

논문 2011-6-19

모바일 클라우드 보안기술의 모델 제안

The Model Proposal of Mobile Cloud Security Technology

신승중*

Seung-Jung Shin

요 약 국내 클라우드 시장은 '14년까지 2조원 규모로 급성장할 것으로 예상하는 반면, 모바일 클라우드 서비스 활성화의 장애요인으로 서비스의 안정성에 대한 우려, 데이터의 보안성 및 기밀성에 대한 불안감 등 보안에 대한 우려가 높다. 이러한 상황속에서 기존 IT 보안 기술로도 충분히 대응 가능한지와 모바일 클라우드 특성에 최적화된 보안 기술에 대한 요구사항에 대한 분석이 구체화되지 못하고 있는 실정이다. 본 연구에서는 모바일 보안의 특성에 대해 살펴보고 모바일 클라우드 장애 사례를 통해 미래 보안기술의 요구사항에 대해 모색하고자 한다.

Abstract The Korean domestic cloud market will reach a value of 2 trillion Korean won by 2014. The domestic market is expected to grow rapidly in size despite the fact that there exist activation barriers in mobile cloud services, concerns about the reliability of service, and concerns about security and confidentiality of data. Under these circumstances, existing IT security technologies may be utilized to provide sufficient response characteristics. Despite this, they must be optimized for mobile cloud computing and enhanced to mitigate inherent security flaws. In this study, mobile cloud security is covered along with use cases that cover the cases where mobile devices are particularly vulnerable and suggest ways to mitigate security vulnerabilities.

Key Words : Mobile Cloud, Computing, Security, Platform, SaaS, PaaS, IaaS

1. 서 론

클라우드 컴퓨팅은 서비스를 이용하는 이들이 하드웨어, 소프트웨어 등의 모든 IT자원을 구매, 설치, 운영할 필요 없이 제3자의 인프라를 이용하여 마치 자신의 컴퓨팅 환경처럼 자유롭게 이용하고, 그에 따른 비용을 지불하는 새로운 컴퓨팅 환경이다.^[1,2]

모바일 클라우드는 모바일 단말기에 최적의 서비스를 지원하기 위한 모바일 플랫폼의 핵심 기술 요소이다. 여기서 모바일의 개념은 매우 다양하다. 스마트폰은 물론이고 이동성을 갖는 기기들, 즉 노트북과 넷북, PDA,

UMPC, 및 thin client 등을 모두 포괄한다. 따라서 모바일 클라우드란 다양한 모바일 단말기를 통해 클라우드로부터 서비스를 지원받는 모델이라고 할 수 있다.^[3]

미래의 모바일 클라우드 기술은 물리적 공간을 뛰어넘는 'Always on Computing' 생활공간을 마련하여 사용자가 언제, 어디서든 클라우드 자원과 개인 스마트폰 자원을 동시에 활용하여 '리치 서비스'를 실행시킬 수 있다. 이러한 상황속에서 기존 IT 보안 기술로도 충분히 대응 가능한지와 모바일 클라우드 특성에 최적화된 보안 기술에 대한 요구사항에 대한 분석이 구체화되지 못하고 있는 실정이다.

이에 본고에서는 2 장에서는 기존 IT서비스와 비교하여 모바일 클라우드의 서비스 특성에 대하여 설명하고 3 장에서는 모바일 클라우드 특성에 따른 보안이슈에 대해

*정회원, 한세대학교 IT학부

접수일자 2011.11.30, 수정완료 2011.12.14

게재확정일자 2011.12.16

살펴본다. 마지막 4 장에서는 모바일 클라우드 기술의 보안사항에 대해 정리한다.

II. 모바일 클라우드 서비스

클라우드 컴퓨팅 환경이 구축되면, 정보이용자는 정보 유통 과정의 첫 단과 끝 단인 입력과 출력 부분만 담당하고 중간 과정, 즉 정보처리, 저장, 관리 및 유통 등의 나머지 모든 과정은 이용자가 인지하지 못하는 제 3의 공간에서 이루어지게 된다. 또한 항상 최신 정보로 업데이트될 수 있도록 동기화하는 서비스도 제공하며, 업데이트 이전 버전까지 유지함으로써, 잘못된 정보 입력 또는 단말기 분실에 대비, 손쉬운 데이터 복원을 보장한다.^[4,5] 다음 아래 그림 1은 클라우드 정의에 대한 구성도를 보여주고 있다.

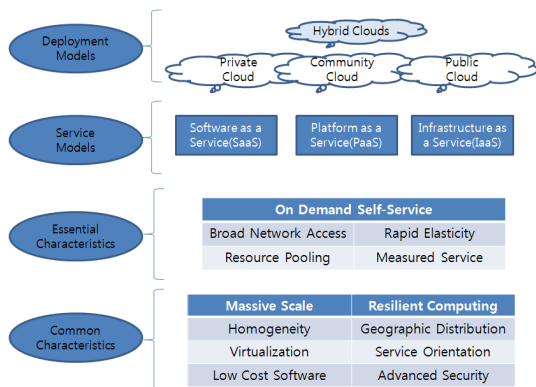


그림 1. 클라우드 정의 구성도
Fig. 1. The Diagram of Cloud Definition

가. 클라우드 서비스 모델

모바일 클라우드 서비스 3가지 모델로서 소프트웨어형 서비스, 플랫폼형 서비스, 인프라스트럭처형 서비스 등으로 나눌 수 있다. 먼저 소프트웨어형 서비스(Software as a Service)는 사용자 특정 소프트웨어를 필요한 시기에만 네트워크에 접속하여 사용하고 그것을 실행시키고 있는 운영체제, 하드웨어, 네트워크에는 접근(제어)하지 못한다. 두 번째, 플랫폼형 서비스(Platform as a Service)로 개발을 위한 플랫폼을 구축할 필요없이 표준화된 플랫폼을 웹에서 빌려 쓸 수 있게 만든 방식으로 가상화된 모든 개발과 관련된 환경 및 프로세스를 제공한다. 세

번째, 인프라스트럭처형 서비스(Infrastructure as a Service)는 소비자는 프로세싱 파워, 스토리지, 네트워크 또는 미들웨어와 같은 기본적인 컴퓨팅 자원을 가상화 환경으로 구축하여 사용자의 필요에 따라 서비스 형태로 제공하는 방식입니다. 소비자는 운영체제, 스토리지, 어플리케이션들, 그리고 방화벽과 부하분산기와 같은 네트워크 컴포넌트들에 대한 제어가 가능하다.

나. 클라우드 서비스 특성

모바일 클라우드는 5가지 필수 특성으로 나눌 수 있다. 수요기반 자가 서비스, 고속 네트워크 접근, 신속한 확장성 제공, 컴퓨팅 자원 공유, 계량 가능한 서비스 등이다. 이러한 세부적 내용으로 첫째 수요기반 자가 서비스로 원하는 만큼 언제나, 어디서나, 어떤 디바이스를 가지고 고도 제공자의 개입 없이 즉각적으로 서비스를 제공한다. 둘째, 고속 네트워크 접근으로 인터넷 등 광대역 네트워크를 통해 다양한 디바이스로 서비스에 접속이 가능하다. 셋째, 신속한 확장성 제공으로 원하는 만큼, 상황에 따라 자동으로 scale-in, out이 가능하다. 넷째, 컴퓨팅 자원 공유로 공유 자원풀을 사용자 별로 나누어서 상호 독립적으로 무한정으로 사용을 가능케 한다. 다섯째, 계량 가능한 서비스로 계량화 되어 사용량에 따라 과금, 제공자는 자원 증/감축 계획을 수립할 수 있다.

다. 클라우드 수용모델

클라우드 4가지 수용모델로서 전용 클라우드(Private cloud), 공용클라우드(Public cloud), 커뮤니티클라우드(Community cloud), 복합클라우드(Hybrid cloud)등으로 나눌 수 있다.^[6] 전용 클라우드는 가상화, 표준화, 자동화 등 클라우드 기술을 활용하여 고객 또는 제공 사업자들의 데이터 센터에 자사 전용의 환경을 구축하는 것으로 컴퓨터 자원을 유저가 유연하게 이용하는 시스템이다. 관리운영 주체에 따라 직접 또는 제3자 관리운영으로 나누어지고 설치장소에 따라 조직내 또는 조직외로 나뉘어진다. 공용 클라우드는 기업의 파이어 월(fire wall)의 외측에 구축되는 형태로, 공중의 인터넷망을 통해 불특정 다수의 기업이나 개인 유저에게 제공되는 클라우드 서비스이다. 시설 소유 및 관리운영 주체는 서비스 제공 사업자이다. 커뮤니티클라우드는 복합클라우드는 공통의 목적을 가지는 특정 기업간 형성되는 “커뮤니티”가 데이터 센터에서 공동 운용되는 시스템이다. 프라이빗 클라우드

와 퍼블릭 클라우드와의 중간적인 형태이다. 마지막 복합클라우드에는 지금까지 설명한 프라이빗 클라우드, 커뮤니티 클라우드, 그리고 퍼블릭 클라우드 등을 활용하는 서비스이다. 이는 2개 이상의 클라우드 시스템이 유기적으로 연계되어있다. 전체가 하나의 시스템처럼 운영되며, 개별 시스템 간에는 표준화된 기술로 연동되고, 데이터나 응용서비스의 이동성이 확보되어야 한다. 이러한 모델로 기업유저는 기간계 시스템을 공용 클라우드로 운용, 정보계 시스템은 퍼블릭 클라우드로 이용하는 경우가 많다.

III. 모바일 클라우드 보안 기술의 한계

1. 모바일 클라우드 위험 요소 및 사례 분석

최근 아마존 EC2 장애 등 일시적으로 서비스가 중단되는 장애와, 데이터 손실 등의 사고가 빈번이 발생하고 있다. 하지만, 클라우드 서비스 제공자들은 사고 발생 경위에서부터 원인 및 중단시간, 피해규모 등을 명확히 밝히지 않고 있으나, 주로 시스템(장비) 에머 및 교체, 관리자 부주의, 자연재해에 의한 것으로 이는 클라우드 컴퓨팅 서비스가 아직 활성화되지 않았기 때문으로 모든 정보가 한 곳에 집중화 되는 서비스 특성상 클라우드 컴퓨팅 서비스가 본격적으로 확산되면 많은 해커들의 주 대상이 될 것으로 예상된다.

아래는 몇가지 클라우드 장애로 인한 사고를 보여준다.

(1) 마이크로소프트 데인저 서비스 중단

T모바일 사이드킵 사용자의 연락처, 일정, 사진, 기타 개인정보가 사이드킵이 서비스 제공업체인 데인저의 서비스 장애 후 손실된 것으로 보인다.

(2) 디도스 공격으로 인한 트위터 다운

2009. 8월초 아침부터 오후까지 서비스가 중단되면서 소셜 네트워킹 분야 전체가 시끄러웠다.

(3) 아마존 S3 스토리지 서비스 중단

2008년 여름, 아마존의 S3 클라우드 네트워킹이 마지막으로 대형사고가 발생하였다. 당시 장애는 78시간이 지속됐는데, 2008년 초에는 인증 요청이 몰리면서 서비스가 중단되기도 했다.

(4) 이베이페이팔 장애로 인한 서비스 중단

8월에는페이팔 온라인 지불결제 시스템이 2시간 정도 장애를 일으키면서 수백만 명의 고객이 거래를 마무리하지 못하고 말았다. 서비스 중단의 원인으로는 네트워크 하드웨어 문제가 지목됐다.

2. 모바일 클라우드 문제점 및 요구사항

가. 모바일 클라우드의 문제점

(1) 사업자 파산

사업자가 파산하는 경우, 기존에 서비스 이용자는 안정적으로 서비스를 이용하지 못해 지금까지 서비스를 이용해 진행하던 업무가 정지되게 되며 또한 데이터가 훼손되거나 손실되는 경우, 지금까지 클라우드 컴퓨팅 서비스에 보유하고 있었던 정보들이나 데이터를 잃게 된다. 만일 서비스 제공자의 파산 이후 또 다른 서비스 제공자를 찾겠다고 하여도 기존에 제공받던 서비스를 동일하게 제공받을 수 있는지, 업체들 간 시스템 부분에서 호환이 가능한지의 문제들이 발생할 수 있습니다.

(2) 서비스 중단 및 장애

클라우드 컴퓨팅 서비스가 중단되거나 장애가 발생하는 경우에도 사용자는 서비스 공급자가 파산하는 경우와 유사한 피해를 입게 된다. 특히 클라우드 컴퓨팅 서비스는 인터넷과 마찬가지로 각각의 서비스와 컴퓨터가 네트워크로 연결되어 있어 바이러스 감염이나 해킹 등의 침해사고 등에 취약하여 언제라도 서비스에 장애가 발생할 수 있는 가능성이 크다. 게다가 클라우드 컴퓨팅 서비스는 사용자의 정보를 서비스 제공자의 서버에 저장해놓는 형태로 제공되기 때문에 서비스 장애에 따른 정보 유실이나 손실의 규모는 여타 다른 인터넷 기반 서비스보다 훨씬 클 것으로 예상된다.^[7]

(3) 플랫폼 독립성 문제

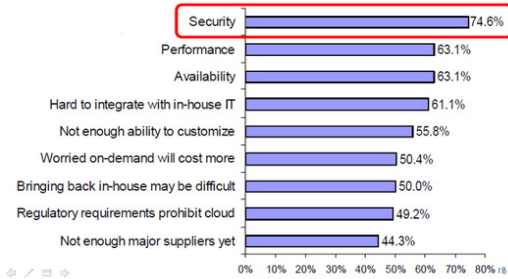
플랫폼의 독립성이란 플랫폼이 운영체제 또는 단말기에 상관없이 작업을 수행할 수 있는 것을 의미한다. 클라우드 컴퓨팅 서비스에서는 플랫폼의 독립성 강화가 무엇보다 중요하다.

클라우드 컴퓨팅 서비스 사업자가 갑작스럽게 파산을 하거나 사업을 폐지하는 경우, 기존에 해당 서비스를 이용하던 사용자들은 다른 서비스로의 전환이 불가피하다.

(4) 기밀성과 데이터 암호화

모바일 클라우드기술은 비용과 자원절약이라는 장점이 있는 반면 집중화에 따른 부작용이 존재한다. 사용자의 데이터와 응용프로그램이 구름 속 서버와 스토리지에 숨어 있기 때문에 데이터는 통제권을 상실하고, 서버는 해커의 새로운 공격 타깃이 된다.

표 1. 클라우드 서비스 해결 과제
Table 1. The solution of Cloud service, IDC Enterprise Panel



따라서 보안은 클라우드 컴퓨팅에서 가장 중요한 요소이다. 위 표1은 IDC에서 244명 IT 관련임원들에게 Cloud 서비스에 관하여 그들의 견해와 활용에 대하여 조사한 것 중의 하나로, 보안(74.6%)을 해결해야 할 첫 번째 과제로 꼽고 있다.^[8]

나. 클라우드 보안 요구사항

모바일 클라우드 도입시 서비스 장애 및 유출에 대한 우려가 크기 때문에 오늘날 클라우드 보안 기술에 대한 중요성이 부각되고 있다. 이에 따른 모바일 클라우드 보안 기술의 요구사항은 다음과 같다.

(1) 사업자 파산에 대비한 임치기관 개설

사업자의 파산은 예상치 못한 상황이기 때문에 클라우드 임치 기관의 사용자 정보에 대한 실시간 자동 백업을 수행할 수 있는 임치기관 개설이 필요하다.

(2) 플랫폼 독립성 강화

플랫폼이 독립적인 경우, 사용자들은 별다른 전환비용 없이 손쉽게 다른 서비스로 옮겨갈 수 있게 된다. 따라서 클라우드 컴퓨팅 서비스에 있어서 플랫폼의 독립성 강화는 사용자들의 권리와 정보를 보호해 줄 수 있는 제도적 장치의 연장선이라 할 수 있다.

(3) 기밀성과 데이터 암호화

개인 및 기업 데이터에 대한 기밀성(privacy) 보호를 위해서는 기본적으로 암호화(encryption) 기술이 제공되어야 한다. 특히 클라우드 컴퓨팅에서는 대용량 데이터의 암호화시 전체 시스템의 가용성이 떨어질 수 있다는 점을 고려하여 이러한 상황에 적합한 암호가 이용되어야 하는데, 예를 들어 DES나 AES와 같은 블록 암호대용으로 스트림 암호를 사용하는 방안 등을 고려해볼 수 있다. 또한 키 저장 서버의 사고시 다수 사용자의 데이터가 접근 불가능해지므로 키 관리 방안에 대한 연구 또한 필요하다.

IV. 모델제안

IT 관리에서는 비즈니스 목표를 달성하기 위해 기업에서 사용하는 소프트웨어 애플리케이션 및 서비스의 종단간(end-to-end) 수명 주기를 다룬다. 수명 주기 단계에는 일상적인 비즈니스 업무를 지원하는 하드웨어, 네트워크, 인프라, 소프트웨어, 서비스로 구성된 IT 포트폴리오를 계획, 구현, 운영 및 지원하는 작업이 포함된다.^[9,10]

SaaS 공급자에게 아웃소싱된 애플리케이션은 사용 기업이 아닌 서비스 제공사의 관리자와 운영자에 의해 유지 관리된다. 또한, 기업에서는 클라우드에서 실행 중인 서비스를 모니터링하기 위한 IT 관리 솔루션 배포 계획을 세워야 한다. 운영 전략에서는 성능 지표 및 관리 규정을 정의해 외부 서비스의 성능 및 가용성을 파악할 수 있도록 해야 한다. 운영 모니터링 시스템은 관리측면의 알림과 경고를 발생시켜 모든 서비스 이상을 조기에 감지할 수 있도록 해야 한다. 그럼으로 이러한 문제점을 보완하는 모델을 제안한다. 제안된 모델은 세가지 유형으로 나눌 수 있다.

첫번째 유형으로 클라우드 서비스 공급자 파산으로 인한 데이터 손실을 방지 위해 제안 모델로 다음 아래 그림 2와 같다.

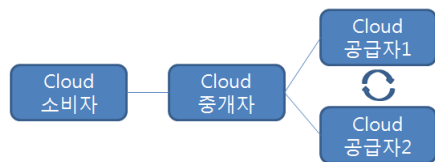


그림 2. 클라우드 서비스 모델 제안 1
Fig. 2. The Proposal of Cloud Service Model 1

이는 중개자를 통한 서비스 안정성 및 경쟁 유도 모델로서 클라우드 중개자는 두 공급자를 유치 관리하면서 예기치 못한 공급자 서비스 중단 및 오류로 인한 사용자의 데이터 손실을 막기 위해 서로간의 실시간 자동 백업을 목표로 운영한다.

두번째 유형으로 클라우드 전용 전송사업자를 통한 전송서비스의 품질 강화 모델이며 아래 그림 3과 같다.



그림 3. 클라우드 서비스 모델 제안 2
Fig. 3. The Proposal of Cloud Service Model 2

이는 전송서비스 품질 강화와 클라우드 운영체제 독립성을 지닌 Cloud 전송사업자를 통해 사용자의 서비스 전환에 어려움을 해소해 줄 것으로 본다.

마지막 번째 유형으로 클라우드 데이터 사용자를 보호하기 위한 서비스 장애에 따른 데이터 암호화 관리를 담당 하기 위한 모델로 다음 그림 4와 같다.

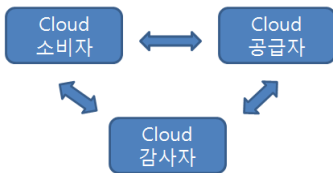


그림 4. 클라우드 서비스 모델 제안 3
Fig. 4. The Proposal of Cloud Service Model 3

이는 Cloud 소비자의 일정부분을 Cloud 감사자가 대신 수행하는 모델이다. 기존 물리적 보안 영역과 가상화 관리영역을 통합적으로 보안관리 기능을 제공한다.

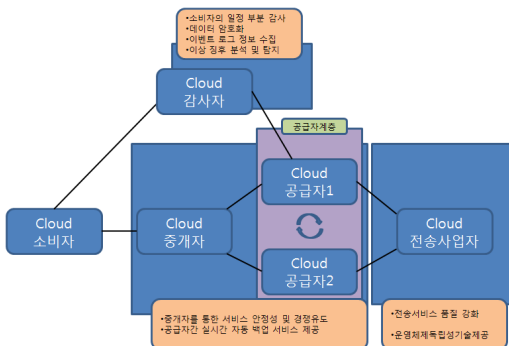


그림 5. 클라우드 서비스 제안 모델의 역할
Fig. 5. The Role of Proposal Model for Cloud Service

특히, 클라우드 가상화 영역까지 인증, 자원 할당등 보안 이벤트 로그 정보를 수집하고 분석하는 클라우드 보안 모니터링을 확대하여 과도한 자원 할당, 과부하에 의한 시스템 장애, 권한 외자원 접근 시도, 계정 도용으로 인한 정보유출 시도 등을 이상 징후를 종합적으로 분석하고 탐지하는 역할을 한다.

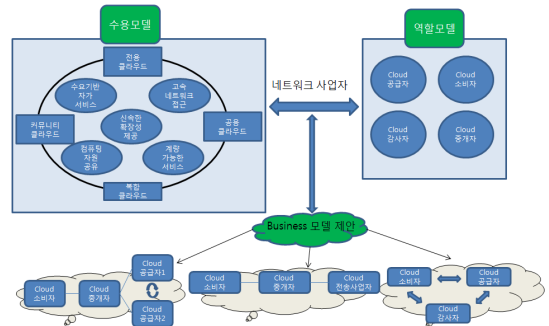


그림 6. 전체적인 클라우드 서비스 제안
Fig. 6. The Overall Proposal of Cloud Service Model

위 그림 6은 종합적인 클라우드 서비스 프레임을 제시하고 있으며 이러한 모델은 클라우드 서비스 특성에 따른 문제점을 어느정도 해소할 것으로 본다.

V. 결론

국내 스마트폰 등 모바일 기기 보급 확산 및 비용절감, 확장성 등의 장점으로 클라우드 도입이 확대되고 있는 실정이다.

그러나 사업자 파산의 경우 기존에 서비스 이용자는 안정적으로 서비스를 이용하지 못해 지금까지 서비스를 이용해 진행하던 업무가 정지되게 되며 또한 데이터가 훼손되거나 손실되는 경우, 지금까지 클라우드 컴퓨팅 서비스에 보유하고 있었던 정보들이나 데이터를 잃게 된다.

또한, 클라우드 컴퓨팅 서비스 사업자의 이용 약관규정에서 서비스 장애에 따른 손해배상의 범위를 명확히 규정하는 것이 필요하고 클라우드 컴퓨팅 서비스 사업자가 갑작스럽게 파산을 하거나 사업을 폐지하는 경우, 기존에 해당 서비스를 이용하던 사용자들은 다른 서비스로의 전환이 불가피하다. 이러한 문제를 해결하기 위해 다음과 같이 클라우드 보안 기술 모델을 제안을 하였다.

첫 번째, 유형으로 Cloud 증개자를 통한 서비스 안정성 및 경쟁 유도도 제안 모델이다.

두 번째, 유형으로 클라우드 전용 전송사업자를 통한 전송서비스의 품질 강화와 실시간 Cloud 공급자간 자동 백업 시스템 모델이다.

세 번째, 유형으로 Cloud 감사자를 클라우드 데이터 암호화 및 이벤트 로그 정보 수집, 이상 징후 분석 및 탐지를 통하여 클라우드 보안을 강화 및 감시하는 모델이다.

본 논문에서는 Cloud 공급자간의 경쟁유도를 통하여 Cloud 공급자와 소비자 간의 신뢰를 구축하고 예상치 못한 사용자 데이터 손실을 대비하기 위해 공급자간 실시간 자동백업을 함으로써 사용자의 불안감을 해소하고 Cloud 감사자를 통하여 클라우드 보안을 강화 및 감시할 수 있을 것으로 본다.

참 고 문 헌

- [1] Nichols, Ryan, 2010 “Five questions to help business and IT think big about cloud computing”, Computerworld
- [2] 한은영 <개인용 클라우드 서비스 경쟁: 아마존, 구글, 애플>, 정보통신정책연구원, 2011.6.3.
- [3] 윤용익 외 <모바일 클라우드 컴퓨팅 기술 동향>, 정보통신 산업진흥원, 주간기술동향 통권 1439호, 2010. 3.31.
- [4] Peter Mell and Time Grance, “The NIST Definition of Cloud Computing”, 2009. 10.
- [5] ChristineGallen, Mobile Cloud Computing Subscribers to Total Nearly One Billion by 2014, ABI research, 2009. 09
- [6] 김학영 외 <모바일 클라우드 기술 동향>, 한국전자통신연구원, 2010.6.7.
- [7] SNIA, “Cloud Storage Use Cases”, Trial-User Draft, June 2009
- [8] “클라우드 컴퓨팅 서비스와 보안.” 『A3 Security New sletter』 April. 2011. <http://www.a3sc.co.kr/newsletter/042011/essay.html>

- [9] Enterprise Mobile Cloud Computation, ABI Research 2009. 1
- [10] Michael Miller, ‘Cloud Computing: Web-Based Applications that Change the Way You Work and Collaborate Online’, Que Publishing, 2009
- [11] Yoon-Sik Kwak외 2명, “Mobile Device Driver for U-Storage System” 한국정보기술학회 Vol.5 No.1 2007
- [12] 최병선의 1명, “모바일 환경을 위한 WIPI 기반의 PKI 시스템 연구” 한국정보기술학회 Vol.5 No.2 2007
- [13] 광윤식의 1명, “유틸리티 컴퓨팅 서비스를 위한 온라인 스토리지 가상화”, 한국정보기술학회 Vol.6 No.1 2008
- [14] 신용진의 4명, “클라우드 컴퓨팅 기반의 U-City 서비스 프로비저닝”, 한국정보기술학회 Vol.7 No.3 2009
- [15] 김병주의 2명, “유비쿼터스 저장시스템을 위한 파일시스템 변환기 설계”, 한국정보기술학회 Vol.5 No.1 2007

저자 소개

신 승 중(정회원)



- 1988년 세종대학교 경영학과 졸업(경영학석사)
- 1994년 건국대학교 전자계산학과 졸업(공학석사)
- 2000년 국민대학교 정보관리학과 졸업(공학박사)
- 2008년 현재 한세대학교 IT학부.

<주관심분야 : 정보관리, 정보전, 정보보호>

※ 본 연구는 한세대학교 연구비를 지원받은 논문입니다.