공공 클라우드 환경에서 안전한 사용자 인증방안

이승아*, 조기환**
전북대학교 *전자정보공학부, **컴퓨터공학부
e-mail: {*salee86, **ghcho}@chonbuk.ac.kr

A Secure User Authentication Scheme for Public Cloud Environment

Seung-Ah Lee*, Gi-Hwan Cho**
*Division of Electronics and Information Engineering, Chonbuk University
**Division of Computer Science and Engineering, Chonbuk University

요 약

IT 업계에도 저탄소 녹색 성장을 추구하는 Green IT 시대가 찾아왔다. 이에 따라 여러 IT 기업들에서 IT 자원을 소유하지 않고 빌려 쓰는 형태의 클라우드 컴퓨팅이 큰 이슈가 되고 있다. 클라우드 컴퓨팅은 기존의 조직이 유지 보수에 사용하던 인력과 비용을 감소시킬 수 있다는 점에서 경제적 이익을 창출하고 있다. 그러나 다수의 이해당사자(Mlti-tenant)가 존재하는 공공 클라우드 환경에서는 사용자의 인증이 보안 문제로 대두되고 있다. 본 논문에서는 공공 클라우드 환경에서 신뢰할 수 있는 클라우드 서비스를 제공하기 위한 사용자 인증 방법을 제시한다. 사용자는 계약관계로 맺어진 클라우드와 조직 사이에서 클라우드 서비스를 제공받으며 조직으로부터 인증 받는다. 클라우드에서는 조직에서 제공하는 인증 정보와 클라우드의 서비스 제공 정책으로 이루어진 보안연계를 통해 사용자를 확인함으로써 사용자에게 적합한 서비스를 제공한다.

1. 서론

최근 Google, Amazon, Microsoft, IBM 등 IT 관련 글로벌 기업들이 선두하고 있는 클라우드 컴퓨팅은 Green IT 시대를 맞이하며 전 세계적으로 큰 이슈가 되고 있다. 국내에서도 삼성, SK 텔레콤, KT, LG 등 많은 기업들이 클라우드 컴퓨팅을 서비스하고 있으며, 일부 IT 기업들은 서비스를 위한 대용량의 데이터를 클라우드 컴퓨팅을 이용하여 처리하고 있다. 클라우드 컴퓨팅 기술이 표준화되고 안정화됨에 따라, 웹 기반, 모바일 장치 기반 등 클라우드 컴퓨팅의 적용 범위가 더욱 넓어질 것으로 전망된다.

클라우드 컴퓨팅은 클라우드 서비스 제공업체를 통해 IT자원 및 서비스를 제공받기 때문에 IT 자원을 소유하지 않고 일부 또는 모두를 아웃소싱하는 형태이다[1]. 이러한 클라우드 서비스는 IT 자원의 이용효율 및 자원 재활용성을 증가시키고, 인적 및 물적 자원을 감소시킴으로써 경제적인 이익을 창출한다. 그러나 시장 조사 기관인 IDC에 따르면 클라우드 서비스의 활용에 있어, 보안을 해결해야 할 첫 번째 과제로 꼽고 있다[2]. 외부 자원을 통해 아웃소싱되는 클라우드 서비스는 관련 조직에서 직접적인 관리가 불가능하기 때문에 여러 가지 보안 위협에 노출된다. 특히 사용자 접근에 관련된 보안문제가 큰 이슈로 떠오르고 있다. 저장된 데이터가 안전하게 보호되고 서비스되기 위해서는 사용자 접근 문제가 해결되어야 한다.

따라서 본 논문에서는 클라우드 환경에서 조직과 클라우드 제공자 모두 신뢰할 수 있는 사용자 인증 기법을 제안한다. 또한, 이 인증 기법을 사용하기 위해 필요한 요소들을 정의하고 인증 절차 및 서비스 절차를 설명한다. 사용자는 조직 내부의 인증구조를 이용해 인증 받는다. 조직은 인증된 사용자의 서비스 이용을 위해 클라우드와 계약을 기반으로 보안연계를 설정하고 이를 바탕으로 클라우드는 사용자에게 서비스를 제공한다. 이러한 인증구조를 통해 조직에서는 공공 클라우드를 사용하면서 개인 클라우드를 구성한 것과 같은 수준의 보안을 유지할 수 있다.

논문의 구성은 다음과 같다. 2장에서는 클라우드 컴퓨팅과 사용자 인증에 대한 관련 연구를 살펴본다. 3장에서는 제안하는 클라우드 컴퓨팅 환경에서의 사용자 인증 방법에 대해 설명하고, 4장에서 결론을 맺는다.

2. 관련연구

클라우드 컴퓨팅은 '인터넷 기술을 활용하여 여러 고객에게 IT 자원을 서비스하는 컴퓨팅'으로 정의할 수 있다[3]. 클라우드 컴퓨팅은 데이터 센터의 위치에 따라 크게 개인 클라우드(Private Cloud)와 공공 클라우드(Public Cloud)로 구분할 수 있다. 개인 클라우드는 기업 내부와 같은 폐쇄된 공간에 클라우드 데이터 센터를 운영하면서 특정 사용자만 사용하도록 하는 개념이다. 이러한 개인 클라우드는 조직 내에서 직접 관리하기 때문에 공공 클라우드에 비해 안전하지만 조직에서 유지 보수해야하므로 비용이 많이 든다. 반면에 공공 클라우드는 외부에 존재하는 데이터 센터를 이용하는 형태이다. 공공 클라우드는 클라

우드 사업자로부터 데이터 센터를 빌려 쓰는 것이기 때문에 조직의 유지보수 비용을 절감할 수 있으며 증설이 용이하다는 장점을 갖는다. 그러나 이러한 공공 클라우드는 공개되어 있는 데이터 센터에 대한 여러 가지 보안문제가 야기된다. 우선, 공공 클라우드에서 조직은 데이터 센터에 대한 직접적인 통제권을 갖지 못한다. 그러므로 데이터를 직접 관리할 수 없으며, 문제가 발생할 경우 클라우드 서비스 제공업체를 믿고 의지할 수밖에 없다. 또한 공공 클라우드에는 다수의 이해당사자가 존재한다. 따라서 공개된 데이터 센터에 대한 권한 없는 사용자의 접근 문제가 우려된다.

H. Sato et. al.[4]는 공공 클라우드 환경에서 내부 신뢰 계층과 계약된 신뢰 계층을 통한 클라우드 보안의 신뢰 모델을 제안하였다. 이 신뢰 모델에서 내부 신뢰는 조직 내부 제어 하에 존재하며, 내부적 신뢰의 관리/운영을 보장하는 플랫폼으로 정의된다. 또한 계약된 신뢰는 조직과 클라우드 간의 어떤 계약에 의해 정의되며 계약된 신뢰는 클라우드 내의 SP(Service Policy)와 조직 내의 IdP(Id Policy)의 계약에 근거한다. 이 IdP에 따라 서비스에 속한 사용자를 인증하며 인증된 사용자는 SP에 따라 서비스 받는다. 즉, 조직 내에 사용자를 인증하는 인증 구조를 두고 조직에서만 사용자를 인증할 수 있으며, 클라우드는 계약에 따라 서비스를 제공한다. 이러한 계층적 신뢰 구조를 가짐으로써 개인 클라우드를 구성할 수 없는 조직에서 개인 클라우드를 사용하는 것과 유사한 레벨의 신뢰를 보장받는다.

지난 연구에서는 공공 클라우드 환경에서 사용자 인증과 데이터 센터 접근에 대한 초기 모델을 제시하였다[5]. 본 논문에서는 더 나아가 사용자 인증에 관하여 좀 더 자세한 모델을 제시하고 그 절차를 설명한다.

3. 본론

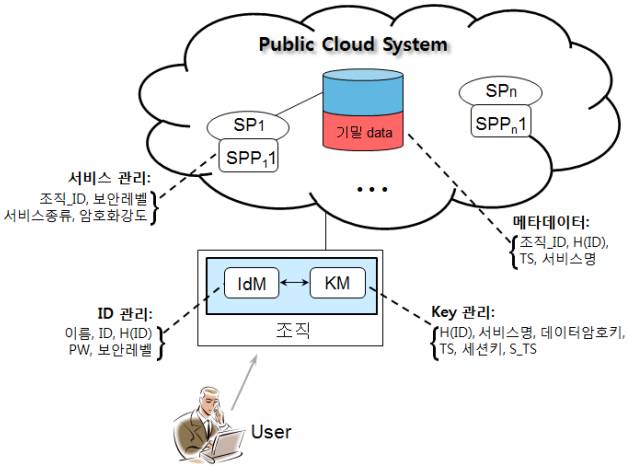
본 논문에서는 다수의 이해당사자로 구성된 공공 클라우드 환경에서 공개된 데이터 센터에 접근하는 사용자에 대해 사용자, 조직, 클라우드 모두가 신뢰할 수 있는 사용자 인증 방법을 제안한다.

3.1 클라우드 시스템 기본 모델

클라우드와 조직은 계약을 통해 서비스를 체결하며, 조직과 클라우드는 서로 신뢰할 수 있다고 전제한다. 본 논문에서 고려되는 클라우드는 공공 클라우드 환경이며, 사용자인증에 관련된 부분은 조직에서만 제공한다.

(그림 1)은 본 논문에서 제안하는 인증 방법을 위한 클라우드 시스템의 기본 모델이다. 그림에서 요약된 단어를 정리하면 다음과 같다.

- SP: 서비스 제공자 (Service Provider)
  클라우드에 존재하는 서비스 제공자
- SPP: 서비스 제공 정책 (Service Providing Policy)
  조직과 SP간의 계약을 통하여 서비스에 대한 보안정책수립 및 조직 내부 Id에 대한 접근 권한을 통제
- IdM: Id 관리자 (Id Manager)
  조직에 속하는 사용자를 관리하고 Id에 따른 서비스 범주를 결정
- KM: Key 관리자 (Key Manager)
  Id별 세션키와 데이터 암호키를 생성 및 관리



(그림 1) 클라우드 시스템 기본 모델

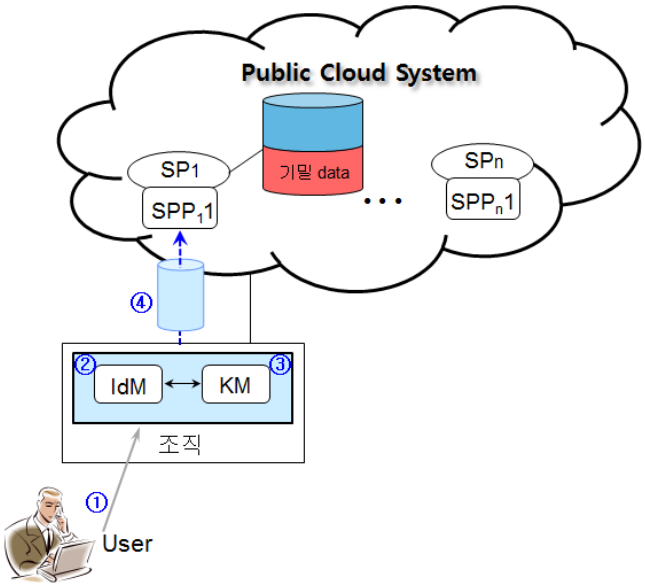
기본 모델에서 데이터 센터는 공공 클라우드 내에 존재하고, 사용자 인증을 위한 인증 서버는 조직 내에 존재한다. 조직의 인증 서버에는 ID관리자(IdM: Id Manager)와 Key관리자(KM: KeyManager)가 존재한다. IdM에서는 사용자의 기본 정보인 이름, ID, PW, 보안레벨 등을 관리하고 보안레벨에 따라 제공받을 수 있는 서비스가 결정된다. 또한 IdM에서는 ID에 대한 해시값 H(ID)을 생성하여 관리한다. H(ID)는 KM에서 각 암호키를 관리하기 위해 사용될 뿐만 아니라 저장된 기밀 데이터 검색을 위한 도구로써 사용된다. KM에서는 각 ID에 따른, 즉 H(ID)에 따른 데이터 암호키와 세션키를 생성하여 관리한다. 세션키는 클라우드와의 통신을 위해 사용되고 데이터 암호키는 클라우드의 데이터 센터에 위탁할 데이터를 암호화하기 위해 사용된다. 일반적으로 개인 클라우드를 구성할 수 없는 사용자의 민감한 데이터는 사용자가 직접 관리하는 키로 암호화하여 저장함으로써 기밀성을 확보할 수 있다[6].

사용자의 세션키와 데이터 암호키는 각 사용자와 조직만이 접근할 수 있고 조직 내에서 안전하게 유지되는 것을 전제로 한다. 각 데이터 암호키에 대한 Time Stamp (TS)와 세션키에 대한 Time Stamp (S_TS)가 존재함으로써 각 키의 사용 시간을 관리한다. SPP는 클라우드와 조직 간의 계약에 의해 생성된다. SPP에 따라 클라우드의 SP는 계약된 조직의 보안 레벨 범위에서 접근하는 사용자의 서비스 범주를 결정한다. 클라우드에 저장되는 사용자의 데이터 중 기밀성이 필요한 민감한 데이터들은 사용자의 데이터 암호키로 암호화되어 저장된다. 데이터에 접근

하기 위해서는 우선 조직으로부터 인증된 사용자여야하며 사용자의 H(ID)와 사용자의 데이터 암호키가 필요하다.

3.2 사용자 인증 모델

조직과 클라우드는 서비스 제공을 위한 보안연계를 맺는다. 보안연계는 IdM과 KM, 그리고 SP의 일부 정보를 사용해 구성되며 사용자에 대한 서비스 정보를 포함한다. 사용자의 인증과정은 다음 (그림 2)와 같다. 사용자는 조직을 통해 클라우드에 접근할 수 있다. 사용자는 조직에 가입된 정보를 이용하여 조직으로부터 합법적인 사용자임을 인증 받을 수 있다. 기존의 로그인 방식의 ID와 PW 입력은 이러한 방식의 가장 보편적이고 간단한 방법이다. (그림 2)의 인증 절차를 서술하면 다음과 같다.



(그림 2) 사용자 인증

① 사용자가 ID와 PW를 입력한다.

② IdM에서는 입력된 정보와 IdM에 보관된 정보와 부합하는지 여부를 판단한다. 올바른 정보가 입력되었다면 조직에서는 사용자를 합법적인 사용자로 인증한다.

③ 사용자가 합법적인 사용자로 확인되면 조직의 KM에서는 ID의 해시값에 따라 세션키를 검색한다. 이 세션키는 사용자가 클라우드와 안전하게 통신하기 위해 사용되며 통신이 완전히 완료되면 세션키는 삭제된다.

④ 사용자의 서비스 요청에 따라 메시지가 클라우드에 전송되면 클라우드의 SP는 사용자의 보안레벨을 적용하여 서비스 범주 내에서 서비스를 제공한다.

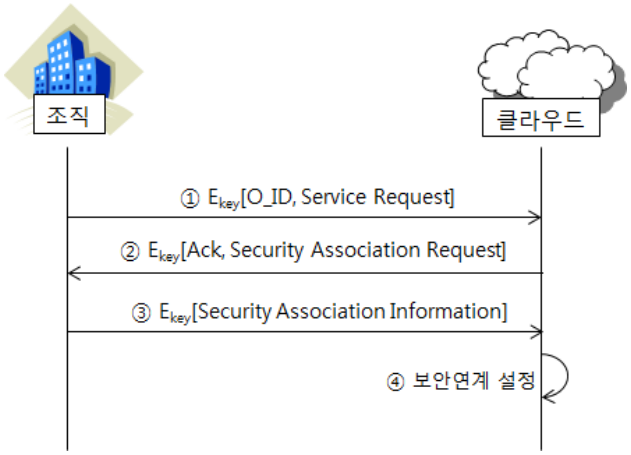
클라우드와 조직은 계약으로 묶여 있으며 서로 절대적으로 신뢰함을 가정한다. 보안레벨에 따른 서비스의 범주는 계약시 결정되며 조직에서 결정된 사용자 보안레벨에 따라 클라우드는 단지 서비스만 제공한다.

3.3 보안연계와 사용자 인증 절차

3.3.1 사용자 확인을 위한 보안연계 절차

클라우드에서는 사용자를 인증하지 않고 조직으로부터 인증된 사용자에게 서비스만 제공한다. 클라우드에서 사용자를 확인하고 적절한 서비스를 제공하기 위해서는 클라우드에서 사용자를 확인하고 구분하기 위한 정보가 필요하다. 보안연계는 조직과 클라우드 사이의 계약을 통해서 구성되며 이 정보는 클라우드에서 사용자를 확인하고 사용자에게 적절한 서비스를 제공할 수 있도록 한다.

(그림 3)은 보안연계가 생성되는 절차를 나타낸 그림이다. 조직과 클라우드 사이의 보안연계를 절차 순으로 표현하면 다음과 같다.



(그림 3) 보안연계 설정 절차

① E_{key}[O_ID, Service Request]
조직은 서비스를 시작하면서 클라우드와 보안연계 과정을 거친다. 조직은 조직을 나타내는 ID(O_ID)와 서비스 요청 내용을 사전에 미리 클라우드와 공유된 Key로 암호화하여 클라우드에게 요청사항을 전달한다. 공유된 Key의 공유방법과 암/복호화 방법은 이미 널리 알려진 Key공유 방식과 같다.

② E_{key}[Ack, Security Association Request]
클라우드에서는 미리 공유된 Key로 복호화함으로써 조직으로부터 전달받은 정보를 확인할 수 있다. O_ID 확인을 거쳐 요청을 수락하는 응답과 보안연계 생성을 위한 필요 정보를 조직에게 요청한다. 이 요청은 미리 공유된 Key로 암호화되어 전달된다.

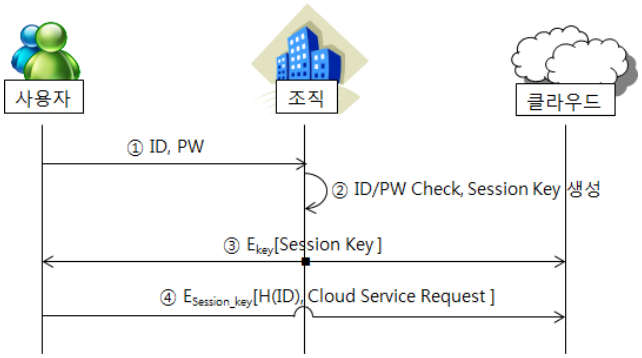
③ E_{key}[Security Association Information]
클라우드로부터 응답을 받은 조직에서는 클라우드에서 보안연계를 위해 요청하는 정보를 공유된 Key로 암호화하여 전달한다.

④ 보안연계 설정
클라우드에서는 조직으로부터 전달받은 정보와 클라우드가 가지고 있는 O_ID에 대한 정보를 이용하여 보안연계를 설정한다. 조직으로부터 받는 정보에는 사

용자 ID의 해시값 H(ID), H(ID)에 대한 보안레벨, H(ID)의 Session Key 관련 정보와 Time Stamp 값 등이 있다. 클라우드 자신이 가지고 있는 정보에는 조직의 ID인 O_ID, O_ID에 대한 보안레벨과 서비스 범주 등이 있다. 이 정보는 대체로 클라우드와 조직이 계약을 통해 설정한 정보이다.

3.3.2 사용자 인증 절차

(그림 4)는 사용자 인증 절차를 나타낸다. 사용자가 조직을 통해 인증 받고 서비스에 접근하는 과정을 절차 순으로 나타내면 다음과 같다.



(그림 4) 사용자 인증 절차

① ID, PW
사용자가 서비스 접근하기 위해서는 조직을 통해 인증을 받아야 한다. 사용자는 조직에 등록된 ID와 PW를 통해 접근을 시도한다.

② ID/PW Check, Session Key 생성
조직의 IdM에서는 사용자의 정보를 접근된 사용자의 정보를 확인한다. 사용자의 접근 ID와 PW를 확인함으로써 접근한 사용자가 합법적인 사용자인지 확인한다. 합법적인 사용자로 확인된 경우에는 KM에서 클라우드와 사용자의 통신을 위한 Session Key를 생성하여 등록한다.

③ E_{key}[Session Key]
앞서 생성된 Session Key는 클라우드와 조직, 조직과 사용자 간에 미리 공유된 Key로 암호화하여 전달된다. 암호화 키는 클라우드와 조직, 조직과 사용자만이 알고 있기 때문에 통신을 위한 Session Key는 안전하게 전달된다.

④ $E_{Session\_key}$[H(ID), Cloud Service Request)]
사용자와 클라우드는 나눠받은 Session Key로 안전하게 통신할 수 있다. 사용자가 클라우드에게 클라우드 서비스를 요청하기 위해서 H(ID)를 이용한다. 특히 이 정보는 데이터 센터에 위탁된 사용자의 데이터에 접근할 때 요구된다. 데이터 센터의 암호화된 사용자 데이터는 메타데이터 검색을 통해 접근하게 된다. 메타데이터 관리자에서 H(ID)에 대한 검색 정보를 제공함으로써 암호화 데이터에 접근하고 이 데이터는 사용자 데이터 암호키를 이용해 복호화 할 수 있다.

사용자의 ID가 아닌 H(ID)를 사용하는 것은 ID를 사용함으로써 노출될 수 있는 사용자의 정보를 최소화하기 위함이다. 해시 함수의 일방향 특성을 이용하여 ID를 직접적으로 사용하지 않고도 각자의 사용자를 유일한 사용자로 구분할 수 있다. 보안연계에는 사용자의 H(ID)와 세션키, 보안레벨, 서비스 등의 정보가 존재한다. 클라우드에서는 조직으로부터 받은 정보인 H(ID)와 세션키 등의 정보를 신뢰하며, H(ID)를 사용해 접근하는 사용자를 인증된 사용자로 인식한다. 또한 보안연계의 H(ID)와 세션키 정보를 함께 이용하여 접근한 사용자의 H(ID)가 올바른 사용자인지를 판단하며 오용되었는지의 여부를 판단한다. 조직을 통한 사용자 인증 방법을 사용함으로써 사용자의 직접적인 정보들은 조직내부에서 관리한다. 공개되어 있는 공공 클라우드의 데이터 센터에서는 부과적인 데이터만을 저장함으로써 사용자, 조직, 클라우드 모두가 신뢰할 수 있는 클라우드 서비스를 유지할 수 있다.

4. 결론

본 논문에서는 다수의 이해당사자가 존재하는 공공 클라우드 환경에서 사용자, 조직, 클라우드 모두가 신뢰할 수 있는 사용자 인증 방법을 제안하였다. 조직과 계약관계에 있는 클라우드는 서비스 제공 정책을 준수하여 서비스를 제공하고 조직에서 사용자 인증을 위한 구조를 유지함으로써 공공 클라우드에 사용자의 직접적인 정보를 제공하지 않고도 신뢰할만한 사용자 인증 방법을 제공한다. 이 인증 방법을 이용함으로써 공공 클라우드 내에 사용자의 직접적인 정보가 노출되지 않으며, 개인 클라우드를 구성한 것과 유사한 보안 수준을 유지할 수 있다.

참고문헌

[1] 은성경, "클라우드 컴퓨팅 보안 기술 동향," 정보보호학회지, 제20권 제2호, pp. 27 - 31, 2010

[2] IDC, "Asia Pacific End-User Cloud Computing Survey," 2009

[3] 김명준, "Korea's Cloud Computing Strategy," IT21 글로벌 컨퍼런스, 2009

[4] H. Sato, A. Kanai, and S. Tanimoto, "A Cloud Trust Model in a Security Aware Cloud," 10th Annual International Symposium on Applications and the Internet, pp. 121 - 124, 2010

[5] 하병래, 이승아, 조기환, "보안에 적응적인 클라우드 컴퓨팅을 위한 사용자 인증 및 데이터 관리 방안," 제4회 정보통신분야학회 합동학술대회, pp. 158 - 161, 2010

[6] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Financial Cryptography and Data Security, LNCS 6054, pp. 136 - 149, 2010