공공 클라우드 환경에 적합한 안전한 데이터 관리 기법 연구

위유경*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : ykwi@sch.ac.kr, jkwak@sch.ac.kr

A Study on Secure Data Management Scheme in Cloud Environment in the Public Sector

Yukyeong Wi*, Jin Kwak**
*ISAA Lab, Dept of Information Security Engineering, Soonchunhyang University
**Dept of Information Security Engineering, Soonchunhyang University

요 약

하드웨어, 소프트웨어 등 각종 IT 자원을 필요한 만큼 빌려서 사용하고 사용한 정도에 따라 과금이 되는 클라우드 컴퓨팅이 대중적으로 보급됨에 따라 공공 서비스에서의 클라우드 컴퓨팅 활용방안에 대해서 관심이 증가하고 있다. 따라서 다수의 사용자가 하나의 공공 클라우드 스토리지를 사용하는 환경에 적합한 안전하고 효율적인 데이터 관리의 중요성이 요구되고 있다. 그러나 신원이 불분명한 사용자의 공공 클라우드 스토리지 무단접근과 악의적인 목적으로 공공 클라우드에 악성코드가 추가된 데이터의 업로드 및 데이터 위변조 등의 다양한 위협이 존재한다. 따라서 본 논문에서는 공공 클라우드 환경에 적합한 안전한 데이터 관리 기법에 대해 제안한다. 제안하는 기법은 공공 클라우드 서버로부터 인증정보를 전송받아 구성원임을 증명받고, 전송받은 서버 인증정보를 바탕으로 사용자 인증값을 생성하여 데이터와 함께 저장하여 데이터를 보호한다. 따라서 신원이 불분명한 사용자의 접근을 막고, 악의적인 데이터의 클라우드 스토리지 저장을 방지하고, 추가적으로 데이터의 출처를 명확하게 하여 공공 클라우드 스토리지의 신뢰성을 높일 수 있다.

1. 서론

사용자가 필요로 하는 서버, 스토리지, 어플리케이션, SW 플랫폼 등의 각종 IT 자원을 구매하여 소유하지 않고 필요할 때마다 네트워크를 통해 서비스 형태로 이용하는 방식인 클라우드 컴퓨팅이 대중적으로 보급됨에 따라 공공 부문에서의 클라우드 컴퓨팅 서비스 도입에 대한 관심이 증가하고 있다. 이에 따라 주요 선진국들은 클라우드 컴퓨팅의 효과를 인식하고, 공공부문에 체계적으로 도입하기 위해 중장기 계획을 수립하여 적극적으로 정책을 실행하고 있다. 하지만 공공분야 컴퓨팅의 특성상 다수의 사용자가 하나의 클라우드 스토리지에 접근하여 각종 데이터를 공유하고 내려받는 환경에서는 신원이 불분명한 사용자의 클라우드 스토리지 무단접근, 악성코드가 삽입된 불법 데이터의 공격 등의 문제점이 발생할 가능성이 존재한다. 따라서 중요한 공공 데이터가 유출 및 위변조될 가능성이 높다. 또한 해당 클라우드 스토리지로부터 내려받은 데이터에 대한 출처를 확인할 수 없어, 해당 공공 클라우드의 신뢰성을 저하시킬 수 있다. 따라서 본 논문에서는 공공 클라우드 환경에서 안전하게 데이터를 관리하기 위한 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 국내외 공공부문 클라우드 서비스 도입 현황에 대해 분석하고, 3장에서 클라우드 환경의 데이터 관리 및 보안에 대하여 문제점과 그에 따른 보안 요구사항에 대해 분석한다. 4장에서는 공공 클라우드 환경에서 안전한 데이터 관리 기법을 제안한다. 5장에서는 제안한 기법의 안전성에 대해 분석하고, 마지막으로 6장에서는 결론을 맺는다.

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2012-010886).

2. 국내외 공공부문 클라우드 서비스 도입 현황

2.1 국외 현황

❒ 미국

오바마 정부는 2009년 인프라 구축 비용절감과 IT 자원 유연성을 제공하기 위해 클라우드 컴퓨팅을 도입하고, 친환경 정보통신기술(ICT) 운영을 통해 환경 영향을 최소화를 위한 연방정부 클라우드 컴퓨팅 계획을 발표했다. 이는 정부부처 및 기관의 클라우드 컴퓨팅 애플리케이션과 서비스를 구매할 수 있는 온라인 앱스토어인 Apps.gov를 제공하는 것이다. Apps.gov에서는 페이스북, 트위터와 같은 소셜 네트워크 서비스(SNS) 어플리케이션은 물론, 시장분석·통계처리 등 고급 업무용 어플리케이션을 구매할 수 있다[1].

❒ 일본

일본정부는 ICT 인프라 구축비를 절감하고 환경을 보호하는 목적으로 클라우드 컴퓨팅을 추진하고, 'i-Japan 전략 2015'에서 정보시스템 효율화를 위한 클라우드 추진 정책을 명시하였다. 또한 총무성은 중앙부처 대상의 가스미가세키 프로젝트와 지자체 대상의 지자체 클라우드를 추진하고 있다. 따라서 총무성 행정관리국을 중심으로 2015년까지 전자정부 지원을 위한 중앙부처의 클라우드 컴퓨팅 도입을 주요 내용으로 하는 '가스미가세키 클라우드'를 구축할 예정이다. 또한 1,000여 개의 지자체를 위한 클라우드 컴퓨팅 도입계획을 추진하고 있다.

ICT를 활용한 행정 정책의 하나로 추진되는 지방자치단체 클라우드 컴퓨팅은 2009년부터 홋카이도, 규슈 등 66개 지방자치단제가 참여하여 실증 실험을 하였으며, 총무성에 '지방자치체 클라우드 컴퓨팅 추진본부'가 설립되었다. 향후 데이터 센터 자원과 행정 서비스에 필요한 업무 어플리케이션을 각 지방자치단체가 공동으로 이용하는 것을 업무 효율화 목표로 하고 있다[1].

2.2 국내 현황

2009년에 정부 차원에서 '범정부 클라우드 활성화 종합계획'과 2011년에 '클라우드 컴퓨팅 확산 및 경쟁력 강화를 위한 전략'을 행정안전부, 지식경제부, 방송통신위원회의 3개 부처가 공동으로 수립·발표하였다. 범정부 클라우드 활성화 종합 계획에서는 국내 클라우드 컴퓨팅 산업을 육성하여 2014년에 클라우드 컴퓨팅 세계시장 점유율을 10%에 이르는 세계 최고 수준의 클라우드 컴퓨팅 강국 실현을 목적으로 하고 있다. 또한 각각의 정부부처별로 클라우드 컴퓨팅 추진 계획 및 전략 수립, 법·제도 개선 등에 대한 논의가 진행되고 있다. 또한 클라우드 컴퓨팅 확산 및 경쟁력 강화 전략에서는 '클라우드 데이터센터, 모바일 클라우드, 전자정부 등의 전략 분야 육성'과 '안전한 이용환경 조성을 통해 5년 내 도입률 15% 달성'의 내용을 담고 있다[2].

<표 1> 국내외 공공부문 클라우드 서비스 도입현황

국가	내용
미국	· 정부부처 및 기관이 클라우드 컴퓨팅 애플리케이션과 서비스를 구매할 수 있는 온라인 앱스토어인 Apps.gov를 오픈하고 정부부처에 서비스 이용을 독려
일본	· (가미스가세키 클라우드 정책) 2015년까지 13개 중앙관청의 모든 IT자원을 클라우드로 통합 · 지자체 대상 클라우드 데이터센터 3개소 구축 등
한국	· 범정부 클라우드 활성화 종합계획, 클라우드 컴퓨팅 확산 및 경쟁력 강화 전략 발표 · 국내 클라우드 컴퓨팅 산업을 육성, 2014년에 클라우드 컴퓨팅 세계시장 점유율 10% 실현 추진

3. 문제점 및 보안 요구사항

3.1 문제점

데이터 수요의 증가로 인해 클라우드 서비스가 보편화되었다. 그에 따른 사진, 텍스트 파일, 동영상, 그림 등의 일반적인 데이터의 클라우드 환경에서 관리 방법에 대해 관심이 높아지고 있다. 일반적으로 공공 클라우드 서비스 환경에서는 다수의 사용자가 하나의 클라우드 스토리지에 접속하여 사용자 간의 각종 데이터를 공유하고, 내려받는다. 하지만 신원이 불분명한 사용자의 공공 클라우드 스토리지 무단접근은 공공의 데이터가 유출될 가능성이 높다. 또한 인증된 사용자일지라도 악의적인 목적으로 공공 클라우드에 악성코드가 추가된 데이터를 업로드 하거나, 위·변조하는 등의 공격을 막기 어렵다. 또한 해당 클라우드로부터 내려받은 데이터에 대한 출처를 확인할 수 없어 해당 공공 클라우드의 신뢰성을 저하시킬 수 있다.

3.2 보안 요구사항

❒ 기밀성

공공 클라우드 서비스의 인증정보는 기밀성이 보장되어야 한다. 인증정보는 사용자가 공공 클라우드 서버로 접속하여 정당한 사용자인지 확인하는 과정에 사용된다. 또한 사용자 인증값 생성단계에 사용되어 이는 클라우드 서비스의 인증 및 해당 데이터의 출처 정보를 가지고 있다. 이를 위해 공공 클라우드 환경의 통신에 사용되는 서버 인증정보는 정당한 사용자만이 확인 가능해야 하며, 서버 인증정보의 발신지 및 수신지, 통신횟수, 길이, 통신상의 트래픽 특성에 대하여 공격자가 알 수 없어야 한다[3].

❒ 무결성

사용자의 인증값은 해당 사용자의 클라우드 서비스 접속 및 데이터 업로드 과정과 연관이 있기 때문에 무결성이 보장되어야 한다. 공공 클라우드 환경에서는 데이터베이스에 저장 또는 네트워크를 통해 전송되는 사용자들의 인증값이 위조, 변조 및 파괴되지 않도록 해야 한다. 따라서 전송받은 데이터의 위변조와 사용자 인증값의 위조 및 변조를 감지하기 위하여 전자서명 또는 해쉬함수 연상 등을 이용해야 한다[3].

❒ 인증

공공 클라우드 환경에서의 인증기능은 서비스 이용을 원하는 사용자가 전송한 메시지 및 데이터의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다[3].

❒ 접근제어

공공 클라우드 스토리지에 대한 읽기 및 변경 등의 모든 접근 행위에 대해 그 권한을 명백하게 구분하여 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 접근제어 기능이 필요하다. 운영체제의 접근통제 기능을 사

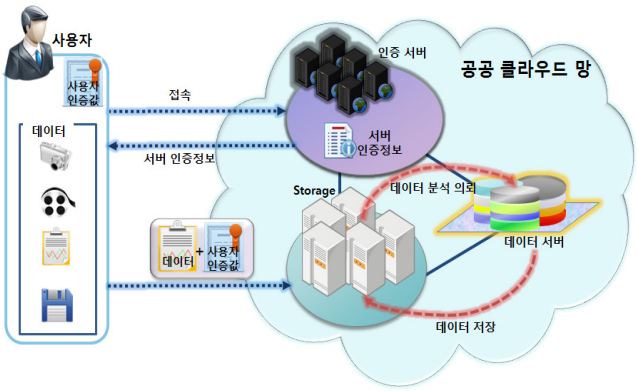
용하며, 네트워크에서는 침입차단 시스템을 사용하여 접근 통제의 수준을 높일 수 있다. 또한 정당하지 않은 사용자는 해당 공공 클라우드 서비스를 이용할 수 없도록 해야 한다[3].

4. 제안방식

본 논문에서는 공공 클라우드 환경에서 안전하게 데이터를 관리하기 위한 기법을 제안한다. 본 제안방식은 다수의 사용자가 하나의 스토리지를 함께 사용하는 공공 클라우드 환경에서 적용됨을 가정한다.

본 제안방식은 공공 클라우드 서버로부터 인증정보를 전송받아 해당 공공 클라우드의 구성원임을 증명받고, 전송받은 서버 인증정보를 바탕으로 사용자 인증값을 생성하여 데이터와 함께 업로드한다. 이는 신원이 불분명한 사용자의 접근을 막고, 악의적인 데이터의 클라우드 스토리지의 저장을 방지하고, 추가적으로 데이터의 출처를 명확하게 하여 공공 클라우드의 신뢰성을 높일 수 있다. 제안하는 프로토콜은 사용자 인증 단계와 데이터 관리 단계의 2단계로 구분된다.

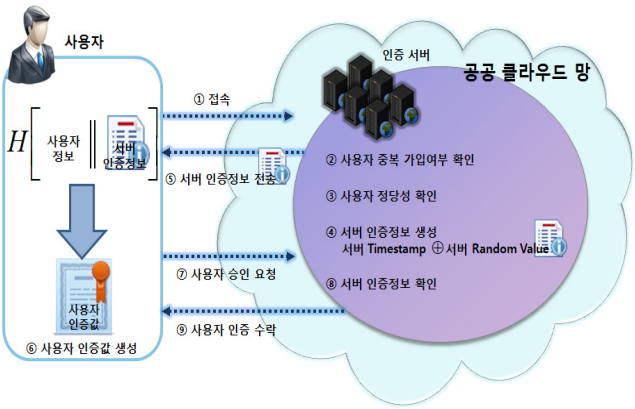
(그림 1)은 본 논문에서 제안하는 공공 클라우드 환경에 적합한 안전한 데이터 관리 시스템의 개념도를 나타낸다.



(그림 1) 제안방식 개념도

4.1 사용자 인증 단계

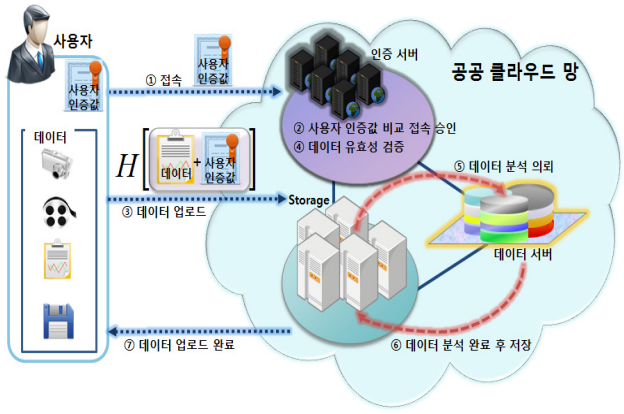
① 사용자는 사용을 원하는 공공 클라우드로 접속을 한다.
② 공공 클라우드 서버는 해당 사용자의 중복 가입여부를 검사한다.
③ 공공 클라우드 서버는 해당 사용자의 공공 클라우드 서비스에 가입이 가능한 정당한 사용자인지 여부를 확인한다.
④ 정당한 사용자인지 확인이 완료된 공공 클라우드 서버는 난수값과 타임스탬프값을 연산한 인증정보를 생성한다.
⑤ 공공 클라우드 서버는 사용자에게 생성된 인증정보를 전송한다.



(그림 2) 사용자 인증 단계

⑥ 사용자는 전송받은 공공 클라우드 서버 인증정보와 사용자 정보를 연접하고 해쉬함수 연산하여 사용자 인증값을 생성한다. 이는 정당한 사용자의 증명과 함께 데이터의 무결성 증명에 대해 유효성을 지니게 된다.
⑦ 사용자는 공공 클라우드 서버로 생성한 사용자 인증값을 전송하여 해당 공공 클라우드 서비스 승인을 요청한다.
⑧ 공공 클라우드 서버는 사용자 인증값에 포함된 클라우드 서버 인증정보를 확인하여 해당 사용자의 정당성을 확인한다.
⑨ 공공 클라우드 서버는 해당 사용자의 인증 요청을 수락하여 인증 단계를 마무리 한다.

4.2 데이터 관리 단계



(그림 3) 데이터 관리 단계

① 사용자는 사전에 가입 승인을 받은 공공 클라우드 서비스에 접속한다.
② 공공 클라우드 서버는 전송받은 사용자 인증값을 클라우드 서버에 저장된 사용자 데이터베이스와 비교하여 접속을 승인한다.
③ 사용자는 업로드하려는 데이터에 사용자 인증값을 연접하여 공공 클라우드 스토리지에 업로드 한다.

④ 공공 클라우드 서버는 전송받은 데이터의 사용자 인증값을 비교한다. 이는 해당 데이터의 유효성을 검증한다.

⑤ 공공 클라우드 서버는 정당한 사용자의 데이터임을 확인이 되면 데이터 분석 서버에서 해당 데이터의 정상 유무를 분석하게 된다. 해당 과정에서 업로드한 데이터가 정상임이 파악되지 않을 경우에 사용자의 데이터 업로드 요청을 거부하고 데이터 관리 과정을 마무리한다.

⑥ 공공 클라우드 서버는 분석과정이 완료된 정상적인 데이터에 한하여 데이터의 형식 등의 정보를 데이터베이스화한다. 이는 효율적인 데이터 관리를 수행하고 추가적으로 데이터의 출처를 명확하게 하여 공공 클라우드의 신뢰성을 높힌다.

⑦ 공공 클라우드 서버는 사용자에게 데이터 업로드 완료 메시지를 전송함으로써 해당 과정을 마무리 한다.

5. 안전성 분석

❒ 기밀성

제안하는 기법의 서버 인증정보는 사용자 ID와 서버의 타임스탬프 정보를 지수승하여 생성된다. 따라서 해당하는 서버의 난수값을 알기 어렵기 때문에 해당 서버 인증정보를 탈취하더라도 공공 클라우드 서비스를 사용할 수가 없다. 또한 데이터 관리 단계에도 클라우드 인증정보가 사용되기 때문에 사용자 인증값을 임의로 변경할 수 없다.

❒ 무결성

제안하는 기법은 해쉬함수 연산을 사용하여 사용자 인증값을 생성하여 저장하게 된다. 생성된 사용자 인증값은 데이터 업로드 과정에서 데이터 분석 서버와 비교를 통해 해당 데이터의 정당성과 무결성을 제공한다.

❒ 인증

제안하는 기법의 사용자 인증값에는 클라우드 서버에서 직접 발급한 난수 기반의 클라우드 서버 인증정보를 사용하여 생성하기 때문에 안전한 인증기능을 제공한다.

❒ 접근제어

제안하는 기법은 공공 클라우드 서버로부터 발급받은 인증정보가 없거나 사용자 인증값이 없다면 서비스 접근이 불가능하다. 클라우드 서버는 인증정보를 통해 해당 사용자의 정당성을 검증하며, 서비스 이용을 가능하게 해준다. 사용자 인증값은 난수 기반의 서버 인증정보를 통해 생성하므로 이를 알아내기는 어렵다. 따라서 서버 인증정보를 탈취하더라도 공공 클라우드 서비스에 접근할 수가 없다.

6. 결론

클라우드 컴퓨팅의 대중적인 보급과 함께 공공부문에서의 클라우드 컴퓨팅 서비스 도입에 대해서 관심이 증가하고 있다. 하지만 공공부문 클라우드 컴퓨팅의 특성과 같이 다수의 사용자가 하나의 클라우드 스토리지에 접근하여 각종 데이터를 공유하고 내려받는 환경에서는 신원이 불분명한 사용자의 클라우드 스토리지 무단접근, 악성코드가 삽입된 불법 데이터의 공격, 공공 데이터의 유출 및 위변조 가능성, 클라우드 스토리지로부터 내려받은 데이터에 대한 출처를 확인할 수 없어 해당 공공 클라우드의 신뢰성을 저하하는 등의 문제점이 존재한다.

따라서 본 논문에서는 공공 클라우드 환경에 적합한 안전한 데이터 관리 기법에 대해 제안하였다. 이를 통해 공공부문 클라우드 서비스 도입 시 인증받은 구성원만 스토리지를 사용할 수 있고, 사용자 인증값과 함께 데이터를 저장하여 데이터의 안전성을 높이며, 추가적으로 데이터의 출처를 명확하게 함으로써 공공 클라우드의 신뢰성을 높일 수 있다.

참고문헌

[1] 신선영, 송석현, “국내 공공 클라우드 서비스 적용 우선순위 도출에 관한 연구: 해외 공공부문 클라우드 사례의 SRM 매핑을 통해”, Internet and Information Security, 제 3권 제 3호, 2012.

[2] 행정안전부, “범정부 클라우드 추진현황 및 향후계획”, 2012

[3] 한국정보통신기술협회, “공공 부분 데스크탑 클라우드 도입 가이드라인”, 2011