클라우드 컴퓨팅에서 신뢰하지 않는 서버 데이터의 안전한 접근

서울여자대학교 ▌김진형* · 김윤정** · 박춘식

1. 서 론

클라우드 컴퓨팅 환경에서 제공되는 클라우드 서비스는 사용자에게 IaaS(Infrastructure as a Service), PaaS (Platform as a Service)와 SaaS(Software as a Service)의 형태로 제공된다[1-3].

사용자가 특정 장치를 이용하여 웹 통신으로 클라우드 컴퓨팅 서비스를 제공받을 때, 서비스를 위한 대부분의 작업은 클라우드 컴퓨팅의 환경에서 이루어지지만 사용자의 개인 정보와 서비스의 일부 정보는 사용자의 단말이 보유하고 있다. 이러한 클라우드 서비스의 이용 흐름에 있어서 그림 1과 같이, 클라우드 컴퓨팅 서비스 제공자, 서비스 제공자와 클라이언트 간의 통신, 보안위협을 내포하고 있는 단말 등 곳곳에서 보안상 문제를 야기할 수 있다.

클라우드 컴퓨팅 환경이 주로 사용자가 데이터를 보유하지 않고 데이터 센터 내에 논리적으로 분리된 저장 공간에서 데이터가 공유되는 환경이기 때문에 데이터 보안의 중요성은 더욱 의미 있게 된다. 즉, 데이터를 외부에서 관리하는 저장소에 저장하는 것이 주요 이슈인 클라우드 컴퓨팅 환경에서는 데이터 보안이 클라우드 컴퓨팅의 성패를 좌우하는 핵심 요소 중 하나임에 분명하다.

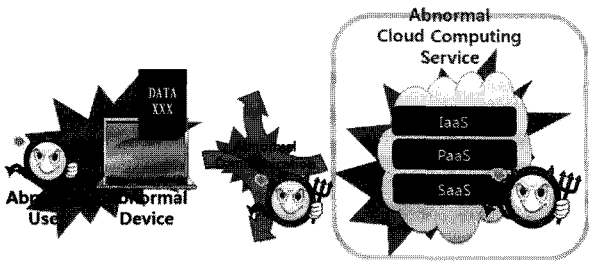

그림 1 클라우드 컴퓨팅 서비스의 보안상 취약점

클라우드 컴퓨팅 서비스에서의 보안 이슈를 분석하고, 데이터를 보관하는 과정에서 발생 가능한 위협 및 취약점에 대한 정리가 필요하며, 이 취약점을 방지할 수 있는 방안이 마련되어 안전성을 보장할 수 있는 서비스 제공이 마련되어야만 한다. 이에 본 논문에서는 이러한 클라우드 데이터 저장 구조에 적합한 보안 모델에 대하여 살펴보고자 한다.

2. 관련 연구

2.1 클라우드 컴퓨팅 서비스 적재 모델 및 큐브모델[3]

클라우드 시큐리티 얼라이언스에서는 그림 2와 같이, 클라우드 컴퓨팅 적재 모델인 Public, Private, Hybrid 모델 별로 기반시설의 소유자 및 관리자를 분석 비교하고 있다. Public 모델의 경우 제 3의 외부 기관이 기반시설을 소유하고 관리하며 따라서 신뢰적이지 않다고 볼 수 있다. 그림 3에 데이터가 저장되는 저장소가 영역별로 구분되어 표시되어 있다. 외부 영역(outsourced)으로 표시된 영역에 데이터가 저장되고 이를 이용한 서비스가 사용될 때 보안 문제는 더욱 중요한 요소로 부각되게 된다.

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization Or Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] Management includes: governance, operations, security, compliance, etc..
[2] Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment
[3] Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control
[4] Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

그림 2 클라우드 컴퓨팅 적재 모델

* 학생회원
** 종신회원

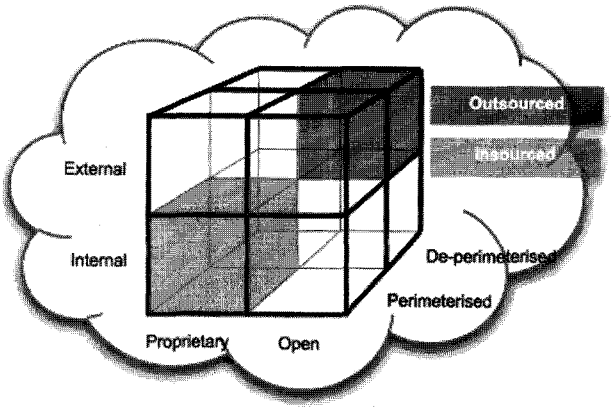

그림 3 클라우드 큐브 모델

클라우드 컴퓨팅 환경에서의 보안 제어는, 대부분, 일반적인 IT 환경에서의 보안 제어와 유사하다. 그러나 클라우드 서비스가 동작하도록 하는 운용방법과 기술들이 이용됨으로써, 전통적인 IT에서 만족했던 해결안만으로 클라우드 컴퓨팅의 보안을 해결하기 어려운 여지가 있다. 클라우드 컴퓨팅 환경에서는, 운영 책임을 맡는 제 3의 기관이 하나 또는 그 이상임을 유지하는 동안 제어를 잃게 될 여지가 높다.

2.2 CSA(Cloud Security Alliance)의 관리 영역(Governance Domains)과 운용 영역(Operational Domains)[3]

CSA에서는 클라우드 컴퓨팅의 분야를 12개의 도메인으로 나누어 제안하고 있으며, 이들은 전략적이고 전술적인 보안상의 취약점을 분류하는데 이용된다. 그리고 클라우드 서비스 및 배포 모델과 다양하게 조합하여 적용할 수 있다.

도메인은 관리영역 및 운용영역의 크게 두 가지 범주로 나눠진다. 관리영역은 클라우드 컴퓨팅 환경 안에서의 광범위한 전략과 정책적 이슈를 초점으로 두며, 운용영역은 더 전술적인 보안 문제 및 아키텍처 내에서 구현에 초점을 둔다.

2.3 전통적인 안전성 지원 기법들

클라우드 컴퓨팅 서비스의 안전성을 향상시키기 위해 암호화 기법을 적용할 수 있다. 적용 가능한 기술적 방안으로 데이터의 안전한 통신을 위한 세션 연결을 가능하게 하는 보안 프로토콜과 이 때 사용되는 암호화 알고리즘 및 키 관리 기법 등이다.

2.3.1 보안 프로토콜

클라우드 컴퓨팅의 보안을 위하여 통신 보안에 사용할 수 있는 프로토콜에는 IPSec, TLS, S/MIME 그리고 무선 보안 기법에 해당하는 WPA/WPA2, 와이브로 보안 기법에 해당하는 PKM기법 등이 있다.

2.3.2 암호 알고리즘

데이터를 안전하게 저장하거나 전달하기 위하여 적용가능한 대표적인 알고리즘은 비밀 키 알고리즘으로 DES(Data Encryption Standard)와 AES(Advanced Encryption Standard)가, 공개키 암호 알고리즘으로 RSA (Rivest-Shamir-Adleman) 방식과 ECC(Eliptic Curve Cryptography)가 있다.

2.3.3 키 관리

키 교환 프로토콜로 사용할 수 있는 Oakley Key Determination Protocol은 인증된 두 사용자가 안전하게 비밀키를 전송하는 방법으로 Diffie-Hellman 키 교환 방식에 기반하고 있다. ISAKMP(Internet Security Association and Key Management Protocol)은 IPSec에서 SA 설정, 협상, 변경, 삭제 등 SA 관리와 키 교환 정의하고 있다. 위의 두 가지 방식의 장점을 취하여 통합한 키 교환 방식이 IKE(Internet Key Exchange)이다. IKE는 키 교환 및 SA 협상을 위하여 Oakley와 ISAKMP를 결합한 프로토콜이라고 할 수 있다.

2.4 경량암호

네트워크 기술의 발달로 클라우드 컴퓨팅 서비스를 무선 환경에서도 제공받을 수 있게 되었다. 이에 데이터의 안전성을 위하여 암호화 기법을 사용하고 있으나, 암호화 기법 적용 시 무선 환경에서는 연산용량이 작은 무선 단말장치들이 범용 암호의 수행 연산을 수용하기가 어려운 것이 현실이다. 이에 용량이 작은 무선 단말 장치에서도 잘 동작하는 경량의 암호 기술이 필요하다.

2.4.1 범용 알고리즘의 경량 구현

범용 알고리즘을 RFID 등의 경량의 무선 단말 장치에 구현하기 위한 여러 연구들이 진행되어 왔다. 대상 알고리즘은 DES[4,5], AES[6], RSA[7,8], ECC[9-11] 등 다양하다.

2.4.2 경량 암호 알고리즘

설계초기부터 경량 암호로 구성된 암호 알고리즘들이 있으며, 여기에는 HIGHT 등이 있다[12].

2.5 서버지원 암호

서버 지원 연산(Server Aided computation)는 신뢰할 수 없는 통신 환경에서 서버를 인증 하는 것을 통해 신뢰된 통신을 보장하고자 제안 된 방법이다. 신뢰할 수 없는 단말 또는 서버와의 통신이 필요할 때, 신뢰

된 서버와의 서명을 통한 인증을 기반으로 신뢰할 수 있는 사용자임을 확인 한다[13].

2.6 클라우드 컴퓨팅에서 사용 가능한 단말

단말 기술이 발달함에 따라 성능은 좋아지고, 크기는 작아지는 효율적인 단말이 나오게 되었다. 또한 스마트 폰 기술이 발달 하면서, 언제 어디에서나 데이터 서비스를 필요로 하는 수요가 증가하게 되었다. 이러한 환경에서의 클라우드 서버를 이용한 데이터 서비스의 제공은 필수 조건으로 부상하고 있다. 기본적으로 컴퓨팅 서비스를 제공해 주는 PC에서부터 노트북 및 스마트폰에 이르기까지 클라우드 데이터 서비스를 사용할 수 있는 다양한 단말에 따라 제공받아야 하는 서비스가 달라진다. 기본적으로 사용하고 있는 PC에서부터, 이동단말의 대표적인 노트북 및 초소형 단말인 스마트 폰을 통한 데이터 통신 등, 다양해진 단말에 따라 데이터 보안 모델을 다르게 적용해야할 필요가 생겼다. 이에 본 장에서는 클라우드 컴퓨팅 데이터 서비스를 수행할 수 있는 단말을 분류 해 보고, 각 단말에 적합한 데이터 보안 모델이 어떠한 것이 있는지 적용해 보고자 한다.

2.6.1 PC(Personal Computer)

일반적으로 가장 많이 사용하고 있는 단말로, 운영체제를 기반으로 서비스를 수행할 수 있도록 해 주는 장치이다. 운영체제 위에 응용 프로그램을 구동하는 형태로 운영되며, 사용자는 브라우저 및 프로그램을 통해 클라우드 서비스를 제공받게 된다. 입출력장치를 통해 사용자는 컨트롤을 수행하며, 유선 네트워크 환경을 통해 클라우드 서버에 접속하여 안정적인 서비스를 제공 받는다. 유선 네트워크 환경을 사용하여 빠른 데이터 이동 속도를 보장할 수 있으며, 단말의 크기가 크고 용량이 크기 때문에 좋은 성능의 장비로 분류할 수 있다. 따라서 고용량의 암/복호화 연산을 적용한 데이터 서비스가 가능하다.

2.6.2 노트북(Notebook)

PC와 같이, 컴퓨터를 사용하는 사용자들이 이동환경에서 가장 많이 사용하고 있는 단말이다. 노트북의 경우 PC의 기능 및 성능을 어느 정도 압축 해 놓은 것으로, 대부분 동일한 기능을 수행하는 운영체제를 사용하는 환경을 가지고 있는 단말이다. PC에 비해 성능이 비교적 떨어지긴 하지만, 칩 기술 등의 발달로 노트북의 경우 고사양의 제품이 많이 나와 있다. 클라우드 서비스는 동일한 형태로 제공받게 된다. 네트워크 환경은 유선 및 무선 환경의 접속이 가능하며, 실내에

그림 4 스마트폰: 아이폰 및 안드로이드폰[14]

고정되어 있는 환경에서 사용하는 경우 성능이 좋은 유선을 사용하며, 이동 환경에서는 무선 네트워크(Wi-Fi 등)를 사용한다. 유선에 비해 무선 환경을 사용하는 경우 성능이 떨어지긴 하지만, 이동성이 있다는 점을 장점으로 꼽을 수 있다.

2.6.3 스마트 폰(Smart Phone)

스마트폰의 경우, 기존의 PDA와 같이 소형 컴퓨터이긴 하지만 기본적인 기능을 탑재하고, 이동성을 보장하기 위한 것으로 개발된 초소형 단말이다. 최근 아이폰 및 안드로이드 폰 등 초소형의 고급 운영체제를 탑재한 단말이 나오고 있다. 3G환경을 사용하는 셀룰러 폰인 전화 및 문자 기능에 데이터 통신 기능을 강화 시킨 단말로 보는 관점도 가능하다. 데이터 통신이 강화된 단말을 사용한 클라우드 데이터 서비스는 적은 용량을 가지고 있는 스마트폰 단말에 적합한 서비스이다. 네트워크 환경은 이동성을 강화 시킨 것으로 무선 환경을 사용하며, 3G 및 Wi-fi, Wibro, Bluetooth 등을 사용한다. 단말에 많은 용량의 데이터를 저장 보관 할 수 없으므로, 서버를 이용하여 읽기 기능을 보완한 서비스를 제공해 주는 형태로 현재 데이터 서비스를 진행 중이다. 데이터의 안전성을 위한 암/복호화 기술 등을 적용하고자 할 때, 효율적인 암/복호화를 위한 기술이 필요하다.

3. 클라우드 컴퓨팅 데이터 보안의 취약점 분석

본 절에서는 클라우드 컴퓨팅 데이터 보안의 취약점을 기존 연구들을 중심으로 기술한다.

3.1 클라우드 컴퓨팅 데이터 보안 취약점 관련 연구들

3.1.1 ENISA의 클라우드 컴퓨팅 위협요소[15]

표 1 ENISA의 클라우드 컴퓨팅 위협요소

위협 요소	설명
운영 상실	클라우드 구조 이용 시에 클라이언트가 클라우드 공급자에 대한 제어를 중단할 수 있다.
내부에의 잠금	데이터, 응용프로그램, 서비스의 이식성에 대한 지원이 가능한지 여부가 고려되어야 한다.
고립 실패	저장소, 메모리, 라우팅 정보 등을 격리하는 것이 실패할 수 있다. 이것은 다른 위협들에 비하여 상대적으로 덜 발생한다.
보증 위협	공개 클라우드 구조를 이용하는 경우 일부 보증(compliance)이 얻어질 수 없다.
관리 인터페이스 손상	공개 클라우드 공급자의 고객 관리 인터페이스는 인터넷 등을 통하여 접근할 수 있으며, 이것은 원격 접근이나 웹 브라우저 취약점으로 인한 보안 위협을 초래할 수 있다.
데이터 보호	클라우드 컴퓨팅은 클라우드 고객이나 공급자에 대하여 여러 가지 데이터 보호 위협에 직면하게 된다.
안전하지 않고 불완전한 데이터 삭제	데이터 삭제가 보통 완전삭제가 아닌 1차 삭제만으로 진행된다.
악의적인 내부사용자	악의 적인 행동을 하는 내부 사용자로 인한 위협

위협 요소를 정리 해 보면 다음 표 1과 같다.

3.1.2 CSA의 클라우드 컴퓨팅 주요 위협 요소[16]

CSA에서는 클라우드 컴퓨팅 주요 위협 요소를, 클라우드 컴퓨팅의 잘못된 사용(Abuse and Nefarious Use of Cloud Computing), 안전하지 않은 인터페이스와 API (Insecure Interfaces and APIs), 악의적인 내부자(Malicious Insiders), 공유되는 기술 요소들(Shared Technology Issues), 데이터 손실 및 손상(Data Loss or Leakage), 계정 또는 서비스 가로채기(Account or Service Hijacking), 알려지지 않은 위험 목록(Unknown Risk Profile)로 분류하여 설명하고 있다.

3.1.3 Coblentz의 클라우드 컴퓨팅 데이터 보안[17]

가. 데이터 손실 및 손상: 조직 관리자의 데이터 삭제
나. 데이터 손실 및 손상: 데이터 센터가 임시적으로 또는 영구적으로 이용가능하지 않게 되는 것.
다. 자국 내 모든 데이터 센터가 임시적으로 또는 영구적으로 이용가능하지 않게 되는 것.
라. 데이터 손실 및 손상: 해커가 데이터를 파괴한다
마. 권한 없는 데이터 접근: 조직 관리자가 데이터를 접근한다.
바. 권한 없는 데이터 접근: 해커가 데이터를 접근한다.

3.1.4 Gartner의 클라우드 컴퓨팅 보안 위협 요소[18]

Gartner에서는 클라우드 컴퓨팅 보안 위협을, 권한 있는 사용자만이 정보에 접근하도록 하는 것(Privileged user access), 법적인 보증(Regulatory compliance), 자국/타국 등 데이터가 저장되는 곳(Data location)이 어디인지 여부, 암호화를 통한 데이터 격리 문제(Data segregation), 재난시의 복구(Recovery), 조사의 어려움(Investigative support), 공급자의 기간 지속여부(Long-term viability) 등으로 나누어 설명하고 있다.

3.1.5 Wang 등의 클라우드 컴퓨팅에서의 데이터 보안 위협[19]

가. 데이터 보안을 위하여 이용되는 전통적인 암호 기법이, 클라우드 컴퓨팅 환경에 직접 적용되지는 않는다. 따라서 클라우드 환경에 맞는 암호 기법이 제공되어야 한다.

나. 클라우드 컴퓨팅은 단순히 제 3의 기관에 데이터를 보관하는 기능만을 제공하는 것은 아니다. 클라우드 컴퓨팅에서 저장되는 데이터들은 사용자에 의하여 빈번하게 삽입(insertion), 삭제(deletion), 수정(modification), 첨부(append), 재순서화(reordering) 등의 갱신이 일어난다. 즉, 동적 갱신(dynamic update)이라는 특성을 갖는 데이터를 안전하게 다루기 위한 방안이 마련되어야 한다.

다. 데이터가 저장되는 데이터센터는 보통 한 곳이 아닌 여러 곳이다. 단일 저장소에서 분산 저장소(distributed storage)로 되었을 때 발생할 위협요소들에 대비해야 한다.

4. 신뢰하지 않는 서버에 저장된 데이터의 안전한 접근 모델

클라우드 컴퓨팅 환경에서는 파일 소유자가 외부 저장소에 파일을 저장하게 된다. 이 때 인증을 담당하는 별도의 제 3의 감사자를 둘 수도 있다. 외부 저장소에 장기간의 대규모 데이터를 저장하는 방안은 가격과 복잡성에서 경제적인 이점을 제공한다. 그러나 클라우드 서비스 제공자(CSP: cloud service providers)들이 데이터 소유자의 내부가 아닌 외부 기관이어서 소유자가 데이터를 전적으로 제어하는 것이 아니라고

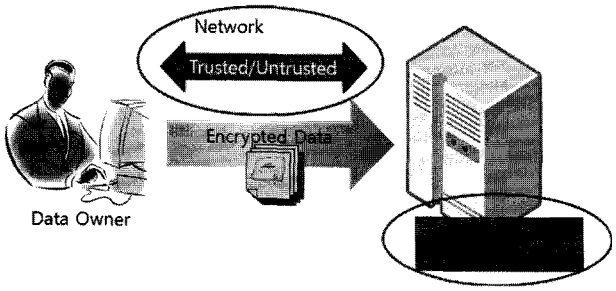

그림 5 클라우드 서버를 이용하는 데이터 보안 모델

볼 수 있다. 결과적으로, 클라우드 컴퓨팅 환경에서의 데이터의 정확성은 내부와 외부로부터 주어지는 광범위한 데이터 무결성 위협에 처해 있다고 볼 수 있으며, 이 위협에는 소프트웨어 결함, 관리적 결함, 장치 이상 및 신뢰적이지 않은 클라우드 서버의 동작 등도 포함된다. 클라우드 컴퓨팅의 저변 확대를 위해서는 외부 저장소에 저장된 데이터를 안전하게 관리하는 효율적 방안이 마련되어야 한다.

클라우드 서버를 이용한 데이터 서비스는 그림 5와 같이 데이터의 소유자가 클라우드 서버에 파일을 보관 하는 과정에서 시작된다. 이러한 과정에서 서버의 안전성과 서버까지 도달하는데 사용하는 네트워크 통신 환경에 대한 안전성을 고려하게 된다. 이러한 과정을 고려하여 생각하면 4가지 경우의 수가 발생한다. 즉, 이때 구분 기준은 서버의 신뢰도와, 서버와의 통신 환경에서 사용하는 통신 환경의 신뢰도이다. 클라우드 컴퓨팅 데이터 보안 모델을 표 2와 같이, 4가지 경우로 나누어 볼 수 있다. 이 중 본 논문에서 고려한 데이터 모델 환경은 안전하지 않은 서버를 갖는 환경이다. 이 경우는 다시, 통신 환경이 각기 안전한 경우와 안전하지 않은 경우로 나눌 수 있다. 안전하지 않은 통신환경은 전통적으로 제공되는 인증 및 암호화 방법을 사용하여 안전하게 처리될 수 있으므로, 이 2가지 경우를 달리 처리하지 않고 본 연구에서는 '안전하지 않은 서버'환경에 집중하여 보안 모델을 살펴보고자 한다.

표 2 클라우드 컴퓨팅 데이터 보안 모델 환경

	서버의 신뢰여부	통신환경의 신뢰 여부	본 논문에서 고려 여부
안전한 서버와 안전한 통신환경	신뢰됨	신뢰됨	고려하지 않음
안전한 서버와 안전하지 않은 통신 환경	신뢰됨	신뢰되지 않음	고려하지 않음
안전하지 않은 서버와 안전한 통신 환경	신뢰되지 않음	신뢰됨	고려 대상임.
안전하지 않은 서버와 안전하지 않은 통신 환경	신뢰되지 않음	신뢰되지 않음	

4.1 이체동형토큰 사용[19]

클라우드 데이터 저장시스템에서는 사용자는 데이터를 클라우드 서버에 저장하고 더 이상 지역적으로는 보관하지 않는다. 따라서 클라우드 서버에 데이터가 올바르고 가용성을 갖도록 저장됨을 보장하는 것은 매우 중요하다. 안전한 데이터 보관을 위해 토큰을 이용하여 데이터를 암호화 하여 보관 하도록 할 수 있으며, 이러한 기법을 통해 데이터의 무결성 및 안전성을 보장할 수 있다.

4.2 속성 값을 통한 인증 방법[20]

데이터에 접속하고자 하는 사용자의 역할이 여러 개 있을 수 있다. 인증서를 통해 사용자를 인증하고자 하는 경우, 여러 가지 역할에 대한 구분을 할 수 없다면, 여러 개의 인증서를 발급 하여 권한별로 확인하거나, 또는 데이터별이 아닌 사용자별로 권한을 관리 하여, 물리적인 서버의 접근 제어만 가능하게 된다. 이에 제안된 방법이 속성기반 데이터 사용자 인증 모델이다. Yu의 논문에서 제안된 방법은 PKI인증서에서 정의한 Extends Field에서의 값을 기반으로 사용자의 역할 속성을 정의 하고, 역할 속성에 따라 사용자를 구분하여

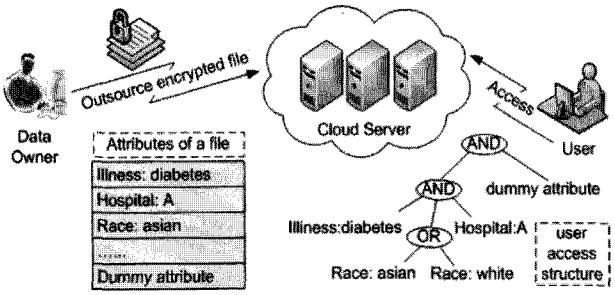

그림 6 속성기반 데이터 사용자 인증 모델

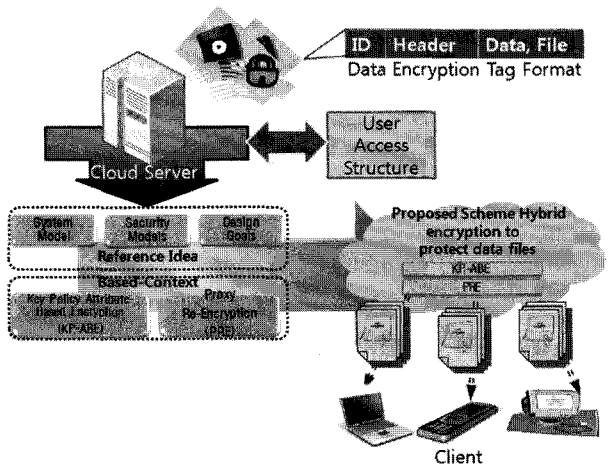

그림 7 클라우드 컴퓨팅 서버에 보관하는 데이터의 속성 기반 암호화 과정에 적용된 기법들

인증 하는 방법을 말한다. 그림 6은 클라우드 서버에 속성 값을 기반으로 암호화키를 만들어, 속성을 가지고 있는 사용자는 파일에 접근할 수 있도록 하는 방법을 나타내고 있다. 이러한 기법을 통해 효율적으로 데이터 접근 권한 관리를 할 수 있다.

그림 7은 그림 6에서 사용하는 속성 기반 데이터 암호화 및 인증 기법에 사용된 기술들을 정리한 것이다. 암호화에 사용되는 키를 기반으로 하는 속성 기반 암호화 기법과, 프록시 서버를 사용한 재 암호화 기술, 그리고 이들을 이용한, 사용자의 속성 트리 구조와의 통신 과정을 나타낸다.

4.3 효율성을 고려한 중재자를 이용한 암호 사용[13]

모바일 단말 등 효율적인 데이터의 이동을 필요로 하는 환경에서는 무거운 암호화 기법보다는 경량 암호 등의 효율적인 암호 알고리즘을 채택하여 적용하여야 한다. 그러나 경량암호의 안전성 및 비용 등의 이유로 이를 사용할 수 없는 경우, 기존의 암호 알고리즘을 사용하나, 중재자를 통해 일부 연산을 기 수행한 후 최종 사용자 단말에서는 일부 복호화만 가능하도록 하는 방법이 있다.

4.4 키 구조를 통한 안전한 데이터 보관

4.4.1 복잡한 키 구조를 통한 안전한 데이터 보관[21]

안전하지 않은 서버에 데이터를 보관 하고자 할 때, 서버에 대한 신뢰가 어렵기 때문에 데이터에 대한 안전한 보관 방법을 필요로 한다. 데이터에 접근 하고자 하는 사용자에 대해 키를 통해 사용자 인증을 하여, 권한이 있는 사용자만이 데이터에 접근할 수 있도록 하는 방안으로 복잡한 키 구조를 사용한 키 분배를 통해 데이터에 접근하는 사용자를 제한 할 수 있다. 데이터에 대한 접근 권한을 제한함으로써 안전한 데이터의 보관이 가능하도록 한다. 키 분배 구조를 복잡하게 구현하여 다단계 인증 등을 통하여 권한을 부여받은 사용자만을 안전하게 인증할 수 있도록 서버를 운영할 수 있다. 그림 8은 복잡한 키 구조를 통해 안전한 데이터를 보관할 수 있도록 하는 시스템의 구조를 의미한다.

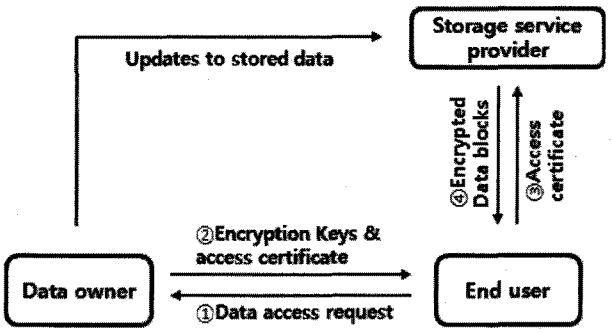

그림 8 복잡한 키 구조를 사용하는 시스템 구조

4.4.2 최소한의 키를 사용할 수 있는 방안을 이용한 사용자 인증/권한관리[22]

안전하지 않은 서버에 데이터를 보관할 때 데이터 보호를 위해 쿼리 테이블을 이용하는 방법을 사용한다. 데이터베이스 저장시 입력하는 쿼리를 통해 최소한의 키를 사용하여 사용자를 인증하는 방법을 사용할 수 있다. 이는 소형 단말(스마트폰 등)을 통한 사용자의 데이터 접근 요청시, 효율적인 인증 과정으로 적용할 수 있다. 키 관리, 권한에 대한 정책 적용 등을 정의할 때 쿼리를 이용하여 중복 연산을 제거하고 연산과정을 최소화 하여 적용하여 효율적이고 안전한 데이터 관리가 이루어질 수 있도록 한다. 그림 9는 정책에 따라 키를 최소화 하는 과정을 나타낸다.

5. 결 론

이상에서, 클라우드 컴퓨팅 데이터 보안의 취약점을 분석하였고, 클라우드 컴퓨팅 데이터의 무결성과 비밀성을 위한 보안 모델에 대하여 살펴보았다.

클라우드 컴퓨팅 데이터를 안전하게 이용할 있는 방안은 클라우드 컴퓨팅 서비스 접근을 안전하게 하는 주요 기반 요소이다. 또한, 안전한 데이터 접근을 위해 사용했던 클라우드 환경에서의 보안 기술을, 클라우드 환경의 다른 서비스에도 적용함으로써 클라우드 컴퓨팅의 전반적인 안전성 증가에 기여할 수 있을 것이다.

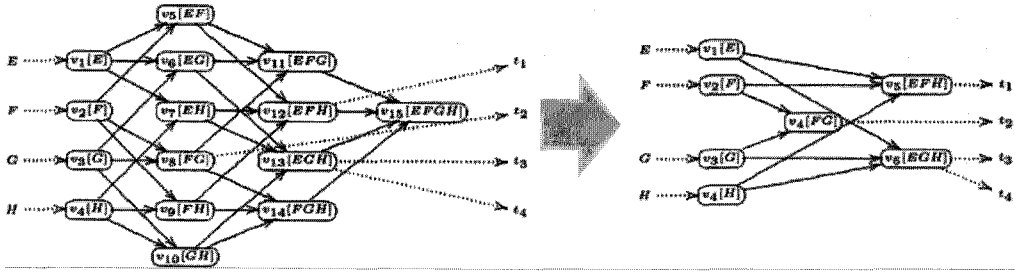
그림 9 정책에 따라 키를 최소화 하는 과정

참고문헌

[1] 민옥기, 이미영, 허성진, 김창수, 훤히 보이는 클라우드 컴퓨팅(ETRI easy IT), 전자신문사, 2009년 10월

[2] 마이클밀러 저, 최윤석 역, 사례로 읽는 클라우드 컴퓨팅, 에이콘출판사, 2009년 2월

[3] Cloud Security Alliance, Security Guidance for Critical areas of focus in cloud computing version 2.1, December, 2009 http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[4] I. Verbauwhede, F. Hoornaert, J. Vandewalle, and H. De Man, "Security and Performance Optimization of a New DES Data Encryption Chip", IEEE Journal of Solid-State Circuits, 23(3):647~656, 1988

[5] Leander, C. Paar, A. Poschmann, K. Schramm "New Lightweight DES Variants", Fast Software Encryption 2007-FSE 2007, Luxembourg City, Luxembourg, März 26-28, 2007.A

[6] M. Feldhofer, J. Wolkerstorfer, V. Rijmen, "AES Implementation on a Grain of Sand", Information Security, IEE Proceedings, Vol. 152, Nr. 1, pp. 13-20, 2005

[7] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-Key Cryptography for RFID-Tags", Proceedings of IEEE International Workshop on Pervasive Computing and Communication Security 2007, New York, USA 2007

[8] Yoonjeong Kim, SeongYong Ohm, Kang Yi, "Privacy-Preserving RFID Authentication Using Public Exponent Three RSA Algorithm", IEICE transaction on Information Systems, Vol.E92-D, No.3, pp. 545-547, March, 2009

[9] Johannes Wolkestorfer, Hardware Aspects of Elliptic Curve Cryptography, PhdThesis, Graz University of Technology, Graz, Austria, 2004

[10] SandeepKumar, ChristofPaar, "Reconfigurable Instruction Set Extension for enabling ECC on an 8-bit Processor", International Conference on Field-Programmable Logic and Applications (FPL) 2004, Antwerp, Belgium, August 30 -September 1, 2004

[11] Sandeep Kumar and Christof Paar, "Are Standards Compliant Elliptic Curve Cryptosystems feasible on RFID?", Workshop on RFID Security 2006, Graz, Austria, July, 2006

[12] HIGHT 블록암호 알고리즘 사양 및 세부 명세서, 한국인터넷진흥원, 2009

[13] Matsumoto, Kato, Imai, "Speeding up secret computations with insecure auxiliary devices", EuroCrypt'92, LNCS 658, Springer-Verlag, 1993, 153-162

[14] www.apple.co.kr, www.samsungmobile.com

[15] ENISA(European Network and Information Security Agency), Cloud Computing: Benefits, risks and recommendations for information security, November, 2009

[16] Cloud Security Alliance(CSA), Top Threats to Cloud Computing v1.0, March, 2010

[17] Nick Coblentz, Cloud Computing Data Security, March, 2004, http://nickcoblentz.blogspot.com/2009/03/cloud-computing-data-security.html

[18] Jon Brodkin, "Gartner: Seven cloud-computing security risks", Network World, July, 2008

[19] Cong Wang, Qui Wang, Kui Ren, Illinois Institute of Technology, "Ensuring Data Storage Security in Cloud Computing", IEEE International Workshop on Quality of Service(IWQoS), 2009

[20] Shucheng Yu., Cong Wan, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE INFOCOM 2010, 2010.3

[21] Vishal Kher, Yongdae Kim, "Securing Distributed Storage: Challenges, Techniques, and Systems", ACM International Workshop on Storage Security and Survivability(StorageSS), 2005

[22] Pierangela Samarati, Sabrina De Capitani di Vimercati, "Data Protection in Outsourcing Scenarios: Issues and directions", ACM Symposium on Information, Computer and Communications Security(ASIACCS), 2010

약 력

김 진 형

2006 서울여자대학교 정보보호공학과 학사
2008 서울여자대학교 대학원 컴퓨터학과 석사
2008~현재 서울여자대학교 컴퓨터학과 박사과정
관심분야 : 정보보호, 개인정보보호, 클라우드컴퓨팅
E-mail : jinny@swu.ac.kr

김 윤 정

1991 서울대학교 컴퓨터공학과 학사
1993 서울대학교 대학원 컴퓨터공학과 석사
2000 서울대학교 대학원 전기 · 컴퓨터공학부 박사
2000~2001 (주) 엔써커뮤니티 제품개발연구소 차장
2001~2002 (주) 데이타게이트 인터내셔널 보안기술연구소 차장
2002~현재 서울여자대학교 컴퓨터학부 정보보호학 전공 부교수
관심분야 : 암호학, 시스템 보안, 암호 응용
E-mail : yjkim@swu.ac.kr

박 춘 식

1995 일본동경공업대 공학박사
1982~1999 한국전자통신연구원 책임연구원
2000~2008 국가보안기술연구소 책임연구원
2009~현재 서울여자대학교 컴퓨터학부 정보보호학 전공 교수
관심분야 : 개인정보보호기술, 클라우드컴퓨팅보안
E-mail : csp@swu.ac.kr