제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

클라우드 CAD에서의 도면 보안 기술 분류

배태원*, 홍미*, 이종근*
*창원대학교 컴퓨터공학과
e-mail: jklee@changwon.ac.kr

Cloud CAD in the Security Technology Category

Tae-won Bae*, Mi Hong*, Jong-kun Lee*
*Dept of Computer Engineering, Changwon National University

요 약

클라우드 CAD는 기존 사용자들의 작업 효율성 증대 및 기업의 자원 절약뿐만이 아니라 설계와 현장간의 협업 등 많은 부분에서 큰 효과를 가져다 줄 것으로 기대하고 있다. 하지만 많은 기업들이 도면, 문서 등이 관련된 보안에 관련된 문제로 인해 클라우드 CAD를 사용함에 있어서 망설이고 있다. 이에 본 논문에서는 현재 시중에 출시되어 있는 대표적인 클라우드 CAD인 AutoCAD WS와 몇몇 기업에서 적용중인 가상화 클라우드 CAD를 기준으로 하여 기업에 적용시 문제가 될 수 있는 보안 문제를 알아보고 그 해결 방안을 제시한다.

키워드: 도면보안, 웹클라우드, 모바일 클라우드, 보안기술, 클라우드 CAD

1. 서론

인터넷 기술을 활용하여 다수의 고객들에게 높은 수준의 확장성을 가진 IT 자원들을 서비스로 제공하는 컴퓨팅 이라고 정의한 클라우드 컴퓨팅은 인터넷 상의 서로 다른 물리적인 위치에 존재하는 각종 컴퓨팅 자원들을 가상화 기술로 통합하여 사용자들에게 언제 어디서나 필요한 정보를 편리하고 저렴하게 사용 환경을 제공하는 기술이다[1]. 이러한 클라우드 컴퓨팅은 서비스의 내용에 따라 크게 인프라 서비스(IaaS, Infrastructure as a Service), 플랫폼 서비스(PaaS, Platform as a Service), 소프트웨어 서비스(SaaS, Software as a Service)로 구분할 수 있다.

IaaS(Infrastructure as a Service)는 클라이언트, 서버, 데이터센터 공간, 네트워크 장비 등 개인이나 기업의 컴퓨팅 기반 자산을 따로 구매하여 구축하지 않고 필요한 컴퓨팅 기반 자산의 일부 또는 전부를 서비스 형태로 빌려 쓰는 서비스이다. PaaS(Platform as a Service)는 이용자(Software 개발자)가 애플리케이션을 개발, 테스트, 구축할 수 있는 통합된 플랫폼을 제공하는 서비스로서 이용자는 PaaS를 통해 새로운 애플리케이션을 개발하기도 하고, 다른 SaaS 서비스를 제공하기도 한다. SaaS(Software as a Service)는 기업이나 다수의 개인 사용자에게 공통으로 필요한 소프트웨어를 웹 등을 통해 임대해 사용할 수 있도록 제공하는 서비스이다. CAD를 사용함에 있어서 항상 이슈화 되어 왔던 문제점은 속도와 안정성이라고 할 수 있다. 대용량 파일을 얼마나 빨리 열고, 작업시 끊어짐이 없이 작업을 하는지의 여부와 대용량 파일에서 작업시 얼마나 문제점 없이 오랫동안 작업이 가능한지가 CAD에서 가장 중요한 것이라고 할 수 있다. 본 논문에서는 기존 이슈화 되고 있었던 속도와 안정성이라는 문제점에 클라우드 컴퓨팅이 더해지면서 발생할 수 있는 보안 문제가 무엇인지 알아보고, 해당 문제를 해결할 수 있는 방안을 찾고자 한다.

2. 관련연구

2.1 웹(Web) 클라우드 CAD

클라우드 컴퓨팅에서 가장 많은 기술이 웹을 활용한 기술이며, 클라우드 CAD 또한 이 방식을 가장 많이 활용할 것으로 예상된다. OS에 관계없이 인터넷 환경만 된다면 어느 자리에서든지, 어떠한 웹 브라우저를 사용하는 것과 상관없이 자신이 원하는 도면을 확인, 편집할 수 있으며 별다른 CAD 프로그램의 설치 없이 사용할 수 있다는 장점이 있다. 또한 하나의 도면을 공유하여 자리가 떨어져 있는 사람들과의 협업이 가능하다는 특징이 있다. 하지만 Client에 설치하여 사용하는 기존의 CAD Program과 비교하면 아직까지 속도와 기능 면에서 많이 떨어진다. (그림 1)와 같이 AutoDesk사의 클라우드 CAD 제품인 AutoCAD WS[2] 를 확인해 보면 웹 클라우드 CAD의 경우 도면 편집기가 Adobe Flash Player로 되어있다. 저용량의 도면을 확인하는 용도로는 무리가 없는 속도이지만, 대용량의 파일을 컨트롤 할 때는 전체적으로 속도가 떨어지는 부분이 발생한다. 또한 새로운 도면 파일을 생성하는 기능이 없으며, 편집에 있어서도 원 CAD Program인 AutoCAD에 비해서 아직까지는 기능이 많이 부족하다.

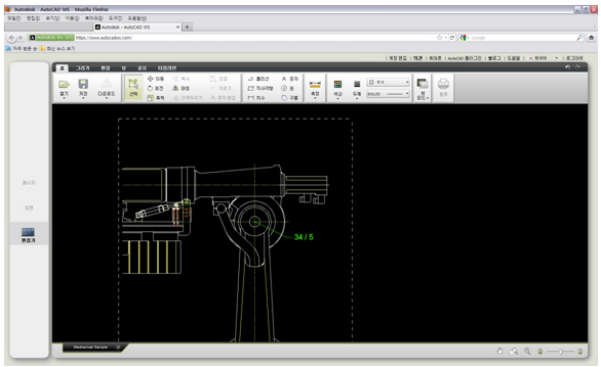

그림 1. AutoCAD WS 도면 편집기 화면

2.2 모바일(Mobile) 클라우드 CAD

스마트 폰 서비스 이용자들이 증가하면서, 기존 CAD 사

용자들은 자신들의 데스크톱에서 이용하던 CAD Program을 스마트 폰에서도 동일하게 제공받길 원하면서 모바일 단말의 이동성과 개인적 소유의 특성이 적용된 모바일 클라우드 CAD가 개발 및 서비스 되고 있다[3].

모바일 클라우드 CAD의 가장 큰 특징은 스마트 폰과 통신이 가능한 지역이라면 어디서든지 CAD 도면에 대한 접근이 가능하다는 것이다. 이 특징은 기업의 입장에서 클라우드 CAD를 접할 때 가장 큰 관심을 보이는 부분이기도 하다. 기존 설계와 생산을 동시에 한 기업의 관점에서 모바일 클라우드 CAD는 작업 효율 향상을 가져다 줄 수 있는 부분일 수 있다.

현시점에서 일반적인 설계와 현장간의 도면 전달 과정은 설계가 완성 되면 해당 도면을 출도 후 현장의 작업자에게 전달하고, 현장 작업자는 그렇게 받은 도면으로 작업을 진행한다. 혹시 도면에 문제가 있거나 도면 수정이 발생이 되면, 상기 방법으로 또다시 현장으로 도면이 전달된다. 현장 작업 중 도면에 문제가 있음이 발견을 하면 현장에서는 설계로 통보를 하고 설계는 설계 수정 작업 후 다시 도면을 현장으로 출도한다(그림 2).

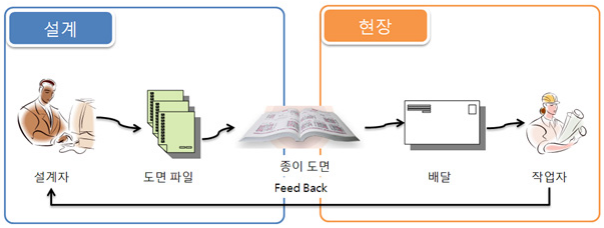

그림 2. 기존 환경에서의 현장 도면 출도 과정

하지만 (그림 4)와 같이 모바일 클라우드 CAD가 적용이 된다면 1차 출도는 그대로 진행 된다고 하더라도 수정이 발생 후 굳이 도면 출도를 우선 진행하지 않아도 현장에서는 스마트 폰을 통해 수정된 도면이 바로 확인 가능하며, 현장에서 문제점 발생 후 도면 수정이 발생되는 부분에 대해서도 좀더 기존보다 빠른 업무의 진행이 가능하게 된다. 또한 문제가 되는 부분을 실시간으로 현장 방문 없이 현장과의 업무 협의가 가능하다.

2.3 가상화(Virtual Machine) 클라우드 CAD

현재 기업들이 적용 중이거나 적용을 검토하고 있는 클라우드 CAD의 방식이라고 할 수 있다. 기업의 입장에서는 그들의 자산일 수 있는 도면의 외부 유출에 대해 상당히 꺼리는 것이 사실이다. 그래서 IT 인프라 구축이 가능한 기업은 자신들 만의 사설망 안에서 그들과 그들의 협력사만이 도면에 대한 접근 권한을 주고자 하며, 이런 상황에서 기업이 가장 원하는 방식은 Private 클라우드 서비스를 이용한 클라우드 CAD라고 할 수 있다. CAD를 사용하는 기업에서 직접 CAD를 개발하여 사용하는 것이 아니라 대부분 전문 CAD 개발 업체에서 만들어 놓은 CAD 프로그램을 사용해야만 하는 기업의 입장에서는 별도로 클라우드 CAD의 개발에 투자를 하지는 않고, 현재 사용중인 CAD 시스템을 자신들의 인프라 안으로 가지고 와서 클라우드 CAD처럼 보이고자 한다. 그들은 자신들의 설계부서에서 도면을 생산할 때 여러 사람들과 협업이 가능해야 하며, 기업 안에서라면 어디서든지 권한이 있는 자가 해당 도면을 수정하기를 원하며, 완성된 도면이 쉽게 현장에서 확인이 가능하고자 하는 것과 동시에 그들의 도면이 그들의 기업 밖으로 나가지 않고, 권한 있는 자에 한해서 안에서만 보이길 원하고 있다.

그래서 기업은 자신들의 서버에 데이터를 저장해 놓고, Citrix 등의 가상화 구축 프로그램을 사용하여 클라우드 CAD를 구축하여 사용하고 있다. 하지만 가상화 클라우드 CAD 내부에서 웹 클라우드 CAD를 사용함에 있어서 가상화 구축 프로그램과 CAD 프로그램의 호환성을 확인해야 하는 문제가 있으며, 단순 도면 확인 차원이라고 할지라도 모바일 클라우드 CAD를 사용하기 위해서는 CAD 개발사에서 어플리케이션을 개발하여 제공해 주어야 하는데, CAD 개발사에서 어플리케이션을 개발할 지의 여부와 개발된 어플리케이션이 해당 기업에서 원하는 방식으로 구동하는지 등 아직 외부에서 도면을 확인 하는 부분 까지는 많은 문제가 있을 것으로 예상된다.

3. 클라우드 CAD에서의 보안 위협요소

클라우드 CAD에서의 보안위협요소문제는 CAD를 하나의 문서 파일로 본다면 클라우드 환경에서의 보안위협 요소에 대하여 정리할 필요성이 있다. 일반적으로 클라우드 컴퓨팅 시스템은 인터넷 서버를 종합 관리하는 IDC(Internet Data Center)와 같은 개념으로 데이터들을 종합 관리하는 시스템이라고 할 수가 있다. 따라서 이러한 클라우드 시스템의 경우 클라우드 서비스 센터로의 데이터 집중은 관리가 편리하고 운영이 효율적이나 집중 공격 대상이 될 수가 있으며 공격을 당하였을 경우 피해는 오히려 극대화 될 수가 있는 단점을 가지고 있다[4-12]. 클라우드 보안 위협요소는 일반적인 보안위협 요소는 물론 클라우드 환경 특성의 요소로 구분이 가능하다[9]. 클라우드 환경에서의 주요 보안위협 요소로는 클라우드 컴퓨팅이 가지는 환경적 보안요소와 기술취약성이 가지는 보안요소, 그리고 내부자에 의한 보안요소 및 네트워크에서의 보안 요소로 본 장에서는 정리한다[5,11,12].

1) 클라우드 환경적 보안

클라우드 컴퓨팅에서의 핵심 기술은 가상화, 대용량분산처리, 운용 및 정보보호기술이다. 이중에서 가상화 기술은 현재 많은 취약점들이 발표되고 있으며 이들 취약점을 이용한 공격도 소개되고 있다. 클라우드의 가상화 환경은 보안이 시스템에 내장되어지고 자동화함으로 보안에 대하여 기존의 PC와 인터넷 환경보다 강화되었다고 하겟지만 서로 다른 클라우드 센터의 연계와 데이터를 내려 받는 인터페이스의 비표준화는 이러한 보안 강화 현상의 개념을 약화 시키기가 쉽다. 또한 서로 연계 되어진 다양한 리소스들을 활용한 악성코드의 공격 시도가 가능하며 또 다른 클라우드 사용자를 공격함으로 연계 되어진 시스템들이 위험에 노출 될 수가 있는 문제점이 있다. 가상화 기술을 통하여 한정 된 스토리지에 상당수의 가상 시스템과의 연계는 복잡한 시스템 구성도를 창출하게 되어 이러한 복잡한 시스템을 관리하기 위한 특별한 솔루션을 요구 할 수가 있으며 각기 서로 다른 솔루션간의 인터페이스 또한 복잡성을 더 가중 시킬 우려가 있게 된다.

2) 가상화 기술 취약성에 의한 공격

가상화 기술 취약성에 의한 공격은, 클라우드 이용자가 공격자가 되어 동일 클라우드 컴퓨팅 환경 내의 다른 클라우드 이용자를 공격 하게 되는 사태가 예상된다. 클라우드

컴퓨팅 환경에서는 인접한 환경에 다른 이용자가 있는 것이 일반적이므로 이용자는 인접한 환경에 있는 공격자로부터 클라우드 컴퓨팅 환경을 통해서 공격 받게 되고 그 결과 중요한 정보를 잃어버릴 가능성이 있다. 이외에도 클라우드 컴퓨팅 센터 내부의 각종 리소스에 대한 다양한 취약점과 공격 루트를 이용한 공격이 예상된다. 하이퍼바이저는 가상화를 가능하게 하는 핵심 기술로서 호스트 시스템에서 다수의 운영체제가 동시에 실행되게 하기 위한 가상 플랫폼을 의미한다[9-12]. 따라서 이러한 하이퍼바이저의 관리자 액세스는 엄격히 통제돼야 한다. 그러나 대부분의 가상화 플랫폼이 이 계층에 대해 복수의 관리적 접근 경로를 제공 가능하여 이에 대한 문제가 발생한다.

3) 클라우드 내부 공격 등에 의한 위협
클라우드 컴퓨팅 센터에는 서로 다른 형태의 이용자 데이터와 각종 서비스가 다양하게 운용되고 있다. 이러한 클라우드 컴퓨팅 환경으로 인하여 더욱 더 내부 사용자에 의한 정보 유출이나 공격 등이 발생할 가능성이 높다[9]. 특히, 이용자가 이용자를 공격하거나 악성코드 등을 유포함으로 상대의 주요 데이터 및 개인정보 유출이 가능하게 되며 이러한 내부자의 소행임을 밝혀 내는데 많은 시간과 노력이 요구 되어 질 수 있다.

4) 가상 기기간의 침입탐지 기능 부재
가상화 머신들 간의 효율적 통신을 위해 대부분의 가상화 플랫폼에는 물리적 호스트 내부에 소프트웨어 기반 가상 네트워크 및 스위치를 생성해 가상화 기기들 간의 직접적인 소통을 실현하는 기능이 포함돼 있다[10]. 현재 개발되어진 침입방지시스템과 같은 네트워크 기반 보안 장치들은 이러한 VM들 간의 통신을 감지해 내지 못한다는 것이다[10]. 따라서, 가상화 기기간의 통신망에서의 침입탐지 기능이나 감지 오류 발생 능력이 증가한다고 한다면 오히려 DDoS와 같은 자체적 기능저하가 발생 할 수가 있다.

5) 네트워크에 대한 위협
클라우드 시스템 환경은 네트워크의 경우에도 사용자와 서비스 제공자간의 네트워크와 서비스 제공자간의 네트워크에 대한 보안 위협 요소 또한 발생 가능하다. 네트워크에서 발생 가능한 위협 요소는 해킹, 도청, 변조 등이 발생하겠지만 사용자간의 데이터 도용 및 서비스의 불법 사용등의 위협 요소 또한 배재 할 수 없다. 물론 이러한 위협은 일반적인 위협이지만 불법 접근이나 권한 밖의 접근이나 이용자를 위장한 공격 또한 예상 가능하다[9].

4. 클라우드 CAD에서의 보안 기술

클라우드 CAD의 기반이 클라우드 컴퓨팅인 만큼 그에 해당하는 기본 보안 기술은 클라우드 컴퓨팅의 보안 기술과 유사하다. 그렇기 때문에 클라우드 컴퓨팅의 안정성 증진과 그것을 위한 사용자 교육을 목적으로 만든 Cloud Security Alliance(CSA)에서 제시한 기업 사용자의 보안 고려사항[11]을 참고할 수 있다(표 1).

상기 위협을 해결하는 데 도움이 되는 도구로는 다음과 같은 것들을 제시하고 있다.

- XML, SOA 그리고 애플리케이션 보안
- 전송중이거나 머물러 있는 데이터에 대한 암호화 도구
- 스마트 키 관리
- 로그(Log) 관리
- ID와 액세스 관리: 가상 방화벽과 다른 가상화 관리 도구
- 데이터 손실 방지

표 1. CSA협회 제시 보안 고려 사항

구분	보안 도메인
거버넌스 (Governance)	·Governance and Enterprise Risk Management ·Legal ·Electronic Discovery ·Compliance and Audit ·Information Lifecycle Management ·Portability and Interoperability
운영 (Operation)	·Traditional Security, Business Continuity and Disaster Recovery ·Data Center Operations ·Incident Response, Notification and Remediation ·Application Security ·Encryption and Key Management ·Identity and Access Management ·Storage ·Virtualization

클라우드 CAD라는 환경에서 상기의 보안 고려사항을 모두 신경을 써야 하긴 하지만 특별히 신경을 써야 하는 부분은 사용자 인증 부분과 암호화 부분, 그리고 활동 감시 부분, 가용성 부분 등이 중요하게 작용할 것이다.

4.1 사용자 인증 기술

사용자 인증의 경우 ID/패스워드 외에 (표 2)과 같이 다양한 형태의 인증 기술을 사용하여 사용자 인증을 강화할 수 있다. 전통적으로 사용자 확인을 위해서 이용했던 전자서명 기술도 많이 활용할 수 있으나, 클라우드 컴퓨팅 환경에서의 전자서명 기술에서 취약점이 발견되기도 하였다. 모바일의 경우 가상 키보드를 활용하여 정보 노출이 되지 않도록 하는 기술이 보장되어야 한다. 또한 단말기에서 입력된 정보가 서버까지 암호화되어 안전하게 전송 및 처리가 되어야 한다.

표 2. 사용자 인증 기술

기술명	내용
ID/Password	가장 기본적인 인증 방식
PKI	공개키를 통한 인증 방식
Multi-factor	몇 가지의 인증 수단을 조합해서 사용하는 기법
SSO	한 곳에서 인증 후 인증확인 정보와 전달을 통해 다른 곳은 인증확인 없이 통과하는 것. SAML(Security Assertion Markup Language)가 대표적인 표준
OAuth	OpenAPI로 개발된 표준 인증 방식
i-Pin	직접 본인 확인을 수행한 기관에서 확인정보를 발급해주는 방식. 한국에서 사용

4.2 암호화 기술

기밀성의 경우 대용량 데이터의 암호화시 전체 시스템의 가용성이 떨어질 수 있기 때문에 적합한 암호화 시스템이 필요하다. 특히나 대용량의 도면 파일에 대한 작업을 진행해야 하는 클라우드 CAD의 경우 암호화로 인한 작업 속도 저하는 생산성 저하로 나타나기 때문에 상당히 민감한 부분 중 하나이다. 최근 DES나 AES와 같은 블록 암호 대용으로 스트림 암호를 사용하는 방법 등이 있을 수 있다(표3).

표 3. 암호화 기술

기술명	내용
AES-NI	인텔의 암호화 기술. 암호화를 하드웨어에서 담당하게 하여 성능의 저하 없이 암호화 실시 가능
블록암호	Data를 정해진 블록 단위로 암호화하는 대칭키 암호 시스템 DES, AES 등이 대표적
대치암호	평문의 각 문자를 영문의 알파벳 순서에 따라 일정한 거리만큼 앞/뒤에 위치한 문자들로 바꾸어서 암호화
RSA	암호화와 인증을 할 수 있는 공개키 암호시스템
스트림 암호	이진화된 평문 스트림과 이진 키 스트림의 XOR 연산으로 암호문 생성. 블록 암호보다 빠름.

4.3 활동 감시 기술 및 기타

클라우드 CAD의 경우 사용자가 Data에 발생되는 각종 이벤트에 대해서 알 수 없다. 그렇기 때문에 클라우드 CAD를 서비스하는 업체에서 Data Center에 접근하는 사용자들의 활동을 감시하고, 분석을 할 필요성이 있다.

이런 활동 감시와 분석은 어떤 문제가 발생했을 때 어떻게 해결할 지에 대한 의사결정에 도움이 되는 결과를 보여준다. 감시와 분석에 대해 크게 2가지의 방법이 있다. 첫 번째는 Event 수집 후, 분석 요청이 있을 경우만 분석하는 방식인 Request-Driven Analysis 방법이 있으며, 두 번째는 Event 발생시 실시간으로 분석하는 방식인 Event-Driven Analysis(Continuous Intelligence) 방법이 있다[12]. Request-Driven Analysis의 경우 이벤트를 계속 수집은 하지만 따로 분석은 하지 않는다. 분석 요청이 들어왔을 때에 과거부터 지금까지의 모든 데이터를 기반으로 분석을 하고 결과를 내게 된다. 분석량이 많다 보니 시간이 오래 걸리게 되며 결과물의 품질이 좋지 못한 경우가 종종 발생하기도 한다. Event-Driven Analysis의 경우 이벤트를 수집하면서 실시간에 가깝게 바로 분석을 한다. 이미 분석을 계속하고 있으므로 결과가 필요할 때에 즉시 사용이 가능하다. 또한 분석 결과를 다시 Input으로 사용하게 되므로 결과 품질이 높은 경우가 많다.

데이터 무결성과 가용성에 있어서, 서버간에 교환되는 메시지에 무결성 검사 루틴이 없어서 발생된 2008년 7월의 AWS 서비스다운 사례와 EBS(Elastic Block Storage)의 미러링 문제로 발생된 2011년 4월의 AWS 서비스다운 사례로 볼 수 있듯이 아직까지 Public 클라우드 CAD가 불안정한 것이 사실이다. 하지만 문제 발생 후 복구 등에 대한 신뢰성은 Private 클라우드 CAD에 비해서 높다는 점이 있다.

5. 결 론

비록 아직 많은 설계 및 제조 기업에서 클라우드 컴퓨팅의 개념조차 잘 모르고 있는 상황이지만, 업체 조사시 설계와 현장과의 협업이 필요하다는 것과 설계와 현장간 협업이 가능하다면 사용을 하고 싶다는 의견을 많이 제시하였다. 그와 함께 자신들의 도면 파일 등 데이터가 외부에 저장되는 것에 대한 우려도 함께 표시하였다.

본문에서 클라우드 CAD 적용시 발생 가능성이 있는 보안 문제점을 도출하였고, 해당 보안 문제를 해결할 수 있는 해결책을 알아보았다. 본 논문은 향후 CAD 개발사 측에서 클라우드 CAD 개발시 보안 위협기술과 취약점을 고려하기 위한 자료로 활용될 수 있을 것이다.

클라우드 CAD는 향후 2D 뿐만이 아니라 3D까지 본격적으로 개발이 되면 낮은 비용과 고 효율성 등 많은 장점으로 CAD업계의 새로운 패러다임으로 떠오를 것이다.

참 고 문 헌

[1] 주현식, 클라우드 컴퓨팅 기술 동향과 관점, *한국인터넷 정보학회*, 2010.12

[2]AutoCAD WS, *Autoddesk*, http://AutoCAD WS.COM

[3] 장은영/김형종/박춘식, "모바일 클라우드 서비스의 보안위협 대응 방안 연구", *정보보호학회논문지*,21(1) 2011,pp.177-186

[4] 김현승/박춘식, 클라우드 컴퓨팅과 개인 인증 서비스, *정보보호학회지*, 2010. 4

[5] 이형찬 외,"스마트 워크 보안위협과 대책",정보보호학회지,21(3),2011,pp.12-21

[6] 은성경,"클라우드 컴퓨팅 보안기술동향",정보보호학회지,10(2),2010,pp.27-31

[7] 임철수, 클라우드 컴퓨팅 보안 기술, 정보보호학회지,19(3),2009, pp.14-17

[8]최주영 외,"클라우드 컴퓨팅환경에서의 가상화 악성코드",정보보호학회지,20(2),2010,pp.44-50

[9] 박춘식, "클라우드 컴퓨팅에서의 보안 고려사항에 한 연구", 한국산학기술학회논문지,Vol. 12, No. 3 pp. 1408-1416, 2011

[10] 구자성, "가상화기술을 이용한 클라우드 컴퓨팅 보안 관리연구", 건국대학교 석사학위논문, 2010.8

[11]박지수,박종혁,"클라우드 컴퓨팅 보안에 관한 연구 및 고찰",한국정보처리학회춘계학술대회논문집,제18권,1호, 2011. 5

[12]김지연 외,"클라우드 컴퓨팅 환경의 가상화 기술 취약점분석연구",정보보호학회지,19(4),2009,pp.72-77