JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 17, No. 10 : 2316~2322, Oct. 2013

익명성을 활용한 사용자의 실시간 위치정보 보호모델

문형진*

Real Time User Location Information Protection Model Using Anonymity

Hyung-Jin Mun*

College of Electrical & Computer Engineering, Chungbuk National University, Chungbuk 361-763, Korea

요 약

ICT 발달로 인해 스마트폰이 WiFi, GPS, 3G 등 다양한 하드웨어가 추가되면서 새로운 기능을 제공하는 어플리케이션이 급격하게 개발되고 있다. 어플리케이션을 통해 개인 사진, 전화번호, 통화목록, 위치정보 등의 다양한 개인정보들이 생성되고, 저장되고, 활용되고 있다. 스마트폰에 저장된 개인정보가 폰 분실이나 어플리케이션에 의한 유출 사례로 인해 프라이버시 침해가 심각하다. 스마트폰의 GPS와 인터넷이 결합된 위치정보 서비스는 다양하게 제공되고 있다. 위치정보유출로 인한 피해가 심각해지면서 허가된 사용자만이 접근할 수 있는 기술들이 제안되고 있다. 본 논문에서는 위치정보주체와 정보사용자의 식별정보를 최소화하고, 식별이 가능한 핸드폰 번호와 같은 정보는 익명화 처리를 하므로 써 개인정보노출의 피해를 줄이고, 위치정보를 저장한 서버에서의 오남용을 막을 수 있는 모델을 제안하였다. 제안모델을 적용하면 프라이버시를 보호하면서 위치이력정보를 통한 이동경로서비스를 제공하는 어플리케이션 개발이 가능하다.

ABSTRACT

Due to the development of ICT, with using hardwares such as WiFi, 3G and GPS and so on, smartphone could have provided a lot of applications with novel functions rapidly. Through such applications, lots of personal information such as personal location, personal images, and list of phone calls is created, saved and widely used. Because there is lots of leakage of the stored personal information due to loss of phone and application, privacy violation have been important issue nowadays. Smartphone with GPS and Internet provides location information. To protect the information, the technologies that only the authorized user can access it while inquiring the location information have been proposed. In this paper, to minimize the identification information for location information subject and information user and anonymize the identifiable information such as phone number, we proposed a model that can reduce the leakage of information and avoid the wrong usage of the stored information in the server. This technique will be used for protecting privacy when developing the application that provides routing service through location history information.

키워드 : 익명성, 위치기반서비스, 프라이버시 보호, 개인정보보호

Key word : Anonymity, LBS, Privacy Protection, Smartphone

접수일자 : 2013. 08. 09 심사완료일자 : 2013. 08. 28 게재확정일자 : 2013. 09. 17

*** Corresponding Author** Hyung-Jin Mun(E-mail:jinmun@gmail.com, Tel:+82-43-276-2253)
College of Electrical & Computer Engineering, Chungbuk National University, Chungbuk 361-763, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.10.2316 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

ICT 기술의 발달로 인해 미국의 90%이상이 핸드폰을 사용하고 성인의 56%가 아이폰, 안드로이드 등 스마트폰의 사용하고 있다[1]. 가트너[2] 리포트에 따르면 전세계 휴대폰의 판매량이 2012년 4분기에 4.72억이고, 스마트폰이 2.07억으로 증가한다. 애플의 앱스토어나 구글의 Play 스토어에서 다양한 어플리케이션들을 다운로드하여 스마트폰 상에서 실행하여 편하게 사용할 수 있기 때문이다[3-5]. 수 많은 개발자들이 안드로이드 어플리케이션들이 개발하여 구글 Play 스토어[6]에 소스 검증 없이 등록하고 있다. 스마트 폰 사용자는 스토어에 등록된 어플리케이션을 신뢰하고 사용함으로 써 주소록, 전화번호, 사진, 위치정보등 다양한 개인정보를 어플리케이션의 데이타베이스와 외장 메모리(SDCard) 등에 저장한다. 많은 회원을 가지고 있는 페이스북이나 카카오톡의 경우, 사용자의 위치 정보, 이메일 주소, 가족 사진 및 전화번호 등 다양한 개인정보들이 어플리케이션의 데이타베이스에 저장되어 있다. 폰 분실이나 악의적인 어플리케이션을 통해 저장된 정보에 대한 안전성 문제가 야기되고 있다[3].

현재, 구글(Google)사는 안드로이드 운영체제와 API를 제공함으로써 많은 개발자들이 스마트 폰에 내장되어 있는 하드웨어 등을 활용하여 다양한 서비스를 제공하고 있다. 특히, 스마트폰의 GPS 모듈을 이용한 스마트폰 사용자의 위치 기반 서비스가 가능해 졌다. 통신사업자 및 위치정보 서비스 사업자는 스마트폰에서 위치정보를 쉽게 수집할 수 있어 스마트폰 사용자의 위치정보에 대한 유출로 인해 프라이버시 침해가 발생한다[5]. 노출시 개인의 프라이버시 침해가 우려되는 위치정보 보호를 위한 시스템들이 연구되어 지고 있다[7-8].

사용자의 위치정보를 보호하는 위치기반 서비스는 위치 정보를 접근할 수 있는 사용자 목록을 작성하여 목록에 있는 사용자만이 접속할 수 있는 시스템이다. 하지만 식별정보를 가지고 있는 서버에서 위치정보 노출시 프라이버시 침해를 막을 수 없다.

본 논문에서 사용자의 식별정보를 익명화 처리하여 서버에 사용자 위치정보와 함께 저장하는 모델을 제안하였다. 제안모델은 서버의 내부사용자에 의해 위치정보가 유출되더라도 식별정보가 익명화되어 프라이버시 침해를 최소화 할 수 있다.

본 논문은 다음과 같이 구성된다. 2절에서는 위치정보 기반 서비스와 어플리케이션 등 기존 시스템의 취약점을 언급하고 3절에서는 익명성을 활용하여 프라이버시 침해를 최소화하는 제안모델을 제안하고, 4절에서는 제안 모델에 대한 분석 및 평가를 한다. 5절에서는 결론과 향후연구를 기술한다.

Ⅱ. 관련연구

2.1. 위치정보 기반 서비스

스마트폰에 내장된 GPS 모듈을 활용하여 사용자의 위치를 파악하여 위치기반 서비스를 다양하게 지원하고 있다. 위치기반서비스(LBS : Location Based Service)는 현재 증강현실을 통해 상업적으로 서비스되고, 안전 및 구난 서비스, 추적서비스, 물류 및 관제 서비스, 교통 및 항법 서비스 등에 다양하게 적용되고 있다[9](표1).

표 1. 위치정보 기반 서비스
Table. 1 Location based Service

대분류	중분류	세분류
개인	안전 및 구난 서비스	구조요청, 가족안전위치서비스, 기상예보
	주변정보 서비스	상점, 엔터테인먼트 시설, 차량 관련시설, 숙식 시설 정보 등
	추적서비스	친구, 가족 찾기, 유명인 찾기
	교통, 항법 서비스	최단 경로, 구간속도, 교통노선 정보 제공, 최적 경로
	광고 및 상거래 서비스	할인쿠폰, 티켓예매, 광고 상거래 등
기관	안전 및 구난 서비스	현장 노동자 응급서비스
	추적서비스	차량 위치추적, 영업사원 위치 파악 및 관리
	교통, 항법 서비스	화물차량 항로 제공

<자료: KISA, 위치정보의 활용현황 조사분석, 2006>

2.2. 스마트폰 어플리케이션의 취약점

스마트폰을 이용하여 금융거래, 결제시스템 등의 사용이 증가되면서 관련정보 유출 및 프라이버시 침해사례가 빈번하게 발생하고 있다[10]. 뿐만 아니라 설치된

어플리케이션에 대한 역공학을 통해 프로그램의 구조 등을 파악하면 다양한 침해가능성이 존재한다[11]. 스마트폰에 저장된 정보 유출이외에도 원격제어, 과금 유도, 유해사이트 접속 등의 문제가 존재한다. 스마트폰의 GPS모듈을 활용하여 수집되는 위치정보로 인해 발생 가능한 공격을 (표2)과 같이 분류할 수 있다[7]. 악의적인 3자에 의해 위치정보의 위조 및 변조의 가능성이 제기 되고, 폰 사용자의 실시간 위치정보가 이동통신사에 의한 노출가능성이 존재한다.

표 2. 위치정보 시스템 공격
Table. 2 Attack on the Location Information System

공격 형태	공격 목적
비인증 취득자	- 스마트 사용자의 위치 파악
인증된 취득자	- 허용된 위치정보의 범위보다 높은 정확도의 위치 획득 - 위치정보를 노출하거나 동의된 것 이상 추적하는 경우
제 3자	- 위치정보 주체의 위치정보가 배포되는 것을 막는 경우 - 위치정보를 수정하고나 파괴하고자 하는 경우 - 허용되지 않은 제3자에게 redirect하고자 하는 경우 - 시스템 자체를 멈추게 하고자 하는 경우

2.3. 프라이버시를 고려한 기존 시스템

폰 사용자의 위치정보는 GPS 모듈을 이용하여 위치기반 서비스 어플리케이션이 해당 서비스 사업자의 서버에 전송한다. 해당 어플리케이션 사용자 간에 자신의 위치정보를 실시간으로 제공함으로써 다양한 서비스를 제공받지만 이로 인해 사용자의 프라이버시 침해 발생이 가능하다. 뿐만 아니라, 스마트 폰 사용자의 실수로 인해 저장된 개인정보가 다른 어플리케이션이나 공격자에게 정보를 제공하는 사례가 발생한다.

프라이버시를 고려한 기존 시스템의 경우, 자신의 위치정보를 불특정 다수에게 제공하고, 위치정보에 대한 개인의 시간대 및 지역 설정의 부재로 인해 새로운 침해 가능성을 야기한다. 사용자의 실수를 원천적으로 차단하고, 자신의 정보를 조회할 수 있는 사용자 선택을 편리하게 하고, 제공시간이나 영역 설정을 부여해야 한다.

그림 1은 장원준이 제안한 프라이버시를 고려한 시스템의 구조를 나타낸 것이다[7].

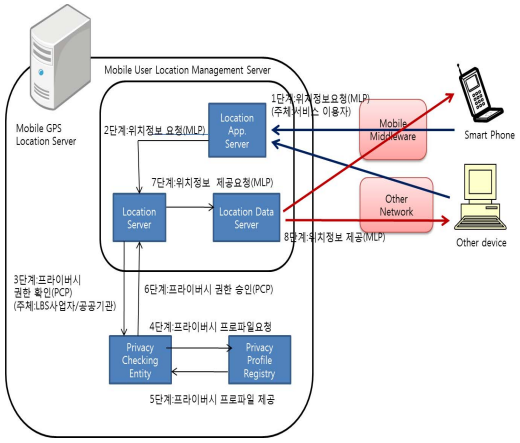


그림 1. 기존 시스템 구조
Fig. 1 The existing System Structure

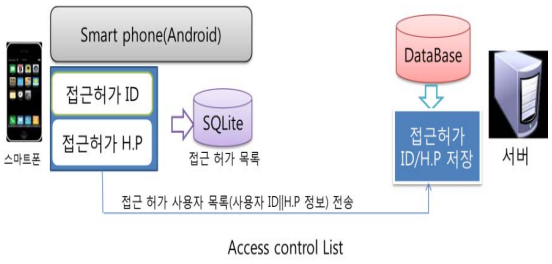


그림 2. 접근허가 목록
Fig. 2 Access Permission List

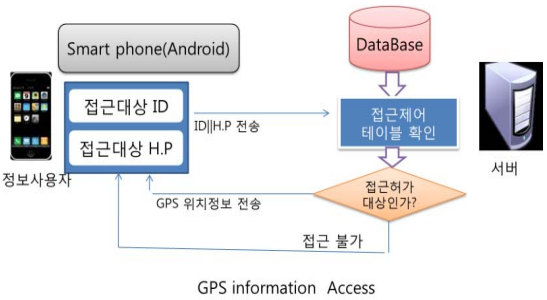


그림 3. 위치정보 조회
Fig. 3 Location Information Searching

그림 2는 위치정보 주체인 폰사용자의 위치정보를 접근할 수 있는 사용자의 ID와 스마트폰 번호를 스마트폰안에 있는 데이타베이스 SQLite 에 저장하고, 작성된 목록을 서버에 제공한다. 그림 3은 다른 사람의 위치정보를 조회하고자 하는 사용자가 서버에 사용자 인증이 끝나고, 위치정보를 조회하는 과정을 나타낸 것이다. 서버에 저장된 접근허가목록에 자신이 있다면 위치정보를 제공하고, 없을 경우에는 접근을 불허한다.

사용자인증은 OTP 방식으로 하고, 위치정보주체가 작성한 허가목록에 의해 정보 접근제어를 했지만 정보를 저장하는 서버에서 위치정보와 함께 개인 식별정보(핸드폰, 이메일 주소 등)이 저장되어 서버 관리자에 의해 유출가능성이 존재한다.

Ⅲ. 제안 모델

폰 사용자는 자신의 위치정보를 이동통신사업자 및 위치기반서비스 사업자에게 정보를 제공하지만 수집된 정보는 위치 관련 서비스에만 사용되어야 한다. 위치정보에 대한 사업자의 오남용을 막기 위해 정보주체의 식별정보를 가능한 익명화하여 저장하므로써 프라이버시 침해를 최소화 할 수 있다.

3.1. Accesss Control List

안전한 서비스를 위해서는 정보 주체인 개인이 자신의 위치정보를 접근할 수 있는 사용자 목록을 작성해야 한다. 위치정보를 조회할 수 있는 사용자는 주체가 알고 있는 지인 중심으로 구성된다. 폰에 저장되어 있는 주소록을 기반으로 자신의 정보 접근 허가 목록을 작성하므로 편리성을 도모하고, 작성에 따른 오류를 차단할 수 있다. 정보 유출의 대부분 관리자나 사용자의 실수로 비롯되는 사례가 많다. 즉, 자신의 전화번호 목록에 있는 사람들 중에 선별하여 작성하는 것이 주체 실수로 상관이 없는 사람이 추가하는 것을 막을 수 있다. 다음은 접근제어목록(ACL : Accesss Control List)를 작성하여 위치관리서버에 전송하는 과정이다.

1. 위치정보주체의 전화번호목록을 조회한다.
2. 이름과 전화번호를 확인후 접근을 허가해 줄 사용자 목록을 작성한다.
3. 전화번호를 익명화 처리를 한다. 11자리의 전화번호에서 2~4의 번호를 * 표시를 함으로써 주체가 확인 가능할 수준으로 익명화 처리한다. 예를 들어, 폰 번호가 010-1234-5678 일때 010-12**-5678로 대치하지만 정보주체는 몇개의 정보만으로도 식별이 가능하고, 목록내에서 충돌가능성이 적다.
4. 정보주체의 ID(=hash(tel) : 주체의 전화번호의 해시값)과 함께 익명화 처리가 된 사용자의 전화번호 목록을 위치관리서버에 전송한다.

위치기반서비스는 특수한 상황에서 불특정 다수에게 자신의 위치정보를 접근허용해야 할 경우가 존재한다. 택배기사의 위치정보를 조회할 수 있는 앱(App)의 경우, 송장번호 정보를 이용하여 인증하고, 자신의 위치정보를 조회할 수 있는 사용자 목록을 배송지의 연락처를 근거로 ACL을 작성하면 택배 수령자는 기사의 위치정보의 조회가 가능하다.

3.2. OTP를 이용한 사용자 인증

개인의 위치정보를 조회하기 위해서는 반드시 인증이라는 보안절차가 필요하다. 주체의 ACL에 등록된 사용자인지를 확인함으로써 주체의 위치정보에 대한 프라이버시 침해를 막을 수 있다.

3.2.1. 회원가입

위치정보의 주체나 사용자는 회원가입을 해야 한다. 접근자의 식별을 위해 회원가입을 하지만 저장된 위치정보와 연계될 경우, 심각한 프라이버시 침해 발생이 가능하다. 제안 모델에서는 ID를 자신의 스마트폰 번호의 해시값으로 생성한다. 위치관리서버에 스마트폰 번호의 해시값과 비밀번호 h(ID⊕PS) 이외의 식별을 위한 정보는 저장되지 않는다. 비밀번호 분실 요청시 임시 비밀번호를 SMS 이용하여 변경이 가능하다.

3.2.2. 사용자인증

자신의 위치정보의 접근제어목록을 제공하거나 다른 사람의 위치정보를 조회할때 정당한 사용자인지를 확인하는 인증이 필요하다. ID/PS 기반의 인증은 무선으로 데이타를 전송하므로 노출의 위험이 존재한다. 이를 위해 PS(비밀번호) 전송없이 변경되는 정보값인 일회성 패스워드(OTP) 방식의 사용자인증을 한다[5].

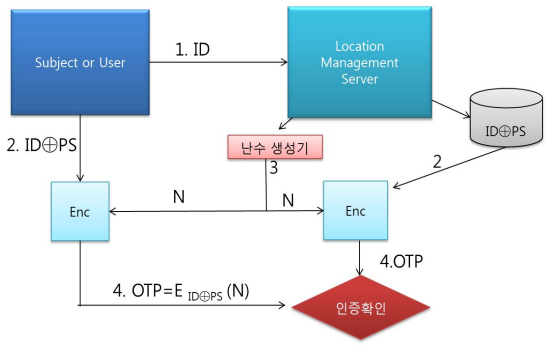


그림 4. OTP를 이용한 사용자인증
Fig. 4 User Authentication using OTP

그림 2에서 보듯이 ID와 OTP 값만 서버에 전송하여 인증을 받기 때문에 PS 노출의 위험성이 현저하게 낮아진다. 전송되는 ID와 난수 N을 알아도 공격자가 PS를 모른다면 h(ID⊕PS)를 계산할 수 없기 때문에 암호화한 OTP 값을 알아낼 수 없다.

3.3. 익명성을 이용한 위치정보 보호모델

그림 3은 위치정보를 정보주체가 허락한 사용자만이 접근을 허용하고, 위치정보를 최소한의 정보만을 저장하여 프라이버시 침해를 최소화하는 제안 모델이다.

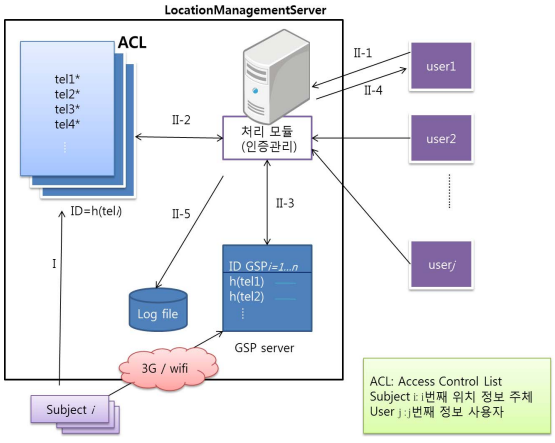


그림 5. 제안 모델
Fig. 5 The proposed Model

단계 I.

택배기사의 위치정보를 제공하는 서비스나 자신의 위치를 필요에 의해 가족, 동료들에게 제공하는 서비스를 하기 위해서는 먼저 정보주체인 개인이 서비스 업체의 위치관리서버에 ACL를 등록한다.

단계 II.

1. 정보 사용자는 위치관리서버의 처리모듈에 자신의 ID와 위치 조회를 하고자 하는 정보주체의 핸드폰번호를 전송하여 인증을 요청한다.
2. 사용자의 ID를 통해 사용자 인증을 한 후 요청한 정보주체의 핸드폰번호를 이용하여 ACL를 조회해서 접근이 허가되었는지를 확인한다.
3. 허가된 사용자인 경우 GPS 정보서버에 접속하여 해당 위치정보를 검색한다. 서비스에 따라 위치정보 이력을 처리모듈에 전달한다.
4. 처리모듈은 GPS 서버로부터 받은 정보를 사용자에게 전송한다.
5. 전송이 완료된 후 서비스 정보를 LOG 파일에 기록한다. 프라이버시 침해 발생시 정보주체가 LOG파일을 조회할 수 있다. 경우에 따라 ACL에 없는 사용자의 접근 실패 로그 기록도 가능하다.

Ⅳ. 모델 검증 및 평가

개인 사용자가 자신의 위치정보를 조회할 수 있는 목록을 작성하고 목록에 있는 사용자만이 인증을 통해서 위치정보를 조회할 수 있는 장원준[5]의 모델과 비교 분석한다.

ID	···	tel	permission	GPS	···
hong		01012345678	true	gps_i	

(a)

ID	···	tel	permission	GPS$_i$	···
s#h4&		01012**5678	true	gps_i	

(b)

그림 6. ACL 구조 비교 분석 (a) ACL 기존모델 (b) ACL 제안 모델
Fig. 6 Comparison of ACL structure (a) ACL in the existing model (b) ACL in the proposed model

4.1. Access Control List 구조

위치기반 서비스관련 어플리케이션은 내장 데이타베이스 SQLite의 주소록을 기반으로 접근이 가능한 사용자 목록을 작성된다.

4.2. 정량적 평가 및 비교 분석

첫째, 제안모델에서는 그림 6처럼 서버에 저장된 정보를 최소화하고, 특히 식별정보에 관련하여 해시값이나 익명화 처리를 통해 정보 노출시 피해를 최소화하였다. 기존모델을 비롯하여 위치기반 서비스를 제공하는 어플리케이션에 회원가입을 통해 서비스를 제공하는데 ID/PS 이외에도 이메일, 핸드폰번호 등 식별정보를 그대로 서버에 저장하여 특정인 위치정보의 노출 가능성이 존재한다.

둘째, 이동경로를 제공함으로써 다양하고, 질 높은 서비스가 필요하다. 기존 모델에서는 실시간 위치정보만을 제공하고 있지만 위치이력정보에 대한 언급이 없다. 영업사원 관리, 택배기사 등의 위치이력정보는 더 나은 위치기반 서비스를 제공할 수 있다. 제안모델에서 위치이력정보를 제공할 수 있도록 서비스를 확장하였다.

셋째, 정보접근목록을 개인이 ACL 작성시 실수로 인해 자신의 위치정보가 노출될 가능성이 존재한다. 제안모델에서는 대체로 접근을 허용하는 사용자는 전화번호목록에 존재하므로 전화번호 목록을 가지고 접근제어목록(ACL)을 작성하므로 편리성과 함께 실수에 따른 유출가능성을 최소화 한다.

넷째, 서버단에서의 정보유출이외에도 정보사용자에 의한 유출가능성도 존재한다. 제안모델에서는 LOG 파일을 서버에 설치하여 조회한 정보사용자의 이력이외에도 허가되지 않은 사용자의 요청 목록을 작성함으로써 향후 유출에 의해 프라이버시 침해시 정보주체의 파일내용을 확인할 수 있다.

Ⅴ. 결 론

ICT 발달로 인해 스마트폰 성능이 향상되고, 전화기기 이상의 다양한 기능을 가지게 되었다. 편리성이 강조되면서 스마트폰에 금융정보를 비롯하여 개인사진, 전화번호, 위치정보 등 다양한 개인정보를 저장하게 되었지만, 스마트폰 분실이나 어플리케이션에 의한 정보유출로 인한 프라이버시 침해가 발생하고 있다. GPS 기능을 이용한 위치기반 서비스는 스마트 폰 사용자 뿐만 아니라 서비스 사업자에게 많은 이익을 제공해 준다. 하지만 위치정보의 오남용이나 악의적인 접근, 위치정보의 위변조시 정보 주체에게 심각한 프라이버시 침해를 발생시킬 수 있다. 악의적인 위치정보의 실시간 조회는 개인의 위치가 감시 받는 사회로 발전되어 사회문제화 되고 있다.

본 논문에서 위치정보 서비스를 제공하는 서버에서 위치정보를 보호하기 위해 익명성을 이용하여 폰 분실 및 프로그램 사용시 스마트폰 안의 개인정보를 보호하는 모델을 제안하였다. 자신의 위치정보를 접근할 수 있는 목록을 작성하여 자신의 정보를 보호할 수 있지만 이 역시 서버에 저장된 자신의 정보 유출 가능성을 배제할 수 없다. 제안 모델에서는 서버에 저장된 정보를 최소화하고, 정보를 제공하는 주체와 정보를 조회하는 사용자의 정보에 대해 익명성 기능을 이용하여 유출피해를 최소화하였다.

로그 파일 및 식별정보를 최소화함으로 영업사원 관리, 택배기사의 위치정보를 이용하여 택배 신청 및 택배 도착시간 예측 등 위치이력정보를 제공하는 서비스가 가능하다. 정보주체의 정책에 기반하여 스마트폰에서 생산된 정보, 서버에 저장된 정보를 사용불능의 상태로 변경하거나 정보폐기에 대한 향후 연구들이 필요하다.

REFERENCES

[1] PewInternet. Smartphone Ownership 2013 [Internet]. Available:http://pewinternet.org/Reports/2013/smartphone-ownership-2013/Findings.aspx

[2] Gartner. November Report(2013) [Internet]. Available: http://www.gartner.com/newsroom/id/2335616.

[3] Yajin Zhou, Xinwen Zhang, Xuxian Jiang, Vincent W.Freeh, “Taming Information-Stealing Smartphone Application (on Android),” in *Proceedings of the 4th International Conference on Trust and Trustworthy Computing* (TRUST 2011), Pittsburgh, PA, pp.93-107, 2011.

[4] Seokhoon Ko, “A Trend of Android Platform,” *The Korea Contents Association Review*, vol. 8, no. 2, pp.45-49, Jun.

2010.

[5] Shane Conder and Lauren Darcey, “Android Wireless Application Development,” in *Addison-Wesley Professional*, 2nd ed. Pearson Education, pp. 54-138, 2010.

[6] Google. Android Market [Internet]. Available: https://market.android.com/

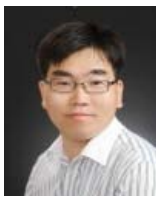
[7] Wo-jun Jang, Hyong-Woo Lee. “Development of Secure Access Control System for Location Information on Smart Phone”, *Journal of the Korea Institute of Information Security and Cryptology* ,Vol. 21, no. 2, pp.139-147, Apr.2011.

[8] In-jai Kim, Jae-won Choi, Woon-Yoeng Kim, “The Application for the Protection System of Location-based Information on a Smart-phone Environment,” *The Journal of Society for e-Business Studies*, vol.17, no.3, pp.129-147; Aug. 2012.

[9] KISA. The Analysis on the Research of Practical Use of Location Information[Internet]. Available: http://www.kisa.or.kr/public/library/reportView.jsp?regno=011546

[10] HyonJun Bea,“ Google Android programming: application Structure Analysis,” Maso Interactive, pp.236-242, 2008.

[11] Hyung-Jin Mun , “Research for Reverse Engineering about Android APP,” In *Proceeding of the IT Convergence Society for SMB*, Korea, pp87-90, 2012.



문형진(Hyung-jin Mun)

2008년 2월 충북대학교 전자계산기학 박사
2009년 3월 ~ 2012년 8월 중국 연변과학기술대학 조·부교수
※관심분야 : 접근제어, 프라이버시보호, 정보보호, 익명성, 스마트폰