한국컴퓨터정보학회 하계학술대회 논문집 제21권 제2호 (2013. 7)

클라우드 데이터의 안전을 위한 가상 저장기술에 관한 연구

조재현[O], 이대성[*]
[O*]부산가톨릭대학교 컴퓨터공학과
e-mail:{jhcho,dslee}@cup.ac.kr

A Study on Virtual Storage Technology for the Safety of the Cloud Data

Jaehyun Cho[O], Daesung Lee[*]
[O*]Dept. of Computer Engineering, Catholic University of Pusan

● 요 약 ●

최근 클라우드 기술의 발전과 더불어 많은 기업들이 다양한 기업용 클라우드 서비스를 개발 및 보급하고 있지만, 많은 연구에서 클라우드 서비스 활성화의 저해요인으로 보안문제를 지적하고 있다. 클라우드 컴퓨팅 환경에서는 사용자의 데이터가 로컬 컴퓨터가 아닌 클라우드 서버에 저장되기 때문에 해킹을 당하거나 악의적인 공격자에 의해 유출될 경우 많은 피해가 우려된다. 본 연구는 해킹이나 악의적인 공격자에 의해 클라우드 서버에 저장되어 있는 데이터가 유출되더라도 그 데이터를 쉽게 읽지 못하도록 데이터를 저장하는 방법을 제시한다.

키워드: 클라우드 데이터(Cloud Data), 클라우드 스토리지(Cloud Storage), 데이터 보호(Data Protection)

I. 서 론

클라우드 컴퓨팅 분야는 2009년 이후로 가트너(Gartner)가 선정한 10대 전략기술로 꾸준히 등재되고 있을 만큼 서비스 개발 및 보급이 빠르게 진행되고 있으며, 최근 빅데이터(Big Data) 기술과 접목되면서 그 중요성이 더욱 커지고 있다[1]. 페이스북, 구글 등과 같은 대형벤더에서도 클라우드 기술을 활용하여 스마트기기와 같은 이기종 장치에서 사진, 동영상, 문서 등을 공유하고, 네트워크를 통해 대용량 데이터를 쉽고 빠르게 전송하는 서비스를 보급하고 있다. 이로 인해 전세계적으로 데이터 성장 발전과 함께 클라우드 스토리지 기술이 새로운 비즈니스 모델로 부각받고 있다[3][4].

이러한 클라우드 컴퓨팅은 IT 자원의 소유없이 일부 또는 전체를 아웃소싱하는 속성 때문에 보안문제로부터 자유롭지 못하다[2].

본 논문은 클라우드 컴퓨팅 환경에서 서버에 저장되어 있는 데이터의 안전한 보호를 위한 저장기술에 관한 연구로, 해킹이나 악의적인 공격자에 의해 데이터가 유출되더라도 그 데이터를 쉽게 읽지 못하도록 데이터를 분산 저장하는 방법을 그 특징으로 한다.

II. 관련 연구

클라우드 서비스는 사용자의 터미널에 IT 자원과 서비스를 직접 설치하지 않고 필요한 만큼 돈을 내고 빌려쓰는 새로운 형태의 컴퓨팅 패러다임으로, 사용자는 터미널의 성능과 무관하게 필요한 서비스만 선택하여 손쉽게 사용할 수 있다[5][6]. IT 자원의 일부 또는 전부를 빌려쓰는 클라우드 컴퓨팅의 근본적인 속성 때문에 보안문제가 항상 해결해야할 우선과제로 꼽히고 있으며[7], CSA(2010)에서는 컴퓨팅 남용 및 오용, 공유기술 취약점, 데이터 유실 및 유출 등 7가지를 클라우드 컴퓨팅 보안 위협으로 제시하였고[8], Gartner(2008)에서는 클라우드 컴퓨팅 보안 위협을 방지하기 위한 기술적 요구사항으로 기밀성과 데이터 암호화, 사용자 인증 등 7가지를 명시하였다[9]. 류준상(2010), 은성경 등(2009)은 클라우드 컴퓨팅을 플랫폼, 스토리지, 네트워크 및 단말기로 구분하여 각각에 필요한 보안 기술을 제시하였으며[10][11], 김태형 등(2012)은 클라우드 컴퓨팅의 데이터 및 시스템 보안기술을 논의한 바 있다[12].

III. 본 론

본 연구는 클라우드 서버에 존재하는 데이터를 악의적인 공격자나 해킹으로부터 안전하게 보호하기 위한 저장기술에 관한 내용으로, 데이터 저장 시에 [그림 1]과 같이 원본 데이터는 일정한 크기의 여러 조각으로 분할되어 각각 다른 영역에 저장된다.

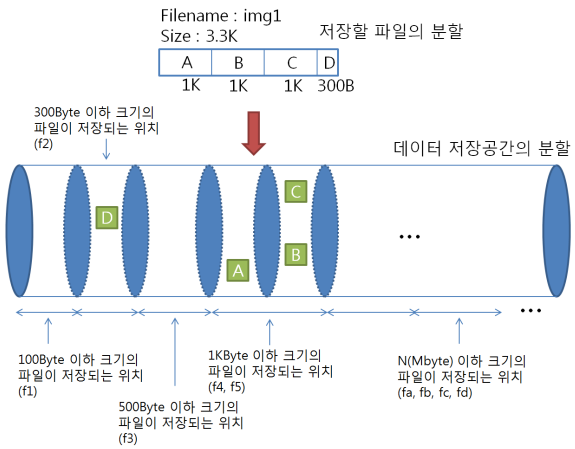

그림 1. 데이터 저장 구성도

예를 들어, 3.3K 크기의 파일을 1K 단위로 3개의 조각과 300Byte 단위의 1개의 조각으로 분할하고, 이 4개의 분할된 조각 데이터를 각각 다른 영역에 저장하는 것이다. 원본 데이터가 여러 조각으로 나뉘어 저장되기 때문에 각 저장위치에 대한 정보를 별도로 기입해야 할 필요가 있다.

[그림 2]는 원본 데이터가 어느 크기로 어느 위치에 저장되어 있는지에 관한 정보를 나타내는 StoreInfoEntry 자료구조이다. 이 StoreInfoEntry 자료구조는 원본 데이터에 대한 메타정보로써 실제 데이터 저장에 관한 모든 정보를 담고 있다.

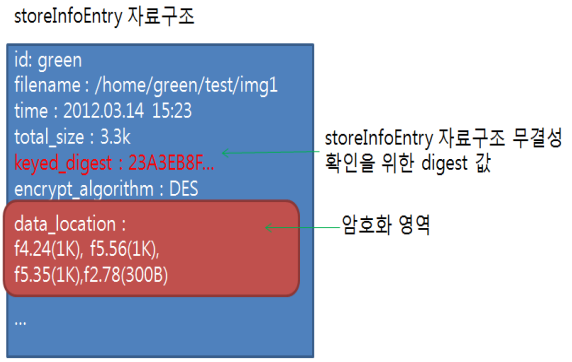

그림 2. StoreInfoEntry 자료구조 주요내용

자료구조 내용에 있어 keyed_digest 멤버는 StoreInfoEntry 정보 자체가 변경되지 않고 무결함을 나타내는 digest 값을 갖는다. 중요한 정보인 각 데이터의 위치 정보는 암호화되어 저장된다. 암호화에 사용되는 키는 OTP(One-Time Password)와 같은 널리 사용되는 방법을 응용하여 사용자 인증과정에서 사전에 공유된 키를 사용한다.

예를 들어, 사용자가 /home/green/test/img1 이라는 파일을 저장하려고 하면, 클라우드 저장 시스템은 먼저 이 파일에 대한 StoreInfoEntry 자료구조를 생성하고 1차 기록 가능한 정보를 기입한다. 중요한 정보인 데이터 저장 위치는 파일의 크기에 따라 일정 크기로 분할하여 저장하고 그 위치정보를 암호화 한다. 이때 암호화에 사용되는 키는 사용자 로그인 (인증) 과정에서 공유된 키를 사용한다.

이와 같은 저장기술에 있어서 파일별로 생성되는 StoreInfoEntry 자료구조가 많이 생성되기 때문에 검색을 위한 속도 개선이 필요하다. [그림 3]과 같이 사용자 계정, 계정 생성시간, 파일이름 등을 사용하여 해시(hash)하고 해시 테이블에 연결하여, 해당 파일(/home/green/test/img1)에 대한 StoreInfoEntry 자료구조를 시스템에서 검색하는 속도를 높이도록 한다.

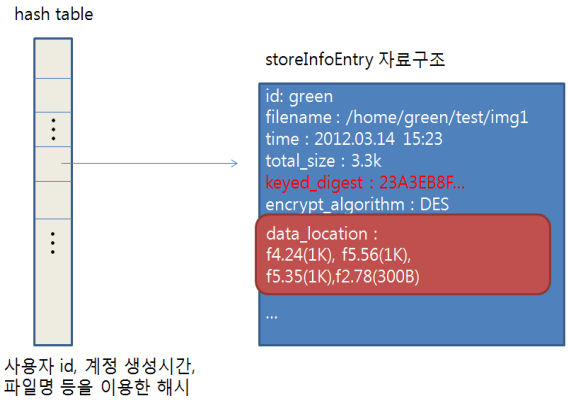

그림 3. 검색 속도 향상을 위한 해시 테이블 구성

IV. 결 론

본 연구는 클라우드 컴퓨팅 서비스 보급에 있어 가장 걸림돌이 되고 있는 보안문제를 해결하기 위한 방법의 한 예를 제시하고 있다. 특히, 악의적인 공격자나 해킹에 의해 데이터가 유출되더라도 그 내용을 쉽게 읽지 못하도록 하기 위해 데이터를 크기에 따라 영역별로 분산 저장하고, 그 저장위치를 암호화하여 기록함으로써 데이터 유출 시에도 원본 데이터에 쉽게 접근하지 못하도록 하였다.

향후 연구로는 파일별로 생성되는 StoreInfoEntry 자료구조 검색 속도를 더욱 개선하는 문제와 암호화에 따른 성능 문제를 해결하기 위한 경량 암호에 대한 연구가 필요할 것으로 판단된다.

참고문헌

[1] Gartner, "Gartner identifies the top 10 strategic technologies for 2011", http://www.gartner.com, 2010.

[2] Korea Communications Commission and Korea Internet Security Agency, "Information Security guide for Cloud Services", 2011.

[3] Jun-wei Ge, Yong-long Deng, Yi-qiu Fang, "Research on Storage Virtualization Structure in Cloud Storage Environment", Multimedia Technology(ICMT), IEEE Conference Publications, pp1-4, 2010.

[4] Steve Lesem. "Cloud Storage and The Innovator's Dilemma",

http://cloudstoragestrategy.com/cloud-ecosystem/, 2009.

[5] S.K.Eun, "Cloud Computing Security Technology Trends", Review of Korea Institute of Information Security and Cryptology, Vol.20, No.2, pp.27-31, 2010.

[6] Korea Communications Commission and Korea Internet Security Agency, "Information Security guide for Cloud Services", 2011.

[7] “Asia Pacific End-User Cloud Computing Security Survey", International Data Corporation, 2009.

[8] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0", 2010.

[9] Gartner, "Assessing the Security Risks of Cloud Computing", 2008.

[10] J.S.Ryu, "Cloud Computing as Green IT and Security Issues", The Graduate School of Computer Information Communications , Korea University, 2010.

[11] S.K.Eun, N.S.Cho, Y.H.Kim and D.S.Choi, "Cloud Computing Security Technology", Electronics and Telecommunications Trends, ETRI, Vol.24, No.4, pp.79-88, 2009.

[12] T.H.Kim, I.H.Kim, C.W.Min and Y.I.Eom, "Security Technology Trend in Cloud Computing", Korea Information Science Society Review, Vol.30, No.1, pp.30-38, 2012.