논문 12-37C-11-03

한국통신학회논문지 '12-11 Vol.37C No.11
http://dx.doi.org/10.7840/kics.2012.37C.11.1027

스마트폰 기반의 클라우드 컴퓨팅 보안 인증 연구

정 윤 수◆, 김 용 태°

A Study of Security Authentication for Cloud Computing Based on Smart Phone

Yoon-Su Jeong◆, Yong-Tae Kim°

요 약

클라우드 컴퓨팅의 편리성과 확장성을 기반으로 웹과 모바일의 기능을 결합한 스마트폰이 최근 큰 관심을 받고 있다. 그러나 현재 출시되고 있는 클라우드 서비스들은 대부분 모바일 단말과 서버간의 단순 데이터 동기화 기반 응용 서비스 수준에 그치고 있어 통신사들이 개발한 비즈니스 모델의 상호운용성에 문제가 있다. 본 논문에서는 클라우드 컴퓨팅의 편리성과 확장성을 유지하면서 스마트폰 간 서로 다른 비즈니스 모델을 사용하는 스마트폰의 사용자를 효율적으로 통합 관리할 수 있는 서비스 보안 인증 모델을 제안한다. 제안 모델은 현재 운영중인 클라우드 컴퓨팅 시스템에서 효과적으로 활용할 수 있도록 스마트폰 사용자의 신분확인 및 권한/접근제어 등을 연동하여 통합 커뮤니케이션 업무의 원활한 서비스가 유지될 수 있도록 스마트폰의 사용자 정보를 인증한다.

Key Words : 클라우드 컴퓨팅(Cloud Computing), 스마트폰(Smart Phone), 보안 구조(Security Structure)

ABSTRACT

Recently, the smart phone including web and mobile service based on the reliability and extendability of cloud computing is receiving huge attention. However, most of current cloud services provide just an application service for synchronizing data between mobile entity and server. Business model developed by communication companies have problems with interoperability. This paper proposes a new service security authentication model to efficiently manage smart phone users using different business models between smartphones and to keep the reliability and extendability of cloud computing. Proposed model authenticates for smart phone users to stay with in the unified communication with smart phone user's identity and access control to effectively use the current cloud computing system.

Ⅰ. 서 론

클라우드 컴퓨팅은 IT 서비스 및 컴퓨터 자원을 인터넷 기반으로 제공하는 컴퓨터 기술을 의미한다. 클라우드 컴퓨팅이 각광을 받고 있는 이유는 과거처럼 일반적인 공급이 아닌 개개인의 사용자가 상호작용하는 것을 중요시 할 뿐만 아니라 컴퓨팅 기술의 발달로 인하여 글로벌 기업들의 전략적 투자 전략과 맞물려 급속히 파급되고 있기 때문이다[1].

클라우드 컴퓨팅은 클라우드 컴퓨팅만이 가지고 있는 구조적 특징으로 인하여 기존 시스템에 잠재되어 있던 보안 위협과 새로운 형태의 보안 위협에 노출되어 있어 보안 위협에 대한 대응책이 미미한 상황이다[2]. 최근 모바일 클라우드 기술이 다양한 분야로

※ 본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.
◆ 주저자 : 목원대학교 정보통신공학과 교수, bukmunro@mokwon.ac.kr, 정회원
° 교신저자 : 한남대학교 멀티미디어학부 교수, ky7762@hnu.kr, 정회원
논문번호 : KICS2012-06-285, 접수일자 : 2012년 6월 21일, 최종논문접수일자2012년 11월 9일

확산되고 있는 상황에서 모바일 클라우드는 클라우드의 편리성과 확장성을 기반으로 다양한 디바이스 플랫폼 및 운영체제의 비종속적인 특성을 나타내고 있다. 모바일 클라우드는 표준화와 플랫폼 등에서 서비스간의 상호 호환성 및 이식성, 보안 등에서 문제가 있어 개발자가 특정 클라우드 플랫폼을 기반으로 소프트웨어를 개발하더라도 다른 모바일 클라우드 플랫폼에서 실행되지 않아 플랫폼간 상호 호환성이 이루어지고 있지 않다[3-5].

대부분의 클라우드 서비스는 PC에 국한되어 제공되고 있으며 모바일 단말기를 지원할 경우 특정 단말에 한정되어 있어 클라우드 서비스가 원활하게 지원되고 있지 않다. 향후 모바일 서비스가 보편화되면 다양한 단말 기기에서 공통으로 서비스해야 할 수요가 커질 것이며 이를 위해 단말기의 독립적인 보안 서비스 또한 요구된다[6-10]. 특히, 클라우드 자원을 이용하는 모바일 클라우드 서비스는 모바일 서비스와 클라우드 서비스가 융합되어 복합적인 위협이 발생될 수 있기 때문에 모바일과 무선네트워크, 클라우드 서비스 중 하나의 자원에 문제가 발생할 경우 클라우드 전체에서 정상적인 서비스 수행이 불가능하게 된다. 모바일 클라우드 서비스는 모바일 단말기를 사용하는 사용자가 모바일 클라우드 환경에서 공유된 자원을 무선네트워크를 통해 서비스 받기 때문에 문제가 발생할 경우 보안 피해가 일반 클라우드 서비스보다 더 커질 수 있다. 최근 휴대폰의 발전과 대중화로 인하여 모바일 클라우드 서비스를 사용하는 사용자가 증가하는 추세에서 모바일 클라우드 서비스는 보안위협이 제거된 안전하고 신뢰할 수 있는 서비스 제공이 필요하다.

본 논문에서는 클라우드 컴퓨팅의 편리성과 확장성을 유지하면서 스마트폰 간 서로 다른 비즈니스 모델을 사용하는 스마트폰의 사용자를 효율적으로 통합 관리할 수 있도록 상호운용성을 향상시킨 스마트폰 기반의 클라우드 컴퓨팅 보안 인증 모델을 제안한다. 제안 모델은 현재 운영중인 클라우드 컴퓨팅 시스템에서 효과적으로 활용할 수 있도록 스마트폰 사용자의 신분확인 및 권한/접근제어 등을 연동하여 통합 커뮤니케이션 업무의 원활한 서비스가 유지될 수 있도록 모바일 클라우드 인증 서버가 스마트폰 사용자의 정보를 통합 관리하여 인증을 수행한다. 또한, 스마트폰 사용자가 다른 지역의 클라우드 컴퓨팅 환경에 접근하더라도 중앙 서버에 존재하는 스마트폰 사용자의 그룹정보를 관리하여 스마트폰 사용자가 서비스를 이중으로 사용하는 것을 예방한다.

이 논문의 구성은 다음과 같다. 2장에서는 모바일 클라우드 컴퓨팅과 보안위협에 대해서 알아본다. 3장에서는 스마트폰 기반의 모바일 클라우드 보안 모델을 제안하고 4장에서는 제안 모델을 보안 공격 유형에 따른 보안 대책을 분석한다. 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1. 모바일 클라우드 컴퓨팅

모바일 클라우드 컴퓨팅은 필요한 만큼 사용하고 쓴만큼 지불하는 클라우드 컴퓨팅과 모바일 서비스를 결합하여 사용자가 언제 어디서든지 클라우드 서비스를 받을 수 있는 환경을 의미한다[5,8]. 모바일 클라우드 컴퓨팅에서는 스마트폰은 물론 이동성을 갖는 기기들 즉 노트북과 넷북, PDA, UMPC(Ultra Mobile Personal Computer) 등이 모두 사용된다. 모바일 클라우드 컴퓨팅에서 사용되는 아이폰, 노트북 등은 모바일 기기와 웹 사이트 간에 자동으로 동기화가 이루어진다.

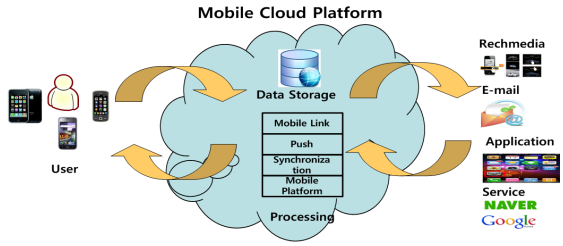


그림 1. 모바일 클라우드의 구성도
Fig 1. Block Diagram of Mobile Cloud

2.2. 모바일 클라우드 보안위협

모바일 클라우드 컴퓨팅 보안은 기존 클라우드 컴퓨팅의 보안 측면뿐만 아니라 단말과 클라우드 서버 사이의 무선구간에서도 보안 문제가 발생할 수 있다[2,8]. 모바일 클라우드 컴퓨팅에서는 클라우드 서비스를 이용하는 이용자의 정보 유출 공격, 무선 AP 등을 통해 인터넷에 연결되는 스마트폰이나 태블릿 등의 이용자 정보의 가로채기 공격, 탈옥, 루팅이라고 부르는 스마트폰 해킹 공격, 모바일 스파이웨어에 의해 통화기록은 물론 위치 정보, e-메일 등의 정보 유

출 공격 등이 존재한다. 보안 공격 중에서 모바일 클라우드 컴퓨팅에서는 모바일 클라우드 컴퓨팅 환경에서는 클라우드 컴퓨팅의 오/남용, 안전하지 않은 API의 사용, 악의적인 내부자 문제, 공유 기술의 문제, 데이터 유실/유출, 계정 탈취 등의 보안 위협에 노출되어 있다[9]. 제안 모델에서는 모바일 클라우드 컴퓨팅에서 사용되는 스마트폰을 서로 다른 비즈니스 모델에서 상호 운용하면서 2팩터(2-factor) 인증 기술과 권한 및 접근제어 등을 통하여 쉽게 서로 다른 비즈니스 모델에서 커뮤니케이션 할 수 있도록 함으로써 모바일 클라우드 보안위협을 예방하고 있다.

Ⅲ. 체내삽입형 장치를 부착한 환자의 프라이버시 보호 프로토콜

이 절에서는 모바일 클라우드 컴퓨팅에서 사용되는 스마트폰을 서로 다른 비즈니스 모델에서 상호 운용할 수 있는 서비스 보안 모델을 제안한다. 제안된 서비스 보안 모델은 2팩터 인증 기술과 권한 및 접근제어 등을 통하여 쉽게 서로 다른 비즈니스 모델에서 커뮤니케이션 할 수 있다.

3.1. 모바일 클라우드 환경에서의 통합 인증 및 권한 관리 모델

스마트폰 기반의 클라우드 컴퓨팅 환경에서 서로 다른 물리적인 위치에 존재하는 사용자는 특정 서버에 존재하는 인증 서버를 통해 사용자의 인증 및 권한을 할당받는다. 이동성이 자유로운 스마트폰 사용자는 클라우드 컴퓨팅 환경에 분산되어 있는 시스템을 통해 서비스를 제공받으며 외부 환경에 있는 사용자는 클라우드 플랫폼이 제공하는 통합 인증 시스템을 이용하여 서버내의 시스템에 접근할 수 있다.

〔그림 2〕는 모바일 클라우드 환경에서 스마트폰을 사용하는 사용자의 보안 피해(키로깅, 피싱 등)을 예방하기 위한 제안 모델의 전체 개념도를 보여주고 있다.

〔그림 2〕의 제안 모델은 스마트폰 등의 단말 통합 인증, 모바일 클라우드 인증서버, 사용자 인증서버로 구성되며 스마트폰을 사용하는 사용자에게 서비스를 안전하게 제공하기 위해서 모바일 클라우드 인증 서버로부터 2팩터 인증 기술을 제공받아 스마트폰 사용자를 인증한다. 이 때, 서로 다른 클라우드 환경에서 인증서버로 접속하는 사용자를 구별하기 위해서 모바일 클라우드 인증서버는 스마트폰 사용자마다 서로 다른 키를 사용하여 사용자를 관리한다. 사용자가 사용하는 키는 모바일 클라우드 환경에서 다수의 사용자가 데이터베이스에 저장되어 있는 데이터를 보호할 수 있는 장점이 있다. 〔그림 2〕에서 스마트폰을 사용하는 사용자는 모바일 클라우드 서버에서 제공되는 서비스가 악성코드로부터 안전하기 위해서 접속 제한 및 해킹 점검 루틴 우회 방지 기술 등을 적용한다.

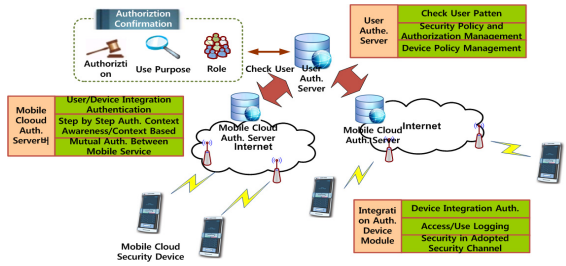


그림 2. 모바일 클라우드 환경에서의 사용자 통합 인증 및 권한 관리
Fig 2. User Integration Authentication and Authorization Management in Mobile Cloud Environment

3.2. 모바일 단말

모바일 클라우드 환경에서 이용자 단말로 이용되는 PC, 스마트폰, 태블릿 등은 키로깅, 피싱 등으로부터 노출되어 있다. 제안 모델에서는 모바일 클라우드 인증서버가 제공하는 서비스를 안전하게 사용자에게 제공하기 위해서 인증서/OTP 기반의 2팩터 인증 기술을 사용한다. 이때, 인증서/OTP 기반의 2팩터 인증 기술은 키보드 보안, 가상 키보드 등의 키 입력 정보보호 기술을 사용하여 기밀성을 제공하며, 인증 환경에 따라 각 시스템에 접근하는 각각 다른 단말을 인증하고 내부 중요정보에 대해서 권한을 부여하여 권한에 따른 데이터 접근을 제한함으로써 모바일 클라우드 단말의 인증을 최적화한다.

서로 다른 클라우드 환경에서 스마트폰을 이용하는 사용자의 서비스 요구를 제공하기 위해서 모바일 클라우드 인증서버는 다른 클라우드 환경에 존재하는 모바일 클라우드 인증서버와 사용자가 사전 등록한 비밀키를 이용하여 공유한다. 공유된 데이터는 사용자 인증서버가 통합하여 사용자에게 권한 및 역할을 확인하고 사용자를 인증한다.

인증서버는 서로 다른 클라우드 환경에 존재하는 모바일 클라우드 인증서버들을 관리하며 스마트폰을 사용하는 사용자들의 상호운용성을 제공하기 위해서 〔표 1〕과 같은 사용자의 i-PIN 정보 코드를 사용한다. 제안 모델에서 i-PIN을 사용하는 이유는 클라우드 환경에서 사용자의 주민번호 대신 i-PIN 아이디와 비밀번호를 사용함으로써 사용자의 무결성 및

프라이버시를 보장받기 때문이다.

표 1. 모바일 클라우드 환경의 사용자 i-PIN 정보코드
Table 1. User I-PIN Information Code of Mobile Cloud Environment

Management Code	Oganization Code	Prefix 1	Prefix 2	Use Code	Serial Code
12 bit	16 bit	4 bit	4 bit	6 bit	6 bit

〔표 1〕은 제안모델을 이용하는 모든 모바일 클라우드 시스템 및 서비스에서 각각의 모바일 클라우드 사용자를 구분하는 기본 키 역할을 수행한다. 만약 동일한 i-PIN 정보 코드를 가진 모바일 클라우드 사용자가 존재하지 않다면 모바일 클라우드 환경의 범위가 확장될 수 있다.

3.3. 모바일 클라우드 인증서버

3.3.1. 사용자/단말 통합 인증

모바일 클라우드 컴퓨팅 환경에서는 사용자들이 서로 다른 위치에서 서비스를 요청하기 때문에 사용자가 서비스를 요청하는 위치에 따라 모바일 클라우드 인증서버가 사용자의 인증 정보를 수집하여 사용자 인증서버에게 사용자 인증을 요청한다.

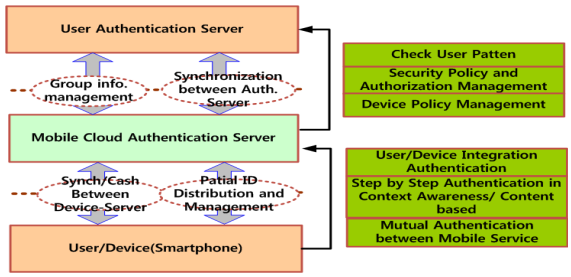


그림 3. 모바일 장치 인증 처리
Fig 3. Authentication Process of Mobile Device

〔그림 3〕은 모바일 사용자가 인증서버에게 서비스를 제공받기 위해 사용자 인증을 요청할 때 모바일 클라우드 인증서버와 사용자 인증서버 사이의 처리 과정을 보여준다. 〔그림 3〕처럼 제안 모델에서는 서로 다른 클라우드 환경에서 사용자의 인증을 처리하기 위해서는 단말 기종과 OS 비종속적인 모바일 응용 개발 플랫폼이 제공되어야 하며, 모바일 단말의 응용 실행 환경(HW 자원, OS, 유틸리티, 응용)을 하나의 인스턴스로 제공하고 사용자 인스턴스들의 이동성 및 확장성을 제공한다. 모바일 사용자의 상황인지 및 내용기반의 다단계 인증을 처리하면서 인증서버의 오버헤드를 줄이기 위해서 제안모델에서는 모바일 단말-서버 간 싱크/캐쉬 기능을 제공하면서 모바일 환경에서 발생하는 작은 크기의 많은 데이터를 처리하도록 한다.

3.3.2. 상황인지/내용기반 다단계 인증

상황인지/내용기반 다단계 인증은 모바일 클라우드 단말이 다른 지역의 모바일 클라우드 인증서버에게 인증을 요청하지 않고 해당 영역의 클라우드 관리 코드를 사용자에게 부여하여 사용자를 인증할 때 사용된다. 제안 모델에서는 모바일 클라우드 인증서버가 〔표 1〕의 사용자 i-PIN 요청 정보코드 중 용도코드를 이용하여 〔그림 4〕처럼 서로 다른 클라우드 환경에 위치한 사용자의 상황을 파악한 후 사용자의 인증을 요청한다. 모바일 클라우드 보안 단말이 클라우드 인증 서버에게 인증을 요청할 경우 제안 모델은 〔그림 4〕처럼 서로 다른 모바일 클라우드 보안 단말은 인증서버에게 인증을 요청과정을 8단계로 구분한다.

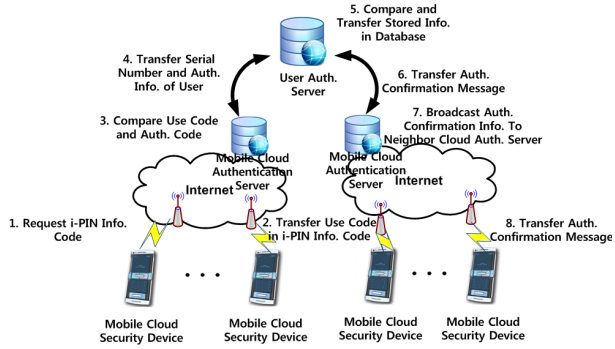


그림 4. 클라우드 인증 서버의 다단계 인증
Fig 4. Step by Step Authentication of Cloud Authentication Server

〔그림 4〕에서 계층적으로 구성된 사용자 인증서버, 모바일 클라우드 인정서버, 모바일 클라우드 보안 단말 등은 단계적으로 인증 과정을 처리한다. 각각 다른 모바일 클라우드 보안 단말은 모바일 클라우드 인증서버에게 i-PIN 정보코드를 요청하고(단계 1) 요청된 정보를 수신받은 모바일 클라우드 인증서버는 모바일 클라우드 보안 단말을 확인하여 모바일 클라우드 보안 단말에게 요청된 i-PIN 코드 중 용도코드를 전송한다(단계 2). 모바일 클라우드 인증서버는 i-PIN 코드의 용도코도와 인증코드를 비교한 후 비교결과가 일치할 경우 사용자 인증서버에게 사용자의 일련번호와 인증 정보를 전달한다. 만약 인증 정보가 일치하지 않으면 프로세스를 종료한다(단계 3~단계 4). 사용자 인증

서버는 사용자의 일련번호와 인증정보를 데이터베이스에 저장된 정보와 비교하여 일치되는 정보가 있을 경우 모바일 클라우드 인증서버에게 전달한다(단계 5~단계 6). 모바일 클라우드 인증서버는 이웃한 모바일 클라우드 인증서버에게 인증 확인 정보를 유포하여 모바일 클라우드 보안 단말이 인증 확인 메시지를 전달받도록 한다(단계 7~단계 8).

〔그림 4〕처럼 제안 모델에서 i-PIN을 사용하는 이유는 클라우드 환경에서 사용자의 주민번호 대신 i-PIN 아이디와 비밀번호을 사용함으로써 사용자의 무결성 및 프라이버시를 제공할 수 있기 때문이다. 만약 사용자의 i-PIN 요청 정보코드 중 용도코드와 모바일 클라우드 인증서버의 인증코드가 일치하지 않으면 사용자의 인증 요청을 취소한다. 인증코드는 사전에 사용자가 클라우드 환경에 접속하기 전에 사전 부여된 코드이다. 만약 인증코드의 정보가 일치하면 사용자 인증서버에게 사용자의 일련번호 코드와 인증 정보를 전달하여 인증서버의 데이터베이스에 사전에 저장한 사용자 정보와 비교를 수행한다. 데이터베이스에 저장된 정보 중 모바일 클라우드 인증서버는 해당 클라우드 관리 코드를 사용자에게 부여하여 사용자를 인증한다. 제안 모델은 사용자를 인증하기 위해서 그룹 코드, 클라우드 관리 코드, 사용자 i-PIN 코드 등을 사용하여 인증함으로써 사용자의 분산 처리가 가능하고 인증 서버의 제어 집중으로 인한 부하를 낮출 수 있다.

3.3.3. 모바일 서비스간 상호인증

모바일 서비스간 상호인증은 모바일 클라우드 단말이 다른 지역의 모바일 클라우드 인증서버에 포함된 모바일 클라우드 단말을 인증하고자 할 때 사용된다. 제안 모델에서는 모바일 클라우드 보안 단말을 사용하는 사용자를 상호 인증하기 위해서 〔그림 5〕처럼 사용자의 i-PIN 코드 중 발급자 코드와 일련번호 코드, 사용자가 사전에 등록한 랜덤값을 이용하여 서로 다른 위치에 존재하는 모바일 클라우드 단말간 상호인증을 수행한다.

모바일 서비스간 상호인증은 〔그림 5〕처럼 10단계의 처리과정을 수행한다. A 지역에 있는 모바일 클라우드 보안 단말은 B 지역에 있는 모바일 클라우드 보안 단말과 통신하기 위해서 인증 요청 메시지를 수신받은 후 모바일 클라우드 정보 확인을 위하여 모바일 클라우드 인증서버에게 확인 메시지를 전달한다(단계 1~단계2). 모바일 클라우드 인증 서버는 클라우드 인증 서버내 데이터베이스에 존재하는 모바일 클라우드 보안 단말 정보를 검색하여 일치하는 정보가 존재할 경우 사용자 인증서버에게 B 지역에 존재하는 모바일 클라우드 인증서버의 확인 요청 메시지를 전달하여 B 지역에 존재하는 모바일 클라우드의 존재 유·무 확인 응답 메세지를 수신받는다(단계3~단계 5). 모바일 클라우드 인증서버는 사용자 인증서버로부터 전달받은 응답메시지를 확인한 후 B 지역에 존재하는 모바일 클라우드 인증서버에게 모바일 클라우드 보안 단말의 존재 확인 요청 메시지를 전달하면 B지역에 존재하는 모바일 클라우드 인증서버는 데이터베이스를 검색하여 요청된 모바일 클라우드 보안 단말의 존재 유·무에 대한 확인 요청 메시지를 전달한다(단계 6~단계8). 모바일 클라우드 인증서버는 A지역에 존재하는 모바일 클라우드 보안 단말에게 B 지역의 모바일 클라우드 인증서버로부터 전달받은 인증 확인 정보 메시지를 전달한다(단계 9). 모바일 클라우드 보안 단말은 인증 확인이 완료되면 B지역의 모바일 클라우드 보안 단말에게 인증 확인 메시지를 전달한다(단계 10).

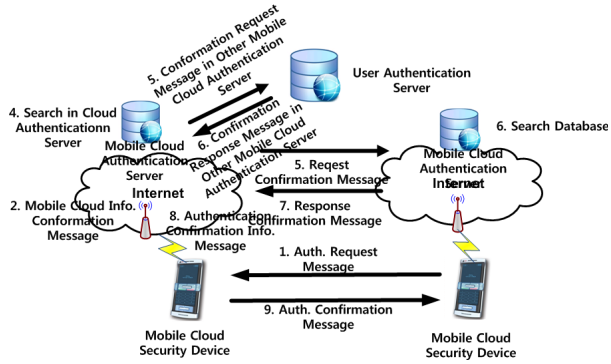


그림 5. 모바일 서비스간 상호인증 처리
Fig 5. Mutual Authentication Process between Mobile Service

제안 모델에서는 모바일 서비스간 인증 처리를 위해서 모바일 클라우드 인증서버가 다른 위치에 존재하는 모바일 클라우드 인증서버에게 모바일 클라우드 단말을 인증하기 위해서 우선 사용자 인증서버에게 모바일 클라우드 인증서버를 인증한 후 상대방 모바일 클라우드 인증서버의 데이터베이스에 존재하는 모바일 클라우드 단말의 정보를 검색한다. 정상적인 단말일 경우 모바일 클라우드 인증서버는 단말의 인증 정보를 전달하여 모바일 클라우드 단말간 상호인증을 처리할 수 있는 정보를 전달한다.

3.3.4. 사용자 인증서버

제안 모델에서 인증서버는 모바일 클라우드 단말과

모바일 클라우드 인증 서버를 중앙 집중방식으로 통합 관리하며 모바일 클라우드 단말과 모바일 클라우드 인증서버의 정보를 사용자가 가지고 있는 i-PIN 정보와 함께 클라우드 그룹 정보를 〔표 2〕처럼 데이터베이스에 연계하여 저장한다.

표 2. 사용자 인증서버의 클라우드 그룹 통합 관리 코드
Table 2. Cloud Group Integration Management Code of User Authentication Server

Cloud Group Code	Management Code	User i-PIN Code
12 bit	4 bit	48 bit

사용자 인증 서버는 〔표 2〕의 관리 코드를 통해 모바일 클라우드 단말이 인증서버에 무분별하게 접근하는 것을 관리한다. 특히 관리 코드는 모바일 클라우드 단말과 인증서버들의 권한 등급에 따라 접근 및 서비스를 제한할 수 있기 때문에 모바일 클라우드 컴퓨팅 환경에서는 사용자들이 서로 다른 위치에서 서비스를 요청하더라도 클라우드 서비스와 확장성에는 아무런 영향을 미치지 않는다.

Ⅳ. 평 가

이 절에서는 모바일 클라우드 단말을 계층적 구조로 구성된 인증서버 수에 따른 인증 지연시간과 오버헤드, 해쉬 함수 충돌확률에 따른 공격확률 등을 평가한다. 여기서, 실험 평가를 위해 사용되는 인증서버는 모바일 클라우드 인증서버를 의미한다.

4.1. 실험환경

이 절에서는 인증서버의 인증 처리시간과 오버헤드, 해쉬 함수 충돌확률에 따른 공격 확률 등을 평가하기 위한 도구로 OPNET을 사용하였다. OPNET을 사용하게 된 이유는 첫째, 성능평가를 위해 모바일 클라우드 단말을 이용하여 직접 테스트베드를 구축하여 실험할 수 없었기 때문이며, 둘째, OPNET이 제공하는 모바일 클라우드 단말 기능을 적용하여 성능 평가를 수행할 수 있기 때문이다. 제안 모델의 실험을 위하여 〔표 3〕의 실험환경을 사용한다. 실험에서 설정된 모바일 클라우드 단말의 수는 100, 300, 500, 1,000명이며 인증 서버의 최대 수는 3으로 설정한다. 실험 시간은 86,400초 동안 실험을 수행한다. 사용자 기기의 버퍼 크기는 100 패킷의 크기를 가지는 것으로 가정하며, 각 패킷은 패킷 전송동안 패킷 드롭 확률을 0.01로 한다. AP의 개수는 서비스 환경 크기에 따라 1개에서 10개를 사용하는 것으로 한다. 이 같은 설정은 현실 모델에 맞는 시뮬레이션을 만들기 위한 설정들이다.

표 3. 실험환경
Table 3. Experimental Environment

Environment Variable	Value
Number of User	100, 300, 500, 1,000
Max Number of Authentication Server	3
Experimental Time	86,400 s
Buffer Size	100 packet/s
Packe Drop Ratio	0.01
Data Packet Size	100 bytes
Querry Packet Size	25 bytes
Heder Packet Size	25 bytes
Number of AP(Access Point)	1 ~ 10

4.2. 성능평가

4.2.1. 인증서버의 인증 지연시간

〔그림 6〕은 모바일 클라우드 단말을 사용하는 사용자 수 증가에 따른 인증 서버의 지연시간을 평가하고 있다.

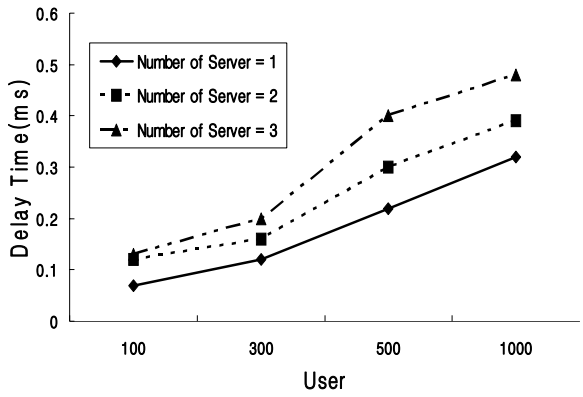


그림 6. 인증 지연시간
Fig 6. Authentication Delay Time

사용자 수가 100명 이하일 경우에는 인증서버의 수에 따른 지연시간의 차이가 없지만 사용자 수가 500이상이 될 경우 인증서버의 지연시간이 100명 이하보다 12.3% 높게 나타났다. 이 같은 결과는 모바일 클라우드 인증서버가 모바일 클라우드 단말의 인증 범위가 증가할수록 사용자 인증서버의 인증 지연시간도 길어

지는 의미를 내포하고 있다.

4.2.2. 사용자 수에 따른 인증서버의 오버헤드

〔그림 7〕은 사용자 수에 따른 인증 서버의 오버헤드를 비교 평가하고 있다. 실험 결과 사용자 수가 증가함에 따라 인증 서버의 오버헤드는 점진적으로 증가하였으며, 모바일 클라우드를 계층적으로 관리할 경우 계층적으로 관리하지 않을 경우보다 인증서버의 오버헤드는 최대 15%까지 낮은 결과를 얻었다. 이 같은 결과는 상황인지/내용기반 다단계 인증에서 사용자 인증서버의 오버헤드가 모바일 서비스간 상호인증 환경의 사용자 인증서버의 오버헤드보다 낮다는 의미를 내포하고 있다.

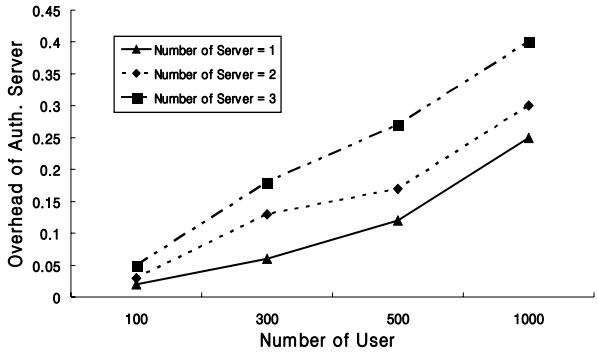
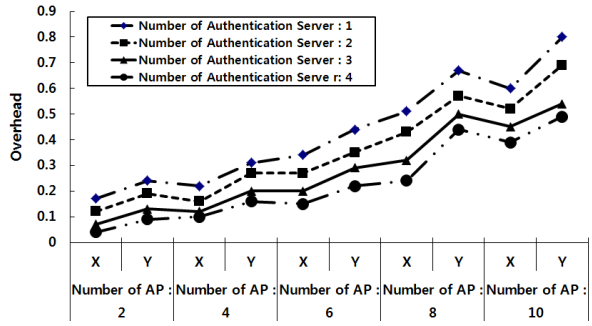


그림 7. 인증서버의 오버헤드
Fig 7. Overhead of Authentication Server

4.2.3. 인증서버와 AP 수에 따른 오버헤드

〔그림 8〕은 인증서버와 AP 수 증가에 따른 인증서버의 오버헤드를 평가한 결과이다. 인증서버의 수를증가시키면서 AP 수를 점진적으로 증가한 결과, AP의 수가 낮은 경우 인증서버의 오버헤드는 평균 0.13으로 낮았으나 AP 수가 6이상일 경우에는 인증서버가 받는 오버헤드가 평균 0.53으로 높게 나타났다. 이 같은 결과는 상황인지/내용기반 다단계 인증과 모바일 서비스간 상호인증 모두 동일한 결과를 나타났으며, 상황인지/내용기반 다단계인증 환경과 모바일 서비스간 상호인증 환경에서 AP 수 증가에 따른 인증서버의 오버헤드를 비교 평가한 결과 이동성에 따른 처리율이 상황인지/내용기반 다단계 인증 환경이 모바일 서비스간 상호인증 환경보다 낮기 때문에 인증서버의 오버헤드는 평균 19% 낮았다.

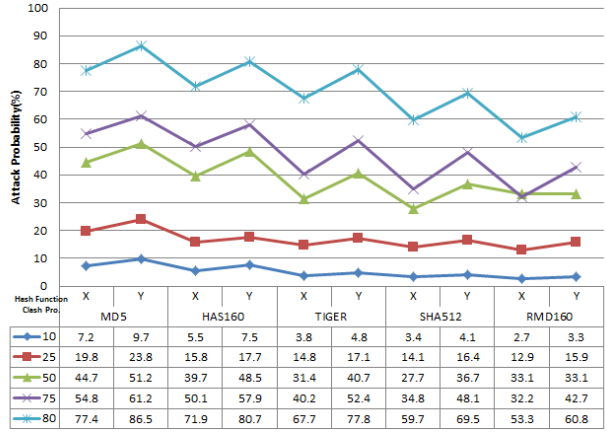


X : Step by Step Authentication of Context Awareness/Contetn based
Y: Mutual Authentication between Mobile Service

그림 8. AP수에 따른 인증서버의 오버헤드
Fig 8. Overhead of Authentication Server through Number of AP

4.2.4. 해쉬 함수 충돌확률에 따른 공격 확률

〔그림 9〕은 상황인지/내용기반 다단계 인증환경과 모바일 서비스 사이에 상호인증 환경에서 해쉬함수(MD5, HAS160, TIGER, SHA512, RMD160 등)의 충돌확률에 따른 공격 확률 결과를 나타내고 있다.



X : Step by Step Authentication of Context Awareness/Contetn based
Y: Mutual Authentication between Mobile Service

그림 9. 해쉬함수 충돌확률에 따른 공격 확률
Fig 9. Clash Probability of Hash Function through Attack Probability

〔그림 9〕에서는 상황인지/내용기반 다단계 인증환경이 모바일 서비스 사이에 상호인증을 수행하는 환경보다 해쉬함수 충돌확률에 따른 공격확률이 낮게 나타났다. 이 같은 결과는 모바일 서비스간 상호인증이 상황인지/내용기반 다단계 인증보다 모바일 클

라우드 단말이 처리하는 인증 과정을 더 많이 요구되기 때문이다. 〔그림 9〕에서 해쉬 함수 충돌에 사용된 해쉬 함수 중 MD5가 공격 확률이 가장 높게 나타난 반면 RMD160이 가장 낮게 나타났다.

4.3. 안전성 평가

이 절에서는 스마트폰 기반의 클라우드 컴퓨팅 환경에서 요구되는 보안 요구사항을 기반으로 인식자 관리, 상호인증, Replay 공격, Man in the middle attack 공격, Impersonation 공격 등에 대한 제안 기법의 안전성을 평가한다.

4.3.1. 인식자 관리

모바일 인증서버는 모바일 클라우드 단말을 인증처리 방법에 따라 중앙 집중적인 방법과 분산처리 방법으로 구분하여 관리하기 때문에 모바일 인증서버는 모바일 클라우드 단말의 인식자를 테이블로 저장하여 관리한다. 제안 모델에서 인증서버는 모바일 클라우드 단말의 위치에 따라 그룹코드와 i-PIN 정보를 이용하여 관리 코드를 부여하여 모바일 클라우드 단말을 관리한다. 제안 모델은 상황인지/내용기반 다단계 인증과 모바일 서비스 사이에 상호 인증에 따라 모바일 클라우드 단말을 인증하고 서비스를 제공하기 때문에 제어 집중으로 인한 부하는 높지 않다.

4.3.2. 상호 인증

제안 모델에서는 모바일 클라우드 보안 단말을 사용하는 사용자를 인증하기 위해서 i-PIN 코드 중 발급자 코드와 일련번호 코드, 사용자가 사전에 등록한 랜던값을 이용한다. 제안 모델에서는 모바일 서비스 사이에 상호인증을 수행하기 위해서 우선 사용자 인증서버에게 모바일 클라우드 인증서버를 인증하여 데이터베이스 내에 존재하는 모바일 클라우드 단말의 정보를 비교한다. 이 때, 데이터베이스에 저장되어 있는 랜덤값은 매 통신마다 다른 값이 생성되기 때문에 평문 공격의 암호 알고리즘 공격을 예방하며 i-PIN 코드는 XOR 연산과 해쉬 함수를 이용하여 사용되기 때문에 제 3자는 알 수 없다.

4.3.3. Replay 공격

제안 기법에서는 인증 과정에서 송·수신되는 메시지 중 단말이 현재 서비스를 사용하는 정보 중에서 시간(Time) 정보를 사용하여 인증 세션의 정상 유·무를 확인하는 과정에서 인증서버와 단말간 공유된 키를 사용하기 때문에 Replay 공격을 예방하고 있다. 제안 기법에서는 모바일 클라우드 단말이 인증을 요청할 때마다 서로 다른 공유키를 사용하기 때문에 클라우드 환경처럼 분산 처리를 수행하는 환경에 적합하며 서비스 형태에 따라 사용자 인증을 개별적으로 수행할 수 있다.

4.3.4. Man in the middle 공격

제안 기법에서는 모바일 클라우드 보안 단말과 인증서버 간에 주고받는 메시지에서 공격자가 사용자 정보를 알고 있다고 가정하면 공격자는 인증서버로부터 인증받기 위해서 사용자 정보 중 i-PIN 코드를 사용하여 인증서버에게 인증을 요청한다. 그러나 제안 모델에서는 i-PIN 코드 중 발급자의 코드와 일련번호 코드, 사용자가 사전에 등록한 난수값을 XOR과 해쉬 함수에 적용한 새로운 값을 계산할 수 없기 때문에 공격자의 man in the middle 공격에 안전하다.

4.3.5. Impersonation 공격

제안 기법은 모바일 클라우드 보안 단말에 사용자의 인식자와 패스워드를 직접 사용하지 않고 i-PIN 코드 중 발급자의 코드와 일련번호 코드, 사용자가 사전에 등록한 난수값 등을 사용하여 모바일 클라우드 보안 단말과 인증서버 사이에 전달되는 동시에 시간 정보를 사용하여 인증과정을 수행하기 때문에 Impersonation 공격을 예방하고 있다.

V. 결 론

모바일 클라우드는 표준화와 플랫폼 등에서 서비스 간의 상호호환성과 이식성, 보안 등에서 문제가 대두되고 있다. 특히, 서로 다른 플랫폼 사이에 소프트웨어가 실행되지 않을 수 있어 상호호환성 문제를 해결할 필요가 있다. 본 논문에서는 서로 다른 비즈니스 모델을 사용하는 스마트폰의 사용자를 효율적으로 통합 관리할 수 있는 서비스 보안 인증 모델을 제안하였다. 제안 모델은 현재 운영중인 클라우드 컴퓨팅 시스템에서 효과적으로 활용할 수 있도록 스마트폰 사용자의 신분확인 및 권한/접근제어 등을 연동하여 통합 커뮤니케이션 업무의 원활한 서비스가 유지될 수 있도록 스마트폰의 사용자 정보를 통합 관리하였다. 향후 연구로 본 연구에서 제안된 모델을 실 환경에 적용하는 연구를 수행할 계획이다.

참 고 문 헌

[1] D. Zissis, and D. Lekkas, "Addressing cloud

computing security issues", *Future Generation Computer Systems*, vol. 28(3), 2012

[2] W. Jansen, and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", 2011.

[3] M. Mannan, B. H. Kim, A. Ganjali, and D. Lie, "Unicorn: Two-factor Attestation for data Security", *Proc. of the 18th ACM conference on Computer and Communications Security*. 2011

[4] F. Zhang, J. Chen, H. Chen, and B. Zang, "CloudVisor: Retrofitting Protection of Virtual Machines in Multitenant Cloud with Nested Virtualization", *Proc. of 23rd ACM Symposium on Operating Systems Principles*. 2011

[5] K. C. Lee, S and Y. Lee, "Mobile Cloud Standard Trend and strategy", Information and Commnunications Magazine, Vol. 28, No. 10, pp. 44-49. 2011.

[6] Y. H. Bang, S. J. Jeong, S. M. Hwang, "Security Requirement Development Tools of Mobile Cloud System", Information and Commnunications Magazine, Vol. 28, No. 10, pp. 19-29. 2011.

[7] I. Y. Jeong, C. Y. Lee, J. Y. Kim, H. K. Kim and Y. C. Jeong,, "Context Awareness Dynamic Authentication and Authorization Management Service in Mobile Cloud Multi-tenancy Environment", Information Security Magazine, Vol 21, No. 8, pp. 14-22. 2011.

[8] ABIresearch, "Mobile Cloud Computing". 2009

[9] Security for Access to Device APIs from the Web – W3C Workshop, http://www.w3.org/2008/security –ws/.

[10] T. H. Kim, I. H. Kim, C. W. Min and Y. I. Yeom, "Security Technical Trend of Cloud Computing", Computer Science Managine 30(1), pp. 30-38, Jan. 2012.

정 윤 수 (Yoon-Su Jeong)

1998년 2월 청주대학교 전자계산학과 학사

2000년 2월 충북대학교 대학원 전자계산학과 석사

2008년 2월 충북대학교 대학원 전자계산학과 박사

2008년 3월~2012년 2월 충북대 및 한남대 시간강사

2012년 3월~현재 목원대학교 정보통신학과 교수

<관심분야> 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안

김 용 태 (Yong-Tae Kim)

1984년 2월 한남대학교 계산통계학과 학사

1988년 2월 숭실대학교 전자계산학과 석사

2008년 2월 충북대학교 전자계산학과 박사

2002년 12월~2006년 2월 (주) 가림정보기술 이사

2006년 3월~현재 한남대학교 멀티미디어학부 교수

<관심분야> 모바일 웹서비스, 정보보호, 센서 웹, 모바일 통신보안