# 클라우드 컴퓨팅 환경에서 사용자 인증을 위한 효율적인 접근통제 기법 설계

김영곤*, 전문석*
*숭실대학교 일반대학원 컴퓨터학과
e-mail : {kyg994, mjun}@ssu.ac.kr

# A design on efficient access control method for user authentication on cloud computing environment

Young-Gon Kim*, Moon-Seog Jun*
*Dept of Computer Science, Soongsil University

요 약

최근 클라우드 컴퓨팅에 대한 관심이 높아지면서 많은 제품과 서비스들이 나타나고 있지만 아직은 많은 보안 문제점이 있다.. 개인 사용자의 관점에서는 개인정보 노출 등의 보안문제가 있으며 기업의 관점에서는 기업 정보나 고객 정보 등의 유출 및 훼손에 대한 보안문제로 클라우드 컴퓨팅을 기피하는 사례도 발생한다. 따라서 본 논문에서는 클라우드 컴퓨팅 환경에서 사용자가 이용하는 서비스의 접근에 대해 자체적으로 보안수준을 설정하여 보안이 필요한 서비스에 대해서는 재인증 절차를 거친 뒤 서비스 접근이 가능하도록 하여 안전하고 정확한 사용자 인증을 위한 효율적인 접근통제 기법을 제안한다.

## 1. 서론

최근 새로운 트렌드를 형성하고 있는 클라우드 컴퓨팅은 사용자가 애플리케이션을 개발하거나 혹은 서비스할 때 서버나 스토리지 등 컴퓨팅 자원 등을 자체적으로 보유하지 않고 이 같은 자원을 갖고 있는 클라우드 컴퓨팅 플랫폼 제공자를 통해 운영하는 것을 의미한다. 구글(Google), 마이크로소프트(MS), IBM, 아마존(Amazon) 등 대표적인 IT 기업들은 클라우드 컴퓨팅을 차세대 핵심 비즈니스로 꼽고 SaaS(Software as a Service), PaaS(Platform as a Service), Iaas(Infrastructure as a Service) 등 다양한 클라우드 컴퓨팅 서비스 및 제품들이 출시되고 있다[1][2]. 그러나 아직은 많은 보안 문제들이 존재하며 클라우드 보안 협회(CSA)에서 발표한 클라우드 컴퓨팅 7대 보안 위협은 클라우드 컴퓨팅의 남용 및 오용, 불안정한 환경 및 응용프로그램 환경, 악성 코드 공격, 기술 인프라의 공유, 데이터 손실 또는 유출, 계정 혹은 서비스 침해, 알려지지 않은 위험이다. 이러한 보안 문제 때문에 개인 사용자나 기업 사용자가 자신들의 정보의 유출이나 훼손 등의 문제가 발생할 수 있다고 생각하여 클라우드 컴퓨팅을 기피하는 사례도 발생하게 되었다[3][4]. 따라서 본 논문에서는 많은 보안 문제 중 사용자 인증에 관점을 두고 클라우드 컴퓨팅 환경에서 사용자가 과금한 서비스의 접근에 대해 자체적으로 보안설정을 할 수 있도록 하여 설정이 되어 있는 서비스의 접근에 대해서는 재인증 절차를 거친 뒤[5], 서비스를 사용할 수 있도록 하여 안전하고 정확한 사용자 인증을 위한 효율적인 접근통제 기법을 제안한다.

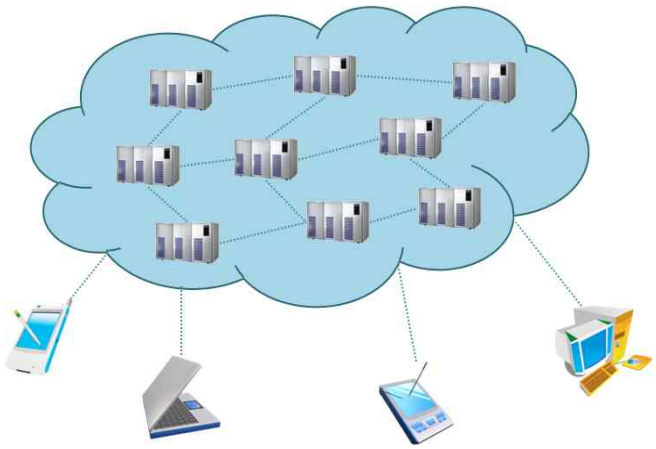
본 논문의 구성은 다음과 같다. 2장에서는 클라우드 컴퓨팅에 대해서 설명하고, 3장에서는 제안하는 클라우드 컴퓨팅의 환경과 사용자 인증 방법에 대해 설명하며 마지막 4장에서는 결론을 맺는다.

## 2. 관련 연구

### 2.1 클라우드 컴퓨팅

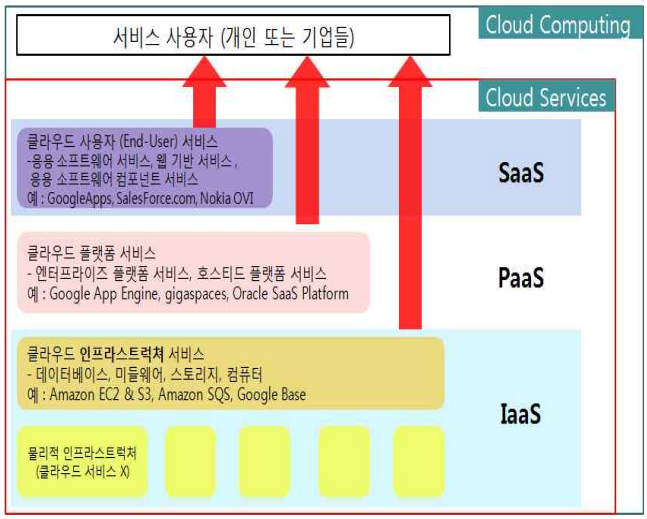
클라우드 컴퓨팅은 서로 다른 물리적인 위치에 존재하는 컴퓨터들의 자원을 가상화 기술을 통하여 제공하는 기술이다. 현재 개인용 PC나 기업의 서버 등 개별적으로 저장했던 자원들을 인터넷으로 접속이 가능한 대형 컴퓨터에 저장을 하며, 여러 단말기를 통하여 필요한 애플리케이션을 실행하여 작업을 수

행할 수 있도록 하는 사용자 중심의 컴퓨터 환경을 말한다[1]. [그림 1]과 같이 인터넷이 연결된 단말을 통해 데이터 센터에 접속하여 사용자가 원하는 필요한 자원을 사용하고 사용량에 기반 하여 대가를 지불한다.



[그림 1] 클라우드 컴퓨팅 환경

클라우드 컴퓨팅에서도 내부를 살펴보면 몇 가지 유형이 있다. 표준화 된 환경과 애플리케이션을 제공하는 SaaS(Software as a Service), 인프라만을 제공하는 IaaS (Infrastructure as a Service), 표준화된 플랫폼을 제공하는 PaaS(Platform as a Service)로 [그림 2]와 같이 분류 할 수 있다[2].

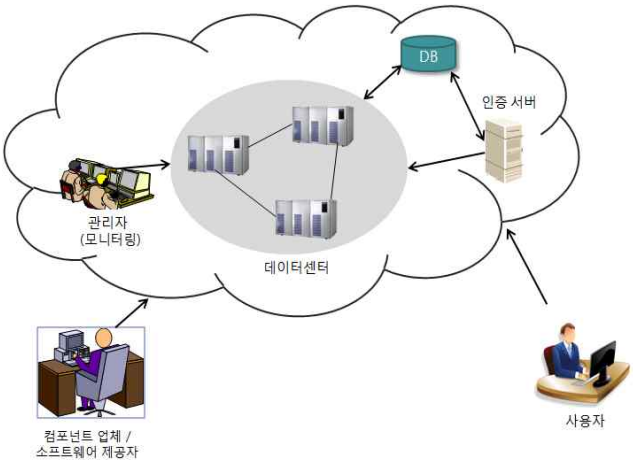



[그림 2] 클라우드 컴퓨팅 분류

## 3. 제안하는 인증 기법

### 3.1 클라우드 시스템 구조

본 논문에서는 클라우드 컴퓨팅 환경에서의 사용자 인증을 위한 효율적인 방식을 제안한다. 전체적인 환경은 [그림 3]과 같다.




[그림 3] 클라우드 컴퓨팅 환경

클라우드 시스템 내부는 데이터센터, 인증서버, DB, 모니터링 및 내부요소 관리를 하는 관리자로 구성이 되어 있으며, 사용자는 클라우드 시스템 내부 구성은 모르지만 시스템에 접근하여 인증을 거친 뒤 자신이 과금한 서비스를 사용할 수 있게 되는 환경이다.

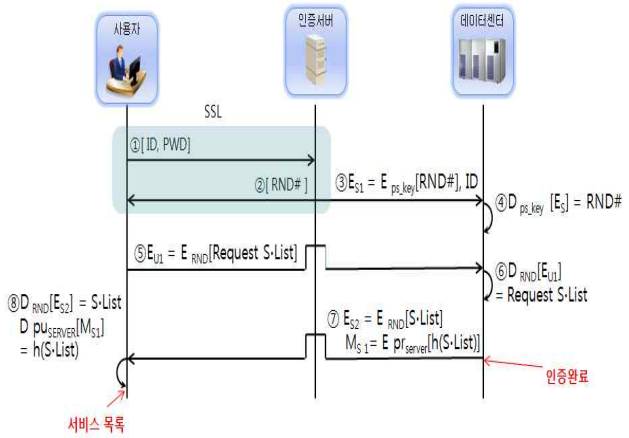
[표 1]은 제안하는 인증 기법에서 사용하는 용어에 대한 설명을 나타낸다.

[표 1] 용어 설명

| 용어 | 설명 |
|---|---|
| RND | 사용자와 데이터센터 사이에 사용되는 대칭키 |
| ps_key | 클라우드 컴퓨팅 내에서 사용되는 사전에 안전하게 공유된 대칭키(Pre_Shared key) |
| $E_{prSERVER}$ | 서버의 개인키로 암호화 |
| $D_{puSERVER}$ | 서버의 공개키로 복호화 |
| S • List | Service List(서비스 목록) |
| TS | TimeStamp (Reply Attack 공격방지를 위한 수단) |
| SSS | Service Security Setup(서비스 보안설정) |
| $E_{puUSER}$ | 사용자의 공개키로 암호화 |
| $D_{prUSER}$ | 사용자의 개인키로 복호화 |
| NRND | 새로운 RND 값을 의미 (새로운 대칭키) |

### 3.2 사용자 초기 인증방식

본 논문에서 제안한 서비스 구조는 사용자는 클라우드 환경에서 어떤 구성요소와 통신을 하고 있는지 알 수 없으며, 사용자가 클라우드 시스템을 사용하기 위하여 접근했을 경우 내부적으로는 [그림 4]와 같은 방식으로 초기 인증이 동작한다.




[그림 4] 사용자 초기 인증방식

사용자가 클라우드 시스템에 접근하여 로그인 시, 클라우드 내부의 인증서버와 사용자 사이에 SSL(Secure Sockets Layer) 연결이 확립된다. 사용자는 아이디와 패스워드를 전송하고 인증서버는 전송 된 내용을 확인 뒤 사용자와 클라우드 시스템 사이에서 사용되는 *RND* 를 사용자와 데이터센터에게 각각 전송해 준다. 이 때 데이터센터에게 전송을 할 때에는 클라우드 컴퓨팅 내에서 사전에 안전하게 공유된 *ps_key* 로 암호화 하여 전송하게 된다. 그 후 사용자와 클라우드 시스템 사이의 SSL 연결은 종료하고 사용자는 데이터센터에게 서비스목록 요청 메시지를 인증서버로부터 받은 *RND* 로 암호화하여 보내고, 데이터센터 역시 인증서버로부터 받은 *RND* 를 이용하여 메시지를 복호화 함으로써 사용자에 대한 인증이 완료하여 사용자에게 서비스목록을 보낸다. 이때 무결성을 위해 해시된 서비스목록을 서버의 개인키로 서명하여 같이 보내면 사용자는 메시지들을 복호화 하여 이를 검증 후 서비스목록을 받음으로써 초기인증 절차가 종료 된다.. 초기 인증절차를 마친 사용자는 서비스를 요청하여 사용할 수 있다.

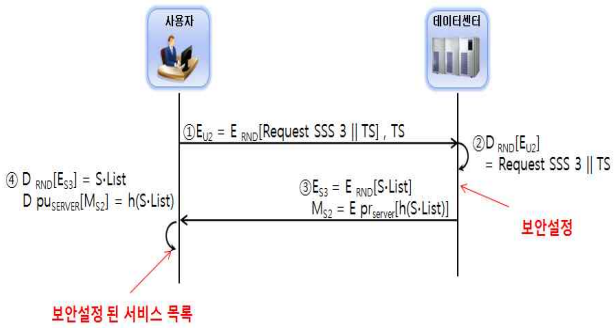
### 3.3 자체 서비스 보안 설정

앞 절의 초기 인증이 끝나면 데이터센터는 [표 2] 와 같이 사용자에 대해 설정되어 있는 테이블을 접근할 수 있고 사용자는 클라우드 컴퓨팅에서 과금한 서비스를 접근 하여 사용 할 수 있다.

[표 2] 사용자 테이블

| 사용자 | | | |
|---|---|---|---|
| 서비스 목록 | Office | Game | Visual Studio |
| 신청 기능 | PT, Excel | ~ | C#, Basic |
| 보안 설정 | X | X | X |

본 논문에서는 사용자가 서비스를 사용함에 있어 개인 프라이버시의 기밀성 등 보안문제를 해결하기 위해 각각의 서비스에 대해 사용자가 자체적으로 보안설정을 할 수 있도록 하는 방법을 제안한다. 일반적으로 사용자는 서비스를 이용하기 위해 데이터센터에게 서비스 접근 요청 메시지를 보내게 되고 이때, 데이터센터는 사용자로부터 받은 메시지를 확인하여 요청한 서비스의 보안설정 여부를 확인 한 후 보안 설정이 되어있지 않은 경우에는 사용자가 곧바로 서비스에 접근 할 수 있도록 한다. 하지만 앞서 말한 여러 보안적인 문제들의 해결을 위해 사용자는 서비스에 대해 자체적으로 [그림 5]와 같이 보안 설정을 할 수 있다.




[그림 5] 서비스 보안 설정

사용자가 보안설정을 원하는 서비스에 대해서 데이터센터에게 서비스 보안설정 요청 메시지를 *RND*로 암호화하여 보내며, 이때 연접해서 보내는 *TS*는 재전송 공격을 방지하기 위해 사용한다. 데이터센터는 사용자로부터 받은 메시지를 복호화 하여 원하는 서비스의 보안설정을 하고 변경된 서비스 목록을 *RND*로 암호화해서 보내며 무결성을 위해 해시 된 서비스 목록을 데이터센터의 개인키로 서명 하여 함께 사용자에게 보낸다. 사용자는 복호화 하여 검증 후 보안 설정된 서비스 목록을 받고 보안 설정 요청에 따라 [표 3]과 같이 서비스목록의 3번째 서비스의 보안설정 부분이 변경된다.

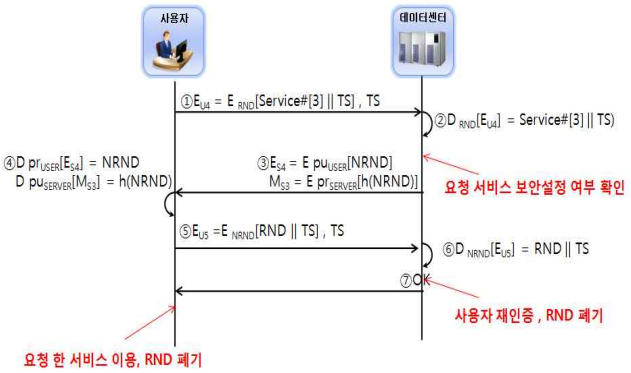
[표 3] 변경 된 사용자 테이블

| 사용자 | | | |
|---|---|---|---|
| 서비스 목록 | Office | Game | Visual Studio |
| 신청 기능 | PT, Excel | ~ | C#, Basic |
| 보안 설정 | X | X | O |

### 3.3 보안설정 된 서비스 접근 방식

3.2 절에서 서비스에 대해 사용자가 자체적으로 보안 설정하는 방식을 제안했다. 이와 같은 과정을

거쳐 보안설정을 한 서비스 접근은 설정을 하지 않은 서비스 접근과는 다른 방식으로 동작한다. 보안설정이 되지 않은 서비스에 대한 요청은 확인 후 바로 접근을 할 수 있도록 하지만 보안설정이 되어 있는 서비스에 접근을 요청할 경우 [그림 6]과 같은 방식으로 재차 사용자를 인증 할 수 있는 방식을 제안한다.




[그림 6] 보안설정 된 서비스 접근 방식

보안설정을 하지 않은 서비스와 보안 설정을 한 서비스 모두 처음에 요청방식은 동일하다. 사용자가 재전송 공격 방지를 위한 *TS* 값을 연접한 서비스 요청 메시지를 *RND* 값으로 암호화 하여 보내면 데이터센터는 요청 메시지를 확인한 뒤 해당 서비스에 대한 보안설정 여부를 확인한다. 보안설정이 안 되어 있는 경우는 바로 서비스 접근을 할 수 있도록 하지만, 보안설정이 되어 있는 서비스 접근을 요청 한 경우는 사용자 확인을 위한 메시지를 보낸다. 메시지는 *NRND*, 즉 새로 사용하려는 키를 사용자의 공개키로 암호화 한 메시지를 보내서 사용자에 대해 재인증을 할 수 있도록 한다. 무결성을 위해 자신의 개인키로 서명한 해시 된 *NRND*를 같이 보낸다. 사용자는 데이터센터로부터 받은 두 개의 메시지를 복호화 하여 검증 한 후 새로운 비밀 키인 *NRND*를 이용하여 *RND*와 TS값을 연접하여 재전송 공격을 막는 동시에 사용자 본인을 인증하는 암호화 된 메시지를 보내면 데이터센터는 메시지를 복호화 하여 사용자를 인증하게 되고 서비스에 접근할 수 있도록 한다. 이때 사용자와 데이터센터는 이전에 사용했던 대칭 키인 *RND*를 폐기한다. 이와 같이 보안설정이 되어있는 서비스에 접근하기 위해서는 총 2번의 인증절차를 거침으로써 클라우드 시스템의 보안문제를 해소할 수 있다.

## 4. 결론 및 향후 연구과제

본 논문에서 제안한 기법은 사용자가 자체적으로 보안을 원하는 서비스에 대해 보안설정을 할 수 있도록 하여 재인증을 통해서 서비스에 접근을 할 수 있도록 하는 방식으로써, 안전한 접근통제를 실시하여 사용자에게 클라우드 컴퓨팅 환경의 보안위협으로부터 벗어날 수 있게 한다.

향후 연구과제로는 각 서비스에 대한 세부적인 보안설정을 할 수 있는 방법과 경량화 된 방법을 찾아 속도를 높일 수 있는 방안을 모색하여 연구한다.

## 참고문헌

[1] 민옥기, 김학영, 남궁한, “클라우드 컴퓨팅 기술 동향”, 전자통신동향분석, 2009.

[2] 이종숙, 박형우, “국내외 클라우드 컴퓨팅 동향 및 전망”, 정보처리학회지, 2009.

[3] J.Heiser and M. Nicolett, Assessing the Security Risks of Cloud Computing, Gartner, 2008. 6.

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing. 2009. 4

[5] OpenID, http://openid.net/