클라우드 스토리지의 보안과 효율성, 그리고 개선 방향

한국과학기술원 ▌구동영 · 윤현수*

1. 서 론

클라우드 컴퓨팅에서는 이용자들의 정보가 인터넷상의 서버에 저장되고 처리되며, 필요한 경우에 한하여 자신의 데이터를 잠시 로컬 머신에 다운로드하여 저장하고 접근하게 된다. 다시 말하면, 구름(cloud)으로 표현되는 추상화된 인터넷상의 서버로부터 하드웨어, 소프트웨어, 네트워크 등의 컴퓨팅 자원을 필요한 만큼 빌려 이용하고 이에 대한 사용요금을 지불하는 컴퓨팅 서비스라 할 수 있는데, 모든 데이터가 인터넷상에서 저장, 처리, 및 관리되는 IT 자원의 주문형 아웃소싱 서비스로 볼 수 있다. 현재 클라우드 컴퓨팅 서비스는 아마존 웹 서비스, 구글, 마이크로소프트 등의 글로벌 IT 기업에 의하여 주도적으로 제공되고 있으며, 전세계 수많은 서비스 제공자에 의하여 다양한 클라우드 컴퓨팅 서비스가 활발히 개발되어 제공되고 있다.

클라우드 컴퓨팅 서비스를 이용함으로써 이용자들은 자신의 로컬 머신에 데이터를 저장함으로써 발생 가능한 하드웨어 및 소프트웨어 장애 등에 의한 데이터 손실의 위험 부담을 줄일 수 있을 뿐 아니라, 저장 공간의 제약에서 벗어나 필요한 만큼의 자원을 서비스 형태로 신속하게 이용할 수 있기 때문에 장비의 구매에서부터 환경 설정 및 관리에 소요되는 유지관리 비용을 절감할 수 있다는 장점이 있다. 또한 무선통신 기술의 발전과 스마트기기의 대중화와 더불어 개별 이용자는 데스크톱, 노트북, 스마트폰 등의 다양한 단말을 이용하게 되면서, 데이터를 기기에 따라 별도로 관리하지 않더라도 인터넷에 연결되어 있으면 언제, 어디서나, 손쉽게 클라우드에 접근하여 원하는 데이터를 이용하고 일관성 있게 관리할 수 있다는 특징이 있다.

* 종신회원

† 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2011-0016584).

개인의 DNA 데이터를 온라인으로 제출하고 그 결과를 온라인에서 받아볼 수 있는 시대를 가능하게 하는 클라우드 컴퓨팅 서비스를 구성하는 가장 기본적인 부분은 바로 클라우드 스토리지라고 할 수 있는데, 모든 데이터가 클라우드 상에서 처리되고 저장되기 때문에 이러한 데이터의 관리에 대한 관심이 집중되고 있다. 빅데이터의 개념이 도입되면서 인터넷상에 존재하는 수많은 데이터를 보다 효율적으로 처리하기 위한 노력이 다방면으로 이루어지고 있는데, 클라우드 서비스 제공자들 또한 자신의 서비스 경쟁력 강화를 위하여 클라우드에 중복되어 저장되는 데이터로부터 발생하는 자원 관리의 비효율성을 극복하고자 데이터 중복 제거 기술을 적극 도입하고 있다.

본 고에서는 클라우드 스토리지의 효율성 향상을 위한 데이터 중복 제거 기술의 동향 및 데이터 프라이버시 향상을 위한 암호화 접목 기술에 대하여 살펴보고 향후 지속적인 클라우드 스토리지 시장의 활성화를 위하여 해결해야할 개선 방향에 대하여 살펴보도록 한다. 제 2장에서 클라우드 스토리지의 실상과 효율성 향상을 위한 데이터 중복 제거 기술에 대하여 언급한다. 제 3장에서는 점차 강조되는 보안 이슈를 해결하기 위한 암호학적 접근 동향을 정리하고, 제 4장에서 클라우드 스토리지 서비스의 향후 개선 방향에 대하여 살펴본다. 제 5장에서는 본 고를 요약하면서 마무리하도록 한다.

2. 클라우드 스토리지의 실상

클라우드 스토리지라 하면 CDN 또는 파일 호스팅이 생각날 정도로 기본 개념이 비즈니스적으로 왜곡되어 있다. 이는 서비스 제공자들이 클라우드 스토리지의 근본 취지보다는 다수의 고객 확보를 통한 수익성 향상을 최우선시하면서 최종적으로 고객에게 보여지는 서비스 상품의 다양성 및 제공 서비스의 품질에만 관심이 있기 때문이다. 클라우드 스토리지의 실상을

클라우드 스토리지 서비스의 목적 및 서비스 제공자의 측면에서 살펴보도록 한다.

• **저장(Online storage)**

클라우드 서비스에서 데이터에 대한 가공이 이루어지기 위해서는 대상이 되는 데이터가 저장되어야 하며, 클라우드 스토리지는 가공을 위한 일시적인 저장과 더불어 개별 데이터 저장소로서의 기능을 수행한다.

• **공유(Data sharing)**

클라우드 스토리지에 저장된 데이터는 다수의 이용자에 의하여 공유될 수 있으며 다양한 클라우드 응용 기술에 적용되기 위하여 공유될 수 있다.

• **협업(Collaboration)**

동일한 목적을 지닌 이용자 집단에 의하여 개발 등의 특정 업무를 수행하기 위한 협업시스템으로서 클라우드 스토리지가 활용될 수 있다.

범용 스토리지 기능을 제공하는 클라우드 스토리지 서비스로는 드롭박스(Dropbox), 구글드라이브(Google-Drive), 왈라(Wuala), 모지(Mozy), 스카이드라이브(Sky-Drive), 박스(Box) 등이 있다. 이들은 로컬 머신과의 동기화, 클라우드 응용 기능, 보안 모듈 제공 등의 특징을 지니고 있으며, 무료 저장 공간의 제공 및 서비스 편의성을 통해 많은 이용자를 보유하고 시장에서 서비스 기반을 확보한 대표적인 서비스이지만 데이터 유출을 비롯한 다양한 사고 사례에서 보여지듯 효율성과 안전성이 미흡하여 이에 대한 개선이 절실히 필요하며 지속적인 보완이 이루어져야 할 것이다.

2.1 클라우드 스토리지의 효율성 향상

클라우드 서비스 제공자는 동일한 자원으로 더욱 많은 이용자에게 양질의 서비스를 제공하기 위하여 자원의 낭비를 최소화하고자 한다. 이를 위하여 데이터 중복 제거 기술을 적용하는 서비스 제공자가 늘어나고 있다. 데이터 중복 제거는 데이터를 레퍼런스 포인터(reference pointer)로 변환하는 방법으로 클라우드 스토리지 상의 중복된 데이터를 제거하고 하나의 사본만을 저장하여 동일한 데이터를 소유한 이용자들이 레퍼런스 포인터를 이용하여 자신이 아웃소싱한 데이터에 접근할 수 있게 함으로써, 저장되는 데이터의 양을 축소하기 위하여 각광받고 있는 기술이다.

• **저장 공간(Storage space)**

클라우드 스토리지 서비스의 이용이 증가함에 따라 다수의 독립적인 이용자들이 동일한 데이터를 소유하고 이를 클라우드 스토리지에 아웃소싱하는 경우가 증가하고 있으며, 서비스 제공자는 데이터 중복 제거 기술을 적용하여 클라우드 스토리지 상에서의 저장 공간을 효율적으로 관리하고자 한다.

• **네트워크 대역폭(Network bandwidth)**

동일한 데이터가 클라우드에 이미 존재할 때 중복된 데이터를 다시 아웃소싱하지 않게 되면, 해당 데이터 소유자는 업로드 과정에서 소요되는 비용을 줄일 수 있고, 서비스 제공자는 가용한 대역폭의 절약을 통하여 네트워크를 통하여 효율적으로 전송할 수 있는 정보의 양을 늘려줌으로써 네트워크 혼잡을 회피하고 이용자들에게 보다 빠른 응답을 가능하게 한다.

2.2 데이터 중복 제거의 분류

유일한 데이터를 단 한번만 저장할 수 있도록 하는 데이터 백업의 혁신적인 기술로서, 데이터 중복 제거 기술은 클라우드와 같은 분산 환경에서의 백업을 효율적으로 수행할 수 있게 한다. 이와 같은 데이터 중복 제거 기술의 핵심 구성요소는 1999년 Rocksoft사가 처음으로 특허 출원한 이래 지속적으로 다양한 분야에 적용되어 왔는데, 클라우드 스토리지에서의 데이터 중복 제거는 수행 주체 및 대상 등 다양한 기준에 따라 분류될 수 있다[5].

• **주체에 따른 분류**

데이터 중복 제거의 수행 주체에 따라 서비스 제공자 기반 또는 데이터 소유자 기반으로 구분될 수 있다. 데이터 소유자 기반의 중복 제거는 데이터 소유자가 자신의 데이터를 아웃소싱하기 전에 데이터의 해시값을 구하여 클라우드 스토리지에 이미 동일한 데이터가 저장되어 있는지를 확인한다. 클라우드 서비스 제공자는 저장된 데이터에 대한 해시값을 해시 저장소로부터 검사하고 해시값이 이미 저장되어 있으면 대응되는 데이터 또한 데이터 저장소에 존재하는 것으로 간주하여 그림 1과 같이 데이터 소유자에게 실질적인 데이터 업로드 요청을 보내지 않고 추후에 해당 데이터에 대한 접근 권한을 제공한다. 중복 데이터의 업로드를 미연에 차단함으로써 네트워크 대역폭을 절감할 수 있다는 장점이 있지만, 클라우드에 존재하는 데이터를 공격자가 미리 파악하는 식별 공격(identification attack)이 가능하다.

그림 2와 같이 서비스 제공자에 의한 데이터 중복 제거에서는 데이터 소유자가 클라우드 스토리지에 동일한 데이터가 존재하는지 확인할 수 없기 때문에 외부 공격자에 의한 식별 공격으로부터 안전하다. 데이터

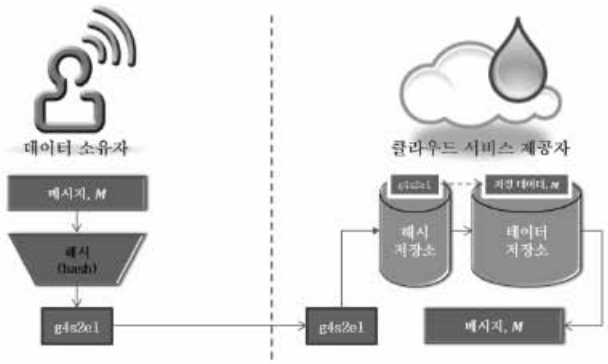

그림 1 데이터 소유자에 의한 중복 제거

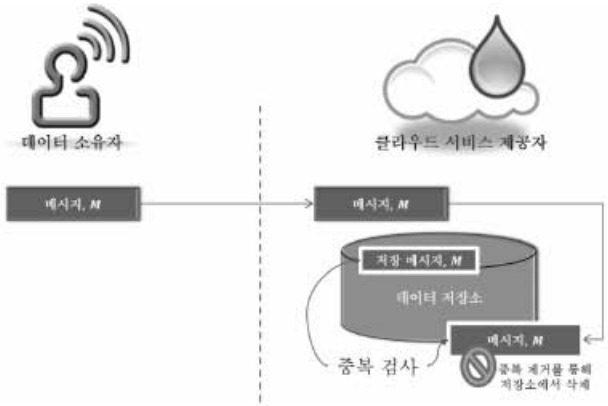

그림 2 서비스 제공자에 의한 중복 제거

소유자는 중복 여부에 상관없이 자신의 데이터를 클라우드에 아웃소싱하고 클라우드 서비스 제공자는 자신이 관리하는 데이터 저장소에서 중복 제거를 수행하게 된다. 하지만 중복 제거가 실시간에 이루어지기 어렵고 백그라운드에서 항상 데이터의 중복성을 검사해야하기 때문에 디스크 I/O, 전력 소모 등에서 자원의 추가적인 소요가 이루어지며 중복된 데이터의 업로드로 인한 네트워크 대역폭의 낭비가 심하다는 문제점이 있다.

• 대상에 따른 분류

중복 제거의 대상에 따른 분류로는 블록 수준과 파일 수준으로 구분된다. 그림 3의 블록 수준에서의 데이터 중복 제거에서는 단일 파일을 동일한 크기의 여러 블록으로 분할하고 각각의 블록에 대하여 데이터 중복여부를 판단하는 것으로 중복 제거의 대상 크기가 작아 섬세한 중복성 체크가 가능하기 때문에 보다 많은 공간 확보에 용이하다는 장점이 있지만, 중복 제거 대상의 수가 많아져 클라우드 스토리지 전반에 걸친 중복성 체크에 많은 비용이 소요된다는 단점이 있다. 반면 파일 수준에서의 데이터 중복 제거는 단일 파일에 대하여 중복 제거를 수행하기 때문에 블록 수준에

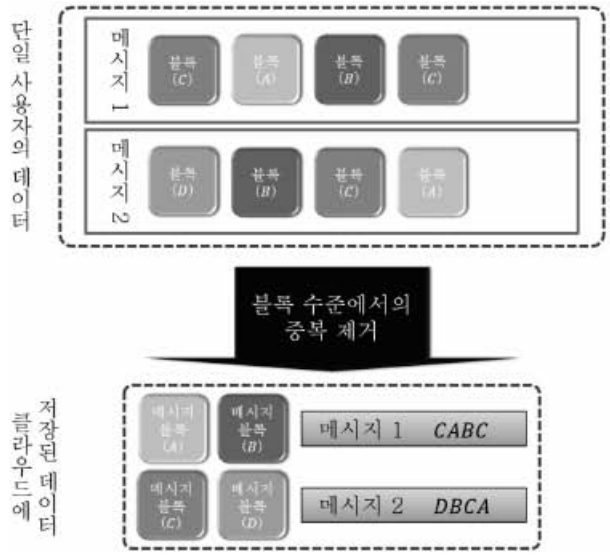

그림 3 블록 수준에서의 중복 제거

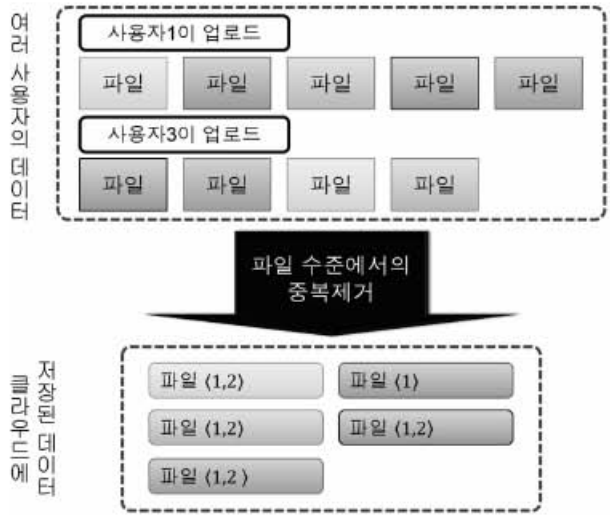

그림 4 파일 수준에서의 중복 제거

비하여 신속한 중복성 체크가 가능하지만 파일의 아주 미세한 변화에 대해서도 파일 전체가 동일시 되지 않아 블록 수준에 비하여 중복 데이터에 의한 저장 공간의 절약 효과는 상대적으로 적은 편이다.

이외에도 데이터 소유자의 범위에 따라 개인 이용자 및 다중 이용자 수준에서의 데이터 중복 제거 등으로 구분될 수도 있으나, 현재 서비스 중인 대부분의 기술은 평문에 대하여 적용되고 있으며 이에 대해서는 다중 이용자 수준에서 중복 제거 기술이 적용되고 있는 상황이다.

3. 클라우드 스토리지 보안의 이해

클라우드 컴퓨팅 서비스의 경우, 이용자들의 데이터

가 클라우드 상에 집중되면서 데이터 유출의 피해 또한 유래없이 심각해질 수 있는 만큼 공격자들의 타깃이 될 확률 또한 증가한다. 기존의 보안은 레거시 시스템의 구조에 따라 다양한 제품들을 추가함으로써 시스템을 보호하였으나, 클라우드 상에는 아직 알려지지 않은 취약점들이 존재하며 클라우드를 구성하는 다수의 이기종 서버 간 충돌 및 중복 기능을 제거한 효율적인 보안 솔루션이 제시되지 못하고 있다[4].

eWeek에 의하면 클라우드 스토리지 서비스 이용자의 41%가 클라우드 서비스 제공자에게 정보보호의 책임이 있다고 생각하며, 일부 서비스 제공자들이 과중한 부담으로 책임을 서로 떠넘기는 상황이 많이 발생했으며, 57%의 서비스 제공자가 보안에 책임이 있다고 생각하였다[1,2]. 또한 2012년 4월, Infosec Europe 행사 간 진행된 클라우드 스토리지 위협과 관련된 Sophos poiled conference 참석자들의 64%가 클라우드 스토리지에 보안위협이 있다고 응답했으며, 45%는 이러한 보안위협에도 불구하고 계속 사용하고 있다고 응답하였다[3].

3.1 클라우드 스토리지 보안을 위한 데이터 중복 제거 기술 동향

경제성을 중요시하는 비즈니스 측면에서 자원의 효율적인 활용에 편중된 서비스 제공자들은 데이터 중복 제거 기술을 적용하면서 발생하는 보안 문제에 상대적으로 소홀하였으며, 최근 정보 유출 사고가 빈번히 발생함에 따라 암호화를 적용함으로써 데이터의 프라이버시 보장을 꾀하고 있다. 하지만 대다수의 암호화는 서비스 제공자에 의하여 이루어져 관리되고 있는데, 이용자 계정 정보의 유출 또는 내부 공격자로부터의 위협에는 여전히 취약하다. 클라우드 서비스 제공자가 직접 암호화를 수행하기 때문에 이용자 계정에 접근 가능한 공격자는 해당 이용자가 아웃소싱한 데이터에 대한 평문에 접근이 가능할 뿐 아니라 클라우드 서비스의 내부 공격자는 복호화키를 직접 획득함으로써 권한 없는 데이터에 대한 임의 열람이 가능해지기 때문이다.

데이터 중복 제거 기술의 적용은 동일한 데이터를 소유한 이용자들에 의하여 자율적으로 데이터를 공유하는 것이 아니라, 서비스 제공자의 자원 효율성 향상을 위하여 이용자들의 의지와 상관없이 수행되므로 데이터의 프라이버시를 보장받기 위해서는 이용자가 먼저 암호화를 수행하고 생성된 암호문만을 클라우드 스토리지에 아웃소싱함으로써 암호문이 불의의 사고에 의하여 노출되더라도 암호문에 사용된 키의 접근을 차단함으로써 공격자에 의한 평문으로의 접근을 방지하도록 해야 하는 것이다.

- **해시 트리를 활용한 소유권 증명에 의한 데이터 중복 제거**

2011년에는 Halevi 등에 의하여 신뢰할 수 있는 클라우드 서비스 제공자 기반의 안전한 데이터 중복 제거 기술이 제안되었다[8]. 이는 그림 5에서와 같이 2007년

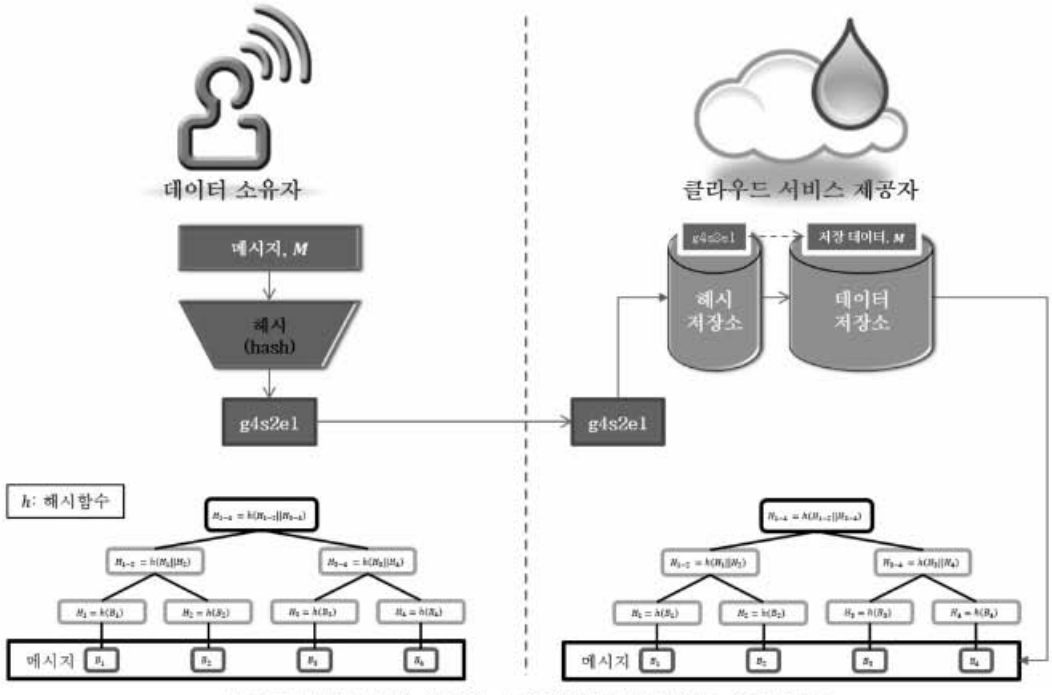

그림 5 해시트리를 이용한 소유권 증명 및 데이터 중복 제거

에 제시된 PoR(Proof of Retrievability)[6] 및 PDP (Provable Data Possession)[7] 기법에서 제시되었던 해시 트리를 이용하고 있다. PoR 및 PDP는 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.

데이터 소유자 및 클라우드 서비스 제공자는 검증하고자 하는 데이터를 일정 크기의 블록으로 분할하고 각각의 블록의 해시값을 전체 트리의 리프 노드(leaf node)로 할당한다. 이후 인접한 두 노드의 값을 연결하여 다시 해시값을 계산함으로써 두 노드의 부모 노드를 생성하는데, 이러한 과정을 반복함으로써 하나의 완성된 트리를 형성하게 된다. 중복된 데이터를 소유한 경우에는 동일한 해시 트리를 생성할 수 있기 때문에 해시 트리 상의 임의 노드에 대한 질의-응답을 통하여 높은 확률로 중복 데이터를 소유하고 있다고 주장하는 이용자의 진위를 판단할 수 있게 된다.

하지만 클라우드 스토리지에 평문이 저장되기 때문에 외부 공격 및 예상치 못한 서비스 오동작으로부터 민감한 데이터를 안전하게 보호하지 못하여 이후에는 암호화를 적용한 개선 방안이 연구되고 있다.

• 암호화 키를 공유하는 데이터 중복 제거

Ng 등은 평문에 대한 소유권 검증을 수행하고 실제로는 암호문을 아웃소싱하는 최초의 다중 사용자에 대한 파일 기반의 데이터 소유자에 의한 데이터 중복 제거를 제시하였으나, 검증에 사용한 평문과 실제 업로드한 암호문 사이의 연관성을 증명하지 못하여 악의적인 데이터 소유자에 의한 공격에 취약하다는 단점이 있었다[9]. 이후의 연구는 데이터 소유자가 먼저 암호화를 수행한 후에 클라우드에는 암호문을 업로드하고 이에 대한 소유권 증명을 수행하는 방안이 제시되었는데, 이들은 모두 처음 데이터를 아웃소싱한 데이터 소유자가 지정한 암호화 키를 이후에 중복 데이터를 아웃소싱하고자 하는 데이터 소유자들이 유도해내도록 강제하는 방법을 제시하고 있다.

- 해시 트리에 기반한 암호문에 대한 데이터 중복 제거

Xu 등은 자신이 고안한 해시함수를 이용하여 해시 트리를 생성하기에 충분히 큰 해시값을 얻을 수 있도

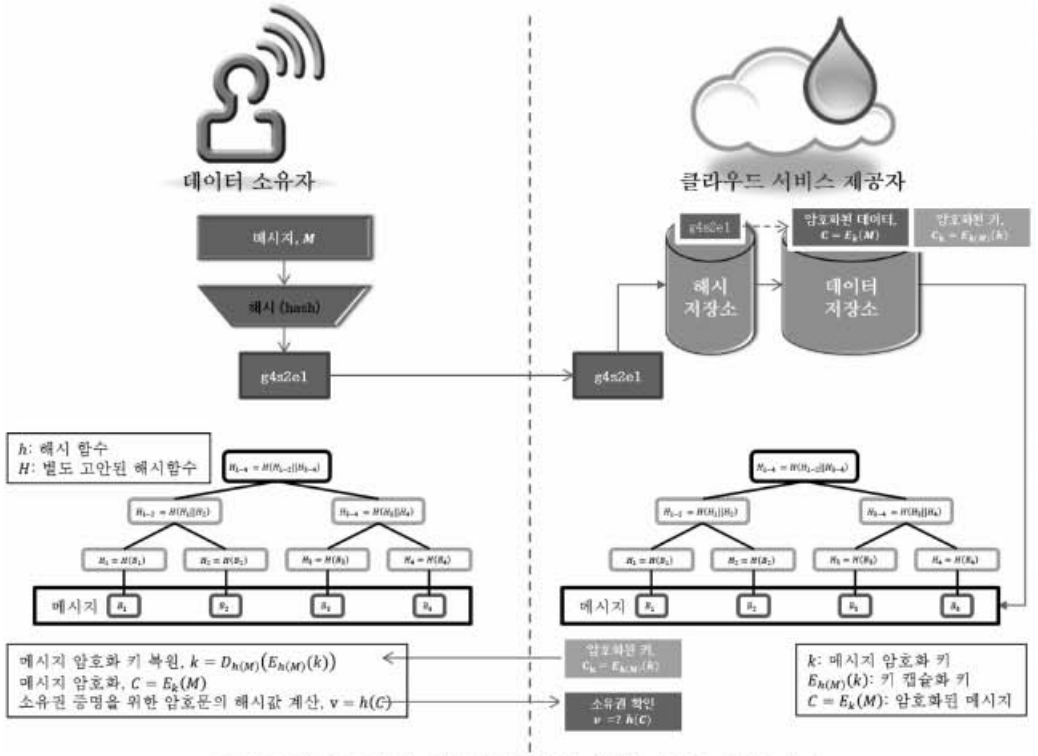

그림 6 해시 트리에 기반한 암호문에 대한 데이터 중복 제거

록 하였으며, 이로부터 해시 트리를 생성하여 소유권 증명을 수행하고 있다[10]. 소유권 증명 과정에서는 이와 같은 평문에서의 해시 트리를 이용한 증명과 더불어 그림 6과 같이 일차적인 증명을 통과한 데이터 소유자에게는, 평문의 해시값을 암호화 키로 하여 암호화된 실제 아웃소싱된 암호문에 대한 암호화 키를 전달함으로써 동일한 암호문을 생성할 수 있도록 한다. 키-캡슐화-키를 이용하여 아웃소싱된 데이터와 동일한 암호문을 생성한 데이터 소유자는 암호문의 해시값을 전달함으로써 중복 데이터의 진정한 소유자임을 증명하고 데이터 아웃소싱 과정을 종료한다.

• 수렴 암호화 기법을 활용한 데이터 중복 제거

수렴 암호화 기법은 메시지에 대한 해시값을 암호화의 키로 이용함으로써 별도의 사전 키 공유를 필요로 하지 않는 암호화 기법을 의미한다. 따라서, 독립적인 클라우드 스토리지 이용자는 사전에 합의된 키를 유도해낼 필요 없이 자신이 소유한 메시지로부터 유도된 해시값을 이용하여 암호문을 생성할 수 있게 된다. Bellare 등은 이러한 수렴 암호화 기법을 일반화하여 데이터 중복 제거 기술에 적용할 수 있는 방안을 제시하였다[11].

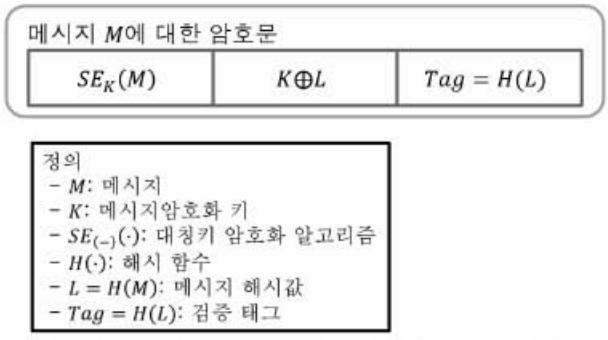

그림 7 수렴 암호화 기법을 활용한 데이터 중복 제거

현재까지 제안된 데이터 소유자에 의한 암호문에 대한 중복 제거 기술은 모두 데이터 소유자가 동일한 암호화 키를 공유하는 방법으로 데이터의 갱신 또는 삭제 등에 의하여 데이터 소유자의 집합이 변경되는 경우에는 암호문에 대한 키 노출 및 이로 인한 민감한 데이터의 유출 가능성이 존재한다.

4. 클라우드 스토리지의 데이터 중복 제거 기술의 한계 및 개선 방향

클라우드 스토리지의 효율성 증대 및 보안성 향상을 위하여 산업계 및 학계에서 지속적인 연구개발이 이루어지고 있지만, 안전성에 대한 신뢰를 통하여 민감한 정보의 아웃소싱을 이끌어내기에는 해결해야 할 문제가 많이 있다. 본 장에서는 클라우드 스토리지의 특징 및 개선이 필요한 사항에 대하여 살펴본다.

• 민감한 데이터의 기밀성

앞 절에서 언급한 암호화를 통한 데이터 중복 제거 기술 동향에서는 아웃소싱된 민감한 평문에 대한 접근을 방지함으로써 데이터 프라이버시를 보장하고 저장 공간 및 대역폭의 절감을 통한 자원의 효율성 증대를 위한 연구를 소개하였으나, 데이터 소유자에 의한 중복 제거에 기반하고 있으므로 특정 데이터가 클라우드 스토리지에 존재하는지를 공격자가 여전히 확인할 수 있다. 이를 보완하기 위하여 서비스 제공자에 의한 중복 제거에 기반한 암호문을 지원하는 데이터 중복 제거 기술에 대한 연구가 수행될 필요가 있다.

• 효율적인 키 관리

현재까지 제안된 데이터 소유자에 의한 암호문에 대한 데이터 중복 제거 기술은 최초로 데이터를 아웃소싱한 이용자들에 의해 암호화 키가 결정되고, 추후의 중복 데이터를 업로드하고자 하는 데이터 소유자는 사전에 결정된 키를 유도해내도록 한다. 이는 최초로 데이터를 아웃소싱한 데이터 소유자가 아닌 경우에는 업로드하는 데이터의 개수에 비례하는 키를 유도해내어 별도로 관리해야 하기 때문에 동일한 데이터를 소유한 이용자라 하더라도 아웃소싱의 순서에 따라 효율적인 키 관리가 어려워질 가능성이 농후하다. 따라서 개별 이용자들은 데이터의 아웃소싱 순서에 구애받지 않고 스스로 키를 선택하여 관리할 수 있는 체계적인 방안이 필요하다.

• 데이터의 실시간 갱신 및 처리

클라우드 스토리지 서비스에서는 실시간 동기화를 통하여 이용자들의 데이터가 갱신되는 경우, 암호문에 대한 변경이 어려운 문제가 있다. 새로운 암호문을 생성하여 재업로드하는 방법은 중복 제거에 의한 자원 절약 효과를 반감시키므로 암호문에 대한 직접적인 변경이 용이하고 암호문을 복호화하지 않고도 암호문 간의 연산이 가능한 동형 암호화 기법의 적용 방안에 대한 고려가 필요하다.

5. 결 론

클라우드 컴퓨팅 서비스가 보편화되면서 일상생활에서 차지하는 비중이 높아짐에 따라, 이용자의 편의성을 개선하면서도 데이터의 안전한 처리에 대한 관

심이 높아지고 있다. 클라우드 컴퓨팅은 시간 및 공간의 제약에서 벗어나 언제든지 이용자의 요청에 실시간으로 응답하는 서비스를 제공함으로써 새로운 지식정보사회 발전의 모태가 되고 있다. 본고에서는 이러한 클라우드 컴퓨팅에서의 가장 핵심이 되는 클라우드 스토리지의 개념과 중요성, 효율성 증대 및 보안성 향상을 위한 노력에 대하여 살펴보았다. 클라우드 스토리지는 그동안의 클라이언트/서버 기반의 서비스에서의 제약사항을 극복하고, 새로운 시장을 형성함으로써 점점 그 활용도 및 시장 점유율이 증가하고 있다.

클라우드 스토리지에서의 데이터 중복 제거 기술은 자원의 효율적 활용을 통하여 방대한 자료로부터 사용자에게 양질의 서비스 제공을 가능하게 하였다. 민감한 데이터의 노출 위협으로 인한 클라우드 스토리지의 사용 기피 현상을 해결하기 위하여 다양한 암호화 및 보안 기법들이 제시되고 있으며, 이를 통하여 머지않은 미래에는 개인 클라우드(private cloud) 뿐만 아니라 공개 클라우드(public cloud)와 하이브리드 클라우드(hybrid cloud) 시장이 활발히 성장하고 다양한 서비스가 생겨날 것으로 기대한다. 클라우드 컴퓨팅 환경은 여러 정보통신기술을 융합한 차세대 플랫폼으로서의 역할을 하고 있으며, 학계와 산업계는 차세대 클라우드 시장을 선도할 수 있도록 보다 긴밀한 연구 개발의 공조체제를 구축하여야 할 것이다. 클라우드 컴퓨팅은 인터넷에 기반을 둔 기술로 글로벌 관점에서의 연구 협력 체계도 중요하며 연구실의 제한 공간에서 벗어나, 연구 자료와 결과를 공유하고, 글로벌 프로젝트를 선도적으로 이끌어나갈 연구 개발자들의 출현을 기대해 본다.

참고문헌

[1] eWeek.com, “Cloud Storage Security Isn't as Solid as Vendors Want You to Believe”, 2012/5/15

[2] Infomationweek, “Microsoft Sees Cloud As SMB Security Cure”, 2012/5/15

[3] PCWorld, “SMB Conferece in Cloud Security Grows, Survey Say”, 2012/5/14

[4] 정수환, 클라우드 기반 보안서비스 기술 동향, 전자공학회지, Vol.40, No.10, pp.972-977, 2013년 10월

[5] 구동영 외, 스마트기기를 활용한 클라우드 서비스 환경에서 안전한 데이터 중복제거 기술 동향, 전자공학회지, Vol.40, No.10, pp.989-996, 2013년 10월

[6] Ari Juels, et al., “PoRs: Proofs of Retrievability for Large Files,” ACM CCS, pp.584-597, 2007

[7] Giuseppe Ateniese, et al., “Provable Data Possession at Untrusted Stores,” ACM CCS, pp.598-609, 2007

[8] Shai Halevi, et al., “Proofs of Ownership in remote Storage Systems,” ACM CCS, pp.291-400, 2011

[9] Wee Keong Ng, et al., “Private Data Deduplication Protocols in Cloud Storage,” ACM SAC, pp.441-446, 2011

[10] Jia Xu, et al., “Leakage-Resilient Client-side Deduplication of Encrypted Data in Cloud Storage,” IACR ePrint Archive, 15pages, 2011

[11] Mihir Bellare, et al., “Message-Locked Encryption and Secure Deduplication,” EUROCRYPT, pp.296-312, 2013

약 력

구 동 영

2012 한국과학기술원 전산학(석사)
2009 연세대학교 컴퓨터.산업공학(학사)
관심분야 : 클라우드 보안, 암호, 네트워크보안
E-mail : dykoo@nslab.kaist.ac.kr

윤 현 수

1989~현재 한국과학기술원 전산학과 교수
1988 오하이오 주립대학 전산학(박사)
관심분야 : 모바일 애드혹 네트워크, 무선 센서 네트워크, 4G 모바일 통신 네트워크 등
E-mail : hyoon@nslab.kaist.ac.kr