모바일 클라우드 컴퓨팅 환경의 스마트 디바이스용 일회용 인증서 기반 권한 관리 기술+

문종식*, 한승완*, 이임영**
*한국전자통신연구원 지식정보보안연구부
**순천향대학교 컴퓨터소프트웨어공학과
e-mail:moonjongsik@gmail.com

Privilege Management Technology based-on One-time Certificate for Smart Device in Mobile Cloud Computing Environment

Jong Sik Moon*, Seung Wan Han*, Im-Yeong Lee**
*Knowledge Information Security & Safety Research Department, ETRI
**Dept of Computer Software Engineering, Soonchunhyang University

요 약

공인인증서의 사용은 꾸준히 증가하고 있으나 증가하는 사용량에 비례하여 하드디스크에 저장된 공인인증서 해킹으로 인한 피해 사례가 증가하고 있다. 이에 따라 정부는 하드디스크 내 공인인증서 저장을 금지하고 이동형 저장매체에 저장하도록 하는 방침을 내놓았다. 또한 모바일 클라우드 컴퓨팅 환경에서는 중앙의 스토리지에 데이터가 저장되기 때문에 공인인증서를 중앙 스토리지에 저장하는 것은 매우 위험한 일이다. 이러한 방침으로 인해 앞으로 USB 메모리 및 스마트폰과 같은 이동형 저장매체에 대한 중요성이 높아질 것이며, 분실 위험이 높은 USB 메모리 및 스마트폰의 특징에 따라 인증서가 저장된 저장매체 없이도 인증서를 사용할 수 있는 방안이 필요하게 될 것이다. 본 논문은 일회용 인증서에 대한 요구사항 분석 및 형식을 설계하고, PKI 인증서를 기반으로 경량화된 일회용 인증서를 발급받아 인증서를 사용할 수 있도록 하였다. 또한 모바일 클라우드 컴퓨팅 환경에서 일회용 인증서를 이용한 권한 관리 기술을 제안하여 안전성과 효율성을 제공하도록 하였다.

1. 서론

미래 인터넷 기술은 컴퓨팅 기술의 발전과 더불어 더욱더 지능화, 개인화 되어 가고 있는 추세이다. 유비쿼터스 컴퓨팅 환경의 도래와 함께 IT 자원과 소프트웨어는 다양한 서비스 형태로 진화하고 있으며, 차세대 컴퓨팅환경은 언제 어디서나 실시간으로 원하는 만큼의 IT 자원을 서비스 형태로 사용하고 사용자 환경에 구애 없이 작업이 가능한 환경으로 발전하고 있다. 이러한 시대적인 흐름은 IT 산업의 Public 서비스뿐만 아니라 개인 사용자 중심의 Private 서비스 영역까지 확대되고 있으며, 다양한 서비스 요구에 따라 클라우드 컴퓨팅이라는 개념이 나타나게 되었다. 클라우드 컴퓨팅은 여러 가지 개념으로 정의되고 있으나, “대용량의 확장 가능하고 가상화된 자원들이 인터넷 상에서 서비스 형태로 제공되는 컴퓨팅의 한 형태”라는 가트너의 정의가 널리 받아들여지고 있다. 클라우드 컴퓨팅 서비스는 데이터를 보호하기 위해 별도의 자원을 할당하고 관리하므로 개별 기업이나 개인이 직접 데이터를 관리하는 것보다 안전성이 높아지는 것이 일반적이나, 반면에 민감한 데이터에 대한 직접 제어권을 포기해야 하며, 사고 시 피해의 파급효과가 크기 때문에 기업 비밀 관리나 개인의 프라이버시 측면에서 많은 문제점이 존재한다[3]. 또한 클라우드 컴퓨팅 서비스 산업의 활성화를 위해서는 보안문제 해결이 선결해야할 주요 이슈이므로, 2008년 2월의 아마존 AWS S3 서비스의 중단(outage) 사고, 2008년 Carbonite 사의 백업저장소 손상으로 인한 데이터의 영구적 손실 및 2008년 9월의 Google Docs의 데이터 유출 문제 등과 같은 유사 사례들이 재발하지 않도록 하는 방안 마련이 시급하다. 그러나 현재까지 클라우드 컴퓨팅만을 위한 보안 기술이 개발되거나 연구된 사례는 미비한 상태이며, 기존의 보안 제품 및 보안 기술을 접목한 보안권고만 발표되고 있는 실정이다. 또한 2009년 클라우드 컴퓨팅 보안을 위해 최적의 방법을 찾아 보급을 촉진하고 보호하는 방법을 제시하기 위해 창설한 Cloud Security Alliance에서 2009년 12월 발표한 “Security Guidance for Critical Areas of Focus in Cloud Computing”에서도 권고사항만 제시하고 있다. 따라서 클라우드 컴퓨팅 환경에 적합한 보안 요구사항을 만족하는 안전한 보안기술에 관한 연구는 매우 시급한 실정이며, 그 중요성은 아무리 강조를 하더라도 지나치지 않을 것이다. 이에 본 논문에서는 모바일 클라우드 컴퓨팅 환경에서 스마트폰을 이용한 일회용 인증서 기반 권한 관리 기술을 제안 하였다. 본

+ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2010-0022607)
+ 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업(정보통신)의 일환으로 수행하였음. [KI0038421 , 모바일 악성 프로그램 탐지 및 방어 솔루션 개발]

논문의 구성은 다음과 같다. 2장에서는 국내·외 연구동향 및 문제점에 대하여 알아보고 3장에서는 일회용 인증서 기반 권한 관리 기술을 제안한다. 4장에서는 제안 방식을 분석하고 마지막으로 5장에서는 향후 연구 및 결론으로 마치도록 한다.

2. 국내·외 연구현황 및 문제점

국내·외로 클라우드 컴퓨팅에 관한 연구는 활발히 진행되고 있으나, 클라우드 컴퓨팅 보안 기술에 관한 연구는 초기 단계에 머물고 있다. 연구현황을 살펴보면, 국외 클라우드 컴퓨팅 관련 연구는 Amazon, Microsoft, IBM을 중심으로 매우 빠른 성장세를 보이고 있으며, 국내 클라우드 컴퓨팅 관련 연구는 삼성전자, 클루넷 등과 같은 업체를 중심으로 개발이 진행되어 가속화 단계에 이르고 있다. 그 중 데이터센터 접근제어를 위한 인증서 기반 권한 관리 기술은 대규모의 유무선 네트워크로 연결된 컴퓨터가 중앙의 제어 없이 자율적으로 상호 작용하는 동적 환경으로 대표되는 기술로 클라우드 컴퓨팅 보안 분야에서 활발히 연구가 진행 중 이다. 이와 같은 기술은 중앙의 통제가 없을 뿐만 아니라, 응용이 완결되지 않은 채 접속이 종료되는 컴퓨팅 노드들로 인하여 전체적으로 정리된 네트워크 자원 구조가 유지되지도 않는다. 이러한 분산성을 유지하면서 시스템 간의 관계를 정의가 필요하다. 이를 위해 2003년 Hwang 등이 제안한 방식은 그리드 환경에서 인증서를 활용하여 권한관리 기법에 관하여 제안 하였다[1]. 기존의 ID 매핑 방식의 권한부여 시스템 대신에 인증서 내의 확장 필드에 사용자의 권한 등급을 추가하고, 이를 기반으로 자원에 대한 접근 제한 등급을 결정하도록 제안하였다. 2008년 Yang이 제안한 방식은 신뢰도가 낮은 네트워크 환경을 위하여 트리 구조 기반의 권한 관리 기법에 관하여 제안 하였다[2]. Yang 방식은 역할 명세 인증서의 관계구조 트리를 구성하여 권한 정보를 트리 구조 내에서 주고받음으로써 안전하고 효율적으로 권한 관리를 제공한다. 노드의 생성 및 소멸, 패킷 손실률로 인한 신뢰도 저하를 고려하여 역할의 생성 및 갱신에 따른 비용구조를 모델링하고 성능을 측정 분석하고, 역할 명세 인증서를 구조화하여 평균 패킷 전송량을 크게 줄인 것이 장점이지만, 이에 비해 메시지 손실률이 증가 된다는 단점이 있다. 이와 같이 국내·외로 클라우드 컴퓨팅 서비스에 대한 연구가 진행되고 있으나 핵심 요소기술들에 대한 연구는 다양한 요구사항을 만족할 수 없으며, 클라우드 컴퓨팅에 특화되어 있는 보안 기술에 대한 대책이 미비한 실정이다. 이러한 핵심요소 기술들에 대하여 보안에 대한 연구가 선행되지 않는다면, 개인 프라이버시뿐만 아니라 서비스의 발전 및 시장 확대를 저해할 것이다. 이로 인해 새로운 서비스의 개발에 있어 보안 기술에 대한 연구는 반드시 선행되어야 하며 다양한 문제점과 해결방안에 대한 연구를 진행하여야 한다.

3. 일회용 인증서 기반 권한 관리 기술

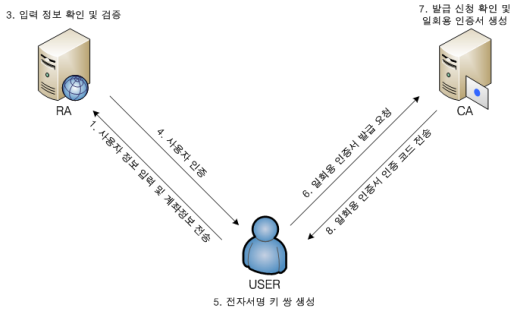
제안방식은 모바일 클라우드 컴퓨팅 환경의 보안 서비스 모델 개발을 통해, 안전한 데이터 관리 기술과 사이버 공격 대응을 위한 보안 기술 및 클라우드 인증서 기반 스마트 디바이스 인증 기술 연구를 수행한다. 클라우드 컴퓨팅 환경에서 사용자는 어느 시점, 어느 장소에서든지 자원과 서비스에 접속할 수 있도록 하기위해서 자원을 누구에게나 접속 가능하도록 가용성을 제공해야 하는 경우, 오픈된 네트워크 환경의 보안을 고려하기 위해서는 중앙의 통제 없이 사용자의 인증과 접근제어를 이룰 수 있어야 한다. 그러나 기존의 연구는 중앙 집중식의 관리 서버 접근제어 방식으로 연산량 및 효율성이 떨어지며, 메시지 손실률이 증가된다는 단점이 있어 모바일 클라우드 컴퓨팅 환경에 적용하기에는 적합하지 않다. 따라서 데이터센터 접근제어를 위한 인증서 기반 권한 관리 기술은 기존의 인증서 기반 권한관리 기술의 효율성 문제를 해결하고 모바일 클라우드 컴퓨팅 환경에 적합한 클라우드 인증서 기반 기술을 개발한다. 또한 모바일 클라우드 컴퓨팅 환경에 적합한 인증서 구조 및 프로토콜을 개발하여 클라우드 인증서를 정의하고, 검색 가능한 암호를 위해 암호화되어 저장된 데이터 및 데이터센터에 접근 시 클라우드 인증서를 기반으로 안전하고 효율적인 인증을 제공하고자 한다.

3.1 제안 시스템 구성

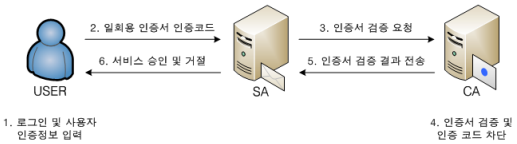
제안 시스템의 구성은 일회용 인증서 발급 단계와 일회용 인증서 기반 서비스 사용 단계로 구분된다.

3.1.1일회용 인증서 발급 단계

(그림 1)과 같이 제안하고자 하는 방식은 무선 PKI를 기반으로 하는 일회용 인증서 발급 시스템으로 인증서의 발급은 모두 온라인상에서 이루어진다. 등록기관과 인증기관을 통해 사용자를 인증을 받은 후 기존에 발급받은 인증서를 기반으로 인증기관이 일회용 인증서를 생성하여 일회용 인증서의 인증코드를 전송하는 방식으로 진행된다. 따라서 사용자가 인증서를 소지하고 있지 않은 상황에서 인증서를 이용할 경우, 일회용 인증서를 발급받아 인증서를 이용한 서비스 이용이 가능하게 된다. 또한 일회용 인증서는 인증서 재발급 절차를 거치지 않고서도 인증서를 사용할 수 있게 된다. 일회용 인증서의 요구사항으로는 기존에 발급받은 인증서를 토대로 생성이 되어야 하고, 일회



(그림 2) 일회용 인증서 발급 절차



(그림 3) 일회용 인증서 사용 절차

용 인증코드를 전송하여 한번만 사용이 가능해야하며, 일회용 인증서 인증코드의 유효시간은 3분으로 제한함으로써 무차별적인 인증서 사용을 방지한다. 또한 인증서 형식에 기존 인증서의 일련번호가 포함되어 기존 인증서와 일회용 인증서의 연관관계를 검증할 수 있다. 일회용 인증서의 발급 과정은 다음과 같다.

Step1: 인증서를 소지하고 있지 않은 사용자가 인증서를 이용한 서비스를 사용하고자 할 때, 사용자는 온라인상에서 등록기관에 접속 후, 아이디와 패스워드를 입력하여 인증을 받는다.

Step2: 사용자는 보안카드, 계좌정보를 포함한 인증서 정보를 등록기관에 전송하면 등록기관은 입력정보 일치 여부를 판단하고 인증결과를 반환한다.

Step3: 사용자는 등록기관으로부터 인증 받은 정보를 이용하여 전자서명 키 쌍을 생성한다.

Step4: 인증코드 및 인증서의 비밀번호를 포함한 일회용 인증서 요청형식을 생성한 후 사용자의 개인키를 이용하여 서명하고, 인증기관에 일회용 인증서 발급을 요청한다.

Step5: 인증기관은 발급 신청자를 확인한 후, 일회용 인증서를 생성한다.

Step6: 인증기관은 생성한 일회용 인증서의 인증코드를 사용자에게 전송하고. 인증서의 유효시간을 카운트한다.

3.1.2 일회용 인증서 사용 단계

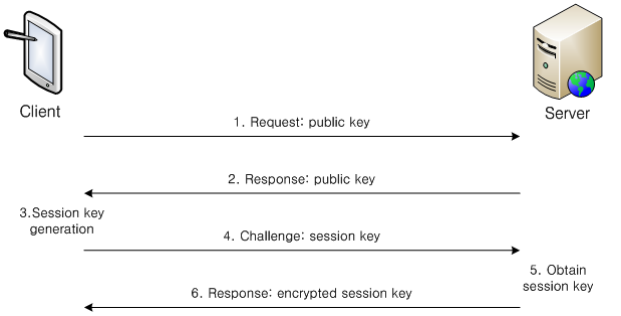
(그림 3)과 같이 일회용 인증서를 사용하기 위해서는 발급받은 일회용 인증서의 인증 코드를 발급받은 후 3분 이내에 서비스를 제공받고자 하는 기관에 전송한다. 사용자의 인증 코드를 전송받은 서비스 요청 기관에서는 일회용 인증서의 유효성 여부를 판단하기 위하여 인증기관에 인증서 검증을 요청하며, 인증기관에서는 일회용 인증서 및 인증 코드의 유효성을 검사한 후 검증 결과를 서비스 요청 기관에 전송한다. 인증기관으로부터 정당한 사용자임이 인증되면 서비스 요청 기관에서는 요청한 서비스를 제공한다.

3.1.3일회용 인증서 형식

제안방식에서 정의하는 일회용 인증서의 형식은 <표 1>과 같다.

<표 1> 일회용 인증서 형식

필드	내용
서명알고리즘	인증기관이 인증서를 생성할 때 사용하는 서명 알고리즘의 OID값을 가짐(RSA사용)
발급자	공인인증서를 발급한 인증기관의 명칭
소유자	공인인증서의 소유자 명칭
소유자 공개키 정보	소유자의 공개키에 대한 알고리즘 및 공개키 정보
기존 인증서의 일련번호	인증서와 일회용 인증서의 일치 여부를 판별하기 위하여 사용



(그림 4) 서버와 클라이언트의 세션키 교환 프로토콜

3.2 제안 프로토콜

제안 프로토콜은 일회용 인증서 발급 시스템의 서버와 클라이언트간의 상호인증, 일회용 인증서 발급, 일회용 인증서 사용, 프로그램 구현 프로토콜로 구성되어있다.

3.2.1 서버와 클라이언트간의 상호 인증 프로토콜

(그림 4)는 제안방식의 서버와 클라이언트간의 세션키 교환 프로토콜이다. 먼저 클라이언트는 서버에게 서버의 공개키를 요청하면 서버는 클라이언트에게 자신의 공개키를 전달한다. 서버의 공개키를 전달받은 클라이언트는 세션키를 생성하여 서버의 공개키로 암호화한 후 서버에 전송한다. 서버는 자신의 개인키로 암호화 된 데이터를 복호화하여 세션키를 획득하고, 세션키를 세션키로 암호화하여 클라이언트에게 보낸다. 다음과 같은 과정을 통해 서버와 클라이언트의 상호 인증이 이루어지게 되며, 서버와 클라이언트 간의 전송되는 모든 데이터는 세션키로 암호화되어 전송된다.

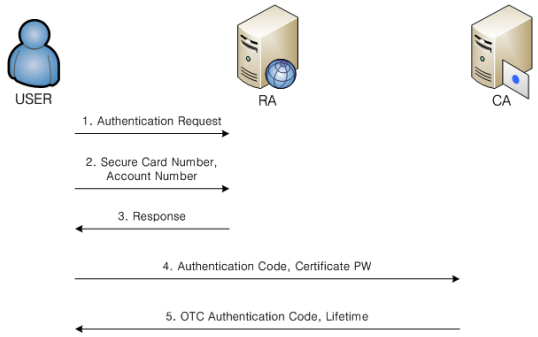
3.2.2 인증서 발급 프로토콜

(그림 5)는 제안방식의 인증 프로토콜이다. 인증기관의 부담을 덜어주고 보다 효율적인 발급 시스템을 구현하기 위하여 사용자는 등록기관을 통하여 정당한 사용자임을 인증 받게 된다. 정당한 사용자임을 인증한 등록기관은 인증기관에 사용자 정보 및 인증코드를 보내 사용자가 일회용 인증서 발급을 원할 시에 요구하는 사용자가 정당한 사용자임을 인증기관이 알 수 있도록 한다. 이렇게 함으로써 인증기관은 별도의 사용자 인증과정을 거치지 않고서도 인증코드의 일치여부 판단으로 사용자를 인증할 수 있다. 그 다음 사용자가 기존에 발급받은 인증서를 토대로 일회용 인증서를 새로 생성하여 일회용 인증서의 인증코드를 사용자에게 전송하는 방식으로 이루어진다. 일회용 인증서의 인증절차는 다음과 같다.

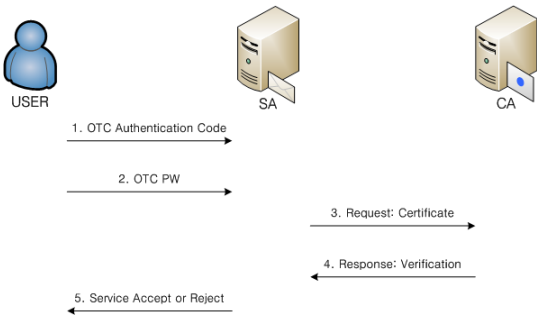
Step1,2: 사용자는 등록기관에 사용자의 ID와 Password를 입력하고 보안카드번호나 계좌번호를 입력하여 전송한다.

Step3: 등록기관은 입력정보와 등록기관내 정보와의 일치 여부를 판단하여 사용자를 인증한다.

Step4: 사용자는 인증코드 및 인증서 비밀번호를 CA에게



(그림 5) 일회용 인증서 발급 시 인증 프로토콜



(그림 6) 일회용 인증서 사용 시 인증 프로토콜

전송한다.

Step5: CA는 사용자에게 전송받은 내용을 토대로 일회용 인증서를 생성하고 인증코드를 생성한다. 또한 유효시간을 적용하여 사용자가 시간 내에만 사용할 수 있도록 조치한다. 적용 후에 사용자에게 인증코드를 전송하게 된다. 일회용 인증서의 인증코드는 제 3자에게 노출되는 것을 방지하기 위하여 암호화가 되어 있어야 하며, 사용자의 편의성을 고려하여 인증서의 인증코드를 숫자 형식으로 변형하여 일련번호를 생성한 후 사용자에게 전송된다. 전송 받은 사용자는 온라인상에서 인증서의 인증코드를 입력하고, 유효시간 내에 기존 인증서와 일회용 인증서의 암호를 입력해야 한다. 유효시간 내에 인증서의 암호가 인증되지 않으면 발급받은 일회용 인증서의 사용은 불가능하게 된다.

3.2.3 인증서 사용 프로토콜

(그림 6)은 제안방식의 인증서 검증 프로토콜이다. 사용자는 서비스 요청기관에 발급받은 인증서의 인증코드와 함께 인증서의 비밀번호를 전송한다. 사용자로부터 서비스 요청을 받은 요청기관은 인증기관에 인증서 검증을 요청한다. 인증기관에서는 인증서 경로를 인증하고 CRL을 확인한 후 검증 결과를 전송하게 되며, 검증 결과에 따라 서비스 요청기관은 사용자에게 서비스 승인 및 거부를 한다.

4. 제안방식 분석

외부의 공격으로부터 안전하기 위해 공개키 방식을 이용하여 클라이언트는 서버에게 서버의 공개키를 요청하고 서버는 클라이언트에게 자신의 공개키를 전달한 한다. 클라이언트는 서버에게 자신의 개인키로 서명한 인증서 요청 형식을 서버의 공개키로 암호화하여 보냄으로써 제 3자가 일회용 인증서를 취득하지 못하도록 하여 기밀성을 제공한다. 또한 해쉬함수를 사용하여 인증서의 해쉬값을 생성하고, 생성된 해쉬값을 서명자의 개인키로 암호화 하여 전자서명을 생성하여 전송한다. 전자서명을 서명자의 공개키로 복호화하고 검증대상 인증서의 해쉬값을 비교함으로써 무결성을 제공한다. 사용자인증은 웹 클라이언트의 ID 및 Password를 바탕으로 제공하며, 부가적으로 보안카드번호를 포함한 계좌정보를 비교하여 인증한다. 모바일 클라이언트에서는 기존에 발급받았던 인증서의 비밀번호를 이용하여 사용자 인증을 제공한다. 부인방지는 공개키 기반 구조를 토대로 전자서명을 생성하게 되는데, 이때 클라이언트의 개인키는 클라이언트만이 가지고 있으므로 부인방지를 제공한다.

5. 결론

현재 클라우드 컴퓨팅 서비스 시장은 이미 형성되어 있고 차세대 클라우드 컴퓨팅 서비스 환경이 다가옴에 따라 클라우드 컴퓨팅 환경에서의 차세대 보안 기술 개발이 필요한 실정이다. 그러나 대부분의 연구가 기존의 연구를 보완하는 단계에 머무르거나 국외의 기술을 도입하는 수준에 머물러 있다. 그러나 본 연구는 클라우드 컴퓨팅 환경에서 차세대 보안 기술 연구는 현재 특화된 기술의 연구로 빠른 개발을 가져올 수 있으며, 그에 따라 클라우드 컴퓨팅 분야 및 응용 시스템 기술 분야에 진출할 수 있는 발판을 마련할 수 있다. 제안방식에서는 이미 발급받은 인증서를 토대로 일회용 인증서 생성 및 발급 시스템을 구성하고, 모바일을 통하여 일회용 인증서를 발급 받을 수 있는 모바일 시스템을 제안하였으며, 발급받은 일회용 인증서의 사용을 보여주기 위한 웹 사이트 및 일회용 인증서를 사용한 안전하고 효율적인 일회용 인증서 기반 접근제어 시스템을 제안하였다. 또한 인증서가 저장된 저장매체가 없을 경우에도 인증서를 사용할 수 있는 대응책이 없던 사용자에게 보다 안전하게 인증서를 사용할 수 있도록 할 뿐만 아니라, 기존의 인증서 사용 시 인증서가 저장된 저장매체의 부재 시에도 인증서를 사용할 수 있는 방안을 제시하였다. 향후 지속적으로 증가할 공인인증서 사용자를 위해 일회용 인증서 외에도 다양한 인증서 사용 방안에 대한 연구가 필요할 것으로 사료된다.

참고문헌

[1] 양수미, “신뢰도가 낮은 네트워크 환경을 위한 트리 구조 기반의 권한 관리 기법,” 한국정보보호학회 논문지, 제18권 제5호, pp.83-91, 2008.

[2] 황영철, 박형우, 김용배, 이성현, 이원구, 이재광, “그리드 환경에서 인증서를 활용한 사용자 권한 부여 모듈의 설계 및 구현,” 한국인터넷정보학회 춘계학술발표대회 논문집, 제4권 제1호, pp.180-183, 2003.

[3] 지식경제부·행정안전부·방송통신위원회, “범정부 차원의 『클라우드 컴퓨팅 활성화 종합계획』 마련”, 지식경제부 보도자료, 2009.