홍 승 필 교수지도

석사학위 청구논문

클라우드 환경 내
안전한 데이터 전송 및 활용 방안 연구

2013

성신여자대학교 대학원

컴퓨터학과

양 새 로 미

클라우드 환경 내
안전한 데이터 전송 및 활용 방안 연구

홍 승 필 교수지도

이 논문을 석사학위논문으로 제출함

2012년 11월

성신여자대학교 대학원

컴퓨터학과

양 새 로 미

인 준 서

신유진의 석사학위 논문으로 인준함.

심사위원 홍 의 석 인

심사위원 변 혜 원 인

심사위원 홍 승 필 인

성신여자대학교 대학원

논문 개요

정보 기술 환경의 발달은 인터넷 사용자에게 다양한 웹 서비스를 통해 정보를 손쉽게 접하고 활용할 수 있게 해주었다. 그리고 최근 몇 년간 스마트기기, 소셜미디어 등 다양한 서비스 및 데이터의 폭증으로 인한 이른바 '빅 데이터' 시대의 도래가 도래했다. 많은 데이터와 과도한 트래픽 문제를 해결하기 위해 인터넷으로 접속 가능한 공간이면 어떠한 단말기로 자원을 이용할 수 있게 해주는 클라우드 컴퓨팅에 대한 관심이 증폭되고 있다. 클라우드 컴퓨팅은 비용과 시간에 효율적이고 정보의 공유에 시간과 공간의 제약을 극복시켜 최근 몇 년 동안 많은 주목을 받으며 급속히 성장한 기술이다. 하지만 신기술의 빠른 성장과 높은 의존도는 문제점을 야기한다. 최근 클라우드 컴퓨팅 환경에서의 스마트 기기를 통한 결제, 금융업무 등을 통해 정보보호 위협요소가 증가하고 있다.

본 논문에서는 클라우드 컴퓨팅이라는 개방된 환경에 저장된 중요 정보를 안전하게 관리하기 위하여 정보보호 문제점을 다각적 요소별로 분석하여, 이를 해결하기 위한 SDTU(Secure Data Transmission and Usage) 아키텍처를 제안한다. 이는 컴퓨팅 자원을 가상화하여 분산 적용하는 컴퓨팅 환경에서 사용자가 안전하게 서비스를 이용할 수 있도록 단계별 보안성 점검 및 관리방안(1. 사용자 인증 메커니즘, 2. 클라우드 신뢰도 검증 메커니즘, 3.데이터 안전성 점검 및 접근제어 메커니즘)을 제안하였다. 마지막으로 클라우드 환경 내 체계적인 정보보호 방안 확립을 위한 시스템 구현방안을 소개함으로써 실제 환경에서의 응용방안의 가능성을 타진한다.

목 차

표 목 차

그 림　목 차

제 1장 서 론

2008년을 전후로 인터넷에서 허가된 컴퓨팅 자원을 이용할 수 있는 다양한 서비스가 출시되면서, 이를 포괄하는 용어로 '클라우드 컴퓨팅'이 사용되기 시작했다. 현재의 클라우드 열풍은 눈에 보이지 않는 컴퓨팅 자원을 사람들이 자유롭게 사용하게 되면서 나타난 모든 제반 변화를 의미한다.[30] 클라우드 열풍은 다음 그림에서 볼 수 있듯이, KISA(한국인터넷진흥원)발표 IT산업 10대 이슈, IT분야 리서치 전문기업인 가트너(Gartner)선정 10대 핵심 전략 기술, NIPA(정보통신산업진흥원)발표 IT 산업 10대 이슈에 모두 클라우드 컴퓨팅이 선정되어 IT 산업에 많은 관심을 받고 있다.

2012 KISA 발표 IT 산업 10대 이슈	2013 Gartner 선정 10대 전략기술	NIPA, 2013 IT 산업 10대 이슈
1. 인터넷 윤리	1. 모바일 대전	1. 빅데이터의 활용
2. 개인정보보호	2. 모바일 앱/HTML5	2. 특허/지재권 중요도 증대
3. IT 거버넌스	**3. 퍼스널클라우드**	**3. 클라우드 컴퓨팅 도입 확산**
4. 망 중립성	4. 사물 인터넷	4. 신정부의 IT 정책방향
5. 클라우드 서비스	**5. 클라우드 컴퓨팅**/하이브리드IT	5. 차세대 반도체/디스플레이

[그림 1] IT 핵심전략 기술 및 이슈

지난 몇 년 동안, 클라우드 컴퓨팅은 급속한 성장을 이루고 있으며, 이는 IT 산업의 많은 부분을 변화시켰다. 그러나 기존 컴퓨터 환경이 클라우드 컴퓨팅 환경으로 전환 되면서 해결되어야 할 많은 이슈들이 지적되고 있다. 클라우드 컴퓨팅이 많은 분야에서 활용되기 위해 보장되어야할 첫 과제는 보안으로 조사

된 바 있으며 서비스, 플랫폼, 인프라 각 서비스 영역에서 데이터 보호와 자원의 관리, 가용성 확보, 개인정보보호 등 해결되어야 할 다양하고 복잡한 보안 문제를 포함하고 있다.

이에 따라 본 연구에서는 클라우드 컴퓨팅 환경에서 안전한 정보 이용을 위해, 단계별 보안성 점검 및 관리방안(1. 사용자 인증 메커니즘, 2. 클라우드 신뢰도 검증 메커니즘, 3.데이터 안전성 점검 및 접근제어 메커니즘)을 통해 SDTU(Secure Data Transmission and Usage) 아키텍처를 제안하였다.

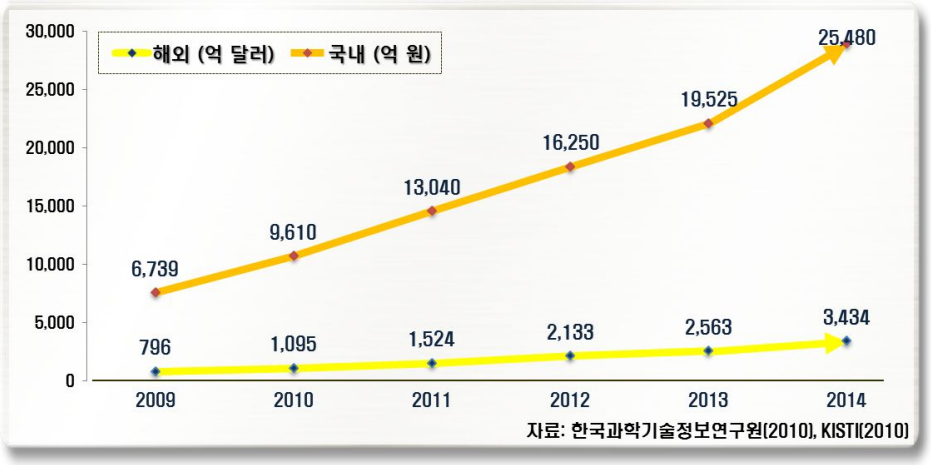
논문의 구성은 다음과 같다. 1장은 논문의 개요와 클라우드 서비스 현황에 대해 간략히 소개하고 2장에서는 클라우드 컴퓨팅의 정의 및 분류와 정보보호 기술 동향에 대해 설명한다. 3장에서는 클라우드 컴퓨팅 환경 내 요소별 정보보호 문제점에 대해서 논의한다. 4장은 안전한 데이터 전송을 위한 아키텍처를 소개하고, 세부구성요소를 설명한다. 5장은 제안하는 아키텍처 분석 및 구현방안을 제시하여 이를 위한 데이터베이스 및 알고리즘을 통한 프로토타이핑 모델을 보여주며 마지막 6장 결론 및 향후연구로 구성한다.

제 2장 관련 연구

1. 클라우드 컴퓨팅

1.1 클라우드 컴퓨팅 정의 및 동향

클라우드 컴퓨팅은 최근 몇 년간 IT시장에서 최대 이슈주체로 꼽히는 등 IT 핵심 트렌드로서 조명 받고 있다. 한국의 클라우드 컴퓨팅 시장규모는 2009년 약 6,700억 원에서 2014년 2.5조원에 이를 것으로 전망되며 이는 연평균 30.5%의 높은 증가율을 보이며 2011년 전체 IT 시장의 성장률이 3.7%에 그친 것과는 대조적으로 높은 증가율을 보이며 급속도로 성장하고 있다.[1] 이는 한국의 높은 유무선 통신 인프라 보급률과 최근 스마트폰, 태블릿 PC 사용 확대에 따라 이동통신사와 포털사이트를 중심으로 클라우드 컴퓨팅 시장이 급속도로 성장하는 것으로 보인다.[2,3,18]



[그림 2] 클라우드 현황 및 전망

이러한 클라우드 컴퓨팅은 [표 1]과 같이 다양하게 정의될 수 있으며, 다음과 같은 가트너(Garthner)의 정의가 널리 받아들여지고 있다.[9,19,20,27] 클라우드 컴퓨팅이란 '대용량의 확장가능(scalable)하고 가상화된(virtualized) 자원들이 인터넷 상에서 서비스로 제공되는 컴퓨팅의 한 형태'이다. 다시 말해, 소프트웨어, 스토리지, 네트워크 등 사용 가능한 대부분의 컴퓨팅 자원들을 필요한 만큼 제공받아 사용하고 이에 따라 일정 비용을 지불하는 방식이다.

[표 1] 클라우드 컴퓨팅 정의

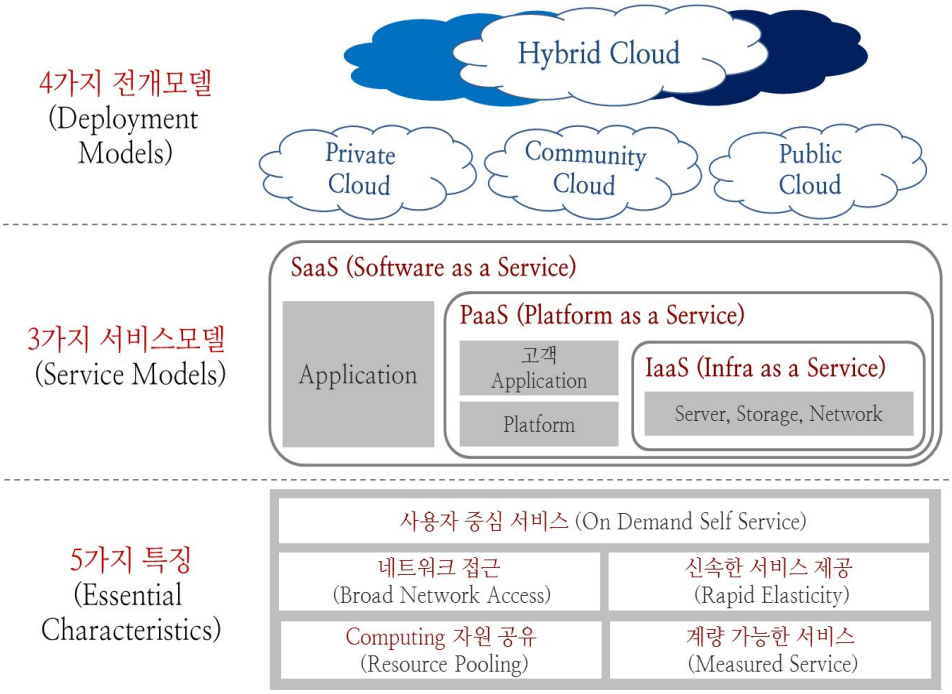
기관명	정의
Ian T. Foster	인터넷을 통하여 외부 고객의 요구에 따라 컴퓨팅 파워, 스토리지, 플랫폼 및 서비스를 제공하기 위해 가상화 되고, 동적 확장성 및 관리가 가능하며, 규모의 경제성이 있는 대규모 분산 컴퓨팅 패러다임
Forrester Research	표준화된 IT기반 기능들이 IP로 제공되고, 언제나 접근이 허용되며, 수요 변화에 따라 가변적이며, 사용량이나 광고를 기반으로 비용을 지불하고, 웹 또는 프로그램적인 인터페이스를 제공하는 형태
Wikipedia	인터넷으로 자원들이 제공되는 형태로 인터넷에 기반을 두고 개발하는 컴퓨터 기술의 활용을 의미함
IBM	웹 기반 응용 소프트웨어를 활용해 대용량 데이터베이스를 인터넷 가상공간에서 분산 처리하고, 이 데이터를 컴퓨터나 휴대전화,PDA 등 다양한 단말기에서 불러오거나 가공할 수 있게 하는 환경
Google	사용자, 업무 중심의 수백 또는 수천 대의 컴퓨터를 연결하여 단일 컴퓨터로는 불가능한 풍부한 컴퓨팅 자원을 활용할 수 있도록 하는 기술
Garter	대용량의 확장가능(scalable)하고 가상화된(virtualized) 자원들이 인터넷 상에서 서비스 형태로 제공되는 컴퓨팅의 한 형태

현재 클라우드 컴퓨팅에 대한 많은 연구가 진행되어 왔으며, Google, 마이크로소프트, Amazon, IBM 등 주요 IT 기업들은 다양한 형태의 클라우드 컴퓨팅 서비스를 제공하고 있으며 최근 들어 Salesforce, Facebook, Youtube,

Mayspace와 같은 기업들도 인터넷 사용자를 대상으로 한 클라우드 컴퓨팅 서비스를 제공하고 있다.[4] 정보보호 솔루션 제공 전문업체인 EMC가 후원하고 IT컨설팅 업체인 IDC가 발간한 '하이브리드 클라우드의 부상: 아시아-태평양 지역 비즈니스 성장을 위한 핵심 전략(Hybrid Cloud on the Rise: A Key Strategy to Business Growth in Asia Pacific)' 분석 보고서에 따르면, 아시아 태평양 최고정보관리자(CIO) 600명을 대상으로 설문한 결과, 응답자의 53%가 이미 클라우드 컴퓨팅을 활용하고 있거나 연구개발 단계에 있는 것으로 나타났으며, 이미 클라우드 서비스를 활용하고 있는 기업은 24%, 향후 12개월 내에 도입예정인 기업은 29%에 달하는 것으로 나타났다. 이러한 결과는 기업이 클라우드 컴퓨팅 서비스를 업무에 활용함으로써 효율성 증대 및 비용절감 등의 기대효과를 예상하는 것을 보여주며 이러한 수치는 더욱 늘러날 것으로 전망된다.

1.2 클라우드 컴퓨팅 분류

클라우드 컴퓨팅은 3가지 서비스 모델, 4가지 전개모델과 5가지 특징을 가진다.[5,13,19,25]



[그림 3] 클라우드 기반 서비스 및 전개 모델

1.2.1 클라우드 컴퓨팅 서비스모델

클라우드 컴퓨팅에서 제공하는 서비스는 대표적인 3가지 서비스(SaaS, PaaS, IaaS)로 분류한다.

소프트웨어형 서비스(SaaS: Software as a Service)는 클라우드 컴퓨팅의 최상위 계층에 해당하는 것으로 다양한 애플리케이션을 멀티테넌트[1]를 통해 온디

1) 하나의 플랫폼을 여러 사용자가 사용하는 것으로, 공통의 하드웨어나 소프트웨어를 사용하는 클라우드에서 권한 없는 사용자가 데이터에 접근하지 못하도록 한 것

맨드 서비스 형태로 제공한다. 제공받는 사용자는 클라우드 환경에서 동작할 수 있는 애플리케이션만을 사용하며, 플랫폼이나 하드웨어 인프라에 대해서는 관리 및 제어하지 않는다.

플랫폼형 서비스(PaaS: Platform as a Service)를 제공받는 사용자는 자신의 어플리케이션을 동작시킬 수 있는 호스팅 환경을 사용하여, 실행되는 애플리케이션들을 제어할 수 있지만 운영체제나 하드웨어 인프라에 대해서는 관리 및 제어하지 않는다.

인프라형 서비스(IaaS: Infrastructure as a Service)를 제공받는 사용자는 연산 프로세싱, 스토리지, 네트워크 등 기본적인 컴퓨팅 자원을 직접 관리하며 애플리케이션에서부터 운영체제까지 제어할 수 있다.

1.2.2 클라우드 컴퓨팅 전개모델

클라우드 서비스 모델과는 별도로 이용 목적에 따라 공공 클라우드, 사설 클라우드, 커뮤니티 클라우드, 하이브리드 클라우드로 나눌 수 있다.

공공 클라우드(Public Cloud)는 일반 사용자에게 제공되는 클라우드 서비스로 다양한 솔루션을 제공하기 위해 유연하고 저렴한 서비스를 제공한다. 클라우드 벤더들은 사용자들을 위해 자원 공유 및 접근 제어 기법을 제공하며, 구글 App Engine과 아마존의 EC2 서비스가 이에 해당한다.

사설 클라우드(Private Cloud)는 기업 내부나 폐쇄된 환경에서 제공되는 클라우드 서비스를 말하며 공공 클라우드에서 제공하는 많은 서비스들을 동일하게 제공하기도 한다. 공공 클라우드와 사설 클라우드의 차이점은 사설 클라우드는 제공하는 기관에서 기밀 데이터를 비롯한 모든 클라우드 운용 및 관리를 담당하여, 클라우드 사용자에 대한 제어권 및 강력한 보안 시스템을 구축할 수 있다.

커뮤니티 클라우드(Community Cloud)는 여러 조직들에 의해 분산되며 클라

우드 인프라는 분산된 관계 사항들을 정리한 특정 커뮤니티를 지원한다.

하이브리드 클라우드(Hybrid Cloud)는 공공 클라우드와 사설 클라우드를 혼용하여 각각의 장점을 극대화하는 클라우드 서비스를 말한다. 공공 클라우드의 저렴하고 안정적인 클라우드 서비스를 최대한 활용하면서 기밀 데이터 운용 및 중요 서비스 제공을 위해 사설 클라우드를 이용하는 형태로 클라우드 보안성 향상을 위한 새로운 대안 모델로 제시되고 있다.

1.2.3 클라우드 컴퓨팅 특징

사용자 중심의 서비스, 자원 공유 및 확장성, 계량 가능한 서비스 및 가용성은 클라우드 컴퓨팅의 대표적인 특징이다.

- 사용자 중심의 서비스

소비자는 서비스 제공자의 개입 없이 필요시에 자동적으로 서버나 네트워크, 저장소 같은 컴퓨팅 능력들을 독자적으로 준비할 수 있다. 또한 폭넓은 인터넷 기반 접근성으로, 클라우드 서비스는 사용자 시스템의 성능에 거의 영향을 받지 않고 클라우드 인터페이스를 통해 접근 가능하며, 네트워크상에서 서비스를 이용할 수 있다. 특히, 모바일 단말 등 다양한 매체를 통해서도 클라우드 환경에 접근이 가능하여 유비쿼터스 서비스를 제공할 수 있다.

- 자원의 공유 및 확장성

제공자의 컴퓨팅 자원은 소비자의 요구에 따라 서로 다른 물리적 또는 가상적인 자원들이 동적으로 할당과 회수되는 멀티테넌트를 통해 여러 사람의 소비자에게 제공될 수 있도록 한다. 컴퓨팅 자원은 사용자의 필요에 따라 컴퓨팅 자원의 양을 신속하게 증가할 수 있게 되어 무한한 자원을 저렴하게 안정적으로 공급받을 수 있다. 서버 관리자 입장에서는 컴퓨팅 자원을 효율적으로 관리할 수 있게 되어 기존 서버 운용과정에서 발생했던 유휴 자원을 최소화하고 이

에 따른 관리 비용을 절감할 수 있으며, 규모의 경제에 따라 비용절감 효과도 볼 수 있게 되고, 컴퓨팅 자원 운용에 최적화된 환경을 구축함으로써 상대적으로 저렴한 비용으로 서비스를 제공할 수 있게 된다.

- 계량 가능한 서비스 및 가용성

클라우드 시스템은 자동적으로 통제되며 서비스 유형에 따라 적정 수준으로 추상화 할 수 있도록 하는 차입(leveraging) 및 계량(metering) 능력을 이용하여 자원의 사용을 최적화 할 수 있다. 최적화된 자원을 소비자에게 컴퓨팅 능력들은 무제한적으로 보일만큼 준비가 가능하며 원하는 시간에 원하는 양만큼을 구매할 수 있다. 또한 서비스 사용의 연속성이나 재난 복구 등을 위해 충분한 여분의 컴퓨팅 자원을 확보하고 효과적인 자원 운용을 통해 사용자들이 서비스를 안정적으로 사용할 수 있도록 지원한다.

1.3 클라우드 컴퓨팅과 타 기술과의 관계

1.3.1 그리드 컴퓨팅

그리드 컴퓨팅(Grid Computing)은 많은 컴퓨팅 자원을 요구하는 문제 해결을 위해 인터넷상에 분산된 다양한 시스템과 자원들을 공유하여 컴퓨팅을 수행하는 모델이다. 분산컴퓨팅의 한 형태로, 슈퍼가상화 컴퓨터는 많은 일을 처리하기위해 자유롭게 결합된 많은 컴퓨터들의 네트워크들로 이뤄져 편리한 인터페이스를 갖는다.[18] 다음 [표 2]는 솔데스크에서 발행한 클라우드 컴퓨팅과 가상화에 대한 칼럼 중 일부분을 발췌한 것이다.

[표 2] 그리드 컴퓨팅과 클라우드 컴퓨팅

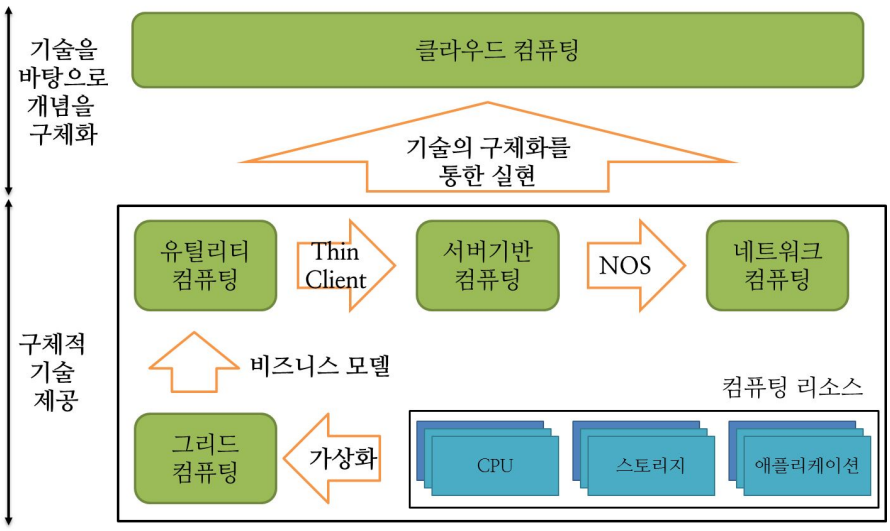
구분	그리드 컴퓨팅	클라우드 컴퓨팅
컴퓨터의 위치와 관리 주체	지리적으로 분산되어 있고, 각기 다른 조직이 관리	지리적으로 분산되어 있지만, 중앙에서 단일 조직이 관리
컴퓨터 구성	다양한 기종 혼재	비교적 동일 기종이 많음
기술 표준	자원 관리나 스케쥴링, 데이터관리, 보안 등의 기술 표준이 존재	기술 표준에 필요성을 절감하고 연구 중
상호 접속성	중시	고려하지 않음
용도	과학 기술적 계산, 대규모 연산처리 등 병렬성이 높은 컴퓨팅	과학 기술적 계산 등과 함께 웹 애플리케이션 등 광범위한 용도로 이용 가능

또한 클라우드 컴퓨팅은 그리드 컴퓨팅 이외에 유틸리티 컴퓨팅, 서버기반 컴퓨팅, 네트워크 컴퓨팅의 기술이 복합적으로 적용되어 구현되었다.

간단하게 정의하자면, 유틸리티 컴퓨팅은 수집된 자원에 비즈니스 모델을 접목하여 사용한 만큼의 비용을 지불하는 컴퓨팅 환경, 서버기반 컴퓨팅은 사용자 PC환경의 Thin Client 기반 하에 사용하는 컴퓨팅 환경으로 자원을 서버에 저장, 관리하여 Client를 경량화하고 소량화 하는 컴퓨팅의 개념, 네트워크 컴퓨팅은 Thin Client환경[2]에 OS까지 경량화하여 네트워크를 통해(NOS[3]) 컴퓨팅을 할 수 있는 컴퓨팅 환경으로 디바이스의 소형과 및 OS, Application의 경량화가 가능하다. 다음 [그림 4]는 클라우드 컴퓨팅과 타 컴퓨팅과의 관계를 비교한 것이다. [6]

2) 각종 프로그램 및 데이터를 네트워크로 연결된 서버로부터 받아쓰는 PC 대체 컴퓨터. 즉 서버에 모든 애플리케이션을 두고 클라이언트는 프로그램이 필요할 때마다 서버에 접속. 모든 애플리케이션이 서버에서 구동되고, 클라이언트와는 단지 키보드와 마우스 입력값, 화면 값만을 주고받아 시스템 속도를 개선

3) NOS: 네트워크OS로 통신망을 관리하고 제어하도록 만든 시스템 소프트웨어로서 기존 운영체제(OS)에서 통신망 관리에 관한 기능을 특화하고 보강한 것



[그림 4] 클라우드 컴퓨팅과 타 컴퓨팅과의 관계

1.3.2 가상화 기술

가상화(Virtualization)는 넓은 의미로는 컴퓨팅 자원에 대한 추상화를 의미한다. 즉, 컴퓨터 리소스의 물리적인 특징을 추상화하여 사용자에게는 논리적 리소스를 제공하며, 이를 통하여 다양한 기술적·관리적 이점들을 제공하는 기술을 말한다. 가상화의 목적은 사용자가 물리 리소스간의 가상화 Layer 구현을 통하여, 컴퓨팅 리소스에 대한 접근 및 인프라관리를 간소화하는 것이다. 가상화는 OS 수준, HW 수준, 프로그래밍 언어 수준 등 다양한 유형의 가상화 기법이 존재한다.

클라우드 컴퓨팅에서 가상화는 자원 가상화(resource virtualization)를 의미하며 자원 가상화는 스토리지 볼륨, 네임 스페이스, 네트워크 자원 등과 같은 구체적인 시스템 리소스에 대한 가상화를 의미한다. 클라우드 컴퓨팅에서는 서버, 스토리지, 네트워크가 대표적인 가상화 대상이다.

서버용 가상화 소프트웨어에는 VMware 및 마이크로소프트의 상용 제품과 함께 오픈소스 소프트웨어인 Xen 등이 있으며, 인텔이나 AMD 등의 칩 제조사가 Processor 수준에서의 가상화 기술 제공하기 시작하여, 오늘날에는 하드웨어 수준의 가상화와 소프트웨어 수준에서의 가상화가 함께 가상화 기술의 진전에 기여하고 있다.

1.3.3 분산 처리 기술

분산 처리 기술은 클라우드 컴퓨팅 하드웨어를 구성함에 있어 인트라넷 또는 인터넷으로 연결된 다수의 컴퓨팅 자원을 하나로 연결하는 기술을 말한다. 관련한 기술로는 분산 파일 시스템, 분산 데이터베이스 등이 있다. 분산 파일 시스템이란 클라이언트가 서버 상에 저장된 데이터를 마치 자신에게 저장되어 있는 것처럼 접근하고 처리할 수 있는 클라이언트/서버 기반의 파일 시스템이다. 분산 컴퓨팅에서는 독립적인 파일 시스템 및 데이터베이스를 단일 시스템으로 인지하고 접근할 수 있도록 하며 대용량 데이터들에 대한 빠른 처리 속도를 가져올 수 있다.

유명한 분산처리 기술에는 구글이 개발한 맵-리듀스(MapReduce)와 이를 오픈소스로 구현한 하둡(Hadoop)이 있다. 이 기술들은 다수의 범용 서버로 구성된 컴퓨터 클러스터에서 대규모의 데이터 처리를 실행하는 데 적합한 프레임워크다.

2. 정보보호관련 기술

정보통신기술은 우리에게 보다 나은 미래를 제공해주는 원동력이자 현대사회에서 없어서는 안 될 필수불가결한 사회기반으로 여겨지고 있다. 한편 우리나라의 인터넷 이용현황을 살펴보면 2011년 인터넷 이용자가 3,718만명(인터넷 이용률 78.0%)에 이르고 있다. 10대와 20대의 99.9%, 30대의 99.4%가 인터넷을 이용하고 있고, 3~9세 어린이는 86.2%, 40대는 88.4%의 인터넷이용률을 보이고 있다.[7]

IT기술의 진전과 정보통신기술의 발달로 정보화 사회가 구현되었으나 개방형 정보통신망과의 상호접속으로 인한 정보유출, 파괴, 위·변조, 바이러스 유포 등의 컴퓨터 범죄가 발생하고 있다. 이러한 피해는 국가에서부터 기업, 개인까지, 누구든지 피해자가 될 수 있으며 피해액수도 천문학적으로 증가하고 있다. 2009년 7월 4일 미국 주요사이트들을 대상으로 공격이 시작되어 지난 2009년 7월 7일부터 7월 10일까지 국내·외 주요 웹사이트를 대상으로 동시다발적으로 분산서비스거부(DDoS) 공격이 발생했다. 현대경제연구원에 따르면 이로 인한 피해 추정 액은 최소 369억 원에서 최대 544억으로 밝혀졌고, 이는 2008년 풍수해 피해액 580억 원과 비슷한 수준으로 그 피해가 엄청났다는 사실은 유명한 일화이다. 또한 빅데이터 시대의 도래와 최근 대규모 개인정보 유출 사고가 심심치 않게 발생하면서 정보보호에 대한 중요성과 관심이 높아지고 있다.

정보보호란 인터넷을 포함한 정보통신망, 단말 등에서 처리되는 정보에 대해서 각종 보안 위험요소로부터 보호하여 정보의 기밀성과 무결성을 유지하고 서비스의 가용성을 보장하고 활성화시키기 위한 기술적 활동이다. [표 3]은 국가정보보호 백서를 참고해 크게 6개 영역별로(네트워크 보안, 시스템 보안, 컨텐츠/정보유출 방지보안, 암호/인증, 보안관리, 정보보호 서비스) 정보보호기술에 관해 간단히 나눈 것이다.[7]

[표 3] 분야별 핵심 정보보호 기술

기술분야	핵심기술	기술내용
정보보호 기반기술	암호설계 기술	- 차세대 핵심 암호 알고리즘 설계 기술
	인증기술	- 출입 접근제어 - 인증기관 개발 - 생체특성 활용기술
	키관리 기술	- 공개키 기반 기술 - 디렉토리 서버 개발 기술 - 안전한 API 개발 기술
네트워크 보호	방화벽 기술	- 다른 네트워크로의 불법침입 저지
	가상사설망	- IP망에서 안전한 커넥션을 구축
	차세대 인터넷보안	- IP security(IPsec) - IPv6
시스템 보호	보안 IC카드	- 안전성 강화를 위한 IC카드 구조 설정 및 설계 - 비대칭형 암호 방식 적용
	보안 OS	- 컴퓨터 운영체제에 대한 각종 해킹으로부터 시스템 보호
	보안 DBMS	- DB 질의어의 접근통제 - 부적당한 질의어에 대한 정보의 흐름방지
응용서비스 보호	전자상거래 정보보호	- 전자문서 공증 - 안전한 전자 입찰 - 전자화폐 보안 - 전자상거래공용 플랫폼 보안
정보보호 표준 및 평가	표준화	- 인터넷 보안 표준화 - 공개키 기반 구조 표준화 - 암호 메커니즘 표준화
	평가기준	- 정보보호시스템 평가방법
보안관리 기술	원격모니터링 기술	- 운용시스템에 대한 원격 보안 관리 - 보안 정보 수집 및 침해탐지
	보안정책 기술	- 보안정책 설정 - 보안정책 유포 및 강제 집행

2.1 사용자 인증 기술

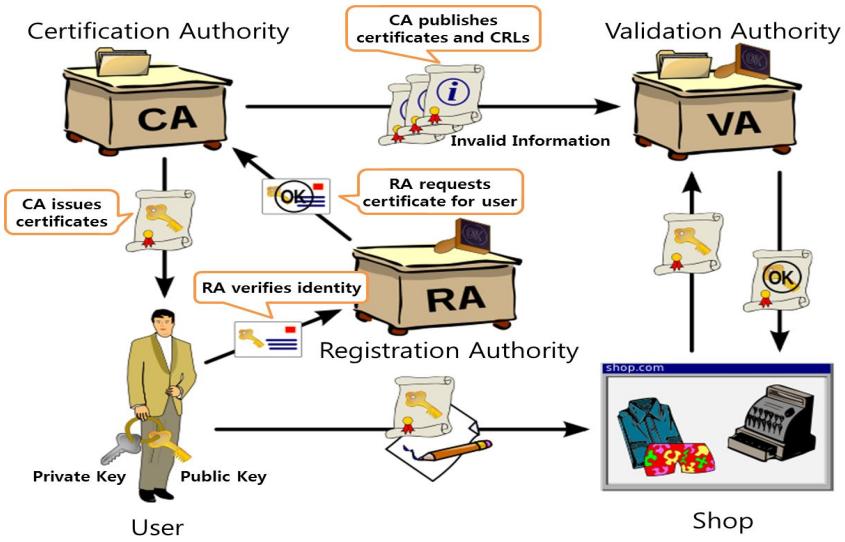
사용자 인증 방식은 여러 사람이 공유하고 있는 컴퓨터시스템이나 통신망의 경우, 이를 이용하려는 사람이나 응용프로그램의 신분(Identification)을 확인하여 불법적인 사용자가 들어올 수 없도록 시스템 보안을 유지하는 방법을 말한다. 즉, 중요한 정보는 아무나 통신망을 통해 접근할 수 없도록 인증하는 절차를 거쳐야한다. 또한 정보 자체에 대한 접근을 통제하는 것뿐만 아니라 권한을 가지지 않은 사람이 함부로 정보를 변경 또는 삭제하거나 잘못된 자료가 입력되지 않도록 감사하기 위해 사용자 인증이 사용된다. 신원확인 방법은 3가지 형태(아는 것에 의한 인증, 소유하고 있는 것에 의한 인증, 사용자의 특징에 의한 인증)를 가지며 2가지 이상의 혼합된 형태의 인증방법을 사용하는 것이 효과적이고 강력한 신분확인을 할 수 있다. 사용자 인증을 위해 사용되는 기술로 대표적인 것들은 다음과 같다.[8]

[표 4] 사용자 인증의 대표적인 기술

기술	설명
ID/Password	대표적 인증수단으로 암기만으로 사용할 수 있지만, 일정 수준 이상의 복잡성과 주기적 갱신만이 보안성을 담보할 수 있다.
PKI (Public Key Infrastructure)	공개키 암호기법을 이용한 인증 수단으로 사전에 공유된 비밀 정보가 없이도 인증서에 기반을 두어서 상대방을 인증할 수 있다.
Multi-Factor 인증	보안강도를 높이기 위해 몇 가지 인증 수단을 조합해서 사용하는 기법이다. ID/PASSWORD 이외에 지문, 홍채 등과 같은 생체인식, 인증서, OTP 등이 함께 사용된다.
SSO(Single Sign On)	한 곳에서 인증 후 인증확인 정보의 전달을 통해 다른 곳은 인증절차 없이 통과하는 인증기술이다.
i-PIN	현재 한국에서 인터넷 이용 시 본인확인을 위해 사용되는 기술로, 직접 본인확인을 수행한 기관에서 확인정보를 발급해주는 방식으로 동작한다.

2.1.1 공개키 기반 구조

공개키 기반구조(PKI: Public Key Infrastructure)는 공개키 암호화 방식을 사용해서 제 3의 신뢰 기관인 CA를 중심으로 사용자에 대해 인증을 제공하는 대표적인 서비스 기반 구조이다. 즉, 암호화와 복호화 키로 구성된 공개키 암호 방식을 이용해 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템을 말한다. 다음은 PKI 구조도이다.[24,26]



[그림 5] 공개키 기반구조

PKI를 구성하는 요소들은 공개키에 대한 인증서를 발급, 공개키 전달 및 데이터베이스 등을 관리하는 PKI를 구성하는 가장 핵심 객체인 '인증기관(CA: Certification Authority)', 사용자들의 인증서 신청 시 인증기관 대신 그들의 신분과 소속을 확인하는 '등록기관(RA: Registration Authority)', 인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 취소 목록 등을 저장·검색하는 장소인 '디렉토리', 또한 다양한 응용에서 공개키를 이용하여 전자서명을 생성하고 검증하며 데이터에 대한 암호, 복호를 수행하는 '사용자' 등이 포함된다. PKI는 광

범위한 기업 응용프로그램에 보안 솔루션을 제공한다. 솔루션은 웹 보안, 전자우편 보안, 원격접속, 전자문서, 전자상거래 애플리케이션 등 매우 다양한 분야에서 사용될 수 있다.

2.2 접근제어 기술

접근제어란 권한이 있는 사용자에게만 특정 데이터와 자원들이 제공되는 것을 보장하기 위한 방법 및 컴퓨터 내 자원에 대한 작업을 가능하게 하거나 제한할 수 있는 수단이다. 접근제어는 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호서비스에 큰 역할을 한다. 대표적인 접근제어 유형에는 강제적 접근제어, 임의적 접근제어, 역할기반 접근제어가 있다.[10,11,23]

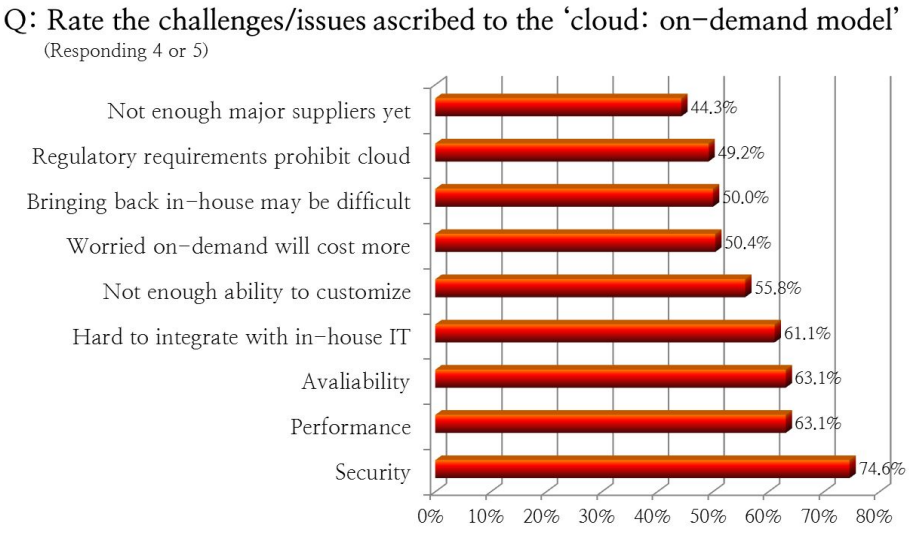
[표 5] 접근제어 기술

유형	설명
강제적 접근제어 (MAC: Mandatory Access Control)	- 필요에 따라 관리자가 권한을 설정하는 접근제어 방식 - 각 정보에 결합된 보안등급과 사용자에게 부여된 인가등급을 사전에 규정된 규칙과 비교하여 만족되는 사용자에게만 접근권한을 부여
임의적 접근제어 (DAC: Discretionary Access Control)	- 사용자에 식별과 권한인가에 기초한 접근제어 방식 - 관리자가 권한을 설정하는 것이 아니라 파일이나 디렉토리의 소유자가 권한을 지님 - 접근권한의 통제가 정보객체의 소유자의 의해 다른 사용자에게 허가되거나 철회 될 수 있으며, 정보객체의 소유자의 재량에 따라 접근통제
역할기반 접근제어 (RBAC: Role Based Access Control)	- 사용자에게 직접권한을 부여하는 대신, 사용자에게 부여된 개인의 직책을 기반으로 역할을 설정하고, 역할에 허용된 권한만 허용하여 최소 자원만을 접근할 수 있도록 하는 접근제어 방식

제 3장 클라우드 환경 내 정보보호 관련 문제점

각종 데이터·소프트웨어를 서버 컴퓨터에 저장해두고 필요할 때 마다 인터넷으로 내려 받아 쓸 수 있는 클라우드 컴퓨팅은 기하급수적으로 늘어나는 데이터의 저장 공간 및 비용절감의 대안으로 주목 받고 있다. 또한 최근 스마트폰·스마트 패드 등 모바일 기기를 활용한 스마트워크가 주목 받으며 스마트워크를 구현할 수 있는 클라우드 컴퓨팅에 대한 관심과 전망은 매우 긍정적이다.

그러나 클라우드 컴퓨팅의 유용성에 비해 실제 이를 도입해 사용하는 기업, 즉 클라우드로의 전환 이행률은 높지 않다. 개인 정보 또는 기업 내부 정보 유출에 대한 불안감 때문이다.[21,22,29]



[그림 6] 클라우드 도입에 가장 우려되는 부분

클라우드 컴퓨팅은 고도로 가상화되고 모든 자원을 공유하는 다중 공유 시스템으로 데이터가 서비스업체의 데이터센터에 분산, 저장되기 때문에 이에 대한

기업에 불안감은 매우 크며 실제로 클라우드가 해킹을 당한다면 데이터가 모두 손실될 위험이 높은 것도 사실이다. 이러한 사실을 수치적으로 보여주는 시만텍의 '2011 기업 클라우드 조사 보고서'에 따르면 클라우드 서비스에 높은 관심을 보인 기업은 78%에 달하지만 현재 구축단계에 있는 기업은 4곳 중 1과에 불과하며 경험의 부재를 클라우드 준비 미흡의 배경으로 들었다. 또한 시장조사기관 IDC가 기업을 대상으로'클라우드 컴퓨팅을 도입하는데 있어 가장 우려되는 부분이 무엇인지 조사한 결과 74.6%가 보안이라고 응답했다.

글로벌 보안업체 시만텍은 자사 보안 전문가와 과거 데이터 분석 결과 등을 바탕으로 '2013년 주목해야할 보안 트렌드 톱5'를 선정하여 공개했다. 이에 따르면 내년도 보안업계가 주목해야 할 이슈는 사이버 분쟁의 일상화, 신종 악성코드 랜섬워어[4] 확산, 매드웨어[5]를 통한 개인정보 수집활동 증가, 소셜네트워크의 수익성 추구로 인해 새로운 위험도래, 사이버 범죄의 모바일과 클라우드로의 이전 등을 선정했다. 특히 모바일 기기와 클라우드 서비스 활용이 급증하면서 사이버범죄 대상이 모바일과 클라우드로 확산될 가능성이 크다고 시사했다.[12]

또한 '2012 차세대 컴퓨팅 R&D 콘퍼런스'에서 지식경제부, 방송통신위원회, 행정안전부 등 3개 부처와 국정원 등은 클라우드 활용 등에 논의하며, 클라우드 기술 경쟁력 향상방안을 주제로 내년 클라우드 R&D분야에서 클라우드 활성화의 장애요인인 보안 문제를 해결하기 위한 클라우드 보안성 강화 기술 개발에 주력할 것이라고 말했다. 이처럼 대부분의 조사와 연구에서 클라우드 전환 시, 가장 우려되는 사안으로 보안문제를 이유로 들었다.

---

4) 신종 악성코드로 피해자의 디지털 데이터 및 시스템을 인질로 몸값을 요구하는 방식. 이러한 사이버 범죄 유형은 과거에도 있었으나 현실 세계의 납치처럼 몸값을 주고받기가 어렵다는 제약이 뒤따랐으나, 앞으로는 오라인 결제방식을 활용해 이 같은 범죄를 저지를 가능성이 있다고 지적

5) 애드웨어(광고성 멀웨어)에 일종. 사용자의 위치정보, 연락처, 기기 식별정보 등을 빼내는 매드웨어를 이용. 이를 통해 특정 계층을 대상으로 한 표적 광고가 가능해, 모바일 광고를 통해 매출 증대를 모색하는 기업이 손쉬운 방법으로 매드웨어를 선택 가능

1. 클라우드 컴퓨팅의 주요 이슈 및 정보보호

클라우드 컴퓨팅은 서비스 모델이나 방식의 다양성으로 인해 전통적인 컴퓨팅 서비스에 비해 훨씬 복잡하고 고려해야할 요소들이 많다.

박춘식[13]은 클라우드 컴퓨팅 도입의 주요 고려사항으로 시스템 안정화, 데이터 서버 위치, 보안, Inter-Cloud 상호운용성, 컴플라이언스 등을 주요 이슈가 될 것으로 판단하였으며, 이슈들 가운데에서 클라우드 컴퓨팅 환경이 갖게 되는 보안 위협 요소로 클라우드 컴퓨팅에 대한 외부 공격, 가상화 기술에 취약성에 의한 공격, 클라우드 환경을 이용한 공격, 클라우드 내부 공격에 의한 위협, 네트워크에 대한 위협, 컴플라이언스 등에 위협을 들어 그에 대한 보안 대책으로 서비스 이용자, 제공자 보안 대책과 서비스 기술적 보안, 관리적 보안 대책을 제시하였다.

최재규와 노봉남[14]은 클라우드 컴퓨팅에서의 잠재적인 위협을 방지하기 위해 가트너의 2008년 'Assessing the Security Risks of Cloud Computing'을 참고하여, 기밀성과 데이터 암호화, 사용자 인증과 접근 제어, 데이터의 무결성, 가용성 및 복구, 원격 확인 및 가상 머신 보호, 네트워크 보안 및 웹 보안, 공격 모델 및 시뮬레이션, 보안 정책 관리 및 비용 분석을 보안 요소 기술로 제시하였다.

김학범, 전은정, 김성준[19]은 인문학적 측면에서 클라우드 환경의 보안관리를 위해 도메인은 거버넌스 도메인과 운영 도메인을 12개 도메인으로 구분하였다. 거버넌스 도메인에는 거버넌스와 전사 위험관리. 법적/전자적 발견사항, 준거성과 감사, 정보의 생명주기 관리, 이식성과 상호운용성에 대한 보안 요구사항을 제시하고, 운영 도메인은 전통적 보안, 사업 연속성과 재해복구, 데이터센터 운영, 사고대응, 공지와 전파, 응용시스템 보안, 암호화와 키 관리, 식별과

접근관리, 가상화의 중요성을 명시하였다.

김태형, 김인혁, 민창우, 엄영익[6]은 클라우드 컴퓨팅에서는 기존 컴퓨팅 환경과 달리 가상화 엔진인 하이퍼바이저에 의한 보안 위협, 관리자에 의한 보안 위협, 네트워크 전송과정에서의 보안 위협이 추가된다고 주요 이슈를 제시하였다. 또한 이를 해결하기 위해 데이터의 무결성, 기밀성, 사용성에 중점을 주어, 클라우드 환경의 시스템 보안기술로 무결성 확인, 신뢰 보장 하드웨어 지원 기술, 가상화 기반 보안성 향상 기술의 연구 동향에 대해 조사하였다.

은성경의 논문[15]에서는 클라우드 컴퓨팅 서비스의 보안 이슈를 개인과 기업 사용자의 두 가지 관점으로 나누어 제시하였다. 개인 사용자 관점에서는 개인정보 노출, 개인에 대한 감시, 개인 데이터에 대한 상업적 목적의 가공을 그 내용으로 열거하였다. 기업 사용자 관점에서는 서비스 중단, 기업 정보 훼손, 기업 정보 유출, 법/규제 준수, e-discovery(전자적 증거 수집)대응의 다섯 가지를 제시하였다. 이를 바탕으로 클라우드 컴퓨팅 환경보호, 기존 보안 기술의 클라우드 적용, Security as a Service, 새로운 보안 이슈를 앞으로 클라우드 컴퓨팅 보안 기술 연구방향으로 제시하였다.

클라우드 컴퓨팅 환경과 정보보호 관련 논문들을 조사하면, 각 연구에서 공통된 주요 이슈들을 제시할 수 있다. 이와 관련해서는 다음 절에서 상세히 다룬다.

2. 클라우드 컴퓨팅 환경 내 정보보호 문제점 도출

대부분의 기존 연구는 클라우드 컴퓨팅의 최대 걸림돌로 정보보안 문제를 꼽으며, 이를 해결하기 위한 방법으로 클라우드 컴퓨팅 서비스를 제공하는 사업자에 대한 신뢰가 우선 조성돼야 한다고 지적한다.[28] 이에 따라 본 논문에서

는 클라우드 컴퓨팅 환경이 갖게 되는 보안 위협을 크게 기술적, 관리적, 정책적, 서비스적 측면으로 나누어 제안하고자 한다. 아래에 위협 중 보안 기술 취약, 관리 시스템의 취약점, 애플리케이션의 위협 등 서비스적 측면을 중점적으로 본 논문에서 해결책을 제안한다.

[표 6] 클라우드 컴퓨팅 환경에서의 정보보호 위협

측면	위협	설명
기술적	가상화 기술 취약성에 의한 공격	가상화 기술의 특성을 악용
	네트워크에 대한 위협	클라우드 서비스 이용자-제공자간, 제공자-제공자간의 네트워크에 대한 보안 위협
	보안 기술 취약	기존 컴퓨팅 환경에 보안 기술을 클라우드 환경에 적용하면서 생겨난 기술적 보안 위협
관리적	관리 시스템의 취약점	클라우드 관리자의 보안성 부재와 관리 부족
	보안 의식 부족	관리자의 보안 의식 부족 및 보안 교육 프로그램의 미비
	표준화 부재	서비스 품질에 대한 만족을 제공할 수 있는 표준 SLA부족으로 시스템 안정성 우려
정책적	컴플라이언스 등 위협	어떤 보안 규정이나 보안 관리 체계를 통하여 보안을 준수 하고 있는 지를 외부에서 파악하기가 어려움
	국가적 법률 적용문제	데이터 서버의 위치에 따른 자국 외에 경우에 발생 할 수 있는 국내 정보의 국외 유출 문제, 외국 정보의 정보 제공 여부, 재판 관할권 등의 문제
서비스적	애플리케이션의 위협	결함이 있는 클라우드 서비스 제공자에게 종속되는 애플리케이션의 위협
	클라우드 환경을 이용한 공격	클라우드 컴퓨팅 환경을 공격의 도구로써 악용
	서비스 오남용	클라우드 자원을 악의적인 목적으로 오남용

제 4장 SDTU(Secure Data Transmission and Usage) 아키텍처

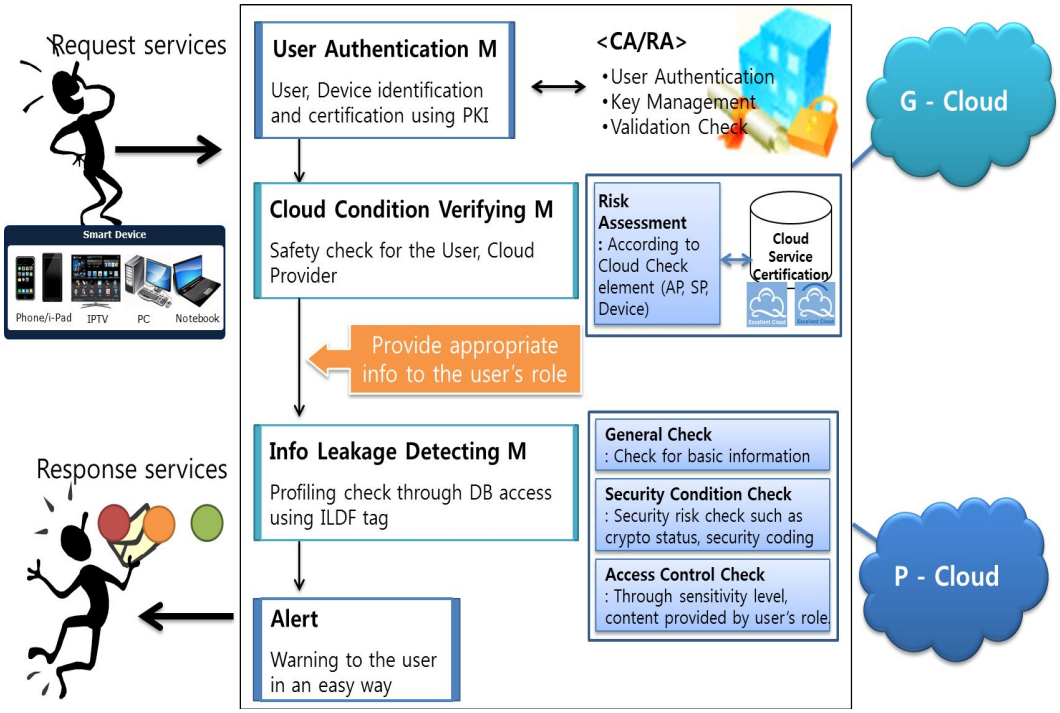
클라우드 컴퓨팅 환경에서의 데이터 신뢰 문제는 클라우드 컴퓨팅 활성화를 위해 가장 먼저 해결되어야 할 과제이다. 현재까지 클라우드 컴퓨팅 환경 내에 발생할 수 있는 문제점에 대해 많은 연구를 해왔다. 이를 분석하여 클라우드 컴퓨팅 내에 신뢰할 수 있는 환경을 조성하여 사용자의 중요한 정보를 안전하게 관리하고 사용하기 위한 아키텍처를 제안한다. 제안된 아키텍처는 클라우드 컴퓨팅 서비스 현황과 정보보호의 동향을 기반으로 단계별 보안성 점검 및 관리 방안으로 크게 3가지 기능(1. 통합사용자 인증 기능, 2. 사용자와 클라우드 간 신뢰성 점검 기능, 3. 안전한 데이터 전송 및 접근제어 기능)을 제공한다.

이에 따라 제안된 아키텍처에서는 사용자의 정보와 클라우드 서비스 제공자 및 콘텐츠에 정보를 수집하여, 세션단계에 프로파일링 점검 및 검증을 통해 접근제어 및 통제를 실시한다. 아키텍처의 구성요소에 대해서는 다음 절에 상세히 다룬다.

1. SDTU(Secure Data Transmission and Usage) 아키텍처 구조

SDTU 아키텍처 구성도는 [그림 10]에 나타내며, 크게 3가지 기능으로 구성된다. 1) 사용자 인증 방법 중 가장 강력한 PKI구조 기반에 공인인증서를 이용한 사용자 식별 및 인증을 통해 네트워크상에 참여하는 기기를 식별하여 통합적인 사용자 인증을 지원하는 UAM(User Authentication Mechanism), 2) 사용자의 기기 식별 정보, AP 정보, 클라우드 인증여부에 대한 정보 등에 수집을

통한 클라이언트 환경에 대한 안전성과 클라우드 서비스 제공자(SP)의 신뢰성 점검을 하는 CCVM(Cloud Condition Verifying Mechanism), 3) 사용자에게 안전한 데이터를 전송하기 위해 데이터의 프로파일링 점검을 통한 데이터 보안성 취약 점검, 주체별 등급분류에 따른 이용 범위를 기반으로 한 접근제어 기능을 제공하는 ILDM(Information Leakage Detecting Mechanism)으로 클라우드 환경 내 안전한 데이터 전송 및 정보보호 아키텍처를 제시한다.

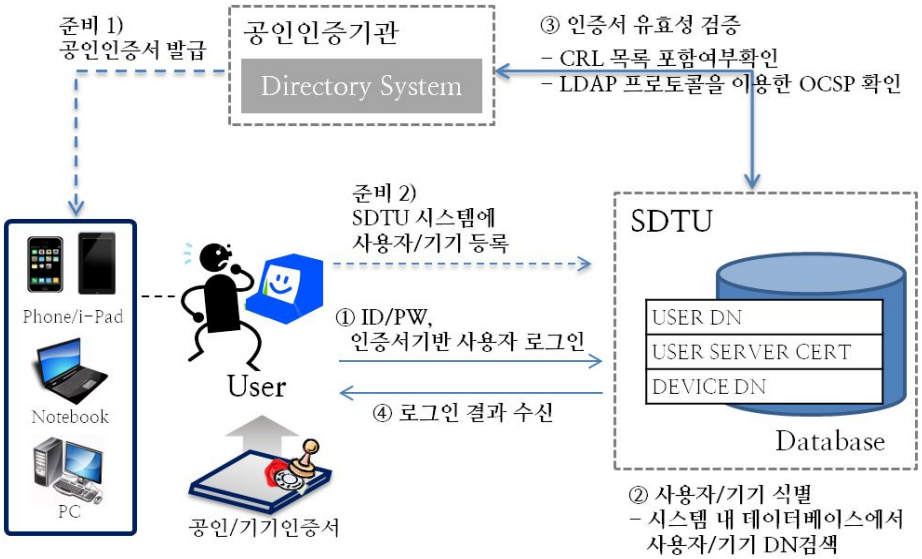


[그림 7] SDTU 구성도

2. SDTU 구성요소

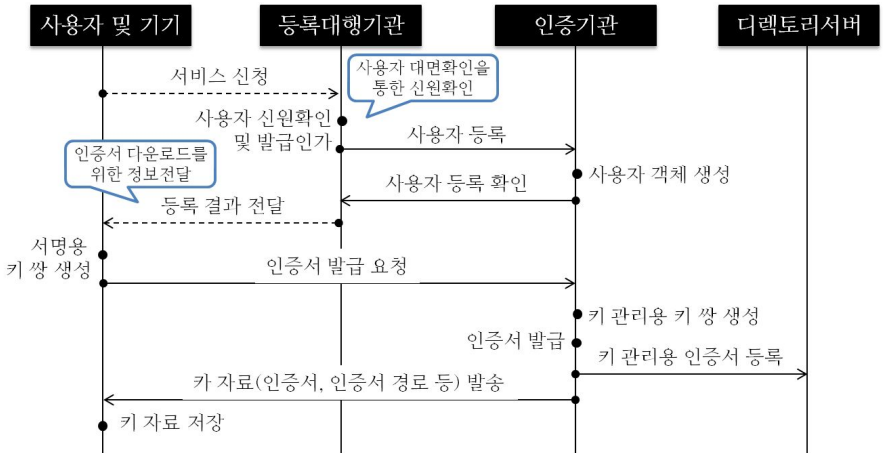
2.1 User Authentication Mechanism

사용자 인증관리는 사용자를 식별하고 해당 사용자가 서비스에 등록되어 있는 정당한 사용자인지의 여부를, 신뢰된 인증체계를 구축하여 확인하는 방안을 제시하며 서비스 간 통신에 암·복호화 및 전자서명 등의 위·변조방지를 제공한다. 또한 클라우드 컴퓨팅 환경에서 활용되는 기기가 다양해지면서 네트워크상에서 이용자와 각 기기의 진위여부의 확인이 요구되고 있다. 사용자가 사용하는 이기종 디바이스 인증은 사용자 인증을 토대로 2차적으로 검증이 이루어지므로 통합적 사용자 인증이 이루어질 수 있다. Multi-factor인증으로 강력한 인증을 제공하며 서비스에 가입된 정당한 사용자인지의 여부를 인증서를 통해, 논리적·물리적 화경을 넘나들며 컴퓨팅 리소스를 제공하는 클라우드 컴퓨팅의 구조적 문제에 대해 신뢰성을 확보한다.



[그림 8] 인증 프로세스

인증서비스는 네트워크에 참여하는 다양한 사용자간 식별 및 인증, 데이터 암·복호화를 지원하기 위해 PKI서비스로써, 현재 국가 공개키 기반 구조(NPKI)는 한국인터넷진흥원을 중심으로 최상위 인증기관, 인증기관, 등록기관, 사용자로 구성되며, 한국정보통신기술협회에서 제공하는 인증서 표준을 기반으로 공인 인증서 라이프사이클을 통해 처리된다. 아래 [그림 12]는 공인 인증서 발급 절차이다.



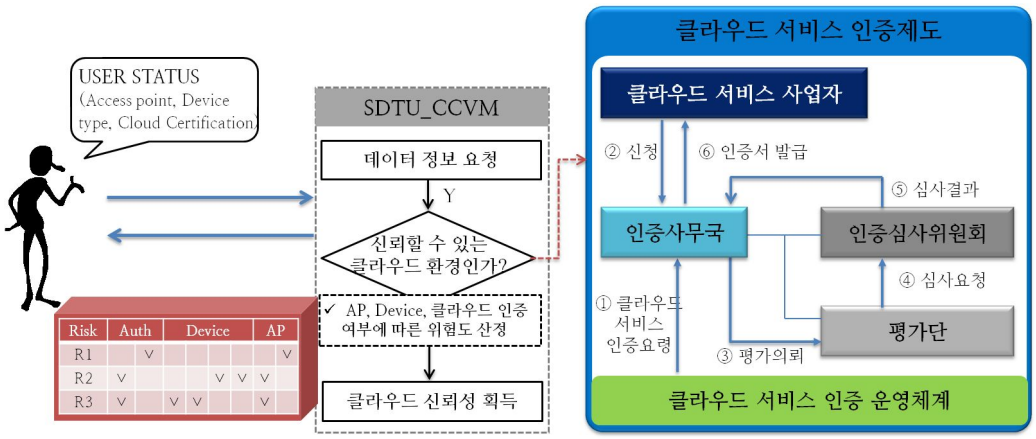
[그림 9] 공인인증서 발급 절차

2.2 Cloud Condition Verifying Mechanism

클라우드 컴퓨팅은 네트워크를 통해 프로그램이나 데이터를 가상 데이터 센터에서 분산 처리한다. 이러한 컴퓨팅 구조는 사용자가 요청하는 정보가 어디서 왔으며, 누구에 정보인지 확인하는 것을 어렵게 하여 문제가 발생했을 때 문제의 근원지를 찾기 어렵게 하여 해결하는 것을 복잡하게 하는 결과를 초래한다.

이에 따라 CCVM에서 사용자와 클라우드 서비스 간에 신뢰도 검증을 위하여, 사용자가 클라우드 서비스를 사용하는 환경(Access Point, Device, Service

Provider)에 따라 위험도를 산정하여 사용자에게 알린다. [그림 13]은 CCVM를 통한 신뢰도 검증 프로세스이다.



[그림 10] CCVM 프로세스

CCVM에서 클라우드 서비스 인증은 국내 서비스에 한정되며, 지난 5월 방송통시위원회와 관계 부처 합동으로 발표한 '클라우드 컴퓨팅 확산 및 경쟁력 강화 전략'의 일환으로 마련된 인증 제도를 기반으로 클라우드 서비스 인증이 이루어진다. 한국클라우드서비스협회가 운영하는 인증제도에 인증을 위한 점검 항목은 크게 서비스 품질, 정보보호, 서비스 기반의 평가가 이루어지며, 세부적으로 서비스 가용성, 확장성, 성능, 데이터 백업 및 관리, 보안, 서비스 지속성, 고객 지원 및 서비스 관리·지원 등에 항목이 있다.[16] 이를 기반으로 Black List/White List를 구성하여 신뢰할 수 있는 서비스 제공자가 관리하는 클라우드 환경인지 점검한다.

이를 통해 클라우드 인증(Excellent Coud) 여부에 따른 결과, 사용자 기기에 따른 신뢰도, 사용자 AP(Access Point) 안전성과 같은 사용자 상태를 확인하여 위험도를 산정한다. 위험도 산정은 사용자 환경에 대한 요소를 추가 확장하여 위험도를 세세하게 나눠질 수 있다. 본 논문에서는 클라우드 환경에 따라 민감

한 대표적인 요소만 추출하여 위험도를 산정하여, 각 요소에 따른 위험도 산정은 [표 6]와 같이 3가지 등급으로 나누어 정의하였다.

[표 7] 요소에 따른 위험도 산정의 예시

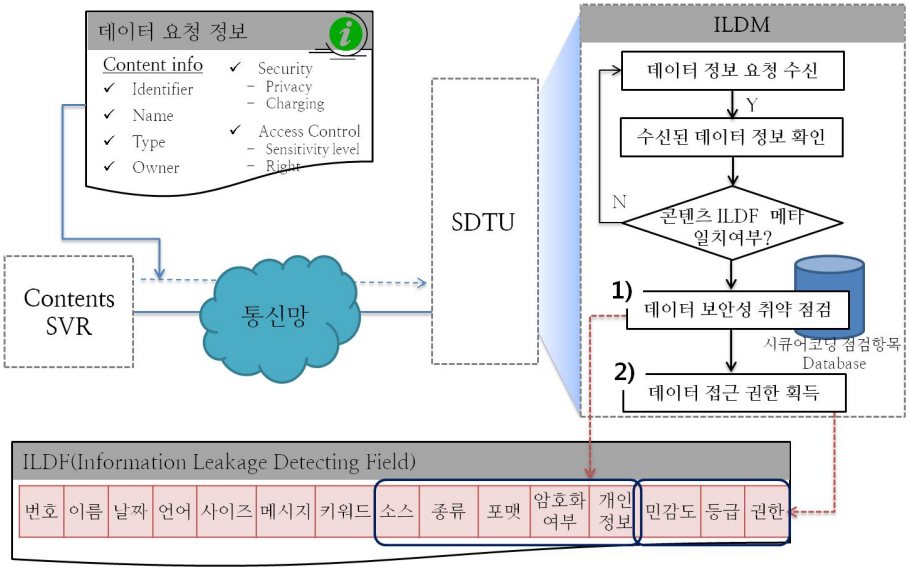
위험 등급	클라우드 인증여부		기기 신뢰도			AP 안전성		
	인증	비인증	PC	Smart Phone	Smart TV	물리적	논리적	
							Close Auth	Open Auth
R1 (DANGER)		V			V			V
R2 (WARNING)				V			V	
R3 (SAFETY)	V		V			V		

위와 같은 클라우드 환경에 대한 신뢰성 검증을 통해 사용자들이 안전하게 데이터 전송 및 관리가 가능하다. 대규모 데이터를 처리하며, 다중 사용자 접속 환경기반의 클라우드 컴퓨팅 신뢰성과 사용자 환경에 따른 위험도를 산정하여 검증함으로써 안전한 플랫폼에서 데이터 전송 및 관리가 가능하다.

2.3 Information Leakage Detecting Mechanism

사용자가 안전하게 서비스를 이용할 수 있도록 세션 단계에 프로파일링 점검 및 검증을 통해 접근제어 및 통제가 가능한 정보보호 메커니즘이다. 사용자 인증과 클라우드 환경에 대한 유효성 검증이 끝난 뒤, 사용자에 요청에 대한 정보를 수집하여 데이터를 표현하기 위한 목적으로 메타데이터를 생성하여 데이터 내부 분석과 접근제어에 빠른 데이터 제공으로 효율적으로 이용이 가능하다. 데이터의 안전성을 보장하기위해 크게 2가지 점검 사항(① 민감 정

보 포함 여부와 데이터 시큐어코딩 점검 항목을 통한 데이터 내부 보안 취약 점검, ② 주체별 등급분류에 따른 이용 범위를 기반으로 한 접근제어 기능을 제공하는 기능)을 분석하여 사용자에게 Alert을 준다.



[그림 11] IDLM 프로세스

사용자에게 안전한 데이터를 전송하기 위해 데이터의 기본정보 점검한다. 그리고 신뢰할 수 있는 데이터에 대한 검색 및 검사를 제공하기 위해 ILDF필드를 활용한다. 더블린코어형식[6]을 참고하여 데이터를 표현하기 위한 목적으로 메타데이터를 생성하여, 정보검색, 내용등급, 저작권관리 등을 제공하여 데이터 내부 분석과 접근제어에 빠른 데이터 제공으로 효율적으로 이용한다. 기본적으로 데이터 type과 format 일치 여부 점검을 통해 데이터 안전성 여부를 점검한다. 콘텐츠 타입 및 확장자 분류는 텍스트, 이미지, 비디오로 분류된다.

6) ISO 15835으로 표준화된 메타데이터 형식. 동영상, 소리, 이미지, 텍스트, 웹 페이지 등의 디지털 매체들을 기술하는데 사용. 보통 XML과 RDF를 사용하여 구현. http://www.dublincore.go.kr/

2.3.1 Security Condition Check

클라우드 컴퓨팅 상에서 사용자가 안전하게 정보를 이용할 수 있도록 정보의 악의적 코딩을 점검 및 데이터 패턴에 따른 민감 정보를 분석하여 제어한다.

[표 8] 시큐어코딩 점검 함수

```
function secureCoding(aciton) {
  //데이터베이스내 시큐어코딩 항목과 비교
  while i=1≤checkMaliciousCoding.length do
    if checkMaliciousCoding[i].idx = action then
      SetErrorMsg("악의적 코드가 데이터 내에 존재합니다.");
      solveidx = SolveCoding-Table(checkMaliciousCoding[i].relatedSolve)
      if solveidx ≠ null then
        //데이터내에 악의적코드를 해결
        Execute-Solving(content.id ,action, solveidx)
      end if
    end if
      i++
  end while }
```

일반 클라우드 서비스는 컴퓨팅 자원을 공유할 수 있지만 데이터의 기술적인 부분까지 점검 할 수 없다는 기술적 취약점을 보안하고자 본 논문에서 데이터의 악의적 코딩 포함 여부 [표 7]과 같은 함수를 통해 확인한다. 행정안전부에서 사이버위협으로부터 예방·대응코자 2012년 9월에 발표하여, 12월부터 시행되는 'SW 개발보안 Android-JAVA 시큐어 코딩 가이드', 'C 시큐어 코딩 가이드', 'JAVA 시큐어 코딩 가이드' 등을 참고하여 점검 항목을 7가지(입력데이터 검증 및 표현, 보안기능, 시간 및 상태, 에러처리, 코드오류, 캡슐화, API 오용)로 나누어 악의적 코딩을 검출한다.

또한 서비스 요청 중 사용자의 입력이 있을 경우, 입력 값을 분석하여 민감

정보 포함여부를 확인한다. 키워드, 숫자 조합을 기반으로 입력 값의 타입을 분석한다. 예를 들어 16자리의 숫자로 구성된 입력 값은 카드번호, 13자리의 입력 값은 주민번호 등으로 예상될 수 있다. 주민번호는 개인정보가 유출될 경우 가장 큰 피해를 입을 수 있는 항목으로 [그림 15]과 같은 구조를 취한다. 신용카드번호의 분석은 [그림 16]을 참고하여 [그림 17]의 알고리즘을 통해 패턴분석을 한다.[17]

Y	Y	M	M	D	D	-	A	B	C	D	E	F	G
탄생년		탄생월		탄생일			성별	지역번호				순서	코드

[그림 12] 주민등록번호 구조

1	2	3	4	-	5	6	7	8	-	9	10	11	12	-	13	14	15	16
Bin 번호 (Bank Identifier Number)							발행기관의 일련번호											검증

[그림 13] 카드번호 구조

이후 사용자에게 정보 제공 사실과 노출 시 피해 정보를 알리고 사용자의 동의를 구한 후 정보 이용여부를 설정할 수 있도록 한다. 이는 사용자가 데이터를 요청할 때도 동일하게 적용된다. 이는 클라우드 컴퓨팅 환경을 이용한 공격을 방지하기 위함이다.

2.3.2 Access Control Check

접근제어 기능은 시스템 보안을 강화하는 것으로 콘텐츠 및 미디어 자원에 대하여 허가되지 않은 접근을 방어하는 것이다. 접근통제는 이용할 수 있는 콘텐츠에 대해 기밀성, 무결성, 가용성 및 합법적인 이용에 기여하게 되며 서비스

이용에 대한 수단이 된다. 기존 접근제어 모델에 이용목적, 조건에 따라 접근이 제한될 수 있도록 모델을 확장하여 접근통제를 실행할 수 있다. 하지만 본 논문에서는 안전한 데이터 전송 및 관리를 위한 접근제어를 위해 사용자의 역할, 정보의 등급에 따라 접근이 제한되고 이용할 수 있는 권한이 달라지는데 초점을 맞춘다.

[표 9] 데이터 등급분류 예시

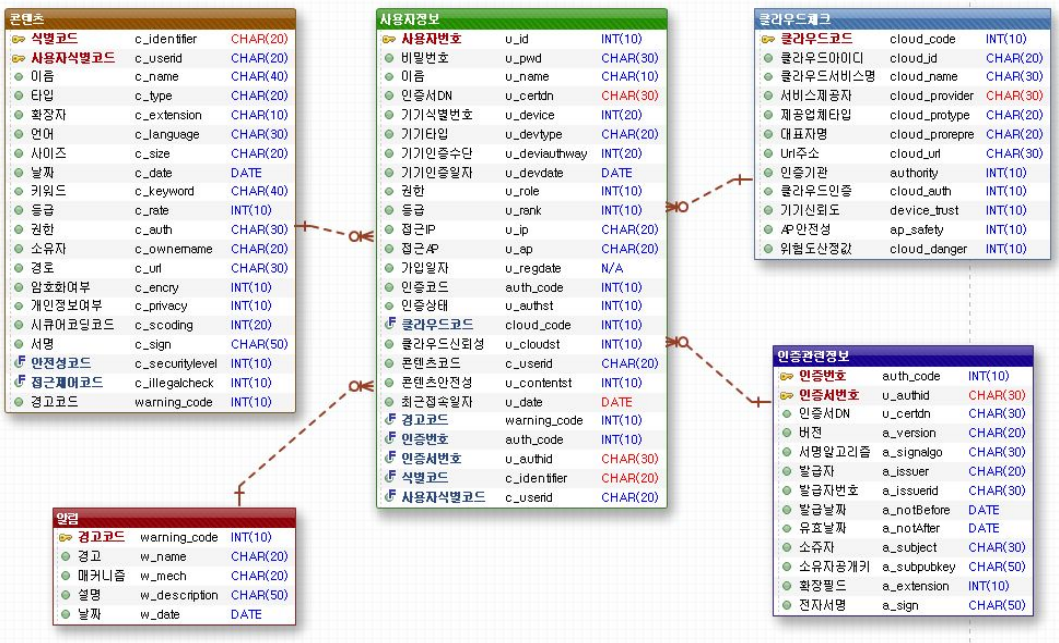
구분		등급	콘텐츠 이용가능 범위
어린이	전체	Level 1	모든 연령에 해당하는 자로써 건전한 가치관 형성을 저해하지 않는 내용
청소년	12세 이상	Level 2	부적절한 부분이 있으나 건전한 인격 형성과 교육적 근간을 저해하지 않는 내용
	15세 이상	Level 3	부적절한 부분이 일부 표현되어 있으나 사회, 가족, 학교 등에서 습득한 지식과 경험을 통해 충분히 소화 가능한 내용
성인	18세 이상	Level 4	청소년의 일반적인 지식과 경험으로는 수용하기 어려워 건전한 인격체로 성장하는 것을 저해할 수 있는 내용

이와 같이 분류된 등급에 사용자를 할당하고 정보이용에 대한 제한적인 권한을 부여한다. 추후 여러 사용자에 접근으로 확대되어 역할이 여러 분류로 확대되어 나뉜다면, 데이터 등급에 따라 접근을 제한하는 것이 아니라 사용자에 따라 접근 가능한 등급을 분류하기 위해 일련에 척도를 두고 콘텐츠의 이용 등급에 따라 접근을 통제하게 된다.

제 5장. 시스템 설계 및 구현

1. 데이터베이스 설계

클라우드 컴퓨팅 환경에서 다양한 위협으로부터 정보를 안전하고 효율적으로 관리하기 위해 본 논문은 SDTU 데이터 통제 방안을 제시하였다. [그림 19]은 SDTU의 데이터베이스 구조 및 관계를 나타낸다.



[그림 14] 데이터베이스 구조 및 관계

사용자 정보 인증, 클라우드 신뢰성 검증, 콘텐츠 안정성, 사용자에게 경고 및 알람을 주는 테이블로, 총 5개의 테이블로 구성된다.

2. 알고리즘

본 논문에서 제안한 안전한 데이터 전송을 위한 아키텍처는 자동적으로 클라우드 컴퓨팅 환경 내 정보를 관리하고 사용자와 콘텐츠 정보를 기반의 접근통제를 통해 사용자에게 안전하고 신뢰할 수 있는 서비스를 제공하는 것을 목표로 사용자에게 easy-way로 경고를 주는 것에 중점을 두고 있다. 이 메커니즘의 표현 및 수행을 위한 주요 기능은 다음 알고리즘으로 표현하였다.

Algorithm Secure Data Transmission and Usage

```
1:  // User Authentication
2:  if SelectCert(user.id, user.pw, cert) ≠ null then
3:      CheckID(user.id, user.pw);
4:      serverCert ← CertNPKICert(cert,"SIGN");
5:      certValid ← CertValidation(severCert, cert);
6:      certSign ← SignCheck(cert, user, serverCert);
7:      if (certValid && certSign) then
8:          user.id_tag ← AuthTag(user, TIMESTAMP);
9:          return user.id_tag
10:     else
11:         return false;
12:     end if
13: end if
14: // Cloud condition verifying
15: user.cloud ← UserFieldCheck(user.id_tag);
16: if user.cloud ≠ null then
17:     AccessCloudServer(http://ip:8080, ACCESS);
18:     cloud.metadata ← SearchMeta(cloud, cloud.field, SCAN);
19:     cloudAuth ← CheckCloudAuth(user.cloud, authCode, SEARCH);
20:     deviceReil ← CheckDeviceReil(user.deviceType);
21:     apInfo ← ReadAPInfo(user.ip, device.macAdd);
22:     apCheck ← CheckAPSafety(apInfo.locaion, apInfo.auth);
23:     RiskAssess(cloudAuth , deviceReil , apCheck) ;
```

```
24: else if user.cloud = null then
25:     SetErrorMsg("클라우드 식별정보 존재하지 않음");
26:     AlertLevel.result ← WARNING;
27:     return false;
28: end if
29: // Information Leakage Detecting
30: user.role ← UserFieldCheck(user.id_tag);
31: content.field ← SearchContent(user.role, content);
32: if content.field ≠ null then
33:     content.metadata ← SearchMeta(content, content.field, SCAN);
34:     return content.metadata
35: else if content.field = null then
36:     SetErrorMsg("콘텐츠 신뢰성 식별정보 존재하지 않음“);
37: return false;
38: // Access control and Security condition Check
39: content.level ← ContentLevelCheck(content.metadata);
40:     if CheckAccess(user.role, content.level) = ACCEPT then
41:         CheckContentTrust(GeneralCheck(content.metadata),
42:                                         SecurityConditionCheck(content.metadata));
43:         AlertLevel(trust_result.toAlertString);
44:     else if CheckAccess(user.role, content.level) = DENY then
45:         Audit(user.id, user.id_tag, user.role, TIMESTAMP);
46:         SetErrorMsg("콘텐츠 접근권한이 없음“);
47:         AlertLevel.result ← DANGER;
48:         return false;
49:     end if
50: end if
51: // Notice and Alert
52: function AlertLevel(result)
53:     if (result = DANGER || WARNING) then
54:         NoticeMsg(result, this.Mechanism);
55:         switch(user.choose)
56:             case OK: return true;
57:             case STOP: return false;
58:     else if (result = SAFETY && this.Mechanism = LAST) then
```

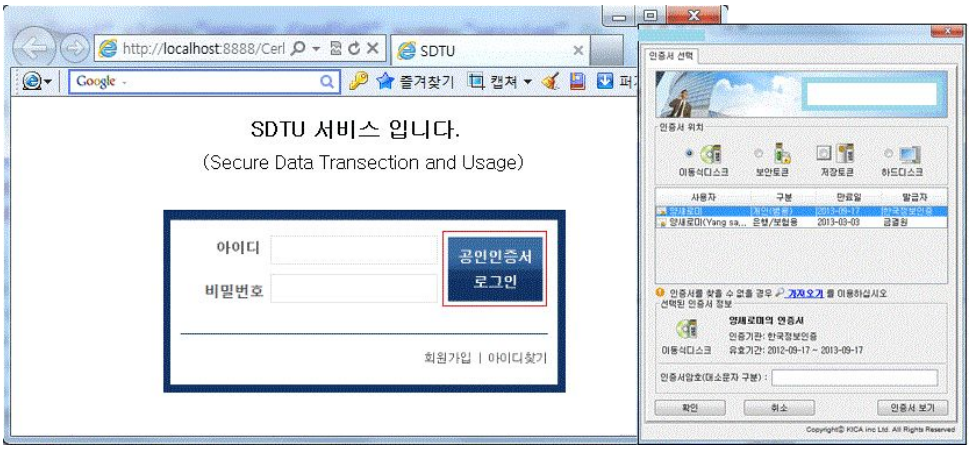
```
59:         return true;
60:     end if
61: end function
```

3. 프로토타이핑

SDTU 모델은 Windows 7 운영체제 하에 구현되며, WAS Server는 Apache Tomcat 6.0.35를 사용하였다. 언어는 JAVA와 HTML을 사용하였으며 데이터베이스는 ORACLE 11g XE를 사용하고, Eclipse JUNO와 Namo WebEditor를 이용하여 구현하였다.

3.1 사용자 화면

사용자 인증은 ID/PW방식과 공인인증서를 통해 사용자 식별 및 검증이 진행된다.



[그림 15] 사용자 인증 화면

사용자 인증 후에 SDTU 클라이언트는 클라우드 신뢰도 검증과 데이터 안전성 점검을 실행한 결과를 사용자에게 알려준다. 이후 사용자는 클라우드 환경으로 돌아가서 안전하게 데이터 이용을 할 수 있다.

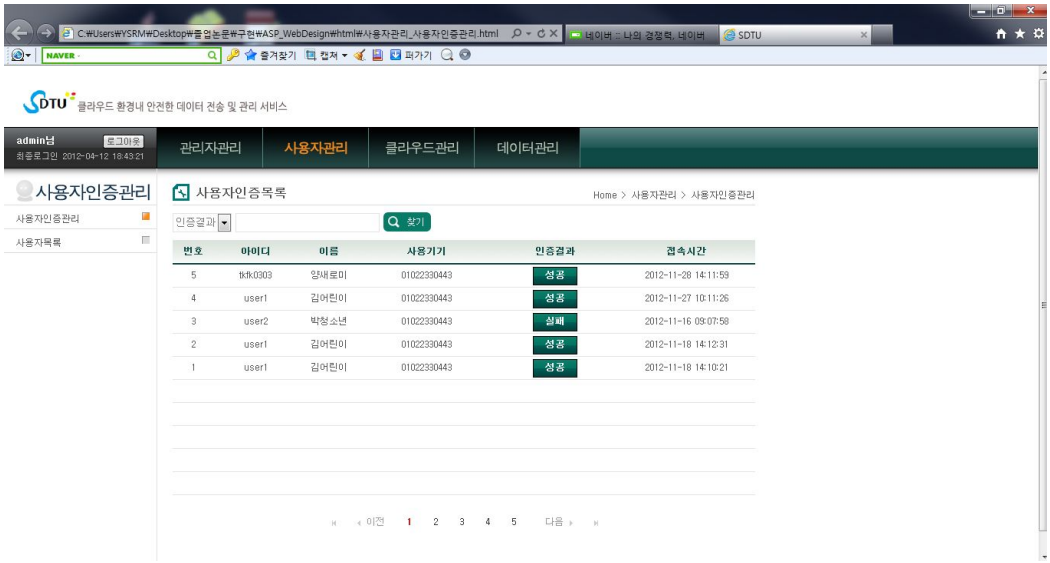
3.2 관리자 화면

관리자는 제안하는 모델을 통해 크게 관리자 정보수정, 사용자 관리, 클라우드 관리, 데이터관리와 같이 4가지 기능을 수행한다. 관리자 로그인은 사용자 화면과 같으므로 생략하고 관리자 정보수정도 본 논문에서는 중요한 기능이 아니므로 생략한다.

3.2.1 사용자 관리

사용자 관리는 사용자 인증목록 관리와 서비스를 이용하는 사용자 목록으로 분류가 나뉜다.

사용자 인증목록메뉴에서는 서비스를 이용하기 위해 사용자들이 인증했던 목록들을 접속시간 순으로 정렬하여 아이디, 이름, 사용기기, 인증결과 항목이 보인다.



[그림 16] 사용자 인증목록 화면

각 사용자에 대한 인증결과 버튼을 누르면 사용자의 상세한 인증정보가 팝업 페이지로 뜬다. 사용자 인증정보에는 사용자의 아이디, 비밀번호, 인증서 DN, 아이디/비밀번호 점검과 인증서 유효성 및 전자서명 검증을 통한 인증결과, 사용자 기기번호, 기기식별 및 인증을 통한 기기인증결과가 보인다.

[그림 17] 사용자 인증정보 상세화면

사용자 목록메뉴에서는 서비스를 이용하는 사용자들의 목록이 나열된다. 번호, 아이디, 이름, 비밀번호, 등급, 연락처, 이메일주소, 인증기기목록, 사용자 인증목록 항목이 보인다.

[그림 18] 사용자 목록 화면

각 사용자에 대한 인증기기목록 버튼과 사용자 인증목록을 누르면 상세정보가 팝업 페이지로 뜬다. 인증기기목록에서는 사용자 아이디, 기기번호, 타입, mac address, 인증방법, 인증일시가 보이며 사용자인증내역에서는 아이디, 기기번호, 타입, 인증일시, 인증여부 등이 보인다.

[그림 19] 인증기기 목록 상세화면

[그림 20] 사용자 인증내역 상세화면

3.2.2 클라우드 관리

클라우드 관리는 클라우드 검증관리와 클라우드 목록으로 분류가 나뉜다.

클라우드 검증관리메뉴에서는 사용자들이 이용하는 클라우드에 대한 검증 결과가 보인다. 사용자는 여러 클라우드 서비스를 사용할 수 있고 그 때마다 검증결과는 클라우드 인증여부와 사용자 환경에 따라 달라진다. 사용자 아이디, 클라우드 식별 아이디, 서비스명, 인증여부, 검증결과, 검증시간이 보인다.

[그림 21] 클라우드 검증관리 화면

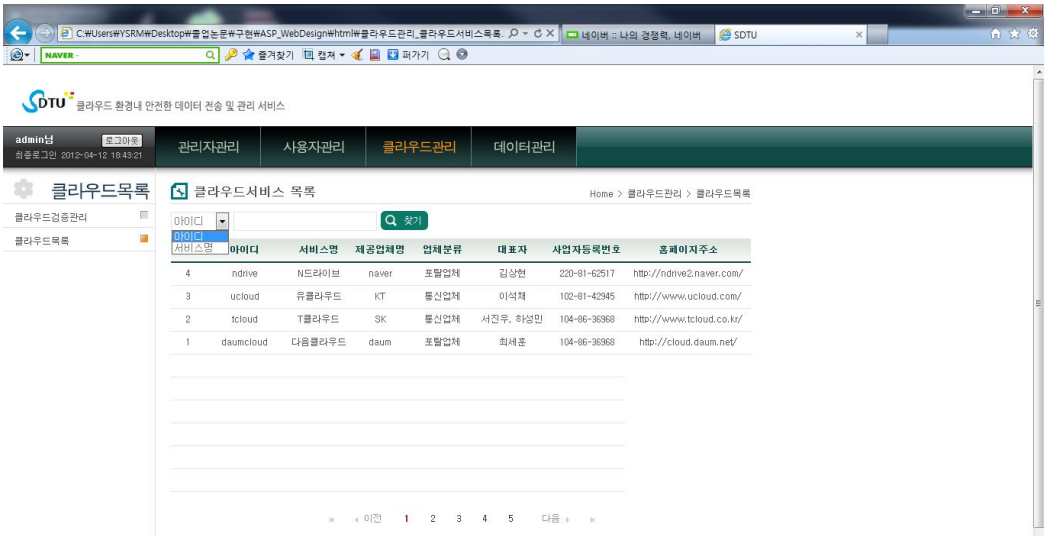
각 사용자에 대한 클라우드 검증결과 버튼을 누르면 상세정보가 팝업 페이지로 뜬다. 클라우드 검증결과에서는 사용자 아이디, 클라우드 서비스명, 클라우드 위험도, 사용자 기기, 기기 위험도, 사용자 AP, AP 위험도, 위험도 산정 기준 항목이 보인다.

위험도 산정 기준표를 통해 관리자도 상세 메커니즘을 알지 못하더라도 관리를 수월하게 한다. 위험도 산정은 등급을 R1(DANGER), R2(WARNING), R3(SAFETY)으로 나누어 사용자가 이용하는 클라우드 인증여부, 기기 타입에

따른 신뢰도, AP의 물리적·논리적 위치에 따른 안전성 항목을 두어 분류한다.

[그림 22] 클라우드 검증결과 상세화면

클라우드 서비스에 대한 정보로 클라우드 식별 아이디, 서비스명, 제공 업체명, 업체분류, 대표자, 홈페이지 주소 등이 보인다.



[그림 23] 클라우드 서비스 목록 화면

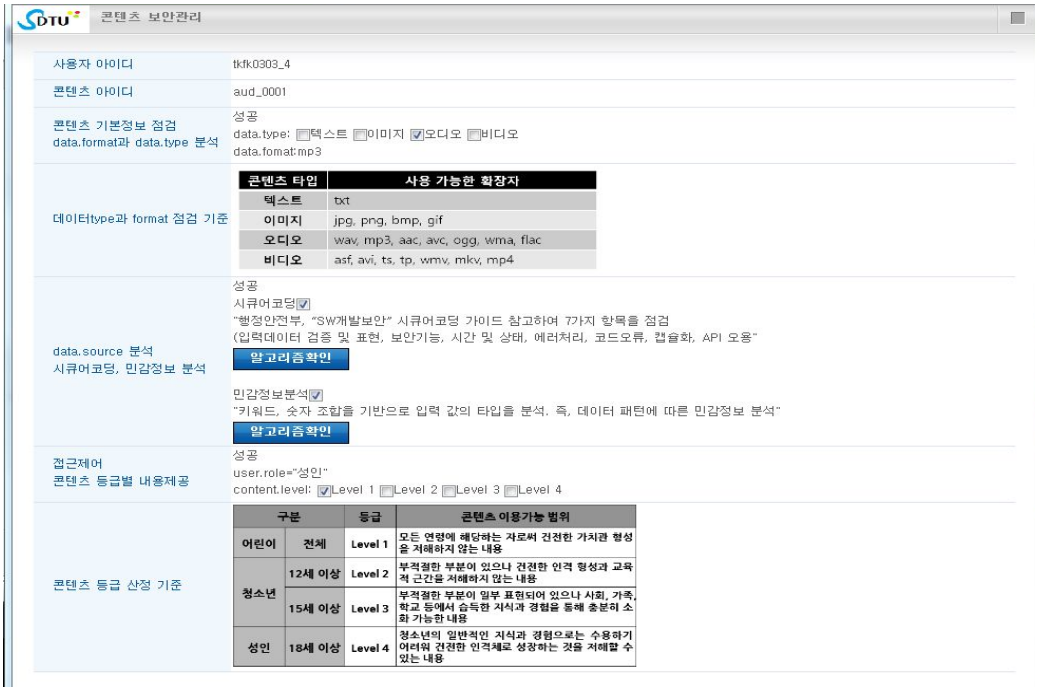
3.2.3 데이터 관리

데이터 관리는 콘텐츠 보안관리와 콘텐츠 목록으로 분류가 나뉜다.

콘텐츠 보안관리메뉴에서는 사용자들이 이용한 콘텐츠에 대한 안전성 점검 결과가 보인다. 사용자 아이디, 콘텐츠 식별아이디, 콘텐츠명, 타입, 보안성 결과, 검증시간이 보인다. 이는 추후에 사용자가 자주 이용하는 콘텐츠에 대해서 좀 더 빠르게 보안성 점검을 할 수 있도록 메타데이터 형식으로 저장된다.

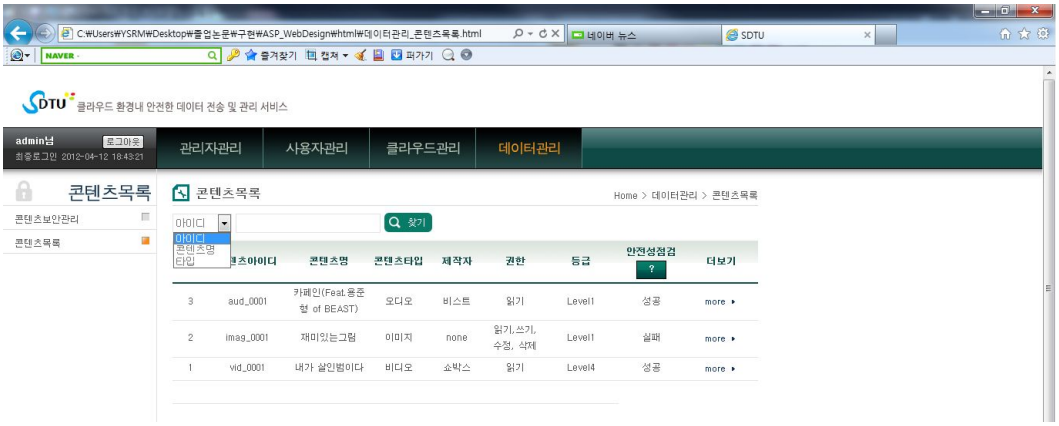
[그림 24] 콘텐츠 보안관리 화면

각 사용자가 이용한 콘텐츠 보안결과 버튼을 누르면 상세정보가 팝업 페이지로 뜬다. 콘텐츠 보안관리에서는 사용자 아이디, 콘텐츠 식별 아이디, 콘텐츠 기본정보 점검결과 및 기준, 콘텐츠 소스분석결과, 콘텐츠 등급별 사용자 등급에 따른 접근제어 결과 및 콘텐츠 등급 산정 기준 등에 항목이 보인다.



[그림 25] 콘텐츠 보안관리 상세화면

콘텐츠 목록메뉴에서는 콘텐츠 아이디, 콘텐츠명, 타입, 제작자, 등급, 권한, 안전성점검 등이 보인다. 안전성 점검은 콘텐츠 기본정보 점검과 소스 분석에 따른 데이터 안정성 점검결과로 사용자와 연계된 접근제어에 관한 정보를 점검하지 않은 결과를 보여준다.



[그림 26] 콘텐츠 목록 화면

제 6장. 결론 및 향후 연구

개인의 데이터에서부터 기업의 민감 데이터까지 정보 유출 시도 및 침해 사례는 날로 증가하고 있으며 피해액도 천문학적으로 치솟고 있다. 현재 웹 환경 내 침해 사고가 가장 많은 부분을 차지하고 있으며 이는 빅데이터 시대에 도래로 더욱 많아질 것으로 예상된다. 특히 빅데이터 시대의 해결책으로 등장한 클라우드 컴퓨팅 환경 내 위협이 가장 우려되는 부분이다.

따라서 본 논문에서는 클라우드 컴퓨팅의 정의와 분류에 대해 살펴보고 정보보호기술 중 사용자 인증과 접근제어에 대해서 조사하였다. 또한 클라우드 컴퓨팅 환경 내에 정보보호의 주요 이슈를 분야별로 분석하여 연구에 이용할 수 있는 문제점을 도출하였다. 이를 기반으로 본 연구에서는 안전한 데이터 전송 및 활용 방안으로써 SDTU(Secure Data transmission and Usage) 아키텍처를 제안하였다. 이는 위에서 제기한 많은 위협들에 노출된 클라우드 환경에서 사용자 인증, 클라우드 신뢰성 검증, 데이터 안전성 점검, 이에 따른 접근제어 기능을 시스템화 하여 사용자에게 안전한 컴퓨팅 환경을 제공하고, SDTU 모델의 활용을 위해 기술적 구현방안을 제시하였다. 이는 실제 IT 환경 내 적용 가능한 연구로 소프트웨어 개발자나 운영자 입장에서 도움이 되는 응용방안 연구가 될 것이다.

향후, 각 메커니즘에서 발생하는 위험관리에 대해 세부적으로 분석, 관리되어야 할 것이며, 정보보호 모니터링 기술화 체계적인 로그 데이터의 분석기술 등에 확장 구현이 요구되며, 이를 통한 사용자 인증서 확장 필드에 이와 같은 정보를 삽입하여 신속한 데이터 처리로 이어 질 수 있도록 연구되어야 할 것이다. 마지막으로 본 논문에서 제안한 모델의 체계적인 관리를 위한 정책적용 시스템과 연동 및 적용성에 대해 연구가 필요할 것으로 사료된다.

참고 문헌

[1] 김우종, 최용민, "한국의 클라우드 컴퓨팅 허브전략과 시사점", Trade Focus IIT보고서 제11권 제12호, 한국무역협회 국제무역연구원, 2012.

[2] 정동원, "클라우드 컴퓨팅에서의 의미 상호운용성을 위한 표준 참조 모델", 한국컴퓨터정보학회지 제17권 제8호, 한국컴퓨터정보학회, 2012.

[3] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", World Privacy Forum, 2009.

[4] 나종희, “클라우드 컴퓨팅 서비스 특성에 관한 질적연구”, 디지털콘텐츠학회지 제12권 제3호, 한국디지털콘텐츠학회, 2011.

[5] 김태형, 김인혁, 민창우, 엄영익, "클라우드 컴퓨팅 보안 기술 동향", 정보과학회논문지 제30권 제1호, 한국정보과학회, 2012.

[6] IT/정보기술, “클라우드, 그리드, 유틸리티, 서버기반, 네트워크 컴퓨팅”, http://i-bada.blogspot.kr/2012/05/blog-post_5343.html#!/2012/05/blog-post_5343.html

[7] 행정안전부, "2012 국가정보보호백서", http://isis.kisa.or.kr/ebook/ebook2.html

[8] 홍승필, “유비쿼터스 컴퓨팅 보안”, 한티미디어, 2006.

[9] Gartner says cloud computing will be as influential as e-business, http://www.gartner.com/it/page/jsp?id=707508

[10] 김경진, "웹 시스템 환경 내 개인정보보호 메커니즘 분석 및 구현방안", 성신여자대학교 석사학위논문, 2009.

[11] R. S. Sandhu, “Role-Based Access Control Models,” IEEE Computer, 1996.

[12] 신동규, "모바일·클라우드 겨냥 사이버범죄 는다", 디지털 타임즈 뉴스,

2012.

[13] 박춘식, "클라우드 컴퓨팅 환경에서의 보안 고려사항에 관한 연구", 한국산학기술학회논문지 제12권 제3호, 한국산학기술학회, 2011.

[14] 최재규, 노봉남, "클라우드 컴퓨팅 환경에서의 보안 평가 요소", 보안공학연구논문지 제8권 제3호, 보안공학연구회, 2011.

[15] 은성경, "클라우드 컴퓨팅 보안 기술 동향", 정보보호학회논문지 제20권 제2호, 한국정보보호학회, 2010.

[16] 한국클라우드서비스협회, “클라우드 서비스 인증”, http://www.excellent-cloud.or.kr/index.asp

[17] 김유진, “개인정보 탐지 및 위험분석 모델”, 성신여자대학교 석사학위논문, 2010.

[18] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared", In Proceedings of Grid Computing Environments Workshop, 2008.

[19] 김학범, 전은정, 김성준, "클라우드 컴퓨팅 환경에서의 보안관리에 관한 연구", 경영컨설팅 리뷰 제2권 제1호, 공주대학교 KNU 경영컨설팅 연구소, 2011.

[20] 이주영, “클라우드 컴퓨팅의 특징 및 사업자별 제공 서비스 현황”, 방송통신정책 제22권 6호, 정보통신정책연구원, 2010.

[21] 서광규, "클라우드 서비스 인증제도 수립을 위한 프레임워크", 정보화정책 저널 제 18권 제 1호, 한국정보화진흥원, 2011.

[22] L. M. Kaufman, "Data security in the world of cloud computing", IEEE Security & Privacy, 2009.

[23] 장은영, "안전한 클라우드 서비스 제공을 위한 규칙기반 Cloud RBAC 모델 연구", 서울여자대학교 석사학위논문, 2011.

[24] 문정경, 김진묵, 김황래, "클라우드 컴퓨팅 환경에서 효과적인 사용자 인증

프로토콜", 한국산학기술학회논문지 제 12권 제 5호, 한국산학기술학회, 2011.

[25] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, 2009.

[26] 이정현, "인증서 생성 관리", 전자서명 인증관리 전문가 교육과정, 한국인터넷진흥원, 2012.

[27] 임철수, "클라우드 컴퓨팅 보안 기술", 정보보호학회논문지 제 19권 제 3호, 한국정보보호학회, 2009.

[28] 정임영, 조인순, 유영진, "클라우드 컴퓨팅 환경의 데이터 신뢰 확보", 한국통신학회논문지 제 36권 9호, 한국통신학회, 2011.

[29] 이병엽, 박준호, 유재수, “클라우드 데이터 서비스를 위한 대용량 데이터 처리 분산 파일 아키텍처 설계”, 한국콘텐츠학회논문지 제 12권 제 2호, 한국콘텐츠학회, 2012.

[30] 크리스토퍼 버냇, "클라우드 컴퓨팅-당신이 알고 있는 컴퓨터의 시대는 끝났다", 미래의 창, 2011.

Abstract

A Study on the Data Processing Method for Effective Utilization and Secure Transmission in Cloud Computing Environment

Saeromi Yang
Dept. of Computer Science
The Graduate School
Sungshin Women's University

The development of the information technology environment gives access to internet users the ability to take advantage of information through a variety of web services. Over the last few years, due to a variety of services and the explosion of data, such as the Internet, smart devices, social media, the advent of the so-called 'Big Data' era has arrived. Interested in cloud computing which can solve the problem of excessive traffic and a lot of data by handset has been amplified. Cloud computing is cost and time efficient and is overcome the constraints of time and space to share information. So it has received a lot of attention during the

last few years, and has grown rapidly. However, the rapid growth of new technologies and the high dependence cause problems. Newly, through Financial affairs, including payments through smart appliances in a cloud computing environment, Information Security threats are increasing.

In this paper, Analysis information Security issues Technical, managerial, political, multifaceted service element-by-element to securely manage important information stored in the open environment of cloud computing. and SDTU(Secure Data Transmission and Usage) architecture is proposed to solve this issues. In the proposed architecture, Proposed information protection through a step-by-step security check and management practices(1. User Authentication Mechanism, 2. Cloud Condition Verifying Mechanism, 3.Information Leakage Detecting Mechanism) so you can safely make available services by Computing resource virtualization. Finally, by introducing information protection measures within a cloud environment and System implementation plan, Explore the possibility of a real-world environment Application Scheme.