모바일 클라우드시스템 보안요구사항명세서 개발지원도구

방영환 | 정성재* | 황선명**
한국생산기술연구원, *(주)스컴씨엔에스, **대전대학교

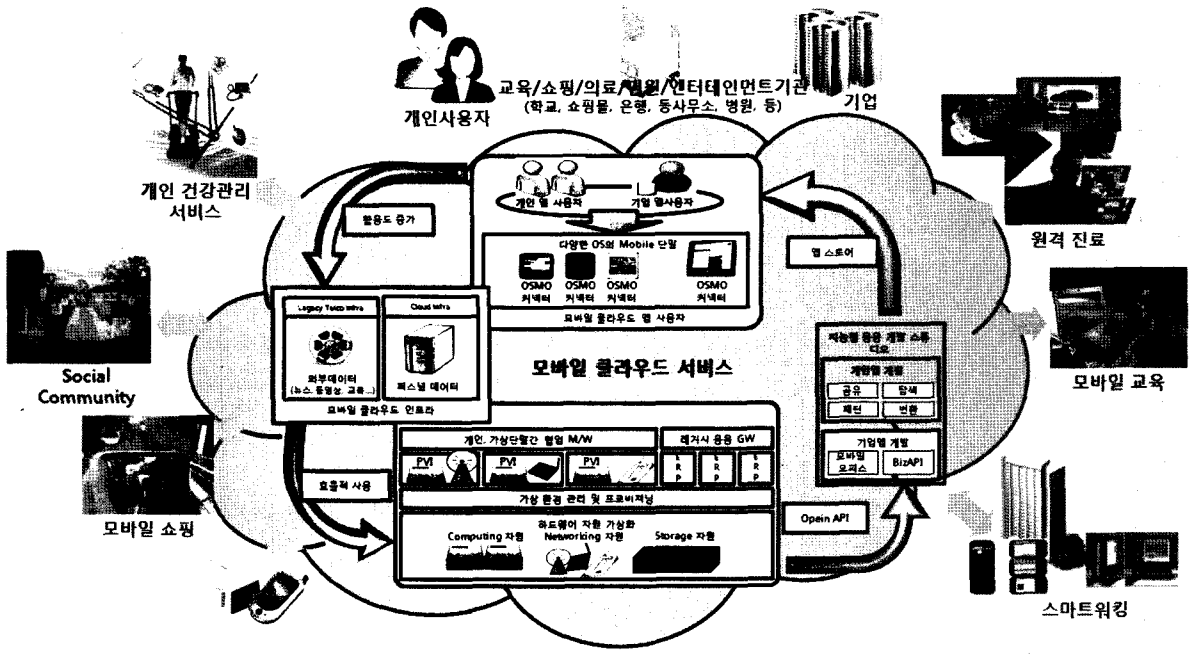
요 약

최근 클라우드컴퓨팅은 국내외 많은 IT서비스 패러다임의 변화를 주도하고 있고, 제2의 디지털 시대를 주도할 핵심 서비스 중의 하나로 정보혁명에 커다란 변화를 가져오고 있다. 특히, 클라우드 컴퓨팅은 무선 네트워크 기술이 고도화되고 모바일 단말 시장이 성장함에 따라, 모바일과 결합하면서 IT 분야의 신 패러다임으로 부각되고 있으며, 이는 클라우드 컴퓨팅의 경제성과 우수성이 모바일의 이동성과 합쳐져 서로 시너지 효과를 거두고 있기 때문이다 [1]. 이처럼 클라우드컴퓨팅 기술 분야가 확대됨에 따라서 해결해야 할 첫 번째 문제는 보안이다. 특히, 모바일 클라우드시스템은 이동성, 휴대편의성, IT자원을 소유하지 않고 정보활동이 가능한 형태이므로 필연적으로 보안문제에 대한 중요성이 강조 된다.

이에 따라서, 본고에서는 모바일 클라우드시스템의 정보보호를 위해 특성과 유형을 파악하고 정보보로분야에서 정보보증(Information Assurance, IA)방법, 여러 정보보증제도(CC, ISMS, CMVP등)를 조사 · 분석하여 모바일 클라우드시스템 보안기능개발을 위한 보안요구사항명세서 지원도구를 제시하고자 한다.

I. 서 론

국내 이동통신 사업자(국내 중소기업을 포함하여)들과 애플, 아마존, 구글, IBM, 마이크로소프트 등 해외 글로벌 기업들은 이미 다양한 서비스를 내놓고 시장 선점을 위해 치열한 경쟁을 벌이고 있다. 미국, 일본, 영국 등 선진국들도 자국의 시장 경쟁력 강화와 IT 인프라 구축비 절감, 환경보 호 등을 위해 클라우드 컴퓨팅 활성화에 힘쓰고 있다. 우리 정부도 클라우드 컴퓨팅 생태계 구축을 통해 시장을 활성화 하기위해 2009년 12월 범정부 차원의 '클라우드 컴퓨팅 활성화 종합계획' 및 2010년 4월 모바일서비스활성화 계획을 발표한 바 있다. 클라우드서비스의 확대 및 무선 네트워크 기술이 고도화되고 모바일 단말 시장이 성장함에 따라, 모바일과 결합하면서 IT분야의 신 패러다임으로 부각되고 있으며, 이는 클라우드 컴퓨팅의 경제성과 우수성이 모바일의 이동성과 합쳐져 서로 시너지 효과를 거두고 있기 때문이다. 모바일 클라우드 컴퓨팅이란 앱스토어에 종속된 특정 운영체제를 기반으로 개발 된 애플리케이션을 한계를 뛰어넘는 기술로 웹의 접속을 통해 소프트웨어, 플랫폼 등의 IT자원을 모바일 단말에 설치하지 않고 제공받을 수 있는 방식을 의미한다. 다양한 IT자원을 서비스로서 제공하는 클라우드 컴퓨팅의 정의를 생각해 본다면 기존 PC보다 더 많은 자원의 한계를 갖는 모바일 단말이 클라우드 컴퓨팅으로 인해 많은 효과를 얻을 수 있을 것 이다. 특히 모바일 단말이 PC기능을 수행 가능하면서 모바일 컴퓨팅이 중시되고 있는 오늘날, 웹기반의 클라우드 컴퓨팅을 적용한 모바일 클라우드 컴퓨팅의 등장은 모바일 단말이 갖는 처리 능력, 배터리 수명, 데이터 저장소와 같은 한계를 극복할 수 있게 하였다. 즉, 모바일 클라우드 서비스는 사용자에게 방대한 IT 자원 및 애플리케이션을 단말의 기능에 제한 없이 효율적으로 제공한다는 한다는 장점이 있지만, 애플리케이션 개발자에게는 단말의 사양과 독



(그림 1) 모바일 클라우드 서비스

립적으로 하나의 애플리케이션만을 개발하여 모든 단말에 제공할 수 있게 한다는 장점을 갖는다. 이러한 이유로 모바일 클라우드서비스는 급격히 증가하고 있으며, 2009년 ABI Research에서는 전 세계의 모바일 클라우드 컴퓨팅 가입자 수가 2008년 4,280만 명(전체 모바일 가입자 수의 1.1%)에서 2014년에는 약 9,998만 명에 이를 것으로 전망하였다 [1].

또한, 기업의 클라우드 플랫폼 도입과 스마트폰 채택에 따라 2015년에는 전 세계 2억 4000만 명의 기업 사용자가 클라우드 컴퓨팅을 이용할 것이고, 여기에서 52억 달러의 매출이 발생할 것으로 전망하고 있다. 또한, Juniper research는 모바일 클라우드 서비스가 2009년은 4억 달러 규모, 2014년까지 88%의 성장률을 기록하며 95억 달러 규모에 이를 것으로 전망하고 있다. Garther는 모바일 앱스토어 시장을 70억 달러 규모로 평가하고 있으며 2013년에는 295억 달러로 성장할 것으로 전망하고 있다 [2].

이처럼 모바일 클라우드 산업이 확대됨에 따라서 해결해야 할 첫 번째 문제는 보안이다. 특히, 모바일 클라우드시스템은 이동성, 휴대편의성, IT자원을 소유하지 않고 정보활동이 가능한 형태이므로 필연적으로 보안문제에 대한 중요성이 강조 된다.

II. 모바일 클라우드시스템

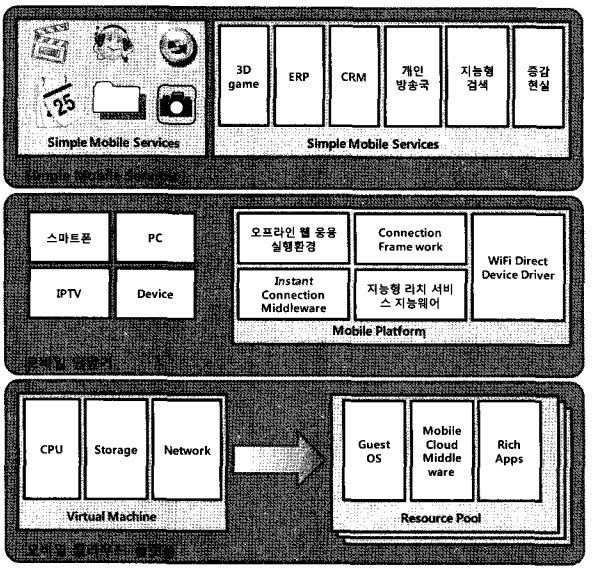
최근 모바일 시장은 기존 사업과 무관하게 다양한 사업자들의 각축장이 되고 있으며, 이는 Mobile Cloud도 예외는 아니다. 기존 포탈 사업자, 솔루션 사업자, 대형 SI들이 초기 시장 선점을 하기 위해 빠르게 움직이고 있다.

1. 모바일 클라우드 개념

모바일 클라우드시스템은 이동성, 휴대편의성을 통한 하드웨어, 소프트웨어 등 IT 자원을 필요한 때 필요한 만큼 빌려쓰고 사용한 만큼 요금을 지불하는 클라우드컴퓨팅이 모바일 영역까지 확대된 개념이다. 또한 클라우드에 있는 어플리케이션과 데이터 액세스에 주로 스마트폰을 사용된다. 모바일 클라우드는 스마트 디바이스와 같은 이동단말에서 고객이 애플리케이션이나 서비스를 이용할 수 있도록 해주는 실행환경을 말한다. 대부분 모바일 클라우드는 크게 단말플랫폼과 서

버플랫폼으로 나뉜다. 단말플랫폼은 운영체제 · 미들웨어 · 브라우저와 같이 단말기에 탑재되는 것을 말하고, 서버플랫폼은 인증 및 과금, 게이트웨이, 온라인마켓플레이스와 같은 서버단에 탑재되는 플랫폼을 말한다. 소비자입장에서는 단말기에 탑재되는 단말플랫폼이 곧 모바일 플랫폼이다[3],[4].

2. 모바일 클라우드 기능요소



(그림 2) 모바일 클라우드 기능요소

모바일 클라우드의 구성요소는 모바일 단말기, 모바일 애플리케이션, 모바일 클라우드 서버플랫폼의 세 요소로 구성된다.

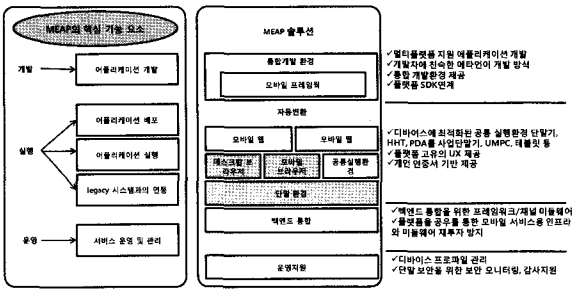
초창기플랫폼은 단순히 하드웨어를 제어하는 기능에 충실했다. 따라서 특별히 UI(사용자환경)라고 불릴만한 것이 존재하지 않았고, 하드웨어를 직접 제어했기 때문에 소비자들이 플랫폼의 매력을 느낄 수는 없었다. 이른바 '보이지 않는 중간자' 의 역할만을 한 셈이다. 그러나 최근의 플랫폼은 애플리케이션과 서비스를 실행해주는 브레인역할을 하고 독자적인 UI까지 갖추는 등 PC의 운영체제수준으로 기술이 발전되고 있다. 더욱이 최근의 모바일 클라우드 기술은 모바일 단말을 사용하여 언제 어디서나 고성능의 컴퓨팅 자원을 활용할 수 있고, 단말과 클라우드 서버간의 협업을 통하여 다양한 단말에서 고성능 응용 프로그램의 운영 및 개인화된 서비스 제공이 가능한 개방형 모바일 클라우드 컴퓨팅 시스템 기술개발도 진행 중이다. 다음은 모바일 클라우드 서비스를 위한 주요 플랫폼 및 기능을 설명한다.

1) 개방형 클라우드 플랫폼

모바일 환경에서 단말이나 사업자 종속성 없이 클라우드 상의 자원 및 응용을 개인과 기업 목적으로 사용할 수 있는 투명한 응용 개발 환경 및 실행 인프라

2) MEAP(Mobile Enterprise Application Platform)

개인모바일 서비스 및 기업의 업무효율성을 위해 기업내부 시스템을 다양한 모바일 단말을 통해 사용할 수 있도록 해주며, 다양한 모바일 서비스 개발 시 개발언어를 다루는 네이티브 코딩(Native Coding)으로 인한 문제를 해결해줄 수 있는 프레임워크 솔루션 제품으로 핵심기능요소는 아래의 그림과 같다.



(그림 3) MEAP의 구성도

MEAP의 용도는 다음과 같다.

- 디바이스 플랫폼 중립적인 개발 및 실행환경 제공
- 통합개발환경을 통한 라이프 사이클(Life-cycle) 관리
- 플랫폼별 SDK(Software Development Kit)와 통합 개발환경과의 연계를 통한 개발 생산성 향상
- 다양한 환경을 고려한 중앙 집중화된 단말기 관리 기능
- 레거시 시스템 또는 외부 시스템과의 연동을 위한 백엔드 통합 기능

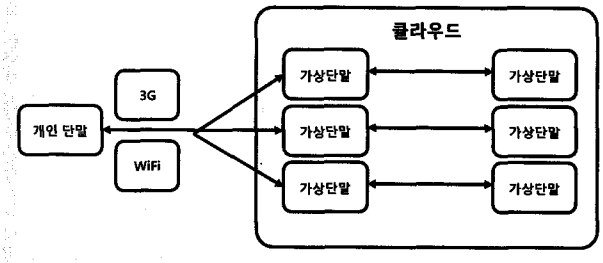
적용분야로는 사내 그룹웨어, 영업지원(SFA : Sales Force Automation), 현장지원(FFA : Field Force Automation), CRM, ERP/MIS 등의 레거시 시스템과 연계되는 모바일 서비스로 활용이 가능하다.

3) 개인 단말-가상 단말 간 협업 기능

스마트 모바일 단말을 사용하는 경우 단말의 종류나 통신 사업자에 종속되지 않고 다양한 서비스와 앱을 사용 할 수 있도록 클라우드에 '가상 단말' 을 구성하고 사용자가 해당 '가상 단말' 을 원할 때 언제 어디서라도 사용할 수 있게 하는 환경을 제공한다. 또한 사용자가 '가상 단말' 을 사용할 때 이 '가상 단말' 은 클라우드 컴퓨팅 기반 위에 구현되기 때문에 '개인 단말' 이 제공할 수 없는 고성능, 대용량 컴퓨팅 능력을 제공받을 수 있게 한다.

개인 단말-가상 단말 간 협업 기능은 다음을 제공 받는다.

- 사용자는 다양한 앱과 서비스를 제공 받을 수 있다.
- 사용자는 모바일 단말 성능 한계를 극복할 수 있도록 클라우드 컴퓨팅 자원을 제공 받을 수 있다.
- 개발자는 단말과 OS에 따라 앱과 서비스를 중복 개발하는 수고를 줄여 개발 효율을 높인다.



(그림 4) 개인 단말-가상 단말 간 협업 개념도

- Any OS on Any Device 구현 요구사항

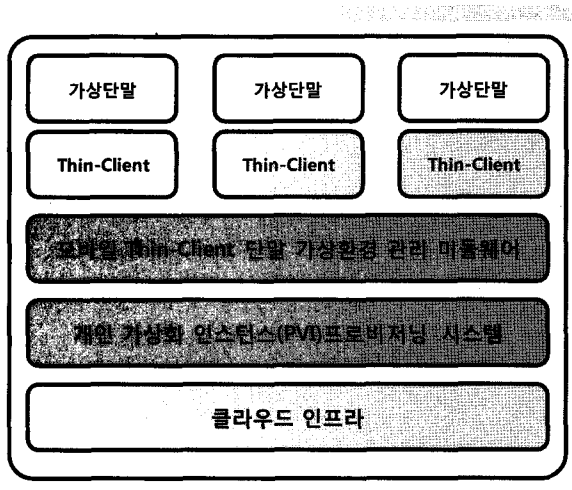
- 모바일 클라우드를 구현하기 위한 첫 단계로 모바일 단말 종류에 구애받지 않고 어떤 OS 든 사용자 단말에서 구현되는 Any OS on Any Device 환경개발
- 모바일 단말 사용자는 클라우드에 '가상 단말' 을 구성하고 이 '가상 단말' 을 사용자 '개인 단말' 에 적용

예를 들면, 아이폰을 사용하는 경우 사용자는 '안드로이드 폰 가상 단말' 을 클라우드로부터 아이폰으로 가져와 최종적으로 안드로이드 폰 사용환경을 이용 가능하다. 따라서 아이폰 사용자도 안드로이드 폰 용으로 만들어진 앱과 서비스를 사용 가능하다. 위 기능을 구현하기 위해 '최적의 모바일 씬 클라이언트 단말 운영을 위한 가상환경 관리용 미들웨어와 씬 클라이언트 앱' 제작이 필요하다.

- 모바일 클라우드 기반 개인 단말 기능 확장 기능

- 모바일 클라우드를 완성하기 위한 단계로 개인 사용자 단말에 구현된 가상 단말에서 실행되는 앱과 서비스가 개인 사용자 단말의 자원을 이용하는 것이 아니라 가상 단말이 실행되고 있는 클라우드 컴퓨팅 자원을 이용가능 환경 제공
- 모바일 클라우드 구현의 핵심인 '가상 단말 실행 환경을 지원하는 개인 가상화 인스턴스(Private Virtual Instance) 프로비저닝 시스템' 을 제작

지금까지 모바일 클라우드 서비스를 위한 플랫폼 및 단말에 필요한 기능을 알아보았다.



(그림 5) 모바일 씬 클라이언트 모델 기본 아키텍처

III. 모바일 클라우드시스템 보안요구사항

모바일 클라우드시스템은 사용자 및 기업에서 정보시스템으로 활용되고 있다. 따라서 모바일 클라우드시스템 또한 정보보호 기능이 필수적으로 요구된다.

본 장에서는 정보보호기술에 대한 정보보증 및 제도들을 알아보고 모바일 클라우드시스템에 대한 보안 요구사항을

도출을 위한 자료로 활용한다.

1. 정보보호 기술

정보보호기술의 발달과 정보화가 확대됨에 따라 정보시스템의 안전한 관리에 대한 중요도가 높아짐에 따라, 정보보증(Information Assurance, IA)에 대한 관심이 증가하고 있다. 이에 따라, 정보보증을 위한 여러 제도들이 시행되고 있으며, 대표적으로 암호모듈수준의 정보보증을 위한 CMVP(Cryptographic Module Validation Program), 정보보호제품수준의 정보보증을 위한 CC(Common Criteria), 정보운영시스템수준의 정보보증을 위한 ISMS(Information Security Management System)등 각 정보보증의 주체에 따라 여러 정보보증제도가 운영되고 있다 [7]. 이러한 여러 정보보증제도 중 정보보호제품 평가인 CC평가에서는 평가를 하기위한 보안요구사항명세서가 필수이며, CC평가 내에서 보호프로파일(Protection Profile, PP)은 보안제품유형별 공통 보안요구사항명세서이며, 보안목표명세서(Security Target, ST)는 특정한 제품의 보안요구사항명세서이다. PP는 CC평가 내의 보안기능 집합으로부터 작성하며, ST는 PP와 평가대상물(Target of Evaluation, TOE)의 가정된 구현환경을 고려하여 작성한다. PP나 ST는 보안제품의 개발을 위한 보안기능요구사항명세서의 역할을 하며, TOE 평가에도 활용된다. 또한 암호모듈평가인 CMVP평가에서도 보안요구사항명세서인 보안정책문서(Security Policy, SP), 아직 국내 · 외에서 평가제도로 시행되지 않는 운영시스템에 대한 평가(ISO/IEC 19791)내의 보안요구사항명세서인 시스템보호프로파일(System Protection Profile, SPP), 시스템보안목표명세서(System Security Target, SST)를 작성한다. 이와 같이 각 정보보증제도내의 평가요소 중 정형화된 보안요구사항명세서 개발에 대한 방법론의 중요성이 점차 증대되고 있다.

2. 모바일 클라우드의 정보보증평가 요구

최근 클라우드시스템은 인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 시스템으로 최근 많은 관심을 받고 있다. 클라우드시스템이 널리 사용되기 위해서 해결해야 할 첫 번째 문제는 보안인 것으로 조사되고 있다. 클라우드시스템의 보안은 사용자의 영역에 따라 개인 사용자와 기업 사용자 분야로 나눌 수 있으며, 개인 사용자는 익명성에 관심을 두고 있고, 기업 사용자는 컴플라이언스에 관심을 두고 있다. 따라서 향후 증가될 것으로 예상되는 클라우드시스템은 이를 사용하는 사용자들의 안정성과 신뢰성을 확보하기 위한 클라우드시스템에 대한 정보보증평가가 요구되고 있다. 그러나 현재 국내 · 외의 정보보증평가(CMVP, CC 평가 등)에서는 클라우드 시스템과 같은 실제 운영 중인 시스템에 대한 평가제도가 확립되지 않았으며, CC와 유사한 체계의 표준문서(ISO/IEC 19791) 개발이 진행 중이다. 클라우드컴퓨팅표준화 관련주요 표준화 동향으로는 OCC, CCIF, OGF, ISO/IEC JTC 1의 SC38/SGCC 등이 있으며, 국내의 경우 지식경제부 기술표준원을 중심으로 클라우드컴퓨팅표준연구회, TTA 클라우드컴퓨팅 포럼등에서 표준화 활동이 진행 중이며 클라우드컴퓨팅 보안 표준은 시작단계라고 볼 수 있다.

이에 따라, 향후 클라우드시스템 평가를 위한 보안요구사항명세서인 클라우드시스템 보호프로파일(System Security Profile)을 개발의 필요성이 크다.

본고에서는 클라우드시스템 보호프로파일의 지속적이고 효율적인 개발을 위하여, 공학적인 개발 방법론과 지원도구의 필요성을 제시한다. 이를 통해, 국가기관들은 정보보호시스템을 효율적으로 구축 및 운영할 것이며 국가기관의 보안관리에 기여할 것으로 기대한다.

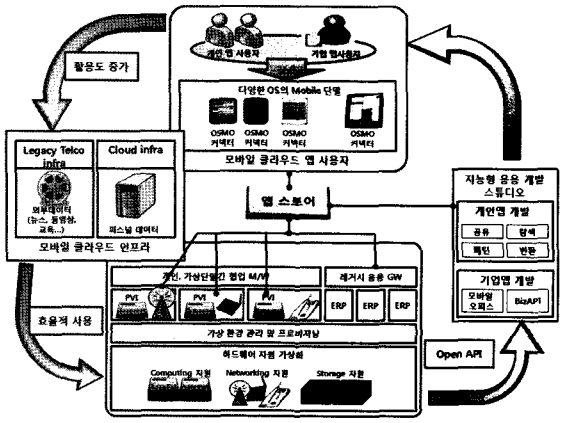
3. 모바일 클라우드시스템을 위한 보호프로파일

본 장에서는 소프트웨어공학 분야에서 보안요구사항을 분석 및 명세하기위한 모델과 정보보호시스템의 평가 및 인증제도들을 조사 및 분석한 결과를 바탕으로 모바일 클라우드시스템의 보안 기술에 대해서 조사하였으며 이를 통해 모바일 클라우드시스템의 보안요구사항명세서를 개발하고 모바일 클라우드시스템 보안요구사항명세서 개발지원을 위한 개발 프로세스를 제시하고 이를 지원하기 위한 지원도구를 제안한다.

1) 모바일 클라우드시스템 서비스 모델

모바일 클라우드시스템 또한 클라우드시스템에서 제공하는 인터넷 기술을 활용하고 IT 자원을 서비스로 제공하는 시스템' 으로 정의할 수 있다. 따라서 기본적인 특징으로는 IT 자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼의 비용을 지불하는 것을 들 수 있

다. 이러한 시스템을 제공하기 위한 서비스로 그 추상화 정도에 따라 분류될 수 있다.



(그림 6) 모바일 클라우드 시스템 구성요소

2) 모바일 클라우드시스템 보안이슈

모바일 클라우드시스템은 IT 자원을 소유하지 않고 일부 또는 모두를 아웃소싱 하는 형태이다. 이런 경우는 필연적으로 보안 문제가 제기될 수밖에 없다.

모바일 클라우드시스템의 보안 이슈는 두 가지 소비자 영역으로 나누어서 생각해 볼 수 있다.

첫 번째는 개인 사용자 관점의 보안이다. 개인 사용자는 이메일, 블로그, 동호회, 사진 및 파일 저장과 공유 서비스를 주로 이용하며, 무료로 제공하는 서비스를 선호하는 특성을 갖는다. 다음은 개인 사용자 관점에서 우려하는 보안 문제는 다음과 같다.

- 개인정보 노출
- 개인에 대한 감시
- 개인 데이터에 대한 상업적 목적의 가공

두 번째는 기업 사용자 관점을 들 수 있다. 기업사용자는 자신이 소유하던 IT 자산을 모바일 클라우드서비스 형태로 제공받기를 원하지만, 자신의 데이터가 타인과 공유되기를 원하지 않는다. 기업 사용자 입장에서 우려하는 보안 문제는 다음과 같다.

- 서비스 중단
- 기업 정보 훼손
- 기업 정보 유출
- 고객 정보 유출
- 법/규제 준수

이와 같이 개인 사용자와 기업 사용자는 모바일 클라우드 시스템에 대한 보안 요구사항이 다르다. 개인 사용자는 익명성 보장에 중점을 두는 반면, 기업 사용자는 IT 컴플라이언스에 중점을 두는 경향이 있다.

기업 사용자의 보안 고려사항은 Cloud Security Alliance에서 가이드로 제시한 것을 참고해 볼 수 있다. Cloud Security Alliance는 클라우드시스템의 안전성 증진과 사용자 교육을 목적으로 만든 비영리 기관으로, 다음과 같은 보안 고려사항을 제시하고 있다 [8],[9].

① Governance and Enterprise Risk Management
② Legal
③ Electronic Discovery
④ Compliance and Auit
⑤ Information Lifecycle Management
⑥ Portability and Interoperability
⑦ Traditional Security, Business Continuity and Disaster Recovery
⑧ Data Center Operations
⑨ Incident Response, Notification and Remediation
⑩ Application Security
⑪ Encryption and Key Management
⑫ Identity and Access Management
⑬ Storage
⑭ Virtualization

4. 클라우드 시스템 패턴 및 보안기능요구 비교

1) NIST SP 800-53A

NIST SP 800-53A는 미연방정보시스템내의 정보보호 통제의 효과성을 평가하기 위한 지침이다. 구체적 목적은 다음과 같다.

- 일관성 있고, 비교가능하고, 반복 가능한 정보보호 통제에 대한 평가
- 정보보호 통제 효과성에 대한 비용-효과적인 평가 가능

〈표 1〉 NIST SP 800-53A와 ISO/IEC 19791의 비교

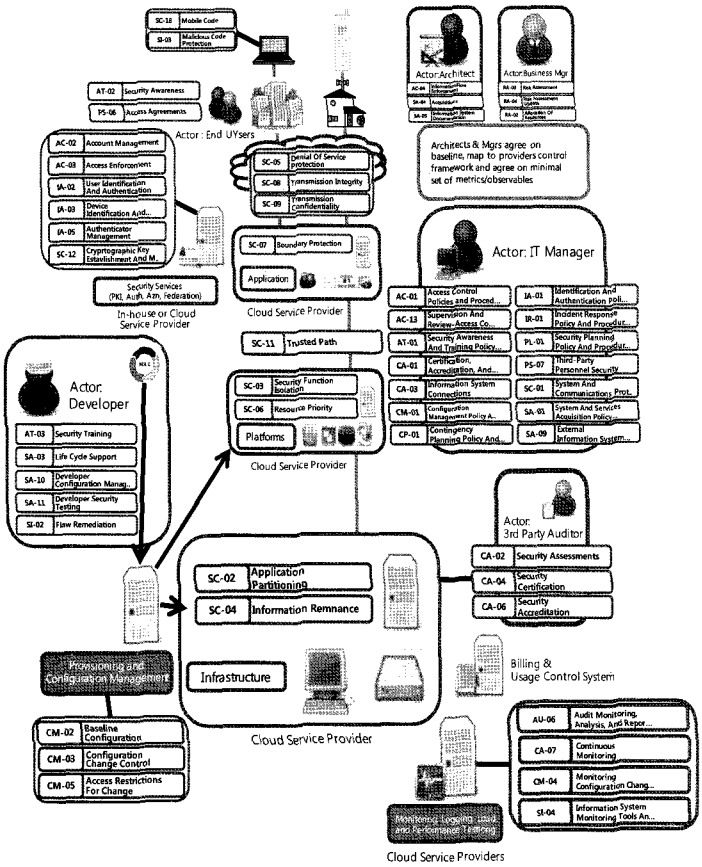
지침 / 통제 영역	NIST SP 800-53A	ISO/IEC 19791
접근통제 영역	AC-01 접근통제 정책 및 절차 AC-02 계정관리 AC-03 접근강화 AC-04 정보흐름 강화 AC-13 슈퍼비전 및 검토-접근통제	FOM_PSN 인사보안책임 관리 FOS_NET 정보시스템 망보안 FOS_MON 정보시스템 감시 FOA_PRO 프라이버시자료보호
의식 및 훈련 영역	AT-01 보안 인식 및 훈련 정책 및 절차 AT-02 보안 인식 AT-03 보안 훈련	FOM_PSN 인사보안책임 관리 FOS_PSN 정보시스템 인사통제 FOS_RCD 정보시스템 기록 FOA_PRO 프라이버시자료보호
감사 및 책임성 영역	AU-06 감사 감시, 분석, 및 보고	FOS_MON 정보시스템 감시 FOS_CNF 정보시스템 형상 FOS_POL 정보시스템 정책
인증, 인가 및 보안 영역	CA-01 인증, 인가, 및 보안 평가 정책 및 절차 CA-02 보안 평가 CA-03 정보시스템 접속 CA-04 보안 인증 CA-06 보안 인가 CA-07 연속적 감시	-
형상관리 영역	CM-01 형상 관리 정책 및 절차 CM-02 베이스라인 형상 CM-03 형상 변경 통제 CM-04 감시 형상 변경 CM-05 변경에 대한 접근 제약	FOS_CNF 정보시스템 형상 FOS_NET 정보시스템 망보안 FOS_MON 정보시스템 감시
비상계획 영역	CP-01 비상계획 정책 및 절차	-
사건대응 영역	IR-01 사건 대응 정책 및 절차	FOS_RCD 정보시스템 기록
계획 영역	PL-01 보안 계획 정책 및 절차	FOS_RCD 정보시스템 기록
인사보안 영역	PS-06 접근 동의 PS-07 제삼자 인사 보안	FOS_MON 정보시스템 감시 FOT_COM 제삼자동의 FOT_MNG 제삼자관리
위험평가 영역	RA-03 위험 평가 RA-04 위험 평가 갱신	-
관리영역	SA-01 시스템 및 서비스 획득 정책 및 절차 SA-02 자원할당 SA-03 생명주기 지원 SA-04 획득 SA-05 정보시스템 문서 SA-09 외부 정보시스템 서비스 SA-10 개발자 형상 관리 SA-11 개발자 보안 시험	FOS_CNF 정보시스템 형상
시스템 및 통신 보호 영역	SC-02 응용 분할 SC-03 보안기능 격리 SC-04 정보 흐름 SC-05 서비스거부 보호 SC-06 자원 우선순위 SC-07 범주 보호 SC-08 전송 무결성 SC-09 전송 기밀성 SC-11 신임된 경로 SC-12 암호키 설립 및 관리 SC-18 모바일 코드	FOS_NET 정보시스템 망보안 FOS_MON 정보시스템 감시 FOS_PSN 정보시스템 인사통제
시스템 및 정보 무결성 영역	SI-02 결함 치유 SI-03 악성 코드 보호 SI-04 정보시스템 감시 도구 및 기법	FOS_RCD 정보시스템 기록 FOP_RMM 삭제가능장비

- 정보시스템 운영으로부터 초래되는 위험에 대한 인식 및 이해도 제고
- 정보보호 인가 및 FISMA 준거를 판단하기 위한 보다 완전하고 신뢰성 있는 정보제공

(그림 7)의 클라우드 시스템 패턴은 OSA에서 제공한 클라우드 시스템 평가 패턴을 보이며, 다음의 표에서는 각 도메인별로 NIST SP 800-53A의 보안통제사항들을 조사한 결과이다. 또한 다음의 NIST SP 800-53A와 ISO/IEC 19791의 기능요구사항과 비교하였다.

2) 모바일 클라우드시스템의 보안요구사항 정의 (SR_MCS : Security requirements of mobile cloud system, 이하 SR_MCS라 칭함)

모바일 클라우드 시스템의 보안기능요구사항을 개발하기



(그림 7) 클라우드 시스템 패턴

위한 절차(Process)가 개발되어야 한다.

첫째, SR_MCS의 기능요구사항은 다음과 같다.
- ISO/IEC 19791의 SPP/SST 패러다임(개념과 용어)을 사용하고 다른 보안평가표준들과 호환적일 것
- 모바일 클라우드 시스템과 관련 "자산"을 파악하고 자산의 가치와 "위험" 및 "취약성" 분석 결과를 바탕으로 하여, 클라우드 시스템내의 "보안목적"과 목적을 달성하기 위한 "보안대책"을 세우고 ISO/IEC 19791로부터 필요한 "보안기능"을 선택함(ISO/IEC 19791의 SPP 개념을 따른 것임)
- 기존의 CC-ToolBox내의 PKB 및 기존 PP와 호환성을 유지하기위해 PKB의 자료와 기존 PP의 내용을 사용함
- 기존의 PKB내의 가정, 위협 및 정책문장과 기존 PP에서의 문장을 고려하여, 일반적이고 객체지향적인 가정(또는 실제 환경), 위험 및 정책문장을 미리 정의하여 데이터베이스를 구축
- 재사용가능하고 일반적이고 정형적인 위험문장, 보안정책문장 등의 작성방법이 필요
- 모바일 클라우드시스템 이외에도 유사한 운영시스템수준의 보안요구사항뿐 아니라 보안제품을 위한 보안요구사항명세서를 개발할 때 사용할 수 있도록 할 것
- SR_MCS Process를 지원하는 도구를 제공할 것
- 다수의 개발자가 협동하여 보안기능요구사항명세서를 개발할 수 있도록, 그룹웨어 기능을 제공할 것

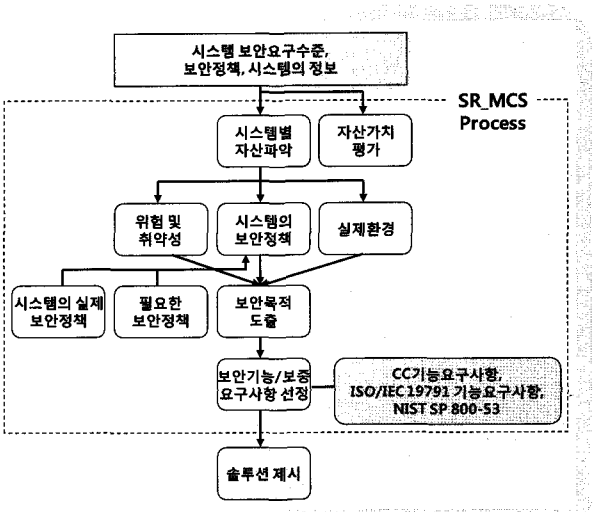
둘째, 성능요구사항은 다음과 같다.
- 모바일 클라우드 시스템의 자원 가치, 위험, 취약성을 결합한 조직의 "위험수준"을 고려하여 최적의 보안기능(보안대책)들을 선택할 수 있도록 함
- 도구는 실시간적으로 작동될 필요는 없음
- 다양한 수준의 사용자를 지원해야함
- 각 조직에서 사용해야함으로 도구의 이식성이 높아야함

셋째, 보안요구사항은 다음과 같다.
- SR_MCS도 보안기능을 요구하므로 도구 사용자의 종류와 각 사용자의 역할에 맞는 자료 및 기능에 대한 접근권한 방식의 통제가 필요함
- SR_MCS 개발 시 조직의 자산 가치 및 취약성에 관한 정보 등은 기밀사항이므로, "기밀성" 기능이 필요함
- SR_MCS문서는 "무결성"이 유지되어야하며 SR_MCS은 "가용성"이 유지되어야 하며, SR_MCS 개발 시의 참여자들의 "책임성(accountability)" 기능도 제공되어야 함

IV. SR_MCS 프로세스 및 보안기능 요구사항명세서 작성도구

1. SR_MCS 프로세스

아래의 (그림 8)은 SR_MCS 프로세의 도출과정을 나타낸다. 특히, 모바일 클라우드시스템 분석, 실제 환경, 위험 및 보안정책을 "모바일 클라우드시스템 보안환경"이라 하며 정확한 보안환경을 분석하기 위해서는 "위험분석"을 우선 실시해야 한다. 위험분석은 본 연구의 범위 밖의 사항이다.



(그림 8) SR_MCS 프로세스

SR_MCS 개발시의 참여자와 그 역할은 다음과 같다.
- SR_MCS 작성자 : 모바일 클라우드 시스템 담당자 또는 자문을 받는 전문가이며, 모바일 클라우드 시스템의 보안환경(업무, 자산, 위험, 취약성, 실제환경, 보안정책)을 분석하여 최소의 비용으로 최대의 보안기능을 수행할 수 있도록, 조직의 CLS-SFRS를 작성함
- 시스템 담당자 : 모바일 클라우드 시스템 담당자이며

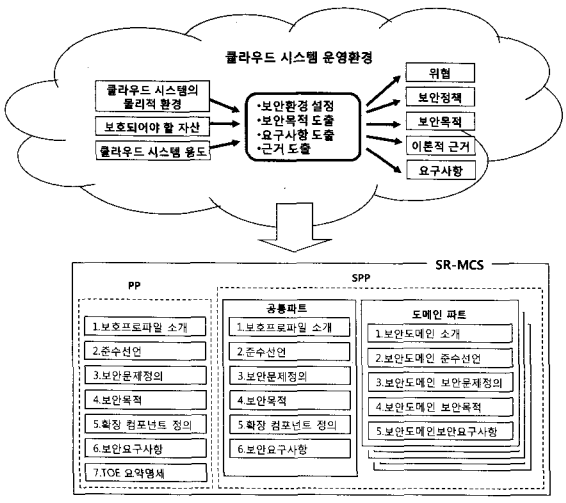
〈표 2〉 SR_MCS Tool의 주요기능

기능클래스	세부기능명	기능설명
보안 환경 분석	시스템 자산 파악	상세 자산 파악 기능
	자산가치 평가	파악된 자산에 대한 정성 / 정량 가치평가 기능
	위협/위험문장 생성	시스템 자산별 위협문장 생성 기능
	실제환경문장 선택	공통실제환경목록 중에서 시스템을 위한 실제환경문장 선택
	보안정책 선택	공통보안정책목록 중에서 시스템을 위한 보안정책문장 선택
보안 요구사항 분석	보안목적 도출	선택된 위협 / 위험 및 정책을 통해 관련 보안목적문장 도출 기능
	보안기능 선정	도출된 보안목적별 구현가능한 보안기능 선택기능
	보안솔루션 제시	선정된 보안기능을 구현한 보안솔루션 제시기능
CLS-SFRS 작성	보안요구사항생성	보안요구사항 생성기능
관리 도구	프로젝트 관리	개발 프로젝트 생성 및 열기 기능
	역할기반 접근통제	CLS-SFRS Tool에 대한 역할기반 통제 기능

SR_MCS 작성자에게 해당조직의 보안환경 정보를 제공함

SR_MCS 개발에 필요한 조직의 정보목록은 다음과 같다.

- 모바일 클라우드 시스템의 주요업무
- 문서화된 보안정책
- 모바일 클라우드 시스템의 응용시스템 구조(HW, 시스템SW, 네트워크, 응용SW 등)
- 모바일 클라우드 시스템에서 관리하는 자료유형 및 비밀수준
- 클라우드 시스템의 각종자산(IT, 자료 등)의 정보보안 취약성 또는 위험
- 클라우드시스템의 주요 보안목적



〈그림 9〉 SR_MCS의 전체 구조

2. SR_MCS 주요기능 및 구조

본 장에서는 모바일 클라우드시스템을 위한 보안요구사항명세서를 개발하기 위하여 조사 및 분석한 모바일 클라우드 시스템의 취약성 및 위협과 제시한 SR_MCS Process를 통해 자동화된 보안요구사항명세서 개발을 지원하기 위한 자동화 도구를 설계 및 구현한다. 특히, ISO/IEC 19791의 SPP 작성지침 및 기존의 IT보안인증사무국에서 발표된 보호프로파일 19종 기반으로 하여 구현하였다. CC나 보안평가 및 관리에 대한 전문적인 지식이 없는 일반 시스템의 관리자 및 사용자라 할지라도 쉽게 보안요구사항명세서를 개발할 수 있도록 도구를 개발하였다.

V. 분석 및 평가

본 장에서는 제시한 방법론과 모델 그리고 지원도구를 타 모델 등과 비교 분석한 결과를 보인다.

〈표 3〉 체계별 보안기능 분류

기능클래스	세부기능명
암호모듈수준 (CMVP)	암호모듈명세, 암호모듈포트와 인터페이스, 역할-서비스-인증, 유한상태모델, 물리적보안, 운영환경, 암호키관리, EMI/EMC, 자체시험, 설계보증, 기타 공격의 완화
보안제품/시스템수준 (CC, 본체계)	보안감사, 통신, 암호지원, 사용자데이터 보호, 식별 및 인증, 보안관리, 프라이버시, TSF보호, 자원활용, TOE 접근, 안전한 경로/채널
보안관리 수준 (FISMA)	관리(위험평가, 보안계획, 시스템 및 서비스 획득, 보안통제 검토, 처리인가), 운영(인사보안, 물리적 및 환경보호, 비상계획 및 운영, 형상관리, HW/SW 유지보수, 시스템 및 정보 무결성, 매체보호, 사건반응), 기술(보안인식 및 훈련, 식별 및 인증, 논리적 접근통제, 책임성(감사추적 포함), 시스템 및 통신보호)
보안관리 수준 (한국 ISMS)	정보보호정책, 정보보호조직, 외부자 보안, 정보자산분류, 정보보호 교육 및 훈련, 인적보안, 물리적 보안, 시스템 개발보안(분석 및 설계보안 관리, 구현 및 이행보안관리, 변경관리), 암호통제, 접근통제(접근통제정책, 사용자 접근관리, 접근통제 영역), 운영관리, 전자거래보안, 보안사고 관리, 검토-모니터링 및 감사, 업무연속성 관리

1. 보안기능의 비교

기존의 평가체계에서는 〈표 3〉과 같이 보안기능을 서로 다르게 분류하고 있다

- 보안관리 수준(FISMA와 ISMS)에서는 관리, 운영, 기술 차원과 보안정책, 조직구성, 위험관리, 대책구현, 사후관리차원에서 각종 보안기능을 분류하고 있다.
- 보안관리 수준에서의 "보안통제" 개념과 본 연구나 CC 및 ISO/IEC 19791에서의 "보안기능" 개념 간에는 유사한 용어를 사용하므로 혼동이 발생한다.
- 본 SR_MCS는 CC와 동일한 보안기능 분류체계를 사용하므로, CC와 호환성이 있다.

2. 보안수준의 비교

CMVP에서는 4등급으로, CC에서는 7등급으로 평가하고 있으며 CMVP와 CC간에는 대응관계가 없다. 한국 ISMS에서 인증결과는 등급이 없이 "인증" 또는 "불인증"이다. 특히, FISMA에서는 정보시스템의 기밀성(C), 무결성(I) 및 가용성(A) 차원에서 각각 3등급으로 "잠재적 영향수준"(즉, 보안분류)을 정의하고 있으므로, 전체적으로 9가지 등급이 존재한다. 본 고에서는 ISO/IEC 19791의 평가등급인 2등급(성공/실패)으로 정하고 있다.

〈표 4〉 CC ToolBox와 SR_MCS v1.0의 비교

비교항목 \ 도구	CC ToolBox	SR_MCS
기능	PP/ST	PP/ST, SPP/SST, SRS
작성과정	PP 작성가이드(ISO/IEC 15446)	CLS-SFRS Process
자산 분석	자산분석기능 없음	자산분류체계 및 가치평가방법제시
등급 분류	없음	보안수준 결정을 통한 2가지 등급 분류
DB크기 (미리 정의된 문장수)	PKB내에 미리 정의된 위협카테고리(7종) - 위협(30종) - 공격(109종) 정책카테고리 - 일반정책문장(10종) - 정책문장(35종) 가정카테고리(6종) - 가정문장(38종) 보안목적(157종) 등급별 공통문장목록 공통가정(71종*3등급=213종)	위협문장(6720종) 공통정책(50종*3등급=150종) PKB문장목록 확장 PKB위협(115종*3등급=345종) PKB정책(41종*3등급=123종) PKB목적(163종*3등급=489종)
문장의 추가여부	개발자가 추가함 각 문장의 생성규칙 없음	개발자가 추가함 각 문장의 생성규칙이 정의됨 (객체지향방법)
도구의 보안기능	없음	역할기반접근통제(RBAC) 기능 가짐
웹기능	Stand alone 용	웹 서버에 설치하여 인터넷으로 사용가능
사용자 인터페이스	문자위주의 윈도우	폼 기반 GUI
출력물	불완전하게 출력	편집된 상태로 출력(PDF 등)
사용자지침	없음	각 단계별로 상세하게 처리함

3. 지원도구의 비교

본 SR_MCS과 유사한 지원도구로써, 기존의 CC ToolBox이 있으며, SR_MCS에서는 단점들을 다소 해결하였다. 〈표 4〉는 두 도구를 비교한다.

- PBK에서는 기존 PP의 환경부분을 모두 포함하지는 못하고 있다. 예를 들어, 보안정책문장은 미 국방부의 보안정책만을 포함하고 있다.
- PBK내의 미리 정의된 정책, 위협 및 가정을 선택하기 위해서는 TOE의 관계자(예, 개발자, 개발관리자, 사용자, 사용관리자)로부터 정보를 얻기 위한 인터뷰에 대한 내용이 부족하며 오직 문장의 선택(즉, 포함 또는 불포함) 기능만 제공한다.
- 평가대상물의 자산에 대한 평가방법 및 분류체계에 대한 지침이 없다. PP를 작성할 때, 평가대상물이 보호해야 할 자산을 파악하는 일은 매우 중요하다.
- 세부적인 PP 생성절차에 대한 지침이 없으며, PKB는 오직 참조용으로 사용될 뿐이다.

VI. 결 론

본 논문에서는 모바일 클라우드시스템의 평가를 목적으로 기존의 보안요구사항을 분석하고 개발 프로세스 및 지원도구를 제시하였다. 본고에서 제시한 내용은 다음과 같이 두 가지로 정리할 수 있다.

- SR_MCS Process : 클라우드 시스템 모델을 토대로 실제 보안요구사항명세서를 개발하기 위한 세부 절차를 제시하였다.

- SR_MCS Process에 따라 보안요구사항명세서를 쉽게 작성할 수 있도록 CC 및 ISO/IEC 19791 활용하여 자동화된 도구를 개발하였다.

특히, 제시한 SR_MCS은 비용 · 효과적이고 보안 공학적으로 각급 조직의 정보보호시스템을 구축함으로써 다음과 같은 장점을 갖는다.

- 측면에서, 첫째, 시스템별로 공통적인 업무에 대한 보안요구사항을 개발 및 보급되며, 이는 도메인 컴포넌트 개발을 위한 보안기능요구사항이 된다. 둘째, 보안요구사항 개발 지원도구에 의한 시스템별 보안요구사항을 쉽게 개발하고 유사시스템 간의 보안요구사항의 재사용이 촉진된다. 셋째, 조직의 정보보호시스템을 필요한 수준만큼의 보증수준으로 개발하므로 경제적이다.
- 보안공학적 측면에서, 10년 이상의 역사를 가지고 표준화된 개념인 CC와 PP 개념을 사용해 체계적으로 정보보호시스템의 개발을 촉진한다. 또한, 보안요구사항은 정형화된 요구사항명세서의 역할을 하며 응용시스템 관리자와 개발자의 소프트웨어 공학 및 보안공학기술력이 향상된다.
- 국가보안적 측면에서, 보안요구사항에 따라 각 조직의 정보보호시스템의 보안기능을 개발하므로 보안성이 제고되며, 향후 운영시스템 평가제도 및 보안성 검토 제도 등과 손쉽게 통합하여 평가 및 인증이 가능해진다.

참 고 문 헌

[1] 이정아, "모바일클라우드 서비스 국내외 정책 추진 현황", KT경제경영연구소 DigiEco Focus, 2010 (http://www.digieco.co.kr).

[2] CC, "Common Criteria for Information Technology Security Evaluation," Version 3.1 Revision 3, CCMB-2009-07-001, http://www.commoncriteriaportal.org, July. 2009.

[3] ISO/IEC DTR 15443-3, "Information technology-Security techniques-A framework for IT security assurance," July. 2005.

[4] 방영환, 고갑승, 신재인, 이강수, "정보보증제도 분석과 보안제품 적합성 평가체계의 설계, 보안공학연구회, 6권 6호, 2009.12

[5] 김영선, 고갑승, 신재인, 이강수, "정보보호 운영시스템 수준의 보안기능요구사항명세서 지원도구 개발", 7권 1호, 2010.2

[6] 한국인터넷진흥원, "2010국가정보보호백서", 2010.4.

[7] 방영환, 고갑승, 신재인, 이강수, "정보보증제도 분석과 보안제품 적합성 평가체계의 설계, 보안공학연구회, 6권 6호, 2009.12

약 력

방 영 환

1997년 한남대학교 컴퓨터공학과 공학사
2002년 대전대학교 컴퓨터공학과 소프트웨어공학전공 공학석사
2006년 한남대학교 컴퓨터공학과 시스템소프트웨어공학전공 공학박사
2006년 한국과학기술정보연구원 선임연구원
2008년 ~ 2010년 클라우드컴퓨팅포럼 사무국장
2010년 ~ 현재 ISO/JTC/SC38 국제표준전문위원
2010년 ~ 현재 클라우드데이터센터포럼 운영위원
2010년 ~ 현재 한국생산기술연구원 선임연구원
관심분야 : 슈퍼컴퓨팅, 개방형모바일클라우드시스템, 정보보호위험분석평가

정 성 재

1998년 한남대학교 컴퓨터공학사
2003년 한남대학교 컴퓨터공학석사
2011년 한남대학교 컴퓨터공학박사
2005년 ~ 2010년 한남대학교 국제IT교육센터 전임강사
2011년 ~ 현재 ㈜스컴씨엔에스 연구지원팀/부장
관심분야 : 리눅스, 오픈소스, 서버 가상화, 클라우드 컴퓨팅 등

황 선 명

1982년 중앙대학교 전자계산학과 이학사
1984년 중앙대학교 소프트웨어공학전공 이학석사
1987년 중앙대학교 소프트웨어공학전공 이학박사
1988년 ~ 현재 대전대학교 교수 공과대학장
2000년 ~ 현재 한국정보처리학회 논문지 편집부 위원장
2000년 ~ 현재 한국 S/W프로세스 심사인 협회(KASPA) 운영위원
관심분야 : 소프트웨어공학, 차세대컴퓨팅기술, 모바일클라우드