클라우드에서 소유권 증명과 무결성 검증이 결합된 기법에 대한 분석†

김동이*, 박효민*, 신상욱**
*부경대학교 대학원 정보보호학협동과정
*부경대학교 IT융합응용공학과
e-mail: nucea44@gmail.com

Analysis of the combined technique with proofs of ownership and verification of integrity in cloud

Dong-ee Kim*, Hyo-min Park*, Sang Uk Shin**
*Interdisciplinary Program of Information Security, Pukyong National University
**Dept of IT Convergence and Application Eng., Pukyong University

요 약

클라우드 컴퓨팅 환경에서 사용자 관점에서는 아웃소싱한 데이터의 기밀성 및 무결성을, 클라우드 제공자 입장에서는 저장 공간 및 대역폭 효율을 모두 제공하는 것이 필요하다. 본 논문에서는 이를 동시에 만족시키기 위해 아웃소싱된 데이터의 중복 제거 기법과 클라우드 스토리지에 저장된 데이터 파일의 무결성 검증 기법이 결합된 기법에 대해 분석한다.

1. 서론

통신 기술의 발전으로 인한 인터넷의 고속화로 클라우드 컴퓨팅의 수요가 증가하고 있다. 이로 인해 클라우드 스토리지에 저장되는 데이터의 양 또한 증가하게 되었다. 결국 클라우드 스토리지 제공업체(CSP)는 효율적인 데이터 관리 방법이 필요하게 되었다.

데이터의 관리 방법 중 중복 제거는 저장된 데이터의 중복을 제거하여 저장 공간의 효율성을 증대하는 방법이다. 중복 제거 방법에서 중복을 제거하는 주체에 따라서 서버 측 중복 제거와 클라이언트 측 중복 제거 방법이 있다. 서버 측 중복 제거 방법에서는 클라이언트는 모든 파일을 업로드하고, 서버에서 중복된 데이터를 제거하는 방식이다. 반면에 클라이언트 측 중복 제거 방법은 클라이언트가 파일의 업로드 전에 서버에 중복된 데이터가 있는지 확인하여 업로드하는 방식이다. 클라이언트 측 중복 제거 방법은 중복된 데이터를 업로드 하지 않아 통신 대역폭 면에서 장점을 가진다. 하지만, 클라이언트 측 중복 제거 방법의 단점은 클라우드에 저장된 데이터의 인가되지 않은 사용자의 파일 접근을 막기 위해 소유권 증명 기법(PoW(Proofs of Ownership)[1])이 필요하다.

또 다른 데이터 관리 방법 중 하나인 무결성 검증은 사용자가 아웃소싱한 파일은 CSP가 데이터 파일을 임의로 삭제 및 변조하여도 클라이언트가 가시적으로 확인할 수 없기 때문에 저장된 파일을 클라이언트나 TPA(Third Party Auditor)를 통해 주기적으로 무결성을 검증 하는 기법이다. 무결성 검증의 기법 중 서버의 데이터 소유를 확인하는 PDP(Provable Data Possession)[2]와 무결성 검증과 손상된 데이터의 복구가 가능한 POR(Proofs of Retrievability)[3]이 대표적이다.

위의 두 기법은 클라우드 스토리지의 효율성 및 신뢰를 증가 시킨다. 이를 한 번에 처리하기 위해서는 소유권 증명과 무결성 검증의 결합이 필요하다. 본 논문에서는 무결성 검증과 중복 제거가 결합된 기존의 기법을 살펴보고, 소유권 증명과 무결성 검증 기법이 결합한 기법의 요구 사항에 대해 분석한다.

2. 관련 연구

2.1 PoW와 PDP/POR

소유권 증명(PoW)은 클라우드에 저장된 파일에 대해 적합한 권한을 가진 사용자인지 판단하기 위한 기법이다. 사용자가 서버에 저장된 데이터의 다운로드 요청 시 서버는 데이터에 대한 소유권이 있는지 확인하기 위해 챌린지를 클라이언트에게 전송하고, 사용자는 그에 대응하는 리스폰스을 제공하여 데이터의 소유권을 검증하는 기법이다. Merkle 트리를 이용한 기법이 대표적이다.

무결성 검증을 위한 기법 중 PDP와 POR이 대표적이다. 두 기법의 차이점은 PDP[2]는 서버의 파일의 소유 유

†본 논문은 ETRI 주요사업의 지원을 받아 수행된 연구임. (15ZS1500)

무를 판단하지만, POR[3]는 파일의 무결성 검증과 손상된 파일에 대한 복구가 가능하다. 일반적으로 클라이언트나 TPA(Third Party Auditor)가 챌린지를 서버에 보내면, 서버가 그에 대응하는 리스폰스을 제공하여 데이터의 무결성을 검증하는 기법이다.

2.2 중복 제거와 무결성 검증을 결합한 기법

중복 제거와 무결성 검증이 결합된 기법은 다음과 같은 안전성 요구 사항을 만족해야 한다.

- 공공 검증 가능성 : TPA는 클라이언트와 관련된 정보와 전체 파일의 복구 없이 아웃소스된 데이터의 정확성과 유효성을 검증할 수 있다.
- 스토리지의 정확성 : CSP는 유저의 데이터를 실제로 가지고 있을 때 TPA의 검증을 통과할 수 있다.
- 프라이버시 : 감사 중에 TPA에게 아웃소스된 데이터에 대한 정보 유출이 없어야 한다. 또한, 중복 제거 정보를 제외하고는 CSP에게 데이터 자체의 유출이 없어야 한다. 사용자의 신원 또한 중복 제거 시에 드러나서는 안된다.
- 안전한 중복 제거 : 중복 제거 정보를 제외하고는 CSP에게 어떠한 정보도 유출되지 않아야 한다.

두 가지 기법을 모두 제공하는 기존 연구들 중에서 대표적인 두 가지 기법으로 PoOR과 POSD 기법이 있다. 먼저 Du 등[4]에 의해 제안된 PoOR은 Merkle 트리를 이용한 데이터의 소유권 증명, 동형 검증 태그와 소거 코드를 이용하여 데이터의 무결성 검증을 결합한 기법이다. 또한 Zheng and Xu 등[5]에 의해 제안된 POSD는 페어링 연산을 사용하여 자주 변화하는 데이터에 대해서도 무결성 검증이 가능한 서버 측 중복 제거 기법이다.

3. 기존 결합 기법의 분석

이 절에서는 위에서 언급한 대표적인 두 가지 기법이 가지고 있는 문제점을 간단히 분석한다. 먼저 PoOR[4] 기법은 해시 값을 이용하여 서버에 같은 파일 이 저장되어 있는지 확인하는 클라이언트 측 중복 제거 방법을 사용한다. 또한 Merkle 트리의 루트 노드의 비교를 통해서 소유권 증명한다. 하지만 루트 노드는 데이터 변경 시에 루트 노드의 값이 변경되어, 데이터 변경될 때마다 지속적으로 트리의 업데이트가 필요하기 때문에 효율성이 떨어진다. 또한 파일의 업로드 시에 평문 형태의 파일을 그대로 서버에 업로드하기 때문에 CSP에 대한 데이터 프라이버시 유출의 문제가 있다.

또한 POSD[5] 기법 역시 파일의 업로드 시에 평문 형태의 파일을 서버에 업로드하여 데이터 프라이버시의 문제가 있으며, 서버 측 중복 제거 방법을 사용하기 때문에 대역폭의 효율성에서 단점이 있다. 또한, 소유권 증명과 무결성 검증에 대해 같은 태그 값을 사용하므로, 소유권 증명과 무결성 검증을 위한 챌린지 값이 같을 경우 동일한 리스폰스가 생성되게 된다. 이를 악용하기 위해 악의적인 사용자가 소유권 증명을 위해 서버로부터 받은 챌리지를 무결성 검증을 위한 챌린지로 속여서 서버에게 전송한다면, 서버는 무결성 검증을 위한 리스폰스를 악의적인 사용자에게 반환하고, 이를 통해 악의적인 사용자는 소유권 증명을 통과할 수 있게 된다. 이는 스토리지 정확성의 측면에서 안전성을 만족시키지 못한다.

따라서 중복 제거와 무결성 검증을 모두 제공하는 기법은 기본적으로 프라이버시 보장을 위해 암호 데이터에 대한 중복 제거와 무결성 검증을 제공할 수 있어야 하며, 또한 대역폭의 효율성을 위해 클라이언트 측 중복 제거를 해야 한다. 그리고, 소유권 검증과 무결성 검증을 위한 두 프로토콜의 결합에 대해 재전송이나 interleaving 공격 등에 대해 안전하도록 설계되어야 하며, 두 가지 인증 태그 계산은 단순 결합 기법에 비해 효율적이어야 한다.

4. 결론

클라우드에 아웃소싱된 파일을 관리하기 위해서는 안전한 데이터 관리 방법이 요구되며, 이를 위해 중복 제거와 무결성 검증 기법의 결합이 필요하다. 기존의 대표적인 두 가지 기법의 분석 결과, 중복 제거 방법에서 대역폭의 효율적 사용이라는 이점을 제공하는 클라이언트 측 중복 제거 방법이 제공되어야 하며, 소유권 증명과 무결성 검증의 두 가지 프로토콜을 위한 인증 태그 계산을 효율적으로 해야 한다. 또한 두 기법이 결합되었을 때, 공공 검증, 스토리지의 정확성, 프라이버시, 안전한 중복 제거의 요건을 만족 시켜야 한다.

참고문헌

[1] Halevi, Shai, et al. "Proofs of ownership in remote storage systems." Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011.

[2] Ateniese, Giuseppe, et al. "Provable data possession at untrusted stores." Proceedings of the 14th ACM conference on Computer and communications security. Acm, 2007.

[3] Juels, Ari, and Burton S. Kaliski Jr. "PORs: Proofs of retrievability for large files." Proceedings of the 14th ACM conference on Computer and communications security. Acm, 2007.

[4] Du, Ruiying, et al. "Proofs of Ownership and Retrievability in Cloud Storage." 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2014.

[5] Zheng, Qingji, and Shouhuai Xu. "Secure and efficient proof of storage with deduplication." Proceedings of the second ACM conference on Data and Application Security and Privacy. ACM, 2012.