

# 이동통신 단말기에서 데이터 보호 및 백업을 위한 원격 제어 시스템 설계

정회원 조인휘\*

## Design of Remote Control System for Data Protection and Backup in Mobile Devices

Inwhae Joe\* *Regular Member*

### 요 약

최근 이동통신 단말기들의 분실 또는 도난을 통해 개인 정보의 유출로 타인의 도용에 우려가 되는 바, 본 논문에서는 이동통신 단말기의 분실 시에 잠금 기능 설정을 설정하지 않은 경우에도 단말기 안의 정보를 원격으로 제어 할 수 있는 방법을 구현하고자 한다. 제안하는 시스템의 주요 기능은 크게 4가지 부분으로 구성 되는 데 사용자가 단말기를 원격 제어할 수 있도록 인터페이스 역할을 하는 웹사이트 제공부, 사용자가 본인임을 확인하며 가입된 이동통신사 시스템으로부터 가입자확인 정보를 수행하는 사용자 확인부, 단말기의 실 소유자임이 확인되면 원격제어 프로그램을 기동시키기 위한 접속코드를 단말기로 전송하여 접속을 설정하는 접속 관리부, 단말기를 원격 제어하기 위한 원격 제어 서비스 코드 및 환경 설정 값을 단말기로 전송하고 단말기로부터 서비스 완료 코드를 수신하는 서비스 실행부를 포함한다.

**Key Words** : Data Protection, Backup, Remote Control, Mobile Communication

### ABSTRACT

The change in performance of the mobile communication field took place due to jumping development of technology, so high performance terminals that anyone can directly search and amend desired information anywhere and anytime, namely, the mobile communication terminals called Smartphone were released to the market. The terminal can store informations that an individual stored, for example, call log, where to make contact and address of acquaintances, transmit/receive message and mail, photographs and videos, etc., but there are worries on surreptitious use of other people due to leaking of personal information through loss or theft of these terminals because of several reasons, so the present thesis aims to realize a method that remotely control information inside a terminal in case of loss of a mobile communication terminal.

### I. 서 론

정부 및 공공기관에서는 정보의 공유와 제공의 목적으로 스마트폰의 어플리케이션을 개발하여 다양한 정보를 제공하고 있으며, 기업에서는 업무의 효율 증대와 시간과 장소에 구애 받지 않는 업무 처리 능력,

고객관리 등의 정보 처리 측면에서 스마트폰을 이용하고 있다. 또한 소비자는 스마트폰을 이용하여 정보 검색, SNS(Social Network Service), 증강현실(Augmented Reality), 개인 GPS(Global Positioning System)등의 서비스를 이용하여 개인의 소비생활의 변화에 까지 영향을 미치고 있는 상태이다.

\* 한양대학교 컴퓨터공학부 이동네트워크 연구실 (iwjoe@hanyang.ac.kr)

논문번호 : KICS2010-10-494, 접수일자 : 2010년 10월 15일, 최종논문접수일자 : 2010년 12월 28일

이러한 기술의 발달에도 불구하고 많은 이동통신 단말기들이 여러 가지 이유로 분실 또는 도난당하고 있으며, 최근 다양한 기능을 제공하는 고가의 단말기들이 급증하면서, 단말기의 분실은 단순히 경제적 손실뿐만 아니라, 단말기에 저장된 개인 정보들, 예를 들어, 지인의 연락처나 주소, 송수신한 메시지 및 메일 등 경제적 가치로 환산하기 어려운 소중한 정보들의 손실까지 그 영향을 미치게 되었다. 따라서 단말기를 분실한 당사자는 무엇보다 개인 정보를 타인이 도용할지도 모른다는 불안한 마음을 가질 수밖에 없는데, 이를 방지하고자 단말기에 잠금 기능을 설정하여 단말기를 사용할 때마다 사용자가 비밀 번호를 입력하도록 하는 방법이 많이 사용되고 있다.

그러나 이러한 방법은 단말기를 사용할 때마다 비밀 번호를 입력해야 하는 매우 번거로운 불편함이 있고, 단말기를 분실하기 이전에 잠금 설정을 하지 않은 경우, 단말기를 분실한 당사자는 개인 정보의 도용에 불안해할 수밖에 없다. 이에 본 논문에서는 단말기를 분실한 경우, 잠금 여부와 상관없이 분실한 단말기를 원격으로 제어하여 타인의 도용을 방지할 수 있는 방안을 살펴보고자 한다.

## II. 제안하는 원격 제어 시스템

### 2.1 시스템 개요

본 논문에서는 분실한 이동통신 단말기를 원격으로 제어하여, 잠금 기능을 설정하지 않은 경우에도 개인 정보에 대한 타인의 무단 도용을 방지하는 원격 제어 서비스 서버 기반의 시스템을 제안하고자 한다. 특히 이동통신 단말기의 응용프로그램 개발은 핸드폰에서의 개발보다는 스마트폰에서의 개발이 용이하며 앞으로의 구매 추이 또한 스마트폰으로의 이동이 강하므로 본 논문에서는 스마트폰에서의 시스템 설계 및 구현을 그 범위로 정하였다.

분실된 이동통신 단말기를 원격 제어하는 방법은 (a) 원격 제어 서비스 서버에 접속한 사용자의 본인 확인을 수행하는 단계, (b) 사용자가 가입한 이동통신사 시스템으로부터 가입자 확인 정보를 수신하여 사용자가 이동통신 단말기의 실소유자인지를 확인하는 단계, (c) 사용자가 이동통신 단말기의 원격 제어 프로그램을 기동시키기 위한 접속 코드를 이동통신 단말기로 전송하는 단계, (d) 접속 코드에 응답한 이동통신 단말기로부터 식별번호를 수신하여 확인하는 단계, (e) 단말기에 대한 원격 제어 서비스 중 선택하여 실행하는 단계, (f) 이동통신 단말기로부터 수행 코드의

제어 서비스가 정상적으로 처리되었음을 나타내는 서비스 완료 코드를 수신하는 단계를 포함한다.

본 시스템의 주요 시스템은 크게 4가지 부분으로 나눌 수 있는데, 사용자가 단말기를 원격 제어할 수 있도록 인터페이스 역할을 하는 웹사이트 제공부, 사용자가 본인임을 확인하며 가입된 이동통신사 시스템으로부터 가입자확인 정보를 수행하는 사용자 확인부, 단말기의 실 소유자임이 확인되면 원격제어 프로그램을 기동시키기 위한 접속코드를 단말기로 전송하여 접속을 설정하는 접속 관리부, 단말기를 원격 제어하기 위한 원격 제어 서비스 코드 및 환경 설정 값을 단말기로 전송하고 단말기로부터 서비스 완료 코드를 수신하는 서비스 실행부를 포함한다.

그림 1은 위 설명을 간략히 도식화한 그림으로 이동통신사로부터의 실사용자임을 확인하는 부분은 생략하였다. 특히 본인 인증 및 가입자 확인에 의해서만 단문 메시지(SMS: Short Message Service)를 발송하여 분실된 이동통신 단말기의 원격 제어 서비스 프로그램을 기동시키므로 타인의 악의적인 단문 메시지로 인해 분실된 이동통신 단말기가 원격으로 제어되는 경우를 방지하고자 한다.



그림 1. 원격 제어 시스템 개요

### 2.2 시스템 구성 및 제어 과정

#### 2.2.1 원격 제어 시스템 구성

분실된 이동통신 단말기를 원격으로 제어하기 위해 원격 제어 서비스 서버는 웹 사이트를 제공한다. 이 웹 사이트는 이동통신 단말기를 분실한 사용자가 분실한 이동통신 단말기를 원격으로 제어할 수 있도록 하는 인터페이스의 역할을 하는 데 사용자가 웹 사이트에 접속한 후, 공인 인증서나 아이디 및 패스워드와 같은 사용자 정보를 입력하여 로그인하면, 원격 제어 서비스 서버는 로그인 한 사용자에게 대한 본인 확인을

수행한다. 이후, 원격 제어 서비스 서버는 로그인 한 사용자에게 대한 본인 확인을 수행하며 원격 제어 서비스 서버는 이동통신사 시스템으로부터 가입자 확인 정보를 수신하여 로그인한 사용자가 분실 단말기의 실소유자인지를 확인할 수 있다.

이를 위해, 원격 제어 서비스 서버는 웹 사이트 회원 가입 시, 원격 제어 서비스를 이용하기 위한 정보, 예를 들어, 성명, 주민 등록 번호나 I-PIN(Internet Personal Identification Number)과 같은 개인 식별 번호, 분실 원격 제어 서비스의 대상이 되는 이동통신 단말기의 전화 번호 등의 입력을 가입자에게 요구하여 상기한 정보들을 미리 저장할 수 있다.

원격 제어 서비스 서버는 사용자의 개인 식별 번호와 분실 단말기의 전화번호를 이동통신사 시스템으로 전송하고, 이동통신사 시스템으로부터 가입자 확인 결과를 수신한다. 원격 제어 서비스 서버의 본인 확인과 이동통신사 시스템의 가입자 확인을 통해 최종적으로 분실 단말기의 실 소유자 확인을 수행할 수 있다.

원격 제어 서비스 서버는 분실 단말기의 실소유자 확인이 완료된 것을 조건으로 하여, 분실 단말기와 통신하기 위한 접속 코드를 분실 단말기로 전송한다. 여기에서 분실 단말기와 통신하기 위한 접속 코드는 원격 제어 서비스를 처리해야 하는 처리 기간 또는 고유의 랜덤한 코드를 포함하며, 접속 코드는 분실 단말기에 설치된 원격 제어 서비스 프로그램을 기동시키는 역할을 한다.

또한, 원격 제어 서비스 서버는 분실 단말기의 원격 제어 서비스 프로그램이 송신한 접속 요청을 수신하여 통신 세션을 설정한다. 이후, 원격 제어 서비스 서버는 분실 단말기로부터 단말기 식별 번호를 수신하여 분실 단말기의 원격 제어가 가능한지 최종적으로 확인 하고 원격 제어 서비스 서버는 사용자로부터 원격 제어 서비스 중 어느 하나에 대한 선택 및 그에 대한 환경 설정 값을 입력 받는다. 여기에서 원격 제어 서비스는 분실 단말기의 사용을 제한하는 잠금(lock) 기능, 문자 메시지 삭제 기능, 지인 연락처(전화번호 및 주소록 등) 삭제 기능, 사진/동영상 삭제 기능, 메일 삭제 기능 또는 출고 당시의 상태로 초기화하는 기능을 포함하며, 각 기능들은 각각의 코드와 매칭 되어 있다. 환경 설정 값을 상기한 원격 제어 서비스를 실행하기 위한 비밀 번호, 특정 단어 또는 문장을 포함하며 원격 제어 서비스에 해당하는 코드 및 환경 설정 값을 식별 번호에 대응하는 분실 단말기로 전송하고 분실 단말기로부터 원격 제어 서비스가 정상적으로 처리되었음을 나타내는 서비스 완료 코드를 수신한다.

한편, 이동통신사 시스템은 원격 제어 서비스 서버로부터 사용자의 개인 식별 번호와 분실 단말기의 전화 번호를 수신하고, 해당 사용자가 자사의 이동통신 서비스를 이용하고 있는지를 확인하여, 그 결과를 원격 제어 서비스 서버에게 전송한다.

이동통신 단말기는 서비스를 제공 받기 전에 원격 제어 서비스를 위한 프로그램(Agent)을 설치하고 이동통신사와 협력하여 단말기의 출시 전에 미리 설치되거나, 사용자가 이동통신 단말기를 이용하여 원격 제어 서비스에 접속한 후 PC에 프로그램을 다운로드 하고 이동통신 단말기와 PC를 연결하여 이동통신 단말기로 프로그램을 전송하여 설치하거나 혹은 이동통신 단말기의 웹 브라우저를 이용하여 다운로드 후 직접 설치한다. 이 프로그램은 사용자가 이동통신 단말기를 분실한 후, 원격 제어 서비스 서버로부터 수신된 단문 메시지(SMS)에 포함된 접속 코드를 수신하여 기동되며, 3G 통신 방식과 같은 무선 통신 방식으로 원격 제어 서비스가 분실 단말기에서 실행될 수 있도록 한다.

분실 단말기에서 프로그램이 구동되면, 분실 단말기는 원격 제어 서비스 서버에게 자신의 단말 식별 번호를 전송하는 데 이때 3G 통신 방식을 사용하여 자신의 단말 식별 번호를 전송할 수 있다. 이후 원격 제어 서비스 서버와 통신 세션이 설정되면, 분실 단말기는 원격 제어 서비스 서버로부터 원격 제어 서비스를 실행하기 위한 코드 및 환경 설정 값을 수신하여, 수신한 코드에 대응하는 원격 제어 서비스를 실행하고, 원격 제어 서비스의 환경 설정 값을 수신된 환경 설정 값으로 지정한다.

### 2.2.2 이동통신 단말기의 서비스 구성

그림 2는 원격 제어 서비스를 실행하는 이동통신 단말기의 서비스 구성을 표시한 블록도이다. 단말기는 네 가지 서비스 형태로 구성되어 있는데 프로그램 설치부(131), 프로그램 기동부(132), 접속 관리부(133), 서비스 실행부(134)를 포함하고 있다.

먼저, 프로그램 설치부(131)는 원격 제어 서비스 서버로부터 원격 제어 서비스를 위한 프로그램을 다운로드하여 설치한다. 참고로, 이동통신 단말기에 설치되는 프로그램은 사용자가 별도의 PC를 이용하여 원격 제어 서비스 서버에 접속한 경우, PC에 제공된 프로그램을 PC로부터 전송 받을 수 있고, 이동통신사와 협력하여 이동통신 단말기의 출고 시 미리 설치될 수도 있는데 미리 설치된 경우는 설치 과정이 생략 가능하다. 프로그램 기동부(132)는 원격 제어 서비스 서

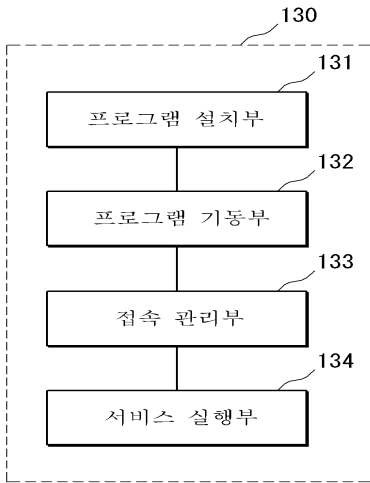


그림 2. 이동통신 단말기 서비스 구성도

버로부터 접속 코드를 수신하는 경우, 원격 제어 서비스를 위한 프로그램을 동작시킨다. 여기서 접속 코드는 분실 단말기로 일련 번호(S/N), 원격 제어 서비스를 처리해야 하는 처리 기간 또는 고유의 랜덤한 코드를 포함한다. 참고로, 상기한 접속 코드가 수신되기 전까지는, 분실 단말기에 설치된 프로그램은 휴면상태에 있으며, 전술한 바와 같이, 접속 코드는 본인 확인 및 가입자 확인이 완료된 경우에만 수신될 수 있다.

한편, 접속 관리부(133)는 프로그램 기동부(132)에서 프로그램을 동작시키면, 자신의 단말기 식별 번호를 원격 제어 서비스 서버에게 전송하는 데 이때, 원격 제어 서비스 서버로의 단말기 식별 번호 전송은 3G 통신 방식을 사용할 수 있으며, 분실 단말기에 설치된 원격 제어 서비스를 위한 프로그램은 원격 제어 서비스를 받기 위한 준비가 완료된다.

서비스 실행부(134)는 원격 제어 서비스 서버와 통신이 이루어지면, 원격 제어 서비스 서버로부터 원격 제어 서비스를 실행하기 위한 코드 및 환경 설정 값을 수신하고, 수신한 코드에 대응하는 원격 제어 서비스를 실행한다. 예를 들어, 원격 제어 서비스 서버로부터 수신한 코드가 원격 제어 서비스 기능 중 잠금 기능에 해당하고, 수신한 코드에 대한 환경 설정 값, 즉, 잠금 기능에 사용할 비밀 번호가 '1234'라면, 서비스 실행부(134)는 분실 단말기에 잠금 기능을 실행하고, 잠금 비밀 번호를 '1234'로 세팅하며 추후, 사용자가 분실 단말기를 찾게 되어 사용하고자 하는 경우, 잠금 비밀 번호인 '1234'를 입력하여 잠금 기능을 해제할 수 있다. 또한 서비스 실행부(134)는 원격 제어 서비스의 실행 및 환경 설정 값이 지정되면, 이를 알리

는 코드를 원격 제어 서비스 서버에게 전송한다.

2.2.3 이동통신 단말기의 원격 제어 과정

그림 3은 사용자가 단말기를 분실한 이후 이동통신 단말기를 원격으로 제어하는 과정을 표시한 흐름도이다. 사용자가 단말기 분실 이전에 잠금 설정 기능과 같은 타인의 사용을 방지할 수 있는 기능을 설정하지 않았으며, 원격 제어 서비스를 위한 웹 사이트에 회원으로 가입하여 원격 제어 서비스를 위한 프로그램을 단말기에 설치한 경우이다.

먼저, 사용자는 분실 단말기를 원격으로 제어하기 위해, 회원으로 가입한 웹 사이트에 접속한다(S401). 이때, 사용자는 웹 사이트에 접속 가능한 모든 단말기로 이용이 가능하다.

단계 S401 후, 원격 제어 서비스 서버는 웹 사이트에 접속한 사용자 단말의 공인 인증서 또는 사용자가 입력한 아이디 및 패스워드와 같은 인증정보를 통해, 로그인 한 사용자에 대한 본인 확인을 수행한다(S402).

단계 S402 후, 원격 제어 서비스 서버는 사용자의 개인 식별 신호와 분실 단말기의 전화번호를 이동통신사 시스템으로 전송한다(S403).

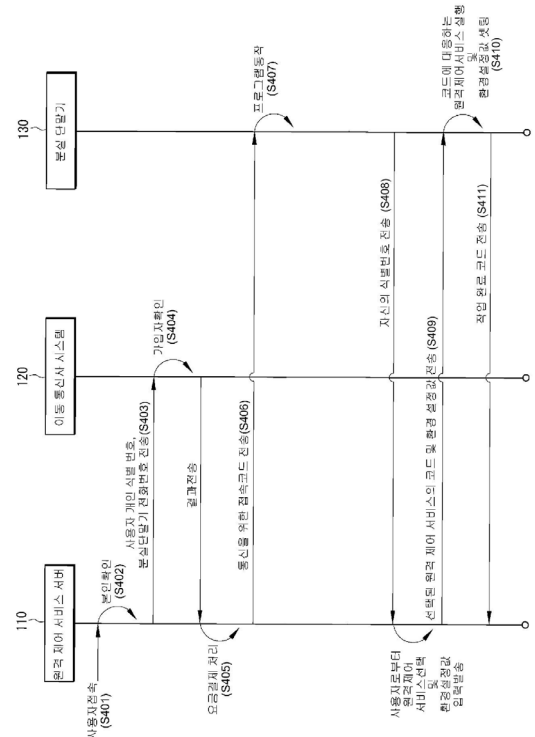


그림 3. 이동통신 단말기의 원격 제어 과정

단계 S403 후, 이동통신사 시스템은 원격 제어 서비스 서버로부터 수신한 사용자의 개인 식별 번호 및 분실 단말기의 전화번호에 기초하여 해당 사용자가 자사의 서비스에 가입되어 있는지, 그리고 해당 사용자가 소유한 단말기와 분실한 단말기가 일치하는지를 확인한다(S404).

단계 S404 후, 원격 제어 서비스 서버는 이동통신사 시스템으로부터 가입자 확인 결과를 수신하고 요금의 결제처리를 수행한다(S405).

단계 S405 후, 원격 제어 서비스 서버는 분실 단말기와 통신하기 위한 접속 코드를 포함한 단문 메시지(SMS)를 분실 단말기에게 전송한다(S406). 여기에서 접속 코드는 원격 제어 서비스를 처리해야 하는 처리기간 또는 고유의 랜덤한 코드를 포함하며, 원격 제어 서비스 서버에서 전송하는 접속 코드는 분실된 이동통신 단말기에 설치된 프로그램을 기동시키는 역할을 한다.

단계 S406 후, 분실 단말기는 원격 제어 서비스 서버로부터 접속 코드를 수신하여 프로그램 동작을 시작한다(S407).

단계 S407 후, 분실 단말기는 자신의 단말기 식별 번호를 원격 제어 서비스 서버에게 전송한다(S408).

단계 S408 후, 원격 제어 서비스 서버는 분실 단말기로부터 단말기의 식별 번호를 수신하고, 사용자로부터 선택된 원격 제어 서비스에 해당하는 코드 및 입력된 환경 설정 값을 분실 단말기로 전송한다(S409).

단계 S409 후, 분실 단말기는 원격 제어 서비스 서버로부터 원격 제어 서비스를 실행하기 위한 코드 및 환경 설정 값을 수신하여, 수신한 코드에 대응하는 원격 제어 서비스를 실행하고 환경 설정 값을 지정한다(S410).

단계 S410 후, 분실 단말기는 원격 제어 서비스의 실행 및 환경 설정 값이 지정되면, 이를 알리는 코드를 원격 제어 서비스 서버에게 전송한다(S411).

### III. 시스템 구현

#### 3.1 원격 제어 시스템 구현

본 논문에서 제안한 원격 제어 시스템의 개발 환경은 크게 원격 제어 서비스 서버와 이동통신 단말기의 두 부분으로 구성되어 있는데, 원격제어 서버는 사용자 로그인과 이동통신 단말기에 대한 정보와 같은 웹 사이트를 제공하며 이동통신 단말기는 안드로이드 운영체제를 이용하는 HTC사의 디자이너를 이용하였다.

표 1. 원격 제어 시스템 개발환경

분류	환경
원격 제어 서비스 서버	운영체제: Windows 2008 Server 개발언어: ASP.NET(C#) 개발 툴: Visual Studio 2008 하드웨어 : Desktop
이동통신 단말기	운영체제: Android 개발언어: Java 개발 툴: Eclipse 하드웨어: HTC Desire

#### 3.2 웹 사이트 제공부

웹 사이트 제공부의 화면 디자인은 실제 유사한 시스템으로 구성되어 있는 Microsoft사의 OWA(Outlook Web Access)를 참고했다. OWA는 Exchange 제품의 웹 버전으로서 Remote Wipe Out이라는 기능으로 단말기 초기화를 제공하고 있지만, 지원하는 스마트폰은 ActiveSync라는 푸시기술을 사용하는 Windows Mobile 운영체제를 탑재한 단말기만 가능하다는 단점과 단지 데이터 삭제 기능만을 가지고 있다.

사용자는 최초에 원격 제어 시스템을 이용하기 전에 웹 사이트에 로그인해야 하며 로그인을 통해 원격 제어 시스템에 접근이 가능하다. 시스템에 정상적으로 로그인 한 이후에는 그림 4와 같이 이동통신 단말기를 제어하기 위한 화면으로 이동이 가능하다. 본인 인증을 거친 후 본인의 이동통신 단말기를 등록 할 수 있으며 등록되지 않은 단말기 일지라도 본인의 이동통신 단말기임이 확인 되면 단말기 내부의 Agent Service의 구동으로 원격제어가 가능하다.

웹 사이트 제공부에서는 개인의 등록된 이동통신 단말기의 운영체제, 전화번호와 현재의 상태 및 최근 단말기의 동기화 상태를 보여주며 단말기의 동기화 정보 등을 알 수 있는 로그 기능을 제공하고 단말기를 원격 제어하기 위한 장치 데이터 삭제 기능을 제공한다.

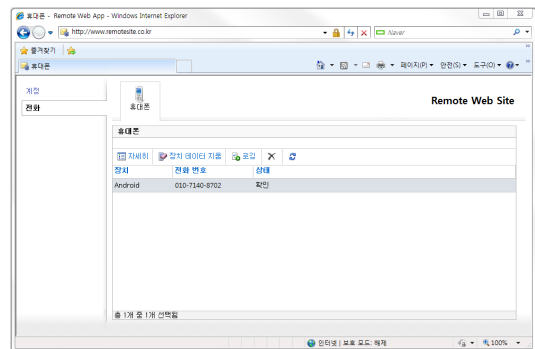


그림 4. 원격 제어 사이트

### 3.3 단말기 관리부

#### 3.3.1 단말기 접속 관리부 구현

그림 5는 이동통신 단말기 접속부 구성 화면으로 SMS를 수신하였을 때 코드상의 환경 정보를 통해 직접 정의한 함수로 이동되어 실행되는 모습을 구조화하였다. 단말기에서는 서비스 형태로 문자메시지는 보이지 않으며 단말기 내부의 Agent Service는 인증된 단말기 사용자로부터의 코드를 인식하여 원하는 원격 제어를 실행하게 된다.

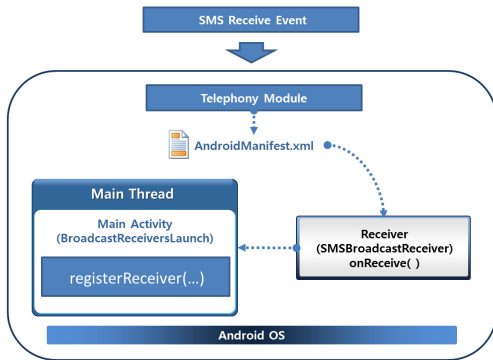


그림 5. 이동통신 단말기 접속부 구성

#### 3.3.2 단말기 서비스 실행부 구현

그림 6은 단말기의 실제 사용자의 데이터를 재설정하는 화면으로 Agent Service는 접속부를 통해 들어온 SMS의 코드를 확인하고 사용자의 데이터 초기화 실행을 통해 단말기를 잠그고 사용자의 데이터 및 정보를 외부사용자로부터 보호하기 위해 단말기를 초기화하는 화면이다.

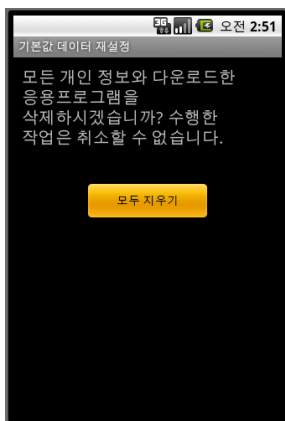


그림 6. 단말기 서비스 실행부 구현

실제 구성에서는 경고 메시지 없이 이동통신 단말기가 초기화되며 데이터 백업 및 전송은 실제 서비스가 실행하기 이전에 압축하여 서버로 전달되고 보관되며 웹 사이트를 통해 정보를 다운로드 할 수 있다.

## IV. 결 론

본 논문에서 제안된 원격 제어 시스템에서는 기존의 시스템과 차별화를 두기위해 분실 이전에 잠금 기능을 설정하지 않은 경우에도 분실한 이동통신 단말기를 원격으로 제어하여 이동통신 단말기 및 개인 정보에 대한 타인의 무단 도용을 방지하는 방법을 제안하고 그 장치를 구현하였다. 단말기의 원격제어 기능을 단계별로 설계하여 단말기 잠금기능, 주요 데이터 전송기능, 개인 정보 삭제 및 초기화기능으로 분류하여 실제 구현에 적용하였다.

## 참 고 문 헌

- [1] 김재영, "스마트폰과 소비자 유형 전망", 2010.04.
- [2] 교육과학기술부, "2009 과학기술연감", 2010.02.
- [3] 송성현, "MITM 공격에 강인한 OTP시스템의 설계", 2009.06.
- [4] 김성개, "사용자 환경과 스마트폰 특성 요인이 인지된 유용성과 사용용이성 및 수용의도에 미치는 영향에 관한 연구", 2009.06.
- [5] 전자통신동향분석 제 23권 제2호 2008.04.
- [6] 문종식, "모바일 환경에서의 티켓을 이용한 AAA 메커니즘에 관한 연구", 2007.12.

조 인 휘 (Inwhee Joe)

정회원



1983년 2월 한양대학교 전자공학과  
 1994년 12월 미국 University of Arizona, Electrical and Computer Engineering, M.S.  
 1998년 9월 미국 Georgia Tech, Electrical and Computer Engineering, Ph.D.

1992년 12월 (주) 데이콤 종합연구소 선임연구원  
 2000년 6월 미국 Oak Ridge 국립연구소 연구원  
 2002년 8월 미국 Bellcore Lab (Telcordia) 연구원  
 2002년 9월~현재 한양대학교 컴퓨터공학부 부교수  
 <관심분야> Mobile Internet, Cellular System and PCS, Sensor Networks, Mobility Management