http://dx.doi.org/10.14400/JDPM.2013.11.12.467

공공기관 클라우드 데이터 센터에 활용 가능한 공개키 기반의 안전한 데이터 관리 기법

위유경*, 곽진**
순천향대학교 정보보호학과 정보보호응용및보증연구실*, 순천향대학교 정보보호학과**

Public Key based Secure Data Management Scheme for the Cloud Data Centers in Public Institution

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

요 약 클라우드 컴퓨팅 서비스가 대중적으로 보급됨에 따라 공공분야에서 해당 서비스의 도입에 대한 관심이 증가하고 있다. 이에 따라 국내에서는 클라우드 컴퓨팅을 공공분야에 도입하거나 계획하고 있으며 점차 구체적으로 구축하고 있다. 하지만 공공분야에서의 클라우드 도입 및 활성화를 위해서는 서비스 가용성 장애요인 및 인증 받지 않은 사용자의 무단 접근, 불분명한 출처로부터 다운로드 받은 데이터로 인한 클라우드 데이터센터의 신뢰성 저하 등의 보안 위협에 대한 해결방안을 모색할 필요성이 있다. 따라서 본 논문에서는 공공기관 클라우드 데이터센터에서 활용 가능한 공개키 기반의 안전한 데이터 관리 기법에 대해서 제안한다. 이를 통해 공공기관에 클라우드 컴퓨팅을 도입할 때 인증 받은 사용자만 데이터센터를 사용할 수 있고, 공공 데이터의 중요도와 난이도를 공용데이터, 개인데이터, 기밀데이터로 설정해주어 체계적이고 안전하며 효율적으로 데이터 관리를 가능하게 한다. 따라서 공공기관에서의 클라우드 서비스에 대해 전반적인 보안성과 편의성을 향상시킬 수 있을 것으로 기대된다.

주제어 : 공개키 기반 구조, 접근 제어, 안전한 데이터 스토리지, 사용자 인증, 공공기관용 클라우드 데이터센터

Abstract The cloud computing has propagated rapidly and thus there is growing interest on the introduction of cloud services in the public institution. Accordingly, domestic public institution are adoption of cloud computing impose and devise a plan. In addition, more specifically, is building a cloud computing system in the public institution. However, solutions to various security threats(e.g., availability invasion of storage, access by unauthorized attacker, data downloaded from uncertain identifier, decrease the reliability of cloud data centers and so on) is required. For the introduction and revitalize of cloud services in the public institution. Therefore, in this paper, we propose a public key based secure data management scheme for the cloud data centers in public institution. Thus, the use of cloud computing in the public institutions, the only authorized users have access to the data center. And setting for importance and level of difficulty of public data management enables by systematic, secure, and efficient. Thus, cloud services for public institution to improve the overall security and convenience.

Key Words : Public key based, Access control, Secure data storage, User Authentication, Cloud data centers in public institution

* 이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012-010886).
* 이 논문은 순천향대학교의 지원을 받아 수행된 연구임.
Received 20 November 2013, Revised 18 December 2013
Accepted 20 December 2013
Corresponding Author: Jin Kwak(Soonchunhyang University)
Email: jkwak@sch.ac.kr

ISSN: 1738-1916

1. 서론

세계 경제위기에 따른 ICT 비용절감, 정보자원 관리의 효율성 향상, 탄소 배출량 감소, 그린 IT 실현을 위한 클라우드 컴퓨팅은 서버, 스토리지, S/W 플랫폼, 어플리케이션 등 ICT 자원을 구매하여 소유하지 않고, 필요할 때마다 네트워크를 통해 서비스 형태로 이용하는 방식이다. 이러한 클라우드 컴퓨팅이 대중적으로 보급됨에 따라 공공기관에서의 클라우드 컴퓨팅 도입에 대한 관심이 증가하고 있다[1]. 이에 따라 미국, 영국, 일본 등 주요 국가들은 클라우드 컴퓨팅을 공공부문에 도입하고, 중장기 계획을 수립하여 적극적으로 정책을 구체화하는 노력을 기울이고 있다[2]. 하지만 다수의 사용자가 하나의 클라우드 스토리지에 접근하는 공공분야에서의 클라우드 도입 및 활성화를 위해서는 서비스 가용성 장애요인 및 신원이 불분명한 사용자의 클라우드 스토리지 무단접근, 악성코드가 삽입된 불법 데이터의 공격, 국가기밀 등의 중요도가 높은 공공 데이터의 유출 및 위변조, 불분명한 출처로부터 다운로드 받은 데이터로 인한 클라우드 데이터센터의 신뢰성 저하 등의 보안 위협에 대한 해결방안을 모색할 필요성이 있다. 따라서 본 논문에서는 공공기관의 클라우드 데이터센터에서 활용 가능한 공개키 기반의 안전한 데이터 관리 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 국내외 주요국의 공공기관 클라우드 컴퓨팅 도입현황에 대하여 분석한다. 3장에서는 클라우드 환경에서 보안 취약점 및 보안 요구사항에 대하여 분석하고, 4장에서는 공공기관 클라우드 데이터센터에 활용 가능한 공개키 기반의 안전한 데이터 관리 기법을 제안한다. 5장에서는 제안사항의 안전성에 대해 분석하고, 마지막으로 6장에서는 결론을 맺는다.

2. 국내외 주요국의 공공기관 클라우드 컴퓨팅 도입 현황

2.1 국외현황

2.1.1 미국

미국은 SaaS를 중심으로 공공업무에 클라우드 컴퓨팅 및 서비스를 접목하는데 적극적이다. 이를 통해 ICT 인프라 구축을 위해서 2007년부터 2009년까지 클라우드 컴퓨팅을 적용하여 66억 달러(전체 예산의 11%)의 예산 절감 효과를 가져왔으며, 2010년에 클라우드 컴퓨팅 기반의 친환경 경제활동을 발표하여 데이터센터 통합, IT 자원의 공유를 통한 원격근무 활성화를 추진하였다. 또한 2010년부터 단계적으로 인프라 구축과 민원서비스 등을 클라우드 컴퓨팅으로 전환하고, 2011년 회계연도에는 모든 정부부처를 대상으로 클라우드 컴퓨팅 가이드라인을 제시할 목표로 추진하였다. 그러나 당해 연도에 FTC(미국연방거래위원회)에서 사생활 침해와 보안문제 등을 제기하여 오바마 행정부에서 클라우드 컴퓨팅 체계의 도입과 확산을 늦추기로 결정하였다[3, 4].

○ 연방정부 포탈(USA.gov)

연방정부 웹 포털(USA.gov)은 2009년에 Terremark 社의 '상용 클라우드 서비스 시스템'을 도입한 것이다. USA.gov는 하루 약 1억 명의 사용자가 방문함에 따라 트래픽이 매우 중요한 사항으로 제시되었는데 과거에 트래픽이 높아지면서 로딩속도가 지연되고, 다운횟수 증가하는 문제점이 발생되었다. 그러나 클라우드 컴퓨팅 도입으로 인해 실시간으로 고객의 요구 대응이 가능하며, 90% 정도의 비용절감 및 성능향상을 기대하고 있다.

○ 국방부 정보시스템계획국의 RACE

계속되는 ICT 인프라 증설 요구에 비해서 일정하지 않은 자원 활용률로 인하여 국회에서 감사 시에 견적이 초과된다는 문제점이 지적되었다. 이에 따라 국방부 정보시스템계획국(DISA)은 2008년에 서버, 웹 애플리케이션 플랫폼 등 필요한 개발 환경을 인터넷을 통해 제공하는 클라우드 서비스 개발 인프라 및 테스트 환경인 RACE(Rapid Access Computing Environment)를 구축하였다. 이러한 RACE를 통해 ICT 인프라의 구매 비용 절감, 각 클라이언트의 요청에 따른 자원할당 소요 시간 단축, 사용자가 스스로 요청 및 결재하는 과금 시스템을 구현함으로써 모든 업무의 자동화를 통한 생산성 증대, 웹을 사용하여 사용자가 서버 환경을 선택할 수 있는 셀프 서비스 제공을 통한 운영비용 절감 등의 기대효과를 나타내었다.

2.1.2 영국

영국은 신속한 공공서비스 제공, ICT 관련 비용 절감, 유연한 애플리케이션 확장 등을 위해 2009년에 공공부문의 데이터센터 혁신전략의 일환으로 정부에서 사용하는 전산자원을 클라우드 컴퓨팅 기반으로 제공하는 'G-Cloud'계획 발표하였다. 따라서 정부 및 공공부문의 ICT 애플리케이션을 클라우드에 기반한 공유 네트워크 전달 서비스(Shared Network Delivery Service) 체계로 전환하는 것을 골자로 하는 다음의 주요 내용이다[3].

○ 가상의 공공서비스 네트워크(PSN : Public Service Network) 구축

범정부 차원의 클라우드 기반 인프라 네트워크를 구축하여, 세계 어느 곳에서나 공공서비스를 제공받을 수 있도록 구현하고, 사용자 중심의 디자인과 표준을 정립하여 서비스 수준 향상 및 보안 이슈를 함께 해결하기 위한 다각적인 노력이 필요하다.

○ 전문적이고 체계적인 도입・활성화를 위한 전략적 접근 방식 채택

공공부문의 데스크톱에서부터 네트워크, 데이터센터, 그린 ICT 등의 적용이 용이한 분야부터 클라우드 기술 접목을 시도한다.

○ 클라우드 기술을 보유한 민간 산업 활성화

공공의 조달 부문을 우선 대상으로 기존 개별 시스템을 클라우드 컴퓨팅 방식으로 통합하여 보다 효율성 높은 조달 체계를 구축한다.

○ 클라우드 컴퓨팅에 기반한 정부 업무 추진 방식의 전환

5백만 명의 공무원들이 모두 G-Cloud를 사용하게 될 것이며, 정부의 전용 애플리케이션 스토어 구축하여 하나의 통합형 데이터 센터 구축한다.

○ 클라우드 컴퓨팅 기술을 이용한 그린 ICT 파급 효과 증대

클라우드 컴퓨팅을 이용하여 인터넷 환경에서 스토리지, 처리 능력, 플랫폼 애플리케이션 이용을 통해 효율성 증대 및 유비쿼터스 이용 환경 구축으로 그린 ICT를 구현한다.

2.1.3 일본

일본은 정부 정보시스템의 통합・집약화 및 각 정보시스템의 보유 데이터를 연계하여 2015년까지 디지털기술에 의한 새로운 행정개혁 추진의 일환으로 2009년에 "스마트 u-네트워크 실현전략"에서 2015년까지 정부의 전산지원 활성화를 높이기 위한 클라우드 컴퓨팅 도입 발표하였고, 총무성에서 중앙부처 클라우드 컴퓨팅 도입을 위한 "가스미가세키 프로젝트"를 발표하여 1,000여개의 자치단체에서 클라우드 도입 추진을 위하여 2,000억원을 투입하였다. 다음은 일본의 정부 공통 플랫폼 정비에 대한 방향성과 검토과제의 주요 내용이다[5].

○ 정부 정보시스템의 통합 및 집약화

국가의 정보시스템 중 개발, 수리, 관리운용의 비용 대비 효과를 고려하여 대상시스템을 선정하여, 정부 정보시스템의 효율적이고 안정적인 개발, 수리, 관리 운용을 위해 정부 공통 플랫폼에서 이용자인증 기능, 워크플로우 기능, 백업 기능과 같은 공통기능을 제공한다.

○ 각 정보시스템의 보유 데이터 연계

정부 정보시스템의 실태파악 조사 결과 및 비용 효과 등을 검토하고, 데이터 연계 및 정보 공유에 따른 업무를 재설계한다.

○ 정부 공통 플랫폼의 정비 및 관리운용

애플리케이션 설계 및 개발에 대한 역할분담과 시스템 구축, 이행, 운용에 관한 비용분담, HW・SW 조달에 대한 역할분담, 장애 및 문제 발생 시의 책임분담 등을 명확하게 한다.

2.1.4 중국

중국은 2008년에 클라우드 컴퓨팅 환경을 구현함으로써, 인터넷 서비스 제공업체가 운영비를 대폭 절감하고, 기업 애플리케이션 개발 시간 단축 및 신규 시장으로 진출과 소프트웨어 산업경쟁력 강화를 위해 클라우드 컴퓨팅 기술을 활용하여 컴퓨팅 자원을 제공하는 우시(Wuxi) 소프트웨어 개발단지를 추진하였다. 따라서 IBM 리서치 중국 지사는 우시 아이파크(iPark)와 협력하여 IBM

System x 및 System p 서버, System Storage DS 장치를 기반으로 클라우드 컴퓨팅 환경을 구축했다. 이를 통해 에너지 및 자원을 절약하고, 또한 필요한 시기와 장소에서 자원을 사용할 수 있게 하는 공유 서비스 제공으로 비용을 대폭 절감 및 비즈니스 애플리케이션의 개발 시간을 단축했다[3].

2.1.5 호주

호주는 2011년 1월에 "클라우드 컴퓨팅 전략"을 발표하여 정부기관의 IT자원을 클라우드 컴퓨팅으로 이전하기 위한 전략을 마련하였다. 이는 IT자원의 보안문제를 검토하면서 다른 국가에 비해 천천히 클라우드 컴퓨팅을 추진하는 것으로 목표한다[3].

2.2 국내현황

2009년 5월에 정부차원의 "그린 IT 국가전략"을 발표하여 클라우드 컴퓨팅 기반 구축, 장비 저전력화를 통한 방송통신 인프라의 그린화를 진행하기로 하였으며, 2009년 말 방송통신위원회, 행정안전부, 지식경제부가 공동으로 "클라우드 컴퓨팅 활성화 종합계획"을 발표하였다. 이어서 2010년에 한국과학기술정보연구원(KISTI)에서 클라우드 서비스 테스트베드 센터를 개소하고, 관계부처 합동으로 2011년 5월에 "클라우드 컴퓨팅 확산 및 경쟁력 강화 전략"을 발표하였다. 또한 서비스 가용성, 데이터 백업·복구 및 보안, 고객지원, 위약금 등의 내용을 담은 클라우드 서비스에 적용할 SLA 가이드와 개인정보보호수칙이 2011년 10월에 방송통신위원회에서 발표되었으며, 이용자의 신뢰를 높여 클라우드 서비스 확산을 촉진하고자 클라우드 서비스 인증 제도를 마련하였다[6, 7, 8, 9].

〈Table 1〉 Present condition on introduction of cloud computing for a major domestic and foreign institution

Nation	Content
USA	Federal government portal(USA.gov), Cloud introduction and deployment on Defense Information System Agency(DISA)
UK	Establishment and implementation of a plan for government cloud computing "G-Cloud"
JAPAN	The Kasumigaseki Cloud Plan is being promoted, joint research is being operated by Ministry of Internal Affairs.
CHINA	Provide Cloud environment to S/W enterprises and developers by building Wuxi S/W development.
AUSTRALIA	Prepare a strategy to transfer IT resource to cloud computing of the government by announcing "Cloud computing strategy"
KOREA	Publish "SLA Guide" and "Privacy Rule" to apply on cloud service, which includes Service availability, Data backup/recovery and security, Customer support.

3. 보안 취약점 및 보안 요구사항 분석

본 장에서는 공공기관 클라우드 환경에서의 데이터 관리 방식의 문제점을 분석한다. 또한 분석한 내용을 바탕으로 클라우드 환경에서 데이터 관리의 문제점을 해결하기 위한 보안 요구사항을 도출한다.

3.1 보안 취약점

3.1.1 데이터 유출

기존의 클라우드 환경과는 다르게 공공기관에 적합한 클라우드 환경은 다수의 사용자가 하나의 클라우드 데이터센터에 접속하여 구성원간의 각종 데이터를 공유하고 다운로드 받는 환경이다. 따라서 허가받지 않은 사용자의 공공 클라우드 망의 데이터센터 접근은 공공기관의 주요문서가 유출될 가능성이 높다. 이는 클라우드 데이터센터에 저장되어 있는 중요한 데이터에 대한 기밀성을 보장할 수 없다[10].

3.1.2 데이터 위·변조

클라우드 데이터센터에는 다수의 사용자가 접근할 수 있는 구조이다. 악의적인 공격자가 자신의 신분을 속이고 내부 스토리지에 접근한다면 데이터를 무단으로 위/변조할 가능성이 높다. 따라서 클라우드 데이터센터에 저장되어 있는 데이터에 대한 무결성을 보장할 수 없다[11].

3.1.3 데이터센터의 가용성 침해

클라우드 데이터센터에는 다수의 스토리지가 집약되어 있어 데이터 저장량과 공유량이 많다. 따라서 악의적인 사용자가 바이러스 및 악성코드를 삽입한 악성 데이

터를 무단으로 업로드 할 경우에 데이터센터의 가용성을 침해하는 심각한 보안 위협이 발생할 가능성이 높다[12, 13].

3.1.4 인증 받지 않은 사용자의 무단 접근

공공기관 클라우드 서비스의 권한이 없는 사용자가 내부 데이터센터에 무분별하게 접근하여 중요한 데이터 및 공공기관 구성원의 개인정보가 유출되는 사례가 발생할 가능성이 높다. 또한 인증 받은 사용자일지라도 악의적인 목적으로 공공기관 클라우드 데이터센터에 악성코드가 추가된 데이터를 업로드 또는 위·변조하는 등의 공격을 막기 어렵다.

3.2 보안 요구사항

3.2.1 기밀성

공공기관 클라우드 데이터센터의 개인 스토리지와 기밀 스토리지에 저장되는 데이터와 해당 데이터에 접근 가능한 사용자 정보는 기밀성이 보장되어야 한다. 해당 정보의 분석은 곧 공격자에 의해 공공기관 망에 접속 가능한 계정정보가 유출될 가능성과 주요 공공 데이터가 안전하게 스토리지에 저장되는 것을 방해할 가능성이 있다. 이를 위해 공공기관 클라우드 환경의 통신에 사용되는 사용자 인증 ID는 정당한 사용자 및 클라우드 서버만이 확인할 수 있어야 하며, 비밀값의 출처 및 수신지, 횟수, 길이 또는 통신선로 상의 트래픽 특성에 대하여 공격자가 알 수 없게 해야 한다[10].

3.2.2 무결성

공공기관 클라우드 데이터센터에 저장되는 데이터는 무결성이 보장되어야 한다. 클라우드 데이터센터의 스토리지는 다수의 사용자가 접근하여 데이터를 공유하기 때문에 데이터의 안전하고 효율적인 관리를 위해서 네트워크를 통해 전송되는 데이터가 위·변조 및 파괴되지 않도록 해야 한다. 따라서 전송받은 데이터와 인증 ID의 위·변조를 감지하기 위하여 전자서명 또는 해시함수 연산 등을 이용해야 한다[14].

3.2.3 가용성

공공기관 클라우드 서비스는 안전한 가용성이 보장되어야 한다. 공공기관의 클라우드 데이터센터에는 다수의 구성원이 접속할 뿐만 아니라, 국가기관의 기밀 데이터도 저장되어 있기 때문에 악의적인 사용자로부터 악성 데이터의 업로드 시도 및 악성코드 삽입 등 악의적인 행위를 사전에 차단하여 클라우드 서비스의 가용성을 보장할 수 있어야 한다[15].

3.2.4 사용자 인증

공공기관 클라우드 환경에서의 사용자 인증 기능은 클라우드 서비스를 이용하고자 접근하는 사용자가 전송한 메시지 또는 데이터의 출처가 명확하고, 그 실체의 신분이 거짓이 아닌 정당한 사용자임을 검증할 수 있어야 한다.

〈Table 2〉 Security threats and security requirements in a public institution cloud environment.

Security Threats	Security requirements
data leakage	·User authentication ID should only be verified by legitimate user and cloud server. ·Attacker should not be able to find about source and destination of a secret value, frequency, length or traffic characteristics of communication.
Data forgery	·Prevent data forgery/modulation for safe and effective data management. ·Use electronic signature or hash function to detect forgery and modulation.
Availability invasion of the data center	·Block malicious activity that attempts to upload malicious data and inject malicious code.
Unauthorized access of unauthorized user	·A source of message or data user sent should be clear, it should be verifiable to identify the user.

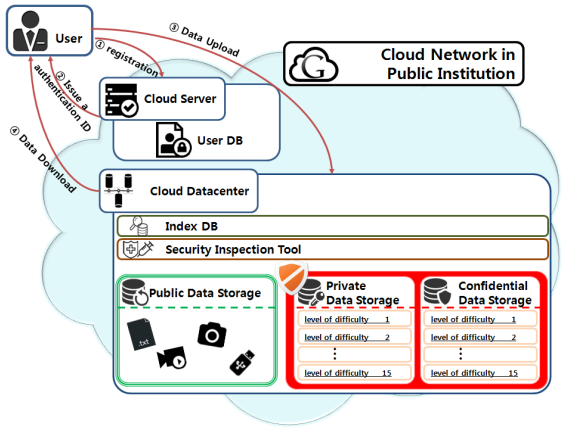
4. 안전한 데이터 관리 기법

4.1 시스템 개요

본 절에서는 공공부분의 클라우드 데이터센터에 데이터를 안전하게 저장하고 관리하기 위한 기법을 제안한다. 이를 위해 본 제안방식의 공공 클라우드 서비스 망은 다수의 사용자가 하나의 공공기관 데이터센터를 함께 사용

하는 공공기관 프레임워크에 특화된 환경에 적용됨을 가정한다.

제안하는 데이터 관리 기법은 공공기관 클라우드 데이터센터에 데이터를 저장할 때 데이터의 중요도를 공용데이터/개인데이터/기밀데이터로 나뉘어 스토리지에 저장하여 효율적으로 데이터 관리를 용이하게 하며, 데이터가 저장되기 전에 해당 데이터의 안전성 검증을 제공하여 데이터센터의 신뢰성과 안전성을 높였다. 또한 허가받지 않은 사용자의 상급 스토리지에 저장된 데이터에 접근을 방지하여 중요도가 높은 데이터의 안전성을 높일 수 있다. 본 제안방식은 공공 클라우드 서버로부터 사용자 인증티켓을 발급받아 해당 공공 클라우드 데이터센터를 사용할 수 있는 그룹의 구성원으로 증명 받고, 발급받은 인증티켓을 기반으로 해당 사용자의 ID를 생성하여 인증절차를 수행하는 사용자 가입 및 인증 단계와 공공 클라우드 데이터센터에 업로드하려는 데이터의 중요도를 공용/개인/기밀로 나누어 저장하는 데이터 저장 단계, 사용자의 권한에 따라 사용을 원하는 데이터의 다운로드를 요청하는 데이터 다운로드 단계의 총 3단계로 구분된다. 다음 [Fig. 1]은 본 논문에서 제안하는 공공기관 클라우드 데이터 센터에 활용 가능한 안전한 데이터 관리 기법의 개념도를 나타낸다.



[Fig. 1] Overview of the proposed scheme

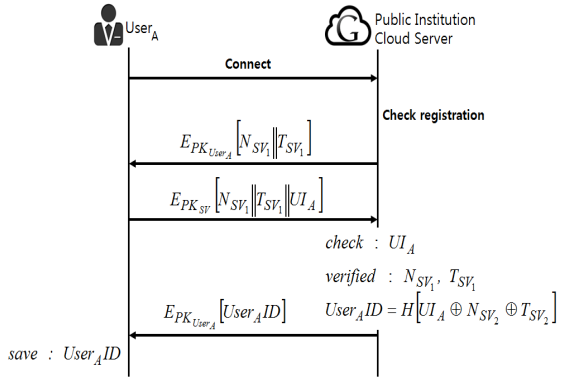
4.2 시스템 파라미터

본 논문에서 제안하는 프로토콜에 사용되는 주요 시스템 파라미터는 다음과 같다.

- $User_*$: 사용자 *
- SV : 클라우드 서버
- E_{PK_*} : *의 공개키로 암호화
- N_{SV_n} : 클라우드 서버의 n번째 난수값
- T_{SV_n} : 클라우드 서버의 n번째 타임스탬프값
- DB_{SV} : 클라우드 서버의 데이터베이스
- UI_* : 사용자의 *의 개인정보값
- $H(\bullet)$: 해시함수 연산
- $User_*ID$: 사용자 *의 인증ID

4.3 사용자 가입 및 인증 단계

다음의 [Fig. 2]는 공공기관 클라우드 데이터센터에 접속하기 위한 사용자 ID를 발급받기 위한 사용자 가입 및 인증 단계이다. 사용자는 공공 클라우드 서버로부터 사용자 인증티켓을 발급받아 해당 공공기관 클라우드 데이터센터를 사용할 수 있는 그룹의 구성원으로 증명 받고, 발급받은 인증티켓을 기반으로 해당 사용자의 ID를 생성하여 발급받는 과정을 보여준다.



[Fig. 2] service registration and authentication phase

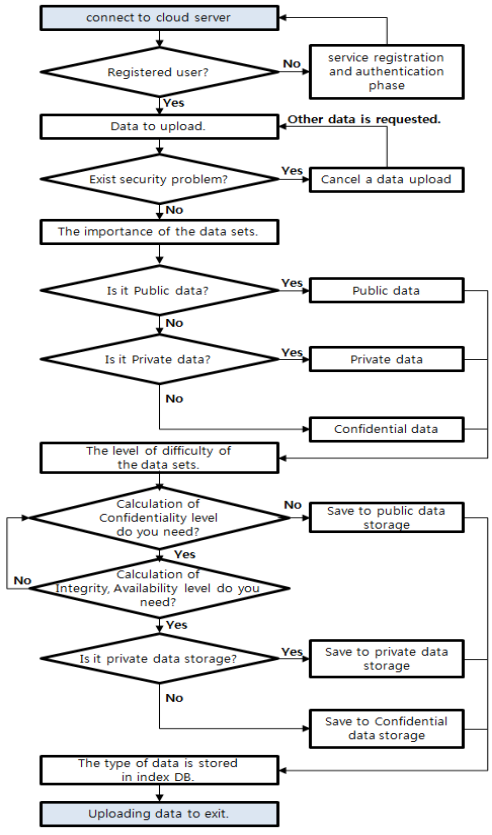
- step 1 : 사용자는 소속된 공공기관 그룹의 클라우드 서버에 접속을 한다.
- step 2 : 공공기관 클라우드 서버는 접속한 해당 사용자가 기존에 가입된 사용자인지 클라우드 서버의 데이터베이스를 통해 중복 가입 여부를 확인한다.
- step 3 : 공공기관 클라우드 서버는 해당 사용자의 중복 가입 여부 확인을 완료한 뒤 사용자 ID 생성을

위해 공공 클라우드 서버 자체의 난수값과 타임스탬프값을 연산한 인증티켓를 생성하여 해당 사용자의 공개키로 암호화하여 전송한다. ($E_{PK_{User_A}}[N_{SV_1} \| T_{SV_1}]$)

- step 4 : 사용자는 전송받은 공공 클라우드 서버의 인증티켓을 자신의 개인키로 복호화한 후, 해당 값에 사용자가 랜덤으로 지정하는 개인정보값을 연접하여 서버의 공개키로 암호화하여 전송한다. 이는 해당 사용자가 정당한 사용자라는 것을 증명하게 된다. ($E_{PK_{SV}}[N_{SV_1} \| T_{SV_1} \| UI_A]$)
- step 5 : 공공기관 클라우드 서버는사용자로부터 전송받은 인증정보를 복호화하여 사용자의 개인정보값을 획득한다. 복호화하여 획득한 난수값과 타임스탬프값이 서버가 생성한 값과 동일하다는 것을 기반하여 해당 사용자와의 통신이 안전하고 정당한 통신임을 확인한다. (UI_A 획득, N_{SV_1}, T_{SV_1} 검증)
- step 6 : 공공기관 클라우드 서버는 획득한 사용자의 개인정보값을 서버의 랜덤값과 새로 생성한 타임스탬프값을 연산하여 사용자 ID를 생성한다. ($User_AID = H[UI_A \oplus N_{SV_2} \oplus T_{SV_2}]$)
- step 7 : 공공기관 클라우드 서버는 생성된 사용자 ID를 서버의 데이터베이스에 저장한 뒤 해당 사용자에게 사용자의 공개키로 암호화하여 전송한다. ($E_{PK_{User_A}}[User_AID]$)
- step 8 : 해당 사용자는 새롭게 발급받은 사용자 ID를 획득하고 가입 및 인증 단계를 마무리한다. ($save: User_AID$)

4.4 데이터 저장 단계

다음의 [Fig. 3]은 공공기관 클라우드 데이터센터에 업로드하려는 데이터의 중요도를 공용/개인/기밀로 나누어 저장하는 데이터 저장 단계를 나타낸다. 사용자는 업로드하려는 데이터를 중요도를 설정하여 공용데이터/개인데이터/기밀데이터 스토리지로 나누어주고, 각각 기밀성/무결성/가용성의 난이도 등급을 나누어 해당 데이터의 난이도를 산정하여 등급에 따라 알맞은 스토리지에 데이터를 저장하는 과정을 보여준다.



[Fig. 3] Data upload phase

- step 1 : 사용자는 사전에 가입을 마친 자신이 소속된 공공기관 클라우드 망에 접속한다.
- step 2 : 공공기관 클라우드 서버는 전송받은 사용자 ID와 서버의 데이터베이스에 저장된 해당 사용자의 사용자 ID와 비교하여 접속을 승인한다. 해당 사용자가 데이터베이스에 등록되어 있지 않은 사용자라면 접속을 불허하고, 가입단계로 돌아간다.
- step 3 : 사용자는 데이터를 업로드 하여 보안성 검사 툴을 통해 1차적으로 해당 데이터의 정당성을 검증 받는다. 결과에 따라 바이러스 및 악성코드 등의 감염과 같이 보안 문제점이 발생할 경우에 공공기관 클라우드 서버는 데이터 업로드를 강제적으로 취소시킨다.
- step 4 : 사용자는 검증이 완료된 데이터에 대해서 중요도를 설정해준다. 데이터는 용도에 따라 공용데이터/개인데이터/기밀데이터 스토리지로 나뉘어준

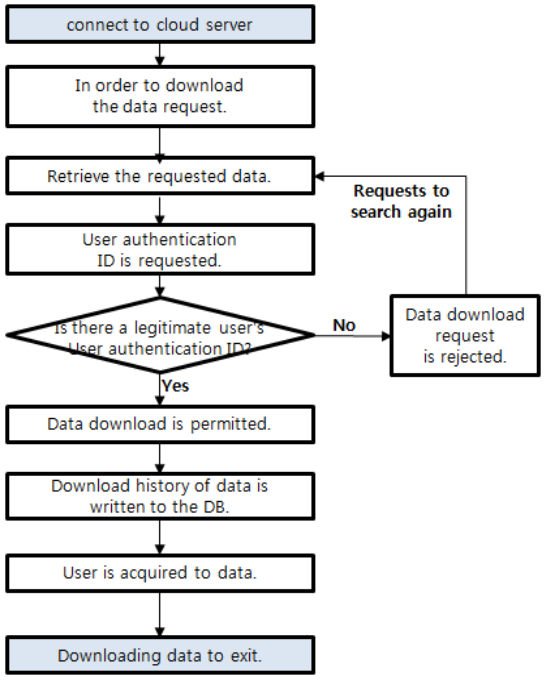
다. 나누어진 데이터에는 각각 기밀성/무결성/가용성의 난이도를 1~5사이의 등급을 산정한다. 산정한 데이터의 난이도 등급에 따라 해당 스토리지에 맞는 구역에 저장한다. 이는 데이터의 중요도에 따라 유형별로 저장되기 때문에 공공기관 클라우드에 특화된 환경에서 안전한 데이터 관리가 가능하며, 난이도에 따라 세부적으로 저장되기 때문에 효율적인 데이터 관리를 가능하게 한다.

- step 5 : 저장이 완료된 데이터는 데이터의 유형 및 제목, 저장된 스토리지 구역번호 등을 데이터센터의 데이터베이스에 별도로 리스트업한다.

4.5 데이터 다운로드 단계

다음의 [Fig. 4]는 사용자가 공공기관 클라우드 데이터센터에 접속하여 사용자의 권한에 따라 사용을 원하는 데이터를 다운로드받기 위한 단계이다. 공공기관 클라우드 서버는 사용자로부터 데이터 다운로드를 요청 받았을 때 접속한 사용자로부터 해당 데이터가 저장되어 있는 등급의 스토리지에 접근할 수 있는 사용자 ID정보를 요청하고, 요청에 따라 해당 데이터가 저장된 스토리지에 접근권한을 판단하여 데이터를 다운로드 요청한 사용자에게 다운로드 되는 과정을 보여준다.

- step 1 : 사용자는 사전에 가입을 마친 자신이 소속된 공공기관 클라우드 망에 접속하여 사용을 원하는 데이터의 다운로드를 요청한다.
- step 2 : 공공기관 클라우드 서버는 데이터센터의 데이터베이스에서 사용자가 요청한 데이터를 검색한다.
- step 3 : 서버는 데이터를 요청한 사용자가 해당 데이터에 접근이 가능한 사용자인지 검증을 위해서 사용자에게 해당 데이터가 저장되어 있는 등급의 스토리지에 접근할 수 있는 사용자 ID정보를 요청한다.
- step 4 : 요청받은 사용자 ID정보를 사용자데이터베이스에 조회하여 해당 데이터에 대해 접근권한이 없는 사용자일 경우 사용자에게 해당 데이터의 요청을 불허하고 재검색을 요구하게 된다.
- step 5 : 서버는 사용자 검증이 완료되면 데이터의 다운로드를 허가한다. 또한 데이터 다운로드 이력은



[Fig. 4] Data Download phase

데이터센터의 데이터베이스에 기록하여 관리한다. 이는 허가받은 사용자로부터 데이터의 다운로드 요청이 수행되어도 해당 데이터의 사용내역 및 다운받은 IP주소 등을 기록함으로써 데이터를 지속적으로 안전하고 효율적으로 관리할 수 있게 한다.

- step 6 : 사용자는 자신의 개인키로 데이터를 복호화하여 데이터를 획득하고 다운로드 단계를 마무리한다.

5. 안전성 분석

본 장에서는 제안하는 데이터 관리 기법의 안전성을 앞선 3장에서 제시한 보안 요구사항에 따라 분석한다.

5.1 기밀성

제안하는 기법의 공공기관 클라우드 데이터센터에 접속하기 위한 사용자 인증ID ($User_A ID = H[UI_A \oplus N_{SV_2} \oplus T_{SV_2}]$)는 클라우드 서버가 생성하는 난수값, 타임스탬프값과 사용자가 랜덤으로 지

정한 개인정보값의 연산을 통해 생성된다. 따라서 해당되는 서버의 난수정보와 타임스탬프 정보를 알기 어렵기 때문에 해당 사용자 인증ID를 탈취하더라도 공공기관 클라우드 서비스를 사용할 수가 없다. 또한 데이터센터에 데이터를 업로드 할 때도 사용자 인증ID를 통해 데이터의 정당성을 검증받기 때문에 데이터를 안전하게 저장시킬 수 있다.

5.2 무결성

제안하는 기법은 해시함수 연산을 사용하여 사용자 인증ID를 생성하여 저장하게 된다 ($User_AID = H[UI_A \oplus N_{SV_2} \oplus T_{SV_2}]$). 생성된 사용자 인증ID는 데이터 업로드 과정에서 클라우드 서버의 데이터베이스와 비교를 통해 해당 데이터의 정당성과 무결성을 제공한다.($User_AID \stackrel{?}{=} DB_{SV}[User_AID]$)

5.3 가용성

제안하는 기법의 데이터 관리 기법은 데이터의 업로드시에 보안성 검사 툴을 사용하여 사전에 해당 데이터의 정당성을 검증 받는다. 결과에 따라 바이러스 및 악성코드 등의 감염과 같이 보안 문제점이 발생할 경우에 공공기관 클라우드 서버는 데이터 업로드를 강제적으로 취소시킨다. 이를 통해 악의적인 사용자로부터 악성 데이터 업로드 시도를 사전에 차단함으로써 서비스의 안전한 가용성을 보장한다.

5.4 사용자 인증

제안하는 기법의 공공기관 클라우드 서버가 생성하는 인증티켓($E_{PK_{User_A}}[N_{SV_1} \| T_{SV_1}]$)은 사용자가 데이터센터에 접속하기 위한 사용자 인증ID의 생성에 대한 정보를 가지고 있다. 악의적인 공격자는 해당 티켓 정보를 가로채더라도 서버에서 직접 발급한 난수값(N_{SV_1})과 타임스탬프 정보(T_{SV_1})를 획득하기 어렵기 때문에 해당 클라우드 서비스의 올바른 티켓 정보를 발급받을 수 없다. 그렇기 때문에 공공기관 클라우드 서비스를 사용하기 위한 사용자 인증ID 또한 발급받을 수 없기 때문에 정상적인 사용자임을 증명할 수 없다. 따라서 안전한 사용자 인증 기능을 제공한다.

6. 결론

사용자가 필요로 하는 각종 IT자원을 필요할 때마다

〈Table 3〉 Security Analysis

Categories	Security requirements	Proposed scheme
Confidentiality	· User authentication ID should only be verified by legitimate user and cloud server.	· User Authentication ID($User_AID = H[UI_A \oplus N_{SV_2} \oplus T_{SV_2}]$), the cloud server-generated random values, timestamp values, the value of your random private information is generated by the operation. · Even if an attacker steals user authentication ID, public Institution cloud service is not available. · When you upload data to the data center, user authentication ID to verify the validity of the data due to receive guarantee the confidentiality of the data.
Integrity	· Prevent data forgery/modulation for safe and effective data management.	· User authentication ID using the hash function operation is generated. · User authentication ID, data upload process of the server in the cloud is compared with the database. Based on the results of the validity and integrity of the data is provided.
Availability	· Block malicious activity that attempts to upload malicious data and inject malicious code.	· When uploading data, and security test tool to use to verify the validity of the data in advance. · In the event of security problems to upload the data to cloud servers forcibly canceled by the availability of the service to ensure safety.
User authentication	· A source of message or data user sent should be clear, it should be verifiable to identify the user.	· The malicious attackers are issued directly from the server random value(N_{SV_1}) and timestamp information(T_{SV_1}), because it is difficult to obtain, and cloud services can not be issued a valid ticket information. · Attacker to use a Public Institution cloud service for user authentication ID because it can not be issued, secure user authentication capabilities.

네트워크를 통해 서비스 형태로 이용하는 방식인 클라우드 컴퓨팅 서비스가 대중적으로 보급됨에 따라 공공분야에서 해당 서비스의 도입에 대한 관심이 증가하고 있다. 이에 따라 해외주요국을 포함한 국내에서는 클라우드 컴퓨팅을 공공분야에 도입하거나 계획하고 있으며 점차 구체적으로 구축하고 있다. 하지만 공공분야에서의 클라우드 도입 및 활성화를 위해서는 서비스 가용성 장애요인 및 보안 위협에 대한 해결방안을 모색할 필요성이 있다. 따라서 본 논문에서는 공공기관 클라우드 데이터센터에서 활용 가능한 공개키 기반의 안전한 데이터 관리 기법에 대해서 제안하였다.

이를 통해 공공기관에 클라우드 컴퓨팅을 도입할 때 인증 받은 사용자만 데이터센터를 사용할 수 있고, 공공데이터의 중요도와 난이도를 공용데이터, 개인터이터, 기밀데이터로 설정해주어 체계적이고 안전하며 효율적으로 데이터 관리를 가능하게 한다. 따라서 공공기관에서의 클라우드 서비스에 대해 전반적인 보안성과 편의성을 향상시킬 수 있을 것으로 기대된다.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2012-010886)

This work was supported by the Soonchunhyang University Research Fund.

REFERENCES

[1] Ministry of Security and Public Administration, “Administration introduced Cloud Office Environment Guidelines”, 2012

[2] Yukyeng Wi, Jin Kwak, “A Study on Secure Data Management Scheme in Cloud Environment in the Public Sector”, The 38th conference of the KIPS, Vol. 20 No.1, pp580-583, 2013

[3] NIA, “CIO report Vol.17”, 2009

[4] KILD, “Local Informatization Magazine Vol 73”, pp60-65, 2012

[5] Sun-Young Shin, Suk-hyun Song, “A Priority Study for Applying Public Cloud Services in Korea by Mapping the SRM with Overseas Cloud Services in the Public Sector”, Internet and Information Security, Vol 3, No.3, pp67-89, 2012

[6] KILD, “Local Info. Issue. No.2”, 2012

[7] Ministry of Security and Public Administration, “Current Status and future plans for a government cloud”, 2012

[8] Shin, Ji-Yeon, Baek, Seoung-Ik, Kim, Joung-Woo, “A Study on Domestic Cloud Computing Service Policy Evaluation and Developmental Direction”, The Korean Operations Research and Management Science Society, pp1109-1118, 2012.

[9] Ministry of Security and Public Administration, “Diffusion cloud computing strategy and competitiveness”, 2011

[10] Hong-Sung Kim, Hyong-Shik Kim, “A Cloud Storage Gateway to Guarantee the Confidentiality of User Data”, Korea Institute of Information Security and Cryptology, Vol 22 No.1, pp131-139, 2012. 2.

[11] Kim Dae Gun, Choi Jun Yeol, Lee Seong Woo, Youn Hee Yong, “Distributed Data Management System based on Cloud Computing”, Korea Multimedia Society, Vol 13 No 2, pp600-604, 2010

[12] Kyong-Ha Lee, Hyunsik Choi, Yon Dohn Chung, “Massive Data Processing and Management in Cloud Computing: A Survey”, korea information science society, Vol 38 No.2, pp104-125, 2011. 4.

[13] Jin Yoo, “A Study on the efficient Data center building in the cloud computing environment”, The 36th conference of the KIPS, Vol. 18 No.1, pp201-203, 2011. 5.

[14] Ju Young Choi, Hyung-Jong Kim, Choon-Sik Park, Myuhng-Joo Kim, “Integrated Security Management for Cloud Data Center”, Korea Society for Internet Information, Vol 12 No 1, pp43-44, 2011

[15] Sang-Yun Lee, Hong-Joo Yoon, “The Study on Development of Technology for Electronic

Government of S. Korea with Cloud Computing", Korea Institute of Electronics Communications Society, Vol 7 No 6, pp1245-1258, 2012. 12.

위 유 경(Wi, Yukyeong)

・2012년 2월 : 순천향대학교 정보보호학과(공학사)
・2012년 2월 ~ 현재 : 순천향대학교 정보보호학과 석사과정
・관심분야 : 정보보호제품평가, 클라우드 컴퓨팅 보안, 제어시스템 보안, 콘텐츠 보안
・E-Mail : ykwi@sch.ac.kr

곽 진(Kwak, Jin)

・2000년 8월 : 성균관대학교 생물기전공학과(공학사)
・2003년 2월 : 성균관대학교 컴퓨터공학과(공학석사)
・2006년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
・2007년 3월 ~ 현재 : 순천향대학교 정보보호학과 교수
・관심분야 : 자동차 보안, 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안
・E-Mail : jkwak@sch.ac.kr