http://dx.doi.org/10.14400/JDC.2014.12.5.263

모바일 클라우드 서비스 환경에서의 보안위협에 관한 연구

한정수
백석대학교 정보통신학부

Security Threats in the Mobile Cloud Service Environment

Jung-Soo Han
Division of Information & Communication, Baekseok Univ.

요 약 모바일 클라우드 서비스는 모바일 단말을 통해 클라우드 서비스를 제공하는 것으로서, 모바일 기기의 컴퓨팅 처리 성능 한계, 저장 공간 제약 등으로 인해 모바일 단말에서 처리해야할 작업 및 데이터의 일부를 클라우드 환경으로 이동시켜 처리하는 서비스이다. 모바일 클라우드 서비스 활성화의 장애요인으로 서비스의 안정성에 대한 우려와 데이터 보안성 및 기밀성의 보안에 대한 우려가 높다. 특히 모바일 서비스와 클라우드 서비스가 융합되어, 각각의 위협이 복합적으로 파생되어 발생될 것으로 예상되고 있다. 이에 본 연구에서는 모바일 클라우드 서비스 유형과 모바일 클라우드에서 발생할 수 있는 보안위협을 정의하고, 모바일 앱에서의 보안 대응방안과 기업의 대응방안을 제시하였다. 모바일 앱에서의 보안은 사용자 정보 보호를 중심으로 한 모바일 애플리케이션 검증을 제시하였으며, 기업의 대응방안으로는 클라우드 제공자와 사용자 관점에서의 대응방안을 기술하였다.

주제어 : 모바일 클라우드 서비스, 보안위협, 모바일 앱

Abstract Mobile Cloud Service will provide cloud services through mobile devices. Because storage space constraints and computing process performance limitations of mobile devices, this service will process in the cloud environment after moving works and data that have to process in mobile terminal. The obstacles of mobile cloud service activity will have concerned high about the reliability service, data security, and the confidentiality security. In particular, in convergence of mobile services and cloud services, each threats are expected to be generated complicatedly. In this paper, we define the type of mobile cloud services as well as security threats that can occur in mobile cloud. Also we suggest security countermeasures in mobile app. and enterprises countermeasures. We suggest verification of mobile applications for user information protection about security countermeasures in mobile app. Also we describe the cloud providers responsibility and user responsibility about enterprises countermeasures.

Key Words : Mobile Cloud Service, Security Threats, Mobile App.

1. 서론

최근 우리의 일상을 가장 많이 바꿔 놓은 기술을 하나만 꼽으라면 단연코 스마트폰을 중심으로 한 모바일 기술이라고 할 수 있을 것이다. 스마트폰이 우리의 생활에 엄청난 영향을 미칠 수 있었던 요인은 CPU 등의 하드웨

* 본 논문은 2014년도 백석대학교 대학연구비에 의하여 수행된 것임.
Received 21 March 2014, Revised 25 April 2014
Accepted 20 May 2014
Corresponding Author: Jung-Soo Han(Division of Information & Communication, Baekseok Univ.)
Email: jshan@bu.ac.kr

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

어 기술과 통신 기술의 발전을 들 수 있지만, 그 이면에는 클라우드의 발전이라는 또 하나의 중요한 요소가 있다. 클라우드는 사용자들의 콘텐츠를 생산하고, 보관하고, 공유하고, 소비하는 활동들을 더욱 편리하게 할 수 있도록 해줌으로써 스마트폰의 가치를 한층 높여 주는 것이라 할 수 있다. 클라우드는 스마트폰뿐 만 아니라 테블릿 등의 모바일기기, 기존의 개인용 컴퓨터, 대용량 서버 등에 이르기까지 큰 변화를 이끌고 있다. 클라우드 기술이 있기 때문에 우리가 즐기는 콘텐츠와 우리가 사용하는 기기와 우리가 활용하는 서비스가 이동성을 갖게 되었다. 스마트폰을 둘러싼 모바일의 발전 때문에 클라우드가 발전할 수 있었지만, 클라우드의 발전이 있기 때문에 모바일의 발전이 견인되는 측면도 있으니 모바일과 클라우드는 서로 상생의 관계를 맺고 있다 할 수도 있겠다.

모바일 클라우드 서비스는 언제 어디서나 인터넷에 접속할 수 있는 모바일 단말을 통해 클라우드 서비스를 제공하는 것으로서, 모바일 기기의 컴퓨팅 처리 성능 한계, 저장 공간 제약 등으로 인해 모바일 단말에서 처리해야할 작업 및 데이터의 일부를 클라우드 환경으로 이동시켜 처리하는 서비스이다[1]. 국내 클라우드 시장은 '14년까지 2조원 규모로 급성장할 것으로 예상하고 있지만, 모바일 클라우드 서비스 활성화의 장애요인으로 서비스의 안정성에 대한 우려와 데이터 보안성 및 기밀성의 보안에 대한 우려가 높다. 특히 모바일 서비스와 클라우드 서비스가 융합되어, 각각의 위협이 복합적으로 파생되어 발생될 것으로 예상되고 있다. 모바일 기기의 분실로 인한 정보유출, 외부에 위탁한 정보에 대한 접근통제 우회, 가상화 취약성을 이용한 공격, 자원 집중화에 따른 DDoS 서비스 장애 등 클라우드 환경에서의 보안 위협에 대해 기존 IT 기술로 충분히 대응이 가능한지에 대한 연구가 제대로 이루어지지 않고 있으며, 모바일 클라우드 특성에 최적화된 보안 기술에 대한 요구사항 분석 또한 구체화되지 못하고 있는 실정이다. 이에 본 연구에서는 모바일 클라우드 서비스 유형과 모바일 클라우드에서 발생할 수 있는 보안위협을 정의하고, 모바일 앱에서의 보안 대응방안과 기업의 대응방안을 제시하였다. 본 논문의 구성 다음과 같다. 본 연구는 서론에 이어 제 2 장에서는 모바일 클라우드와 클라우드 서비스 유형에 대해 살펴보고, 제 3 장에서는 모바일 클라우드 보안 위협 요소를 정의하고, 제 4장에서는 보안 대응 방안에 대해 기술하며, 끝으로 결론을 맺는다.

2. 연구배경

2.1 모바일 클라우드

모바일 클라우드 컴퓨팅 개념은 필요한 만큼 사용하고 쓴 만큼 지불하는 클라우드 컴퓨팅과 모바일 서비스를 결합한 것이다. 모바일의 개념은 스마트폰은 물론 노트북, 넷북, PDA등을 모두 포함한다. 따라서 모바일 클라우드란 다양한 모바일 단말기를 통해 클라우드로부터 서비스를 지원받는 모델이라고 할 수 있다[2]. 모바일 클라우드 서비스는 모바일 단말에서 처리해야할 작업 및 데이터 저장의 일부를 클라우드 컴퓨팅 환경으로 이동시켜 처리하고 모바일 단발에서 처리결과를 보여주는 에플리케이션이다[1]. 대표적인 모바일 클라우드 서비스로는 애플의 MobileMe가 있는데, 아이폰, 노트북 등 모바일 기기와 웹 사이트 간에 자동으로 동기화되는 기능이 핵심이라 할 수 있다. 마이크로소프트는 MyPhone서비스를 제공하고 있는데, 윈도우 모바일 기반의 스마트폰 콘텐츠에 대한 온라인 접속을 제공하고 문자·사진·비디오 등 다양한 데이터에 대한 동기화와 백업·복원 기능을 지원한다. 또한, 실시간 업무를 가능하게 하는 기업형 모바일 서비스는 thinktree office mobile, Enterprise disk, 삼성 모바일 클라우드 서비스 등이 있다. 기존 모바일 서비스에 모바일 단말의 이동성 특징이 적용된 서비스에는 구글 맵 네비게이션, ShopSavvy, Foursqure, Gowalla, Yelp가 있으며, 증강현실 서비스에는 Layer, Acrossair가 있다. 모바일 클라우드 서비스는 이동환경에서 개인이 소유한 단말의 특성을 강화시키고 모바일 단말의 제약을 극복할 수 있는 다양한 서비스를 제공한다.

2.2 클라우드 서비스 유형

IT 서비스 환경이 개인용 PC 환경에서 클라우드 컴퓨팅으로 변하면서 인터넷을 통해 대용량의 컴퓨터 집합에 접속하여 애플리케이션 스토리지 OS 등 필요한 IT 자원을 원하는 시점에 필요로 하는 만큼 골라서 사용하는 IT 서비스 패러다임이 변화하였다. 이에 따라 기존의 컴퓨팅 환경에서는 이용자가 데이터 및 컴퓨팅 자원, 소프트웨어를 직접 소유・관리해야 했지만, 클라우드 컴퓨팅 환경에서는 컴퓨팅 자원 및 소프트웨어를 클라우드 서비스 사업자로부터 임대하여 사용한다. 다시 말해, 이용자는 모든 자원을 가상화된 형태로 인터넷을 통해 제공받

을 수 있다. 따라서 기존의 컴퓨팅 환경에서는 이용자가 모든 자원의 구매, 환경 구축 및 폐기까지의 전 과정을 직접 처리해야 했다. 하지만 클라우드 컴퓨팅 환경에서는 이용자가 온라인으로 필요한 자원을 신청하기만 하면 된다. 구축된 환경을 빠르고 손쉽게 제공받을 수 있는데다 폐기의 과정 또한 간단하다는 이점이 있다. 또한 클라우드 컴퓨팅 환경에서 제공되는 스토리지 제공 서비스, 소프트웨어 임대 서비스의 경우 웹하드, SBC(Server Based Computing), ASP(Application Service Providing) 등 기존의 응용 인터넷 서비스와 유사해 보일 수 있다. 하지만, 클라우드 서비스는 동기화 및 데이터 가공 등 가상화 서버를 기반으로 새로운 기능 제공이 가능하다. 특히, 사용자별로 본인의 환경을 간편히 구성할 수 있고 수시로 변경 가능한 장점이 있다. 기존의 인터넷 서비스와 클라우드 서비스의 차이점은 다음과 같다.

- 기존의 응용 인터넷 서비스
  - 웹하드 : 단순 파일 저장, 파일 다운 로드 후 게인 PC에 저장
  - SBC : 단일 서버로 서비스 제공자가 특정 사용자를 대상으로 환경 구축 후 사용
  - ASP : 사업자가 지원하는 고정적인 서비스만 가능
- 클라우드 서비스
  - 스토이지 서비스 제공 : 다양한 단말기와 데이터 동기화 서비스 제공, 서버에서의 데이터 가공 서비스 지원
  - 가상서버/데스크탑 서비스 : 가상화된 서버 그리드로 서비스 제공자는 서비스 제공을 위한 공동 플랫폼만 구축
  - S/W 제공 서비스 : 사용자가 원하는 S/W들로 사용 환경을 동적으로 구성할 수 있는 기능 제공

클라우드 서비스는 서비스의 특징에 따라서 SaaS, PaaS, HaaS, IaaS 등으로 구분할 수 있다[3,4].

- SaaS(Software as a Service) : 클라우드 서비스 중 SaaS는 어플리케이션을 사용자에게 빌려주는 서비스를 말한다. 일반 컴퓨터는 소프트웨어 자체를 실행할 수 있지만, 스마트폰과 태블릿 PC 같은 기기는 컴퓨터에서 실행하는 모든 소프트웨어를 가지고 있지 않다. 이런 경우 SaaS 클라우드 서비스를 통해 필요한 소프트웨어 서비스를 받을 수 있다. 모든 소프트웨어를 클라우드 서비스만으로 제어할 수 있다. 현재 대부분의 사용자가 클라우드 서비스라고 알고 있는 N드라이브, 구글드라이브 등과 같은 것들이 이에 속한다.
- PaaS(Platform as a Service) : PaaS는 플랫폼을 서비스하는 것을 말한다. 플랫폼이란 프로그램을 실행할 수 있는 윈도우· 리눅스와 같은 운영체제와 특정 프로그램 언어를 개발하기 위해서 만들어진 환경을 뜻한다. 주로 데이터베이스를 포함해서 특정 개발 환경의 플랫폼을 서비스 받아 개발하는 곳에서 사용된다.
- HaaS(Hardware as a Service) : HaaS는 특정 하드웨어가 필요한 경우에 제공 업체로부터 하드웨어를 서비스 받는 것을 말한다. 특정 하드웨어 자체를 구축하기 어려운 경우에 이 서비스를 받을 수 있다. HaaS와 PaaS는 필요에 따라서 동시에 서비스를 진행하기도 한다. 예를 들어 아마존의 가상서버 임대서비스 아마존 EC2, 스토리 임대 서비스 아마존 S3 같은 것들이 이에 속한다.
- IaaS(Infrastructure as a Service) : IaaS는 서버와 스토리지, 네트워크를 가상화 환경으로 만들어서 필요에 따라 자원을 사용할 수 있게 해주는 서비스를 말한다. 특히 기업에서 많이 사용하는 서비스이다.

3. 모바일 클라우드 보안 위협 요소

3.1 보안 이슈

모바일 클라우드는 점점 더 우리 일상의 깊숙한 곳으로 파고들고 있고 우리는 그 변화에 익숙해져가고 있다. 빠르게 진화하고 있는 모바일 클라우드의 장점을 잘 살려서 활용한다면 어디서나 실시간으로 사람들과 소통하고 업무의 생산성을 높일 수 있다. 하지만 모바일 클라우드의 편리함이라는 장점들은 자신의 위치 정보, 성별, 직업 등과 같은 개인 정보의 적극적인 노출을 통해서 이루어지고 있다. 모바일 클라우드는 너무나도 개인화된 기기이기 때문에, 잃어버리거나 도난당했을 경우 돌이킬 수 없는 손실을 입을 수도 있다[5]. 일례로, 스마트폰의 경우 뱅킹 서비스나 증권 서비스와 같은 거래 관련 애플리케이션의 이용으로 단순한 조회뿐 아니라 계좌이체, 증권 거래까지 가능하다. 이처럼 개인정보 유출이 더욱 손

쉬워진 스마트폰은 고정된 형태로 물리적인 보호를 받으며 이용할 수 있는 PC와 다르게 휴대의 편리성으로 인해 그 위협의 수준이 높아졌다. 클라우드의 보편화는 개인의 측면에서만 그치지 않고 기업이나 정부 등에서도 뚜렷하게 나타나고 있다. 콘텐츠와 기기에 이동성을 더 높여주는 클라우드는 안전성과 보안성에 대한 철저한 대비가 필요하다. 모바일 클라우드의 위협은 크게 분실, 악성코드 감염, 정보유출, 금전적 손실, 공격지 활용으로 나누어 볼 수 있으며, 사용자, 통신사업자, 단말기 제조사, 정보제공자(CP, Contents Provider)에게 모두 위협 요인이 될 수 있지만, '개인정보의 유출과 직접적인 금전적 손실을 가져오는 구조'로 되어 있어 사용자의 피해가 가장 크다. 다음은 모바일 클라우드의 5대 위협을 나타낸 것이다.

- 분실
  · 개인적, 업무적 데이터 유출가능
  · 재구매에 따른 사용자의 추가적인 비용 발생
- 악성 코드 감염
  · PC와 Sync., Bluetooth연결, Wi-Fi를 이용한 감염
  · 트로이목마 등을 이용한 단말기 탈취, 정보유출, 공격지 활용
- 정보유출
  · 통화기록, USIM 카드 정보, GPS 이용한 위치 정보
  · 주소록, 이메일 등 개인적 리스트, 사진
- 금전적 손실
  · SMS, MMS 등을 통한 불법적인 유료 콘텐츠 사용 유도
  · 모바일, 인터넷 뱅킹을 이용한 금전적 탈취
- 공격지 활용
  · 사업자 기지국의 DDos 공격
  · 사용자 PC로의 악성코드 다운로드

3.2 보안 위협

클라우드 서비스는 서비스의 특징에 따라서 SaaS, PaaS, HaaS, IaaS 등으로 구분할 수 있다. 모바일 클라우드 서비스의 주요 특성은 SaaS, PaaS, HaaS, IaaS 서비스를 구성하는 요소와 방법에 따라 ①하나의 물리적인 자원을 논리적으로 여러 사람이 공유하기 위해 통합/재분배하여 사용하는 IT자원의 가상화 및 자원공유, ②고객의 정보가 서비스 제공자의 클라우드 서버에 위치하는 정보 위탁, ③PC, 스마트폰, 테블릿 PC 등 다양한 형태의 단말기를 통한 접속 등의 특성을 가지고 있다. 이러한 특징에 따라 모바일 클라우드 서비스 상에서는 정보 유출, 서비스 장애 등 다양한 보안위협이 발생할 수 있다. CSA(클라우드 14가지 보안 도메인)[6,7,8]와 가트너(클라우드 7가지 위협)[9], UC Berkely(클라우드 10가지 보안요소)[10] 그리고 NIST(클라우드 고객관점 위험레벨)[11]에서 제시한 대표적인 보안위협 분석사례로부터 도출한 클라우드 서비스의 핵심 보안요소는 다음과 같다[5].

· 가상화 취약점
· 정보위탁에 따른 정보 유출 위협
· 자원공유 및 집중화에 따른 서비스 장애
· 단말 다양성에 따른 정보 유출
· 분산 처리에 따른 보안 적용의 어려움
· 법규 및 규제의 문제

특히, CSA는 클라우드 환경에서 발생하는 9가지의 보안 위협을 발표하였다[6,7,8].

① 데이터 유출

퍼블릭 클라우드의 경우에는 여러 기업들이 클라우드를 사용하기 때문에 특정 기업의 클라우드 서비스에 대한 공격이 이루어졌을 때 동일한 클라우드를 이용하는 다른 기업의 클라우드 서비스에도 동일한 공격이 이루어질 가능성이 매우 높다. 클라우드의 데이터 저장과 관리는 이러한 관점의 고려가 이루어져야 하며, 그 해결책은 암호화, 키 관리, 인증과 접근제어가 될 것이다.

② 데이터 소실

삭제나 수정은 새로운 데이터로의 갱신으로 이해할 수도 있지만, 기존 데이터의 소실로도 이해할 수 있으며 데이터의 소실은 해커나 어느 성실한 직원의 성실한 업무 수행 과정에서 고의적으로 행해질 수도 있지만, 실수에 의해서 우연히 발생할 수도 있다. 데이터 소실을 막을 수 있는 방법은 데이터를 수정하거나 삭제할 수 있는 권한을 잘 관리하는 것이고, 수정과 삭제에 대해서 이전 데이터를 백업해두는 것뿐이다. 데이터 유출(Data Breaches)는 데이터를 읽는(reading) 과정에서 발생하지만, 데이터 소실은 데이터를 쓰는(wrighting) 과정에서 발생한다.

③ 계정 탈취 · 서비스 탈취

사용자가 클라우드 서비스를 이용할 때 가장 기본이 되는 것은 계정정보이다. 2010년 4월, XSS(Cross-Site

Scripting) 취약성을 활용하여 계정정보를 탈취한 공격은 이러한 위협의 대표적인 사례라 할 수 있다. Two-factor 인증 등으로 인증을 강화하거나 사용자의 활동을 모니터링하는 것이 이에 대처할 수 있는 방법이다.

④ 안전하지 않은 API

안전하지 않은 API의 취약점을 통해서 사용자의 인증을 우회한다거나 정상적인 경로로는 접근할 수 없는 데이터에 대해서 접근할 수 있는 등의 보안 사고가 발생할 수 있다. 운영의 과정에서 응용계층의 보안(Application Security)를 채용함으로써 최소한의 보안을 확보할 수 있다. 클라우드 환경을 위한 클라우드 웹방화벽(Web Application Firewall)은 대표적인 방안이다.

⑤ 서비스 거부

서비스 거부 공격은 서버의 자원을 소진함으로써 서비스의 가용성(availability)를 없애는 형태의 공격으로서 클라우드 환경에서도 여전히 유효한 공격법이다. 클라우드 서비스에서는 클라우드를 구성하는 하드웨어 자원의 가용성을 소진하고 나아가서는 클라우드 서비스를 이용하는 기업의 업무가 원활히 이루어지는 것을 방해하게 된다.

⑥ 악의적인 내부 사용

퇴사한 직원의 계정이 즉시 삭제되지 않았거나, 직무의 조정으로 인해 접근할 수 없어야 하는 권한이 아직 유효한 것을 악용하는 것이 대표적인 사례이다. 악의적인 내부 사용을 막기 위해서는 사용자의 계정과 권한에 대해서 지속적인 관리와 감사가 이루어져야 한다.

⑦ 클라우드 서비스의 남용

클라우드 환경에서는 가상화 기술을 이용하여 여러 개의 가상머신이 동시에 동작하게 된다. 다시 말하면, 서로 다른 기업이나 개인이 사용하는 가상머신이 가상화를 통해 연결될 수 있다. 해커가 가상머신을 이용하여 다른 가상머신을 공격하는 기법에 대한 연구들도 최근에 발표되고 있다. 기술적인 방법보다는 클라우드 이용자에 대한 지속적인 모니터링과 운영 정책의 적용이 방법이라 할 수 있다.

⑧ 클라우드 서비스의 이해 부족

업무시스템이 클라우드의 가상화 환경에서 안전성을 충분히 확보할 수 있는지의 여부를 미리 충분하게 검토할 필요가 있다. 클라우드 환경에 대한 이해의 부족은 가상화된 후의 시스템에 치명적인 취약점을 야기시킬 수 있기 때문이다.

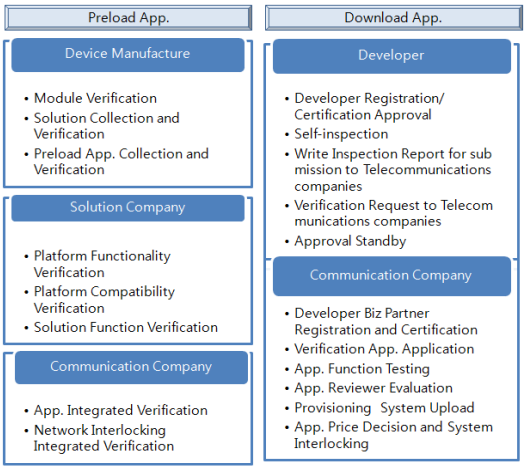
⑨ 공유기술의 취약점

클라우드 기술은 하나의 기술로 구성되는 것이 아니라 그 내부에는 엄청나게 많은 요소기술들이 존재하고 있다. 여러 전산 자원이 여러 요소기술들의 조합에 의해서 IaaS, PaaS, SaaS 등의 서비스 모델 형태로 제공되는 것이 클라우드다. 이러한 점으로 인해서 내부의 요소기술이나 하드웨어에서 발견되는 취약점이 클라우드 전체의 취약점으로 연결될 수 있다.

4. 보안 대응 방안

4.1 모바일 앱에서의 보안 유협 대응

모바일 애플리케이션은 단말이 출시될 때 탑재되어 출시되는 '탑재형 앱(Preload App)'과 사용자가 마켓을 통해 설치할 수 있는 '설치형 앱(Download App)'이 있다. 탑재형 앱은 단말 출시 전 단말 제조사에서 각 기능 모듈 검증, 앱의 취합 및 검증을 수행하고, 솔루션 제공사에서 플랫폼 기능 검증, 플랫폼 호환성 검증 등이 이루어진다. 설치형 앱은 단말 출시 후 서비스사업자(이동통신사)의 주관 하에 사업정책에 의한 평가 및 검증, 배포가 이루어진다. [Fig. 1]은 모바일 애플리케이션 검증과정을 그림으로 나타낸 것이다.



[Fig. 1] Mobile App. Verification Process

이와 같은 검증 방식은 사용자를 고려하지 않은 방식으로써 개인정보를 많이 가지고 있고 금전적인 피해를 입을 수 있는 모바일 클라우드의 특성을 고려하여 좀 더 안전한 검증 방식이 필요하다. <Table 1>은 사용자 정보 보호를 중심으로 하는 모바일 애플리케이션 검증의 발전 방향을 나타내었다. 애플리케이션의 바이너리 단위 분석, 동적 실행 검증, 악성코드 검증 과정을 추가할 필요가 있으며, 설치형 앱의 경우도 마켓을 통해 유통되기 전에 검증할 수 있는 제도적인 장치가 필요하다. 특히, 앱스토어나 마켓을 통해 유통될 때 기능성과 더불어 사용성에 대한 정보를 제공하고, 평판 시스템 등의 도입도 검토되어야 한다.

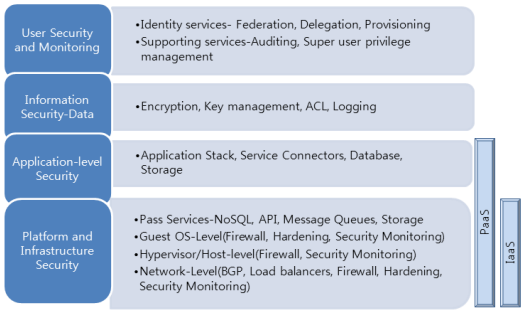
〈Table 1〉 History in Mobile App Verification

	Now	Future
Goal	- System Stability	- Privacy Policy
Object	- App. Verification to affect badly to the system	- App. Verification to affect badly to the user
Method	- Platform Compatibility Verification - Static Source Level Analysis - Network Compatibility Verification	- Binary Level Analysis - Dynamic Execution Verification - Malicious Code Verification
Time	- Pre-market Device Verification - Pre-market Download App.	- Pre-market Download App. - All paths verification before download
Download App.	- Business Verification	- User Protection Stability Verification - Malicious Code Verification

4.2 기업에서의 보안 위협 대응

안전한 클라우드 환경을 확보하는 것은 클라우드 제공자와 클라우드를 이용하려는 기업의 공동 인식이 있어야 한다. 클라우드를 채용하려는 기업은 클라우드를 도입함으로써 보안이 더 강화될 수 있을 것이라 믿을 수도 있지만, 그러한 믿음은 옳은 것일 수도 있지만 환상일 수도 있다. 안전하고 신뢰할 수 있는 클라우드 환경 구축을 위한 클라우드 서비스 구조를 [Fig. 2]에 나타냈다. Platform and Infrastructure Security 레벨과 Application-level Security 레벨은 클라우드 제공자가 지켜야할 몫이고, Information Security-Data 레벨과 User Security and Monitoring 레벨은 클라우드 사용자가 책임져야할 보안 위협에 대한 대응이라 할 수 있다.

클라우드 기술은 우리의 개인 삶과 기업의 활동에 큰 영향을 미치고 있다. 기업의 업무를 위해 클라우드를 활용하고 클라우드 환경에서 업무시스템을 구축하는 것은 시스템의 가용성과 효율성을 높이는데 큰 도움이 될 것이다. 그러나 클라우드에서 업무시스템을 구축하였고 해당 클라우드가 안전성을 보장한다고 해서 클라우드의 업무시스템의 안전성이 보장되는 것은 아니다. 클라우드로의 전이는 서버 중심의 시스템을 서비스 기반의 시스템으로 옮겨가는 것을 의미하고, 클라우드는 서비스 기반의 시스템에서 서비스가 존재할 수 있도록 하부를 제공해주는 것에 지나지 않는다. 클라우드로의 전이는 분명 큰 이점을 많이 가지게 되지만 새로운 보안의 위협도 생겨나는 만큼 클라우드 시대에 알맞은 보안이 필요하다.



[Fig. 2] Structure of Cloud Service

5. 결론

국내 스마트폰 등 모바일 기기 보급 확산 및 비용절감, 확장성 등의 장점으로 클라우드 도입이 확대되고 있는 실정이나, 정보유출, 악성코드 감염, 서비스 장애 등 보안 위협에 대한 우려가 높기 때문에 보안 문제에 대한 보장이 없이 모바일 클라우드 서비스 확대에는 한계가 있을 수밖에 없다. 모바일 클라우드 서비스 활성화의 장애요인으로 서비스의 안정성에 대한 우려와 데이터 보안성 및 기밀성의 보안에 대한 우려가 높다. 그로인한 피해가 커질 것으로 예상되기 때문에 안전한 모바일 클라우드 서비스를 이용하기 위해서는 보안 위협 및 사고 발생에 대한 대응이 필요하다. 이에 본 연구에서는 모바일 클라우드 서비스 유형과 모바일 클라우드에서 발생할 수 있

는 보안위협을 정의하고, 모바일 앱에서의 보안 대응방안과 기업의 대응방안을 제시하였다. 사용자 정보 보호를 중심으로 하는 모바일 애플리케이션 검증과정을 제안하였으며, 안전하고 신뢰할 수 있는 클라우드 환경 구축을 위해 기업이 제공할 수 있는 클라우드 서비스 구조를 제안하였다. 보안이 보장된 클라우드 서비스는 사용자들의 콘텐츠를 생산하고, 보관하고, 공유하고, 소비하는 활동들을 더욱 편리하게 함으로써 모바일 기기의 가치를 한층 높여 줄 것이다.

ACKNOWLEDGMENTS

This research was supported by Research Program funded by Baekseok University.

REFERENCES

[1] F. Samimi, P. Mckinley, S. Masoud Sadjadi, "Mobile Service Clouds : A Self-managing Infrastructure for Autonomic Mobile Computing Sevices", Lecture Notes in Computer Science, Vol. 3996, pp.130-141, 2006.

[2] H.-Y. Kim, O.-G. Min, G.-H. Nam, "The Technology Trend of Mobile Cloud", Electronics and Telecommunications Research Institute Bimonthly, Vol. 25, No. 3, pp.40-51, 2010.

[3] Sun-Sil Yoo, "A Trend of Personal Cloud Service", International Telecommunications Policy Review, Vol. 24, No. 12, pp.43-48, 2012.

[4] Seung-Ik Baek, Ji-Yeon Shin, Jong-Woo Kim, "Exploring the Korean Government Policies for Cloud Computing Service", Journal of Society for e-Business Studies, Vol. 18, No. 3, pp.1-15, 2013.

[5] Eun-Young Jang, Hyung-Jong Kim, Choon-Sik Park, Joo-Young Kim, Jae-il Lee, "The study on a threat countermeasure of mobile cloud services", Korea Institute of Information Security & Cryptology, Vol. 21, No. 1, pp.176-186, 2011.

[6] Dan Hubbard , Michael Sutton, "Top Threats to Cloud Computing V1.0", Cloud Security Alliance, 2010.

[7] Glenn Brunette, Rich Mogull, "Security Guidance for Critical Areas of Focust in Cloud Computing V2.1", Cloud Security Alliance, 2009.

[8] Z. Cheng, "Mobile Malware : Threats and Prevenion", McAfee Avert Labs., 2007.

[9] Jon Brodkin, "Gartner: Seven Cloud-computing securit risks", Network World, July, 2008.

[10] Michal Armbrust, "Above the Clouds: A Berkeley View of Cloud Computing", UC at Berkeley, Feburary, 2009.

[11] Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST, January, 2011.

한 정 수(Han, Jung-Soo)

- 1990년 2월 : 경희대학교 전자계산공학과(공학사)
- 1992년 2월 : 경희대학교 전자계산공학과(공학석사)
- 2000년 2월 : 경희대학교 전자계산공학과(공학박사)
- 2001년 2월 ~ 현재 : 백석대학교 정보통신학부 교수

- 관심분야 : CBD, UML, 3D 모델링, S/W 아키텍처
- E-Mail : jshan@bu.ac.kr