클라우드 저장공간 통합 플랫폼의 보안 방법 연구

이성원, 이민우, 안광은, 정영주, 길준민, 서동만
대구가톨릭대학교 IT공학부
sarum@cu.ac.kr

A Research of Security Method for Integrated Cloud Storage Platform

SungWon Lee, MinWoo Lee, KwangEun An, Young-Ju Jeong,
Joon-Min Gil, Dongmahn Seo
School of Information Technology Engineering, Catholic University of Daegu

요 약

본 논문은 이기종 클라우드 저장공간을 통합하여 하나의 저장공간으로 사용하는 플랫폼 환경에 필요한 보안 방법들에 대해 논한다. USB를 이용한 보안 방법을 제시하고 클라우드 스토리지의 데이터를 안전하게 사용하기 위한 방법에 대하여 논한다.

1. 서론

현재 클라우드 스토리지는 다양한 환경의 기기를 이용하여 언제 어디서나 파일을 읽고 쓸 수 있다는 장점 때문에 많이 활용 되고 있다. 클라우드 스토리지 서비스에서는 일반적으로 제한적인 저장 공간과 기능을 무료로 사용자에게 제공하기 때문에 안정적으로 많은 저장공간을 사용하기 위해서는 추가적인 비용 지불이 필요하다. 따라서 무료로 제공되는 다양한 클라우드 스토리지를 하나로 통합하여 사용하는 환경에 대한 다양한 연구가 있었다.[1, 2, 3] 그러나 다수의 클라우드 스토리지를 하나로 사용하는 만큼 보안에 대한 연구가 필요하다.

본 논문에서는 통합된 클라우드 스토리지를 활용하기 위해 클라이언트에서 필요한 보안적 이슈들을 설명하고 보안 방안에 대해 제시하고, 통합 클라우드 스토리지의 데이터를 안전하게 사용하기 위한 방법에 대하여 논한다. 각 클라우드 스토리지 데이터에 접근하기 위한 접근 토큰(Access Token)과 리프래쉬 토큰(Refresh Token)을 하나의 테이블로 만들어 토큰 테이블의 데이터 보안 방법을 제시한다. 또한 토큰 테이블로 OAuth 2.0[4]의 보안의 위험성을 줄이기 위한 방법을 제안한다. 통합 클라우드 스토리지 클라이언트의 안전성을 증가함으로써 사용자들은 추가적인 비용 없이 안정적으로 대용량의 클라우드 저장공간을 사용할 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 통합 클라우드 스토리지 클라이언트와 OAuth 2.0의 접근 토큰과 리프래시 토큰의 위험성에 대하여 서술한다. 3장에서는 토큰 테이블과 USB를 이용한 보안을 제안한다. 4장에서는 본 논문의 결론을 맺고, 향후 연구 계획을 설명한다.

이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.
(NRF-2015R1C1A1A02036686)

2. 관련 연구

하나의 클라우드 스토리지는 제한적인 용량을 제공하며 대용량의 클라우드 스토리지를 이용하기 위해선 추가 비용 지불이 필요하다. 대용량 스토리지를 추가적인 비용 없이 사용하기 위해 다수의 클라우드 스토리지를 하나로 통합하는 연구가 있었다[1, 2, 3]. [1]의 연구에서는 여러 클라우드 스토리지에 개별적인 로그인은 편의성을 해치기 때문에 한 개의 클라이언트 ID로 여러 클라우드 스토리지의 데이터에 접근을 할 수가 있다. 접근을 위한 ID, 비밀번호 등의 데이터는 통합 플랫폼을 제공하는 측에서 만든 서버에 저장이 된다. 따라서 서버에서 모든 클라우드 스토리지 데이터에 접근이 가능할 위험성이 있다.[5]

OAuth 2.0[4]은 클라우드 스토리지에서 API 인증과 권한 부여를 동시에 제공하는 인증 프로토콜이다. 통합된 플랫폼에서 클라우드 스토리지에 접근하기 위한 ID나 비밀번호를 입력할 필요가 없다. 사용자의 개인정보가 저장이 되지 않기에 보안성이 더 올라가게 된다. 클라우드 스토리지에 접근을 할 수 있게 해주는 인증키. 접근 토큰을 사용하여 클라우드 스토리지 데이터 접근 권한을 얻는다. 접근 토큰을 만료기간 없이 지속적으로 사용한다면 암호화가 되어있더라도 보안이 취약해진다. 이 점을 보완하기 위해 접근 토큰의 만료기간이 명시되어져 있으며 접근 토큰을 새로이 발급 받을 수 있도록 하는 리프레시 토큰은 접근 토큰과 함께 발급 받는다.[4]

<표 1> 토큰 테이블 예시

Vendor Name	UserID	Token	
		Access	Refresh
GoogleDrive	A	Access Token	Refresh Token
Dropbox	B	Access Token	Refresh Token
Box	B	Access Token	Refresh Token

3. 통합 클라우드 스토리지의 보안 방법

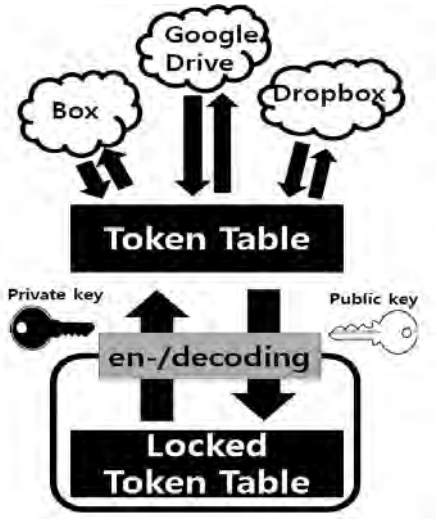
3.1. 토큰 테이블

통합 클라우드 스토리지를 사용하면 토큰들을 받아 각각 저장하게 된다. 토큰 테이블은 표 1이 보여주고 있는 바와 같이 플랫폼 구성은 사용자 ID, 접근 토큰, 리프레시 토큰을 포함하는 테이블이다. 하지만 토큰 테이블이 노출될 경우 토큰 테이블의 정보를 이용하여 모든 클라우드 스토리지에 대해 접근이 가능하게 된다. 따라서 토큰 테이블 또한 추가적인 보안이 필요해진다.

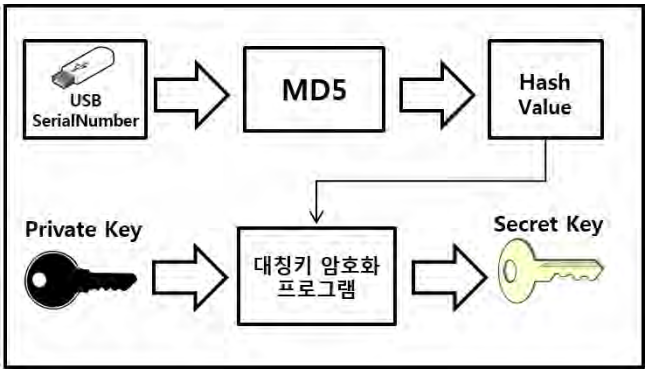
그림 1은 비대칭키 암호화 알고리즘을 기반으로 공개키를 사용하여 암호화 한다. 클라우드 스토리지 서비스를 사용해야 될 경우 개인키를 사용하여 토큰 테이블을 복호화하고 토큰 테이블에 저장된 접근토큰을 사용하여 클라우드 스토리지 서비스를 사용한다.

3.2 USB를 이용한 보안 기법

하나의 토큰 테이블의 보안을 강화 하더라도 언제나 위험성은 존재한다. 하지만 USB마다 가지는 고유 시리얼 번호를 MD5기반의 암호화 프로그램을 통해 해시값을 생성하고 생성한 해시값을 사용하여 개인키를 암호화한다. 그림 2는 USB를 이용해 개인키를 암호화하는 과정을 도식화한 것이다. USB 시리얼 번호를 MD5기반의 암호화 프로그램으로 해시 값을 생성한다. 해시 값과 암호화 기반의 프로그램으로 개인키를 암호화 한다. 개인키를 암호화 하여



(그림 1)토큰 테이블 보안 흐름도 예시



(그림 2) 개인키 암호화과정

생성된 비밀키(Secret key)는 로컬에 저장된다. 결과적으로 USB의 시리얼 번호를 이용한 해시값 없이는 로컬에 저장한 비밀키를 복호화 할 수 없다. 따라서 비밀키가 타인에게 유출되더라도 해시값이 없기 때문에 안전하다. 또한 USB의 분실의 경우 기존의 플랫폼ID로는 누구도 접근을 하지 못하며 사용자는 새롭게 ID와 토큰테이블을 갱신하면 사용가능 하기에 안전하다. 프로그램에서 사용된 암호화 알고리즘들은 상황에 따라 원하는 암호화 알고리즘을 적용시켜도 무관하다.

4. 결론 및 향후 계획

통합형 클라우드 스토리지를 사용하는 목적은 대용량의 클라우드 스토리지를 추가적인 비용 없이 사용하는 것이다. 하지만 사용하는 스토리지 데이터에 대한 보안이 이루어져 있지 않다면 쉽게 사용하지 못할 것이다. 본 논문은 설계 및 구현 되어 있는 아키텍처를 설명함과 동시에 필요한 보안 문제점을 제안하였다. 보안적인 요소만 지켜지게 된다면 사용자들은 자신의 데이터 유출에 대한 걱정 없이 무료의 대용량 클라우드 스토리지를 사용하게 될 것이다. 파일 암호화를 이루게 됨으로써 플랫폼 개발자를 포함한 외부 침입자들도 손쉽게 접근을 하지 못하는 안전한 통합 클라우드 스토리지를 제공하는 것이다. 다양한 웨어러블 디바이스와 스마트 기기들이의 대중화에 따라 데스크탑 PC 뿐만이 아니라 다양한 웨어러블 스마트 디바이스로도 접근이 가능하도록 다양한 환경에서의 통합 클라우드 스토리지 클라이언트 어플리케이션을 개발하면 언제 어디에서나 자기 자신의 데이터에 접근이 용이해질 것이다. 모바일 환경의 어플리케이션에서의 보안적인 특색에 맞게 본 논문의 보안 방법들을 적용한다면 자신의 데이터에 대한 안정성을 높일 것이며 추후 다양한 환경의 어플리케이션에서 동작 가능한 형태의 보안에 대해 연구할 계획이다.

참고문헌

[1] 김지훈,김우현, “웹하드형 클라우드 스토리지를 통합한 통합형 스토리지 플랫폼 설계 및 구현”, 대한전자공학회 학술대회, p.816-p.819, 11월 2013년

[2] Gyuwon Song, Suhyun Kim, and Dongmahn Seo, “SaveMe: Client-Side Aggregation of Cloud Storage”, IEEE Transactions on Consumer Electronics, Vol. 61, No. 3, August 2015
[3] Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernado Andre, Paulo Sousa, “DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds”, ACM Transactions on Storage (TOS), Vol. 9, No. 12, November 2013
[4] D. Hardt, “The OAuth 2.0 Authorization Framework”, Internet Engineering Task Force(IETF), October 2012
[5] 정영곤, 이상래, 장기헌, 염홍열, “안전한 OAuth 인증 프로토콜을 위한 보안 문제점 연구”, 한국통신학회 학술대회 논문집, p.952-p.953, 2월 2011년