암호 알고리즘을 이용한 클라우드 스토리지 데이터 암호화 앱 설계 및 구현에 관한 연구

손민석*, 원유재**
*,**충남대학교 컴퓨터공학과
*e-mail:mss007daum@cnu.ac.kr, **e-mail:yjwon@cnu.ac.kr

A Study on Design and Implementation of Cloud Storage Data Encryption App using Cryptographic Algorithm

Minseok Sohn*, Yoojae Won**
*,**Dept of Computer Engineering, Chung-nam University

요 약

최근 컨텐츠 제공 업체와 사용자들로부터 생성되는 미디어 데이터들의 용량이 늘어남에 따라, 사용자들은 자신이 보유한 단말 외에 추가적인 저장공간이 필요하게 되었다. 이에 추가 저장소 및 백업 장치로써 클라우드 스토리지 서비스의 사용률이 늘어나는 추세이다. 클라우드 서비스에 대한 수요가 증가하고 이와 함께 보안적인 이슈가 늘어남에 따라, 서비스 제공자들은 다양한 보안 기술들을 클라우드 시스템에 적용하고 있다. 본 논문에서는 클라우드 스토리지 서비스의 보안성을 위한 업로드, 다운로드 간 파일 암 · 복호화 방법에 대해 제안한다. 제안한 어플리케이션은 보안 문제들을 해결하는 데에 도움이 될 것으로 기대된다.

1. 서론

최근 스마트폰의 사용이 대중화되고 무선 인터넷 사용량이 많은 만큼 컨텐츠 제공 업체와 사용자들로부터 생성되는 미디어 데이터들의 용량이 늘어났으며, 사용자들은 자신이 보유한 단말 외에 추가적인 저장 공간이 필요하게 되었다. 또한, 단말의 교체 시 이동하는 데이터가 증가하며 이를 제공해주는 서비스에 대한 요구가 늘어나고 있다. 이에 추가 저장소 및 백업 장치로써 클라우드 스토리지 서비스의 사용률이 늘어나는 추세이다. 클라우드 서비스에 대한 수요가 증가하고 이와 함께 보안적인 이슈가 늘어남에 따라, 서비스 제공자들은 다양한 보안 기술들을 클라우드 시스템에 적용하기 시작했다[1]. 정부와 기업에서 클라우드 구축·도입 시 최대 걸림돌은 보안 문제이다. 국내 기업들의 클라우드 이전 준비는 미흡하고, 대다수 기업들은 클라우드 도입 시 장애요인 1순위로 악성코드, 기밀 데이터 해킹 및 유출 등 보안 문제를 가장 우려하고 있다. 트렌드마이크로, 블루코트, 안랩 등 국내·외 주요 보안 업체들은 클라우드 보안 위협이 계속 될 것으로 전망하였으며, <그림 1>과 같이, 클라우드 사용이 늘어남에 따른 솔루션의 시장도 커질 것으로 전망되고 있다. 클라우드의 구축·도입 시 기존 보안 위협을 상속하고 클라우드 특성에 따른 신규 보안 위협존재하며, 가상화, 원격지에 정보 위탁·사업자 종속, 모바일 기기 접속, 데이터 국외이전, 침해사고 대형화, 데이터센터 안전성 등 이슈가 발생한다. 클라우드 컴퓨팅에서는 특권을 가진 사용자의 접근제어, 데이터 무결성, 데이터의 분산관리 등이 중요한 보안 요소이지만, 클라우드 컴퓨팅을 통해 데이터가 연동되고 자원을 다양하게 활용하는 것에는 데이터 보호와 자원의 관리 정책, 기업 비밀 관리나 개인의 프라이버시 측면에서의 문제점 해결이 필요하다[2]. 클라우드 보안 사고는 관리자의 실수, 서버 중단 등의 중요 사고가 발생하였으며, 개인 정보 유출 및 데이터 손실로 사용자에게 손실 및 신뢰를 잃었다. 특히 개인 정보 유출 및 손실은 클라우드 사용자 및 기업 모두에게 중요한 이슈이며 클라우드 도입에 가장 저해하는 원인이 되기도 한다. 2012년 애플은 해킹으로 인한 데이터 손실, 2010년 MS는 관리 부주의로 인해 기업정보가 유출된 사례가 있다[3]. 보안 및 개인 정보보호 문제를 해결하는 직접적인 방법은 클라우드로 전송되기 전에 데이터를 암호화하는 것이다[4]. 따라서 본 논문에서는 클라우드 데이터를 암호화 저장하여 보안성을 높이고, 다중 클라우드 스토리지 연동을 통한 모니터링 방법으로 가시성을 확보한 프로그램 설계를 하고자 한다.

<그림 1> 국내 클라우드 환경 구현을 위한 스토리지 솔루션 시장 전망(단위: 억 원)

2. 관련 연구

2.1 사용자 인증과 데이터 보호

이미 서비스하고 있는 클라우드 스토리지 앱에서는 사용자가 클라우드 스토리지 로그인시 입력하는 ID와 패스워드를 이용하여 해쉬값을 만든다. 그 해쉬값을 이용하여 사용자, 인증서버, 클라우드 스토리지 관리서버는 공개키와 개인키를 이용하여 전자 서명의 기능을 이용하여 사용자 인증을 한다. 협업시 데이터는 사용자, 데이터, 데이터의 버전의 해쉬값을 같이 저장하며, 다른 사용자가 파일에 접근시 이전 사용자의 해쉬값과 비교하여 파일을 읽는다. 이를 통해 클라우드에 접근할 때와 파일에 접근할 때 두 번 검사를 하기 때문에 보안성이 향상된다[5].

2.2 데이터 중복 제거 기술

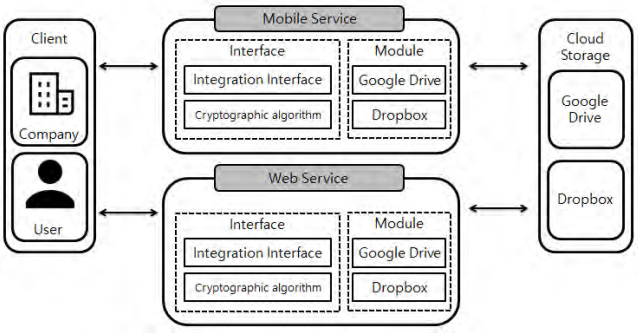
데이터를 저장하는 서버에서의 무결성을 데이터 소유자에게 검증하기 위한 기법으로 해시 트리를 사용하고 있는데, 상호간의 역할을 변경함으로써 클라우드 스토리지에 저장된 데이터와 동일한 데이터의 소유를 증명하기 위하여 해시트리를 이용하고 있다. 기존의 단순한 해시값을 이용하는 데이터 중복 제거에서는 앞서 기술한 식별 공격을 통하여 임의의 값을 생성한 공격자가 우연히 이용자 데이터에 대한 접근이 가능하며, 무결성 검증을 위해 공개될 수 있는 해시값으로부터 권한없는 이용자의 접근을 차단하기 어렵다는 문제를 해결하고 있다[6].

2.3 데이터 보호의 필요성

현대의 컴퓨팅 인프라가 클라우드로 이동함에 따라 개인, 기업, 기관에서는 작업 환경뿐만 아니라 데이터의 보관 또한 클라우드에서 하고 있다. 새로 제안되는 프로그램 중에는 클라우드 서비스를 제공하는 것을 넘어서서 클라우드에 저장된 데이터에 접근하여 필요한 데이터를 별도로 저장하는 기능을 가진 것도 있다. 이렇게 다양한 인프라를 보호하기 위해 전 세계적으로 정보 보안 및 개인 정보 보호에 상당한 금액을 지출하고 있다[7][8].

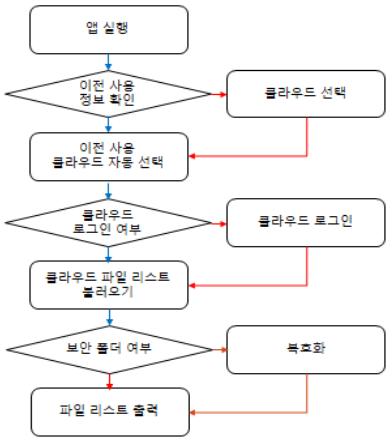
3. 연구 내용

사람들이 많이 사용하는 클라우드 스토리지 중 하나인 Dropbox는 Dropbox 앱(데스크톱, 모바일, API, 웹사이트)과 서버 간에 파일을 전송할 때 128비트 이상의 AES 암호화 방식으로 보호된 보안 터널을 생성하는 SSL(Secure Sockets Layer)/TLS(전송 계층 보안) 기술을 사용하고 있다. 데이터를 전송하는 과정에서 암호화를 하면 스니핑, 스푸핑 등 앱과 서버 사이에서 들어오는 공격은 대비할 수 있다. 하지만, 개인 계정 정보의 유출로 인해 공격자가 직접 클라우드에 접속하거나, 클라우드 스토리지에 저장된 데이터가 유출되었을 경우에는 데이터의 노출을 피할 수 없다. 연구는 클라우드 스토리지 다중 연동 및 업로드되는 파일에 대한 암호화가 가능한 앱을 설계하였다. 클라우드 스토리지 다중 연동은 한 개의 앱에서 여러 클라우드 스토리지 로그인이 가능하도록 하여, 불필요하게 업로드된 파일의 확인과 불필요한 파일에 대한 식별이 용이할 것이다. 업로드되는 파일에 대한 암호화는 기존 클라우드에서 파일 전송시 암호화되는 부분뿐만 아니라 클라우드에 저장되는 파일 자체에 대한 암호화를 통해 데이터 유출시의 피해를 줄일 수 있다.



<그림 2> 클라우드 스토리지 데이터 암호화 시스템 구성도

<그림 2>는 클라우드 스토리지 데이터 암호화를 제공하기 위한 서비스 설계를 위한 구성도이다. 모바일과 웹에서 서비스를 제공하고자 하며, 아래의 <그림 3>은 앱 실행시부터 클라우드 스토리지의 파일 리스트 확인까지의 단계이다.



<그림 3> 앱 실행 및 폴더 리스트 확인 Flowchart

3.1 클라우드 데이터의 암호화 방법

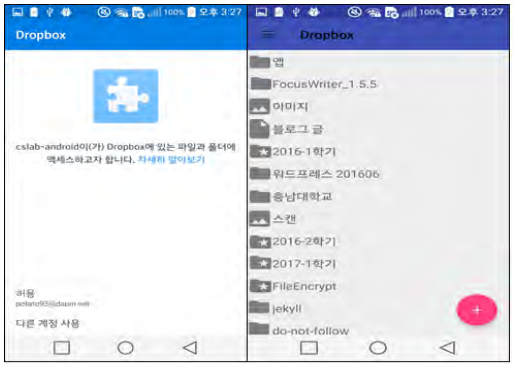
클라우드 데이터 암호화를 하는 방법으로는 패킷 캡쳐 및 변조를 이용하거나, 패킷 캡쳐 및 변조를 통한 방법으로 Winpcap Library를 이용하여 프로그래밍하는 방법이 있다. Winpcap Library를 이용한 기존의 툴로는 Wireshark, Fiddler, Microsoft Network Monitor 등이 있다. 또한 Proxy를 이용해서 패킷 캡쳐 및 변조도 가능하다. DLL Injection을 이용한 방법으로는 윈도우 소켓 API를 후킹하는 방법이 있으며, 브라우저의 확장 프로그램에서 클라우드로 업로드하는 파일에 대한 암호화 방법도 있다.

4. 클라우드 데이터 암호화 구현

본 논문의 3장에서 설명한 클라우드 드라이브 데이터 암호화 및 클라우드 가시화를 제공하는 기능을 하는 결과물은 모바일과 PC 두가지 환경에 대해 제안한다.

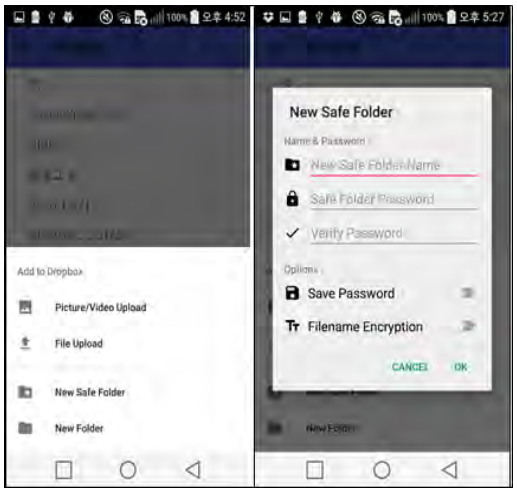
4.1 모바일 환경

<그림 4>는 클라우드 스토리지에 로그인을 하며, 클라우드를 로그인하면 암호화 폴더와 비암호화 폴더가 구분되도록 가시화되어 보여진다. 별표 표시가 있는 폴더가 보안 폴더로써 선택시 암호 입력을 해야 사용이 가능하다.



<그림 4> 앱 실행 및 파일 리스트 화면

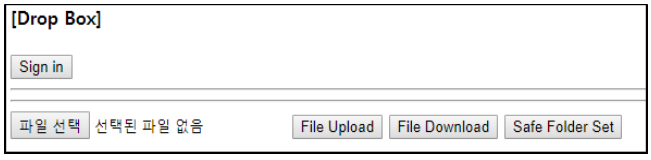
파일 업로드 및 다운로드 시 암호 알고리즘은 AES 256으로 정하였다. 클라우드 드라이브마다 제공해주는 API를 이용해 기존의 클라우드 스토리지와 유사한 환경에서 기능을 추가하는 방향으로 정하였다. 기존의 클라우드 드라이브 앱과의 차이점은 암호 폴더를 생성할 수 있는 것으로, 해당 암호 폴더에 업로드 시 파일을 암호화하여 클라우드에 저장하는 것이다. 또한 파일 다운로드 시에는 암호 폴더의 파일의 경우 파일을 받은 다음에 복호화하여 읽도록 한다. <그림 5>에서 보이는 것처럼 메뉴에는 암호화 폴더 생성 버튼이 있으며, 해당 메뉴 선택시 암호 폴더의 이름과 비밀번호를 입력한다. 이때 이 비밀번호는 AES256 알고리즘의 키를 해쉬로 만드는 데에 사용된다.



<그림 5> 클라우드 스토리지 메뉴 및 암호 폴더 생성시 메뉴

4.2 PC 환경

<그림 6>과 같이PC 환경에서는 평소 사용하는 웹 상에서 클라우드 스토리지 데이터 암호화 기능을 사용하기 위해 웹 페이지를 구현하였다.



<그림 6> 웹 페이지 형태의 클라우드 스토리지 서비스

'Sign in' 버튼을 통해 클라우드 스토리지에 로그인을 하며, 로그인 후에는 <그림 7>과 같이 클라우드 스토리지 폴더 목록이 확인 가능하다. 'Safe Folder Set' 버튼을 통해 암호 폴더를 생성하며, 암호 폴더 생성 후에 해당 경로에 업로드, 다운로드되는 파일들에 대해서는 암호화가 적용된다.

<그림 7> 클라우드 스토리지 로그인시 파일 목록

5. 결론

본 논문에서는 클라우드 스토리지에 파일 암호화를 적용하는 프로그램의 설계 및 구현에 대해 제안하였다. 드라이브 다중 연동을 통해 클라우드 드라이브에 저장되어있는 데이터에 대한 가시성을 확보하고자 하였으며, 파일을 암호화 저장하도록 하여 보안성 향상에 도움을 주었다. 다양한 해킹기법으로 인해 개인정보 유출이 잦은 현재 사회적 환경에서, 클라우드 스토리지 보안은 해커의 공격으로부터 보다 안전하게 데이터를 지킬 수 있는 장점이 있다. 현재 구현한 프로그램의 파일 업로드다운로드 속도는 기존의 클라우드 스토리지 앱에 비해 약 2배정도 느린 속도이다. 속도가 느린 이유로는 암·복호화에 따른 속도 저하로, 암호화 폴더에 파일을 업로드, 다운로드하는 경우에만 속도 저하가 발생되었다. 하지만 암·복호화 속도가 느림에도 이 프로그램이 필요한 이유는 클라우드 스토리지에 저장되는

데이터가 민감한 경우, 노출 되었을 때 발생되는 2차 피해를 줄일 수 있기 때문이다. 향후 연구로는 프로그램 최적화를 통한 속도 개선으로 암호화 파일의 경우에도 충분한 속도가 나오도록 하고자 한다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행 되었음(2015-0-00930)

참고문헌

[1] 유요셉, 김기천, “클라우드 스토리지 전송단계에서의 보안성 강화를 위한 LPES 제안”, 한국통신학회 동계종합학술발표회, 505-506, (2017).
[2] 차영태, “클라우드 컴퓨팅 보안 기술동향과 산업전망”, 한국산업기술평가관리원, 12(6), (2012).
[3] 박상노, “클라우드 컴퓨티 서비스의 보안 전략 방안에 관한 연구”, 석사학위논문. (2013).
[4] T. Zhu, X. Zou, and J. Pan, “Query with SUM Aggregate Function on Encrypted Floating-Point Numbers in Cloud”, Journal of Information Processing System, 13(3), 573 - 589 (2017).
[5] 이재영, “협업을 위한 클라우드 스토리지에서의 사용자 인증과 데이터 보호에 관한 연구”, 한국디지털정책학회, 12(9), 153-158, (2014).
[6] 구동영, 윤현수, “클라우드 스토리지의 보안과 효율성, 그리고 개선 방향”, 한국정보과학회, 59-65, (2014).
[7] A. Buschettu, D. Sanna, G. Concas, and F. E. Pani, “A Platform based on Kanban to Build Taxonomies and Folksonomies for DMS and CSS”, Journal of Convergence, 6(1), (2015).
[8] N. Keegan, S. Y. Ji, A. Chaudhary, C. Concolato, B. Yu, D. H. Jeong, “A survey of cloud-based network intrusion detection analysis”, Human-centric Computing and Information Sciences, 6(19), (2016).