기업에서 클라우드 컴퓨팅 사용을 위한 사용자 인증기법 연구

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

A Study on User Authentication Method for Using Cloud Computing in an Enterprise

Young-Gon Kim○, Hyo-Jong Kim, Moon-Seog Jun
Dept of Computer Science, Soongsil University

요 약

최근 새로운 트렌드를 형성하고 있는 클라우드 컴퓨팅은 인터넷 기술을 활용하여 다수의 사용자들에게 IT 자원을 서비스하는 시스템이다. 이러한 서비스들이 많이 나타나고 있지만 아직은 많은 보안 문제점이 있다. 기업의 입장에서는 기업 정보나 고객 정보 등의 유출 및 훼손에 대한 보안문제로 클라우드 컴퓨팅을 기피하는 사례도 발생한다. 따라서 본 논문에서는 기업에서 클라우드 컴퓨팅 사용을 위한 기본적인 사용자 인증은 클라우드 컴퓨팅을 제공하는 업체에서 하며, 보안과 접근통제가 필요한 서비스에 대해서는 기업 자체에서 인증을 한다. 즉, 온전한 클라우드 컴퓨팅 서비스를 받기 위해서 총 2번의 인증을 거쳐 필요한 서비스에 접근이 가능하도록 하는 안전하고 정확한 인증기법을 제안하였다.

1. 서 론

최근 새로운 트렌드를 형성하고 있는 클라우드 컴퓨팅은 각 기업이 애플리케이션을 개발 혹은 서비스할 때 자체적으로 컴퓨팅 자원을 보유하지 않고 자원을 갖고 있는 클라우드 컴퓨팅 제공자를 통해 운영하는 것을 의미한다. 대표적은 몇몇의 IT 기업들은 클라우드 컴퓨팅을 차세대의 핵심 비즈니스로 꼽고 있으며, 다양한 클라우드 컴퓨팅 서비스 및 제품들이 출시되고 있다[1]. 크게 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service)으로 분류하여 필요에 맞게 서비스를 제공받을 수 있다[2].

최근 클라우드 보안 협회(CSA)에서는 클라우드 컴퓨팅에 대한 7대 보안 위협을 발표 하였다. 이렇듯 아직까지는 많은 보안 문제들이 있기 때문에 개인이나 기업에서는 자신들의 정보의 유출 혹은 훼손 등의 문제로 클라우드 컴퓨팅을 기피하는 사례가 발생하였다[3][4][5]. 특히 기업의 경우는 금전적인 문제가 동반되기 때문에 우려하는 바가 더욱 크다고 볼 수 있다. 따라서 본 논문에서는 보안 문제점 중 인증부분과 서비스를 제공받는 기업 입장에서 관점을 두었다. 클라우드 컴퓨팅에 접근하는 기본적인 인증은 서비스 제공업체에서 이뤄지고, 세부적인 서비스에 대한 인증은 기업 내에서 재인증을 할 수 있도록 한다. 즉, 온전한 클라우드 컴퓨팅 서비스를 받기 위해서 2번의 인증을 거쳐 접근이 가능하도록 하여 기업의 안전성을 높일 수 있는 기법을 제안하였다[6].

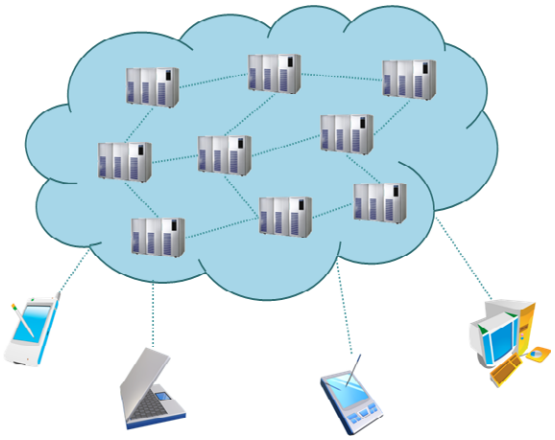
본 논문의 구성은 다음과 같다. 2장에서는 클라우드 컴퓨팅에 대해서 설명하고, 3장에서는 제안하는 클라우드 컴퓨팅 환경과 인증 방법에 대해서 설명하며, 마지막 4장에서 결론을 맺는다.

2. 관련 연구

2.1 클라우드 컴퓨팅

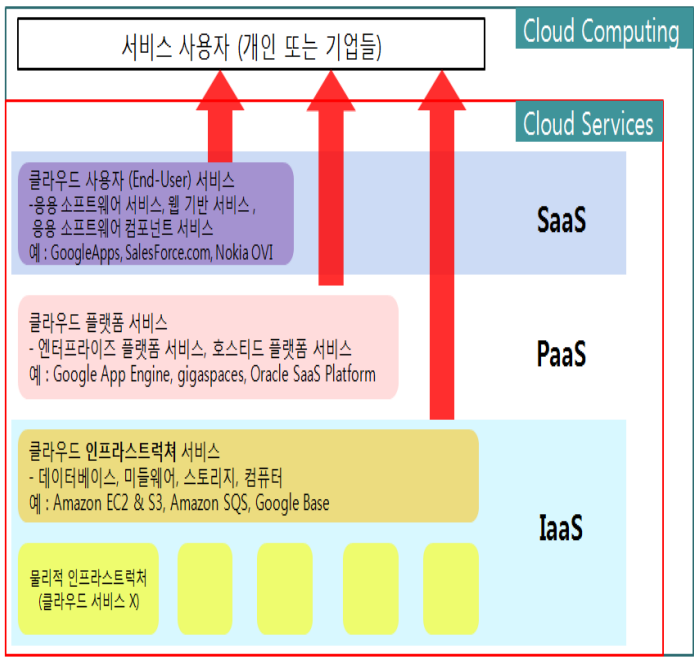
클라우드 컴퓨팅은 서로 다른 물리적인 위치에 존재하는 컴퓨터들의 자원을 가상화 기술을 통하여 서비스를 제공하는 기술이다. 현재 개인용 PC나 기업의 서버 등 개별적으로 저장했던 자원들을 인터넷으로 접속이 가능한 대형 컴퓨터에 저장을 하며, 여러 단말기를 통하여 필요한 애플리케이션을 실행하여 작업을 수행할 수 있도록 하는 사용자 중심의 컴퓨터 환경을 말한다. 아래 [그림 1]과 같이 인터넷이 연결된 단말을 통해 데이터 센터

에 접속하여 사용자가 필요한 자원을 사용하고 대가를 지불한다.



[그림 1] 클라우드 컴퓨팅 환경

클라우드 컴퓨팅의 내부를 살펴보면 몇 가지 유형이 있다. 표준화된 환경과 애플리케이션을 제공하는 SaaS(Software as a Service), 인프라만을 제공하는 IaaS (Infrastructure as a Service), 표준화된 플랫폼을 제공하는 PaaS(Platform as a Service)로 아래 [그림 2]와 같이 분류 할 수 있다[1][2].

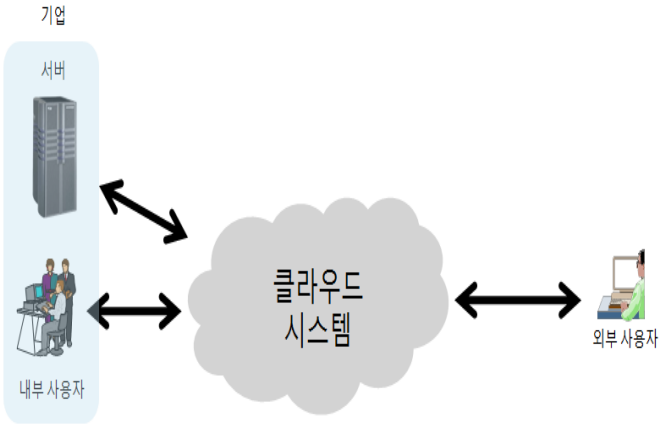


[그림 2] 클라우드 컴퓨팅 분류

3. 제안하는 인증 기법

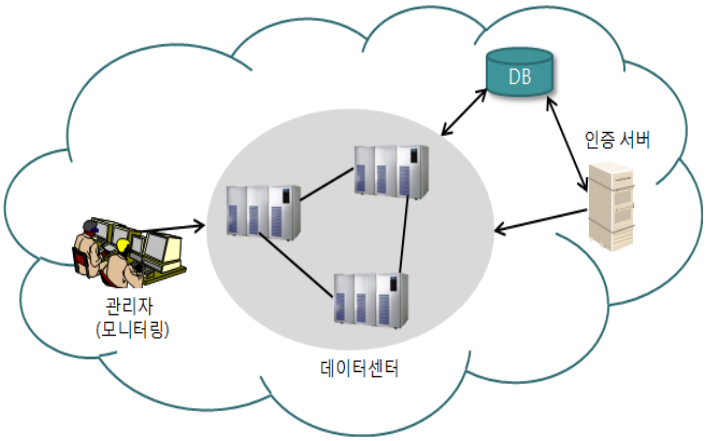
3.1 기업 내 클라우드 시스템 구조

기업에서 클라우드 컴퓨팅 사용에 대한 보안 문제점을 해결하기 위한 사용자 인증 기법을 제안한다. 전체적인 구조는 [그림 3]과 같다.



[그림 3] 클라우드 컴퓨팅 환경

[그림 3]은 기업이 과금한 클라우드 시스템은 기업 내·외부에서 모두 사용이 가능하며 클라우드 시스템 내부 구성을 알지 못하는 사용자(사원)는 시스템에 접근하여 초기 인증을 거친 뒤 서비스를 사용할 수 있는 환경을 나타낸다.



[그림 4] 클라우드 시스템 내부 구조

[그림 4]는 클라우드 시스템의 내부구조를 나타낸다. 클라우드 시스템 내부는 데이터 센터, 인증서버, DB, 모니터링 및 내부요소 관리를 하는 관리자로 구성이 되어 있다. 인증 서버를 통해 초기 인증을 거치면 사용자는 기업 공동의 서비스에 접근 할 수 있지만 부서나 직책이 구분되어 있는 서비스에 접근 할 경우, 기업에서 자체적으로 사용자의 접근에 대한 허용 여부를 판단하여 클라우드 시스템에 재인증을 거치는 방법으로 인증에 대한 신뢰도를 가질 수 있다. 접근 허용 여부를 판단하기 위

해 기업은 사원에 대한 정보를 XML로 저장하여 안전한 관리가 가능하다.

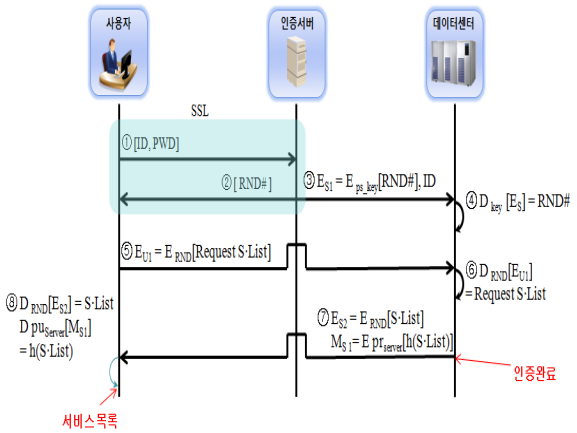
[표 1]은 제안하는 인증기법에서 사용하는 용어에 대한 설명을 나타낸다.

[표 1] 용어 설명

RND	사용자와 데이터센터 사이에 사용하는 대칭키
ps_key	클라우드 컴퓨팅 내에서 사용하는 사전에 안전하게 공유된 대칭키 (Pre_shared key)
S·List	Service List(서비스 목록)
E_{RND}, D_{RND}	RND를 키로 암·복호화
Epu_{Server}, Dpr_{Server}	기업 서버의 공개키, 개인키로 암·복호화
Epu_{Data}, Dpr_{Data}	클라우드 시스템의 공개키, 개인키로 암·복호화
h()	해시 함수
AN	Authentication Number(인증번호)

3.2 클라우드 시스템 초기 인증 방식

본 논문에서 제안하는 서비스 구조에서 초기 인증은 기업 내부와 외부의 접근은 같은 방식이다. 내·외부 사용자가 클라우드 시스템을 사용하기 위해 접근했을 경우 시스템은 [그림 5]와 같이 인증을 하게 된다.

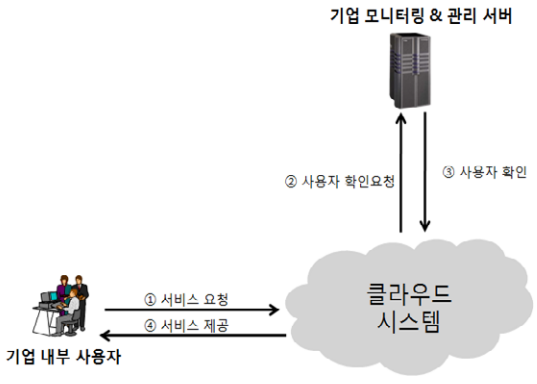


[그림 5] 초기 인증방식

클라우드 시스템에 접근하여 로그인 시, 클라우드 내부의 인증서버와 사용자 사이에 SSL (Secure Socket Layer) 연결이 확립되게 된다. 확립된 SSL을 통해 사용자는 아이디와 패스워드를 전송하고 전송된 내용을 확인한 인증서버는 사용자와 클라우드 시스템, 즉 데이터 센터와 통신에 사용되는 키 값인 *RND*를 사용자와 데이터 센터에게 각각 전송을 한다. 인증 서버가 데이터센터에게 *RND* 를 전송할 때는 클라우드 시스템 내에서 사전에 안전하게 공유된 *ps_key* 로 암호화하여 사용자의 ID와 함께 전송을 한다. *RND*를 전송 한 후 사용자와 클라우드 시스템 사이의 SSL 연결을 종료하고 이 후 사용자는 인증서버로부터 받은 *RND*로 암호화한 서비스 목록 요청 메시지를 데이터센터에게 보낸다. 데이터센터 또한 인증서버로부터 받은 ID와 매칭 되는 *RND*를 이용하여 메시지를 복호화 하고 사용자에게 서비스 목록을 보냄으로써 사용자에 대한 인증을 완료하게 된다. 이때 무결성을 위해 해시된 서비스 목록을 개인키로 서명하여 같이 보내면 사용자는 두 개의 메시지를 복호화 하여 이를 검증 후 서비스 목록을 받음으로써 초기 인증 절차가 종료 된다. 초기 인증절차를 마친 사용자는 원하는 서비스를 요청하여 사용할 수 있다.

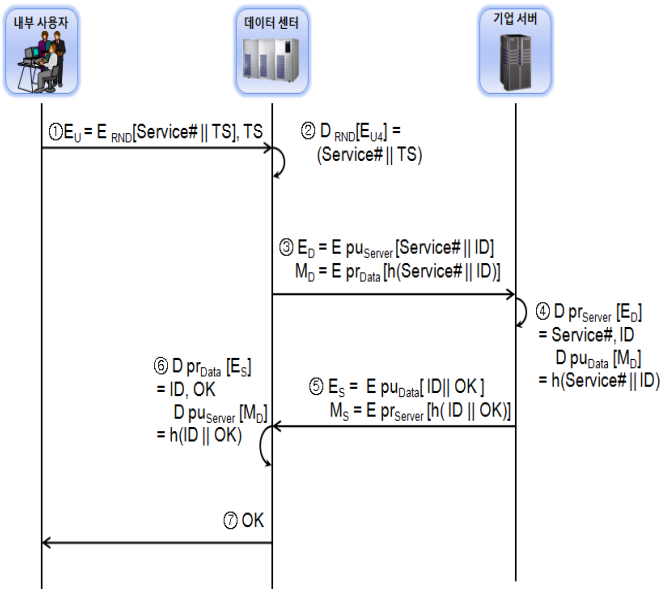
3.3 기업 자체 판단 구조

초기 인증 절차를 통해 사용자는 클라우드 시스템의 서비스를 사용할 수 있게 된다. 기업의 공용 서비스에 접근할 경우는 단순한 서비스 요청을 통해 이용할 수 있게 된다. 사용자의 ID는 기업에서 사원 번호 등을 이용하여 직접 부여하고 클라우드 시스템 내의 서비스에 대해 부서나 직책에 따른 접근권한을 기업에서 정할 수 있도록 한다. 보안정책이 지정된 서비스에 접근한 사용자를 확인요청 하고 이를 기업에서 판단하여 사용자를 인증 하도록 함으로써 기업의 입장에서 클라우드 시스템의 보안에 대한 신뢰도를 높인다. 먼저 기업 내부 사용자가 클라우드 시스템에 초기인증을 한 뒤 보안정책이 지정된 서비스에 접근 할 경우 인증절차는 [그림 6]과 같다.



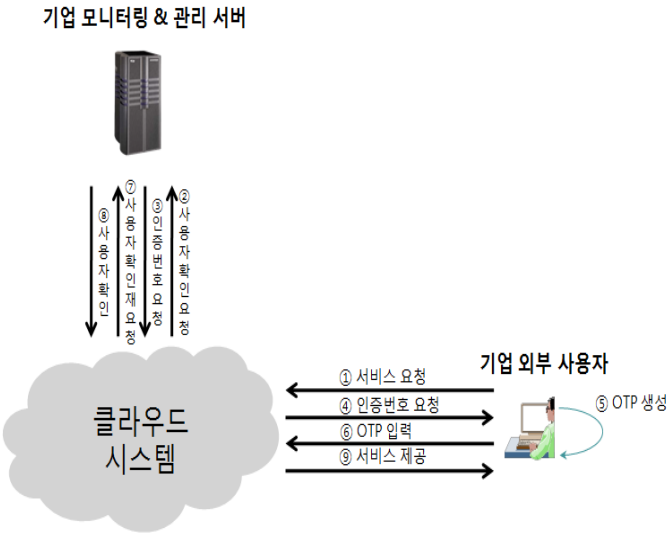
[그림 6] 기업 내부 사용자 인증

기업 내부 사용자가 클라우드 시스템에서 보안정책이 정해져 있는 서비스에 접근 할 경우 데이터 센터는 기업 서버에게 서비스에 접근하는 사용자를 확인요청 한다. 기업서버는 현재 모니터링 되는 사용자를 확인하고 데이터 센터에 확인 메시지를 전송하며, 그 후 데이터센터는 사용자에게 서비스를 제공한다. 이 때 기업서버와 클라우드 시스템은 서로 신뢰하는 상태이다. 세부절차는 [그림 7]과 같다.



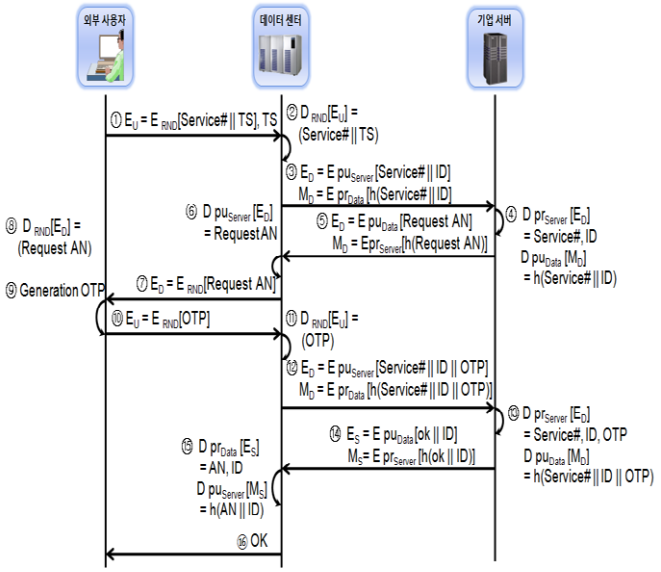
[그림 7] 기업 내부 사용자 인증 절차

사용자는 재사용 공격 방지를 위한 *TS* 값과 서비스 요청 메시지를 연접하여 *RND*로 암호화하여 전송하면 데이터센터는 메시지를 복호화 하여 요청 서비스를 확인한다. 해당 서비스가 기업으로부터 정책이 설정되어 있는 경우에 데이터센터는 기업 서버의 공개키로 암호화 하여 요청 서비스와 사용자의 ID를 연접하여 전송한다. 이 때, 무결성 보장을 위해 해시 된 다이제스트를 자신의 개인키로 서명하여 같이 전송한다. 기업 서버는 두 개의 메시지를 복호화 하여 검증하고 ID에 대한 사용자를 모니터링 한 결과를 통해 사용자의 정보가 확인이 되면 데이터센터의 공개키로 암호화하여 사용자 확인 메시지를 전송한다. 무결성을 위해 기업서버는 해시된 다이제스트를 자신의 개인키로 서명하여 같이 전송한다. 데이터센터는 받은 두 개의 메시지를 복호화 하여 검증 한 뒤 사용자에게 서비스를 제공하는 방식이다. 기업 내부에서 접근한 사용자에 대한 인증은 [그림 7]과 같지만, 기업 외부에서 접근한 사용자(사원)에 대해서는 모니터링이 되지 않기 때문에 기업 내부에서 접근하는 방식과 다른 인증 절차를 거친다. [그림 8]은 이와 같은 인증 절차를 나타낸다.



[그림 8] 기업 외부 사용자 인증

[그림 8]과 같이 기업 외부 사용자가 클라우드 시스템에서 보안정책이 정해져 있는 서비스에 접근 할 경우 데이터 센터는 기업 서버에게 사용자 확인을 요청한다. 확인 요청된 사용자는 모니터링이 되지 않은 외부접근이므로 기업 서버는 클라우드 시스템에 인증번호를 요청한다. 클라우드 시스템은 사용자에게 인증번호를 요청하면 사용자는 OTP를 생성하여 보낸다. OTP를 받은 클라우드 시스템은 기업서버로 사용자 재확인 요청을 하고 기업서버는 OTP를 확인 후, 사용자 대한 확인응답을 함으로써 접근에 대한 인증이 되어 사용자는 서비스를 제공받는다. 세부적인 절차는 [그림 9]와 같다.



[그림 9] 기업 외부 사용자 인증 절차

서비스 요청에 대한 부분은 [그림 9]의 ①~③과 같이 내·외부 사용자의 인증 절차가 동일하지만 외부 사용자는 모니터링이 불가능한 사용자이기 때문에 기업 서버는 데이터센터의 공개키로 암호화 하여 인증번호를 요청하며 무결성을 위해 해시 한 다이제스트를 자신의 개인키로 서명하여 전송한다. 데이터센터는 메시지를 복호화하여 검증한 후 사용자에게 *RND*로 암호화하여 인증번호를 요청한다. 사용자는 기업으로부터 발급받은 OTP 생성기를 통해 만들어진 *OTP*를 데이터센터에게 전송한다. 데이터센터는 요청한 서비스와 사용자 *ID,* 전송받은 *OTP*를 기업 서버의 공개키로 암호화 한 메시지와 무결성을 위해 해시 한 다이제스트를 자신의 개인키로 서명하여 기업서버로 전송한다. 기업서버는 메시지들을 복호화 하여 검증한 후, 사용자 확인 결과 메시지를 데이터센터로 전송하면 확인 메시지를 받은 데이터센터는 사용자에게 서비스를 제공한다. 이와 같은 보안정책이 정해져 있는 서비스에 대한 접근을 총 2번의 인증절차를 거침으로써 클라우드 시스템의 보안문제를 해소할 수 있다.

4. 결론 및 향후 연구과제

본 논문에서는 기업에서 클라우드 컴퓨팅을 사용하기 위한 사용자 접근을 효율적으로 통제할 수 있도록 하는 방법을 제안하였다. 기본적인 클라우드 시스템의 접근에 대한 초기인증은 서비스를 제공하는 업체에서 하고 보안문제로부터 노출을 원하지 않는 서비스와 정책이 필요한 서비스를 기업 자체적으로 분류 및 설정이 가능하다. 보안정책이 정해져 있는 서비스에 대한 접근을 기업의 내·외부에서 시도 할 경우 사용자를 재인증 한다. 이때 기업에서 판단하여 인증하는 방식으로써, 기업에서 클라우드 컴퓨팅 사용에 대한 보안위협으로부터 좀 더 안전하고 높은 신뢰성을 갖는다.

향후 연구과제로는 사용자와 클라우드 시스템 간에 안전한 데이터 전송 방식과 보안정책 부분도 안전하게 보호할 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] 임철수, “클라우드 컴퓨팅 보안 기술”, 정보보호학회지, 2009.

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

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

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