리지 보안성에 관한 자료는 끊임없이 변화하는 클라우드 스토리지 시장의 업데이트 소스 정보를 사용자들에게 제공하기 위함이다.

본 논문에서는 상기 두 모델을 참조하여, 효율적인 클라우드 스토리지 보안 평가를 위한 새로운 방법론을 제시한다.

앞서 설명한 KISA의 클라우드 서비스 보안 평가 가이

‡ 본 논문은 미래창조과학부, NIPA, 정보통신연구기반구축사업(과제번호:I2221-14-1002, 과제명: 대용량데이터 초고속처리 장비연구 인프라 구축)의 지원으로 수행되었음.
† 교신저자: 박 기 웅 (woongbak@dju.kr)

드라인과 SIT의 클라우드 스토리지 보안 자료를 분석한 결과 다음과 같은 문제점을 파악하였다.

첫째, 클라우드 스토리지 시스템은 사용자, 구축 및 개발 환경에 따라 매우 다양한 형태로 운영이 됨에도 불구하고, 일괄적인 보안 검증항목 기반의 평가가 이루어진다.

둘째, 다양한 보안 검증 항목이 단위별로 정의는 되어 있으나, 각 항목별 종속성, 독립성 등에 대한 고려가 결여되고, 항목별 순차적 검증이 수행된다. 그래서 검증 환경 및 중간 결과에 따른 불필요한 보안 항목까지 일괄적으로 모두 수행되어 과도한 검증 오버헤드가 발생된다.

셋째, 보안 평가 가이드라인에서 제시한 요소들은 독립되어 있으나, 각각의 요소들을 검증하는 과정에서 일부 반복적으로 수행되는 트랜젝션이 44%이상 확인되었으며, 불필요한 리소스 낭비가 발생한다.

이에 본 논문에서는 위에서 언급한 문제를 해결하기 위하여 다음과 같은 해결책을 제시하였다.

첫째, 클라우드 스토리지 시스템의 사용자, 구축 및 개발 환경에 따라 다양한 검증 기준을 수립, 환경 인지형 프로세스에 수립한 검증 기준을 적용한다.

둘째, 모듈화를 통해 다양성을 고려한 클라우드 스토리지 시스템에 각각의 요소들을 재조합 가능한 최적화된 모델을 디자인하여, 검증 시간 및 과도한 오버헤드의 발생을 줄인다.

셋째, 반복되는 트랜젝션의 중복 제거를 통해 불필요한 리소스 낭비를 방지, 비용절감 혜택이 있다.

이를 통해 다형성, 종속성, 중복성을 고려한 효율적인 클라우드 스토리지 보안 평가 프레임워크를 제시한다.

본 논문의 구성은 2장에서 관련 연구로서 기존의 클라우드 스토리지 보안성 검증 방법의 소개를 통해 기존연구의 동향 및 차별점에 대해 살펴보고, 3장 에서는 클라우드 스토리지 보안 검증이 최적화된 프로세스 디자인을 제시하며, 4장에서는 결론 및 향후 연구방향을 도출한다.

2. 관련연구 및 차별점

본 장에서는 관련 연구로서 기존의 클라우드 스토리지 보안성 검증 소개를 통해 기존 연구와의 차별점에 대하여 살펴본다.

2.1 관련연구 및 차별점 클라우드 스토리지 평가에 관한연구

클라우드 스토리지 서비스는 온라인 저장 및 온라인 공유가 가능하며, 사용자의 콘텐츠를 서버에 저장해 두고 단말기에서 다운로드 후 사용 할 수 있는 서비스이다. 그러나 개인정보 해킹에 대한 우려로 보안 검증과정[12][13]이 이루어지고 있다.

기존의 클라우드 스토리지 서비스 보안성 검증 방법은 보안 평가를 위해서 적합한 검증 방법이기는 하지만, 클라우드 스토리지 시스템의 사용자, 구축 및 개발 환경에 따라 매우 다양한 검증 방법이 있음에도 불구하고, 일괄적인 보안 검증 항목 기반의 평가가 이루어진다. 또한 기존의 클라우드 스토리지 서비스 보안 검증 과정은 항목 단위로만 되어있어 각 항목들은 종속성, 독립성 등에 대한 고려가 결여되어있고, 항목별 순차적 검증이 수행된다. 그렇기 때문에 검증 환경 및 중간 결과에 따른 불필요한 보안 항목까지 일괄적으로 모두 수행이 되어 과도한 검증 오버헤드가 발생된다는 단점이 있다. 기존에 정의된 보안 평가 가이드라인에서는 항목을 이루는 각각의 요소들이 순차적으로 검증 수행 되어 왔으나, 요소들을 검증하는 과정에서 분석 결과 반복적으로 수행되는 트랜젝션이 확인되었다.

2.2 기존 연구와의 차별점

본 논문에서 제안하는 클라우드 스토리지 보안성 검증 프로세스는 기존에 사용되었던 검증 방법에서 독립성, 병렬성, 종속성, 중복성 등의 특성을 고려한 효율적인 검증 방법을 제시한다.

2.1에서 설명한 기존의 보안성 검증 방법의 문제점을 극복하기 위하여 효율적인 보안 검증 프로세스를 제안하였다. 제안된 검증 프로세스는 다음과 같은 특성을 갖는데. 적용된 특성으로는 다형성, 종속성, 병렬성, 중복성 등이 있다. 클라우드 스토리지 시스템의 다양한 구축 환경, 개발 환경에 따라 보안 검증이 수행되며, 검증 환경 및 중간 결과에 따른 불필요한 보안 항목ㄱㆍ지 수행할 필요 없이 검증될 수 있도록 하였고, 반복되는 트렌젝션의 중복제거를 통해 불필요한 리소스 낭비를 방지하도록 함으로써 비용절감 혜택과 시간 및 과도한 오버헤드의 발생을 줄였다.

3. 클라우드 스토리지 보안성 검증 최적화

본 논문에서 제안하는 클라우드 스토리지의 효율적인 보안성 검증 프로세스를 이용하여 클라우드 스토리지 보안 검증 디자인 요구사항에 대해 설명하였고, 최적화된 보안 검증 프로세스를 설계하였다.

3.1 효율적인 클라우드 스토리지 보안 검증 디자인 요구사항

2장에서 설명한 바와 같이 본 논문에서는 기존의 클라우드 스토리지 보안성 검증 시스템의 한계를 해결하기 위해, 클라우드 스토리지의 효율적인 보안성 검증 프로세스를 디자인 하였다. 효율적인 클라우드 스토리지 보안 평가 프로세스는 다음과 같은 목적을 기반으로 디자인 하였다.

- **시스템 환경 인지형 검증 프로세스:** 클라우드 스토리지 시스템은 사용자, 구축환경, 개발 환경에 따라 매우 다양한 형태로 운영되고 있다. 따라서 보안 검증 시에도 다양한 환경에 최적화된 검증 절차가 적용되어야 한다.
- **검증 프로세스 평가항목별 종속성 분석을 통한 프로세스 최적화:** 검증 환경 및 중간 결과에 따라 불필요

하게 수행되는 평가 항목을 제거하기 위해 검증 프로세스의 보안 평가 항목별 종속성을 판단하여 평가 항목들의 모듈화를 통해 최적화된 보안 검증을 수행해야 한다.

- **클라우드 스토리지 보안 평가 요소를 검증하는 과정의 반복되는 트랜젝션 중복제거:** 보안 평가 요소를 개별적으로 보안 검증시 반복되는 내부 로직을 제거하여 검증 시간을 단축 시켜야 한다.

본 논문에서는 이러한 세 가지 요구사항을 충족시키기 위해, 으로 일괄적인 보안 평가 과정에서 다양한 환경에 최적화된 검증 절차가 적용된 상황과 종속성과 병렬성을 고려한 상황, 그리고 반복적으로 수행되는 트랜젝션의 중복 제거 때의 상황을 분석하여 최적화된 보안 검증 프로세스를 설계하였다.

3.2 최적화 프로세스 설계

본 논문에서 제안하는 최적화된 보안 검증 프로세스는 3.1장을 기반으로 3가지의 요구사항을 반영하며, 총 3 State로 구성된 검증 평가이고, 방법을 제시하였다.

State1. 클라우드 스토리지 시스템의 사용자, 구축 및 개발 환경에 따른 다양한 검증 기준을 수립, 보안 검증 프로세스에 수립한 검증 기준을 적용하여 환경 인지형 프로세스를 추출하였다.

State2. 검증 프로세스에 대한 평가항목별 종속성 및 독립성을 분석하여 종속성 & 병렬성을 추출하였다.

State3. 보안 평가 요소들을 개별적으로 검증시 반복되는 내부 로직을 제거하는 과정에서 Divide & Merge 기법을 추출하였다.

앞서 설명한 3 State는 다형성, 종속성, 병렬성, 중복성 등을 고려한 기법이다. 기법의 단계별 수행과정을 3.2.1절, 3.2.2절, 3.2.3절에서 설명한다.

3.2.1 State1: 환경 인지형 검증 기법

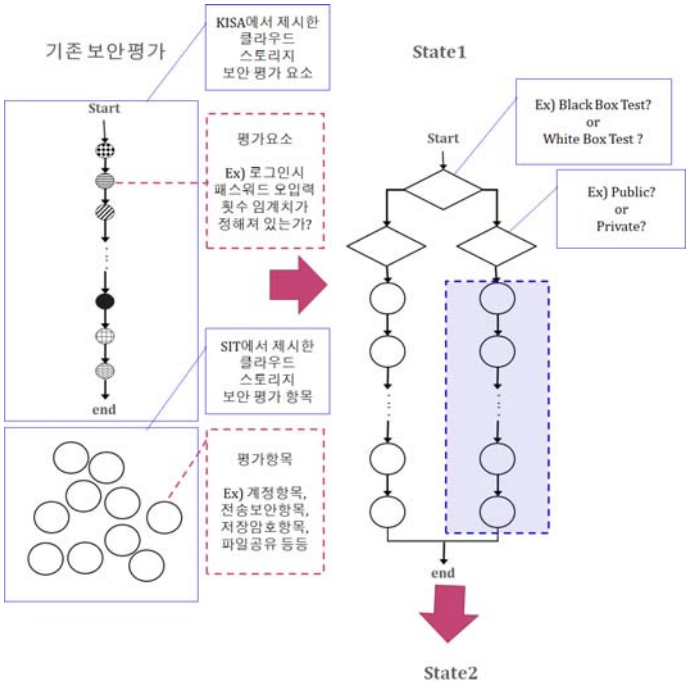
기존의 클라우드 스토리지 시스템은 사용자, 구축 및 개발 환경에 따라 매우 다양한 형태로 운영이 됨에도 불구하고, 일괄적인 보안 검증 항목 기반의 평가가 이루어진다.

본 논문에서는 다양한 검증 기준을 수립, 보안 검증 프로세스에 수립한 검증 기준을 적용하는 과정을 수행하였다. 여기서 말하는 검증 기준은 예를 들어, 보안 검증시 Black Box테스트, White Box테스트인지 또는 Public, Private인지 등등 다양한 환경에 따라, 검증 방법을 분류할 수 있도록 하는 것을 말한다.

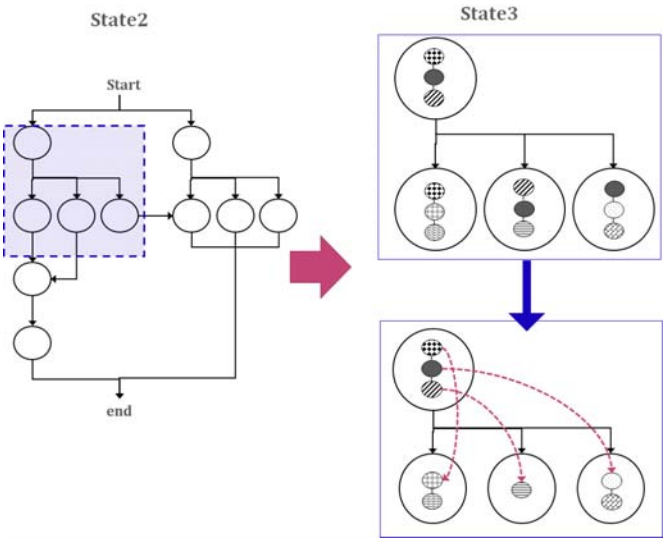
(그림 1)에서 State1과 같이 환경 인지형 검증 기법을 수행함으로써, 클라우드 스토리지 시스템 환경에 따른 최적화된 검증 절차를 수행할 수 있다.

3.2.2 State2: 종속성 & 병렬성 추출

기존의 클라우드 스토리지 보안 평가 모두 검증 환경



(그림 1) 환경 인지형 검증 기법 추출 과정



(그림 2) 종속성 & 병렬성, Divide & Merge 기법 추출 과정

및 중간 결과에 따라 불필요하게 수행되는 평가 항목을 반복적으로 검증하였고, 순차적 검증으로 검증 시간 및 과도한 오버헤드가 발생 된다.

본 논문에서는 (그림 2)에서 State2과 같이 보안 평가 항목별 종속성과 병렬성을 판단하여 보안 검증을 수행하였다. 예를 들어, 예를 들어 전송 암호화 항목과 저장 암호화 항목이 계정 항목과 상호종속성을 가지고 있다고 할 수 있다. 즉, 계정 등록시 패스워드가 서버측으로 전송될 때, 암호화 되어 전송된다. 그 다음 서버측에서 패스워드가 저장 되는데, 암호화 저장이 된다. 그렇기 때문에 계정 항목, 전송 암호항목, 저장 암호항목 등이 종속되어 있다고 할 수 있다. 또한 전송암호화 항목 검증과 저장 암호화

항목 검증을 병렬적으로 수행할 수 있다. 이와 같이 종속성 및 병렬성을 추출하여 검증 시간 및 과도한 오버헤드가 발생 되는 것을 줄일 수 있다.

3.2.3 State3: Divide & Merge 기법 추출

기존의 보안 평가 가이드라인에서 제시한 요소들은 독립되어 있으나, 각각의 요소들을 검증하는 과정에서 일부 반복적으로 수행되는 트랜젝션이 존재한다. 이러한 검증 과정은 불필요한 리소스 낭비가 발생한다.

본 논문에서는 (그림 2)에서 State3와 같이 보안 평가 요소들을 Divide 기법을 통해 내부 로직을 나누고, 반복되는 트랜젝션에 대한 중복성 검출 연산을 수행하였다. 그다음 Merge 기법을 이용하여 제거된 로직을 다시 합쳐 반복적으로 검증 수행되었던 트랜젝션을 한번만 검증할 수 있도록 하였다. 위와 같이 Divide & Merge기법을 통해 불필요한 리소스 낭비를 방지, 비용 절감 효과가 있다.

4. 결론 및 추후연구

본 논문에서는 다형성, 종속성, 병렬성, 중복성 등을 고려한 클라우드 스토리지 보안 검증 프로세스를 제안하였고, 그를 이용하여 최적화된 보안 검증 프로세스를 나타내었다. 본 논문의 최적화된 보안 검증 프로세스는 첫째, 클라우드 스토리지 시스템의 사용자, 구축 및 개발 환경에 따라, 환경 인지형 기법을 수행한다. 이러한 기법을 사용함으로써, 다양하고 최적화된 보안 검증 과정이 이루어진다. 둘째, 검증 환경 및 중간 결과에 따라 불필요하게 수행되는 평가 항목을 판단하여, 종속성 & 병렬성 기법을 수행해 검증 시간 및 과도한 오버헤드 발생을 줄였다. 마지막으로, 각각의 요소들을 검증하는 과정에서 일부 반복적으로 수행되는 트랜젝션을 Divide & Merge기법을 통해 불필요한 리소스 낭비를 방지, 비용 절감 효과가 있다.

추후 연구로서 본 논문에서 제시한 클라우드 스토리지 보안 검증 프로세스 수립 방법론을 기반으로, 1) 실제 클라우드 스토리지 시스템에 적용이 가능한 검증 프레임워크를 설계하고, 2) 성능분석 및 유용성 판단 근거를 제시하여, 3) 체계적이고, 효율적인 클라우드 보안 검증 프레임웍을 실현할 것이다.

참고문헌

[1] DropBox, https://www.dropbox.com/, Cloud Storage Service Web site, 2008

[2] Ubuntu One, https://one.ubuntu.com/, Cloud Storage Service Web site, 2014

[3] Mozy, https://www.mozy.com/, Online backup service Web site, 2013

[4] CrashPlan, http://www.ceejay.net/, Code42 Software 2014

[5] CloudMe, www.cloudme.com/, File Storage Service, 2014

[6] Wuala, www.wuala.com/, Wuala - Secure Cloud Storage - Backup, Sync, Share Services, 2014

[7] 김민철, "클라우드 서비스 이용현황", KISDI, 2014.1.25.

[8] CIOCISO, http://www.ciociso.com/news/articleView.html?idxno=9222, 2011

[9] Bard Darrow, "Dropbox: Yes, We were Hacked", dropbox, 2012.8.1.

[10] Dancho Danchev, "DreamHost CEO issued the following statement", DreamHost, 2012. 1. 21

[11] 박기웅, "클라우드 보안인증체계(FedRAMP) 프로세스 분석 및 정부 정책연구", 한국표준협회, 2013.1

[12] "국내 클라우드 서비스 보안 취약점 점검", 한국 인터넷 진흥원(KISA), 2012.

[13] SIT, "On the Security of Cloud Storage Services", SIT-TR-2012-001, 2012.