SNS 환경에서 신뢰성이 강한 사용자 프라이버시 모델 설계

정윤수*, 김용태

Design of User Privacy Model for Strong Reliability in SNS Environment

Yoon-Su Jeong*, Yong-Tae Kim

요 약 최근 페이스북(Facebook)과 트위터(Twitter) 등의 폭발적인 성장에 따라 SNS는 사회적·학문적인 관심의 대상으로 부상하고 있다. 그러나, SNS는 이용자의 신상 정보와 사적인 의견 교환을 근간으로 사용자의 프라이버시가 노출될 수 있는 문제가 존재한다. 본 논문에서는 현재 SNS에서 이용자의 개인 프라이버시를 보호하기 위해 사용되고 있는 블록킹 대신 데이터 분리와 데이터 허위 정보를 이용한 SNS 사용자 프라이버시 보호 모델을 제안한다. 제안 모델은 사용자의 내용 정보를 분리하여 분리된 내용 정보에 허위 정보를 추가함으로써 제3자가 사용자의 내용 정보를 수집하여도 정확한 정보를 추출하지 못하도록 하고 있다. 또한, 제3자가 이용자의 정보를 불법적으로 악용하지 않도록 SNS 서비스 제공자가 이용자의 정보를 활용할 경우 이용자에게 사전에 동의를 구한다.

주제어 : SNS, 사용자 프라이버시, 신뢰성

Abstract SNS is emerging as an academic and social interest, as Facebook and Twitter are developed explosively. But, SNS has a problem of exposing user's privacy because it is originated by exchanging user's personal information and opinion. This paper proposes SNS user privacy protecting model using data separation and false data information instead of blocking which is using to protect user's personal privacy. The proposed model do not let the third party extract precise information after collecting user's context information by adding false information to separated context information. Also, it gets user's agreement beforehand if SNS service provider uses user's information not to be used illegally by the third party.

Key Words : SNS, User Privacy, Reliability

1. 서 론

최근 인터넷의 발전은 페이스북, 트위터, 링크드인, 구글 플러스 등의 소셜 네트워크 서비스(SNS, Social Network Service) 이용자를 폭발적으로 증가시키고 있다[1]. 소셜 네트워크 서비스는 기관이나 조직에 저장된 개인정보를 분석하여 의학연구, 인구 통계 등 다양한 분야에서 활용되고, 새로운 정보 생성 및 소통의 도구로써 널리 이용되고 있다[2].

소셜 네트워크 서비스는 다양한 정치, 경제, 문화, 미디어의 사회적 변화에 민감하게 반응하고 있으며, 최근 무선 인터넷의 활용과 스마트폰의 등장으로 소셜 네트워크 서비스에서 제공되는 사회적 규범과 문화, 법, 제도적인 측면의 내용들이 온라인과 오프라인의 공간적 구분이 융합되어지고 있다[3].

소셜 네트워크 서비스는 사회 전반에 걸쳐서 이용자들의 생활을 윤택하게 해주고 있지만 이용자들의 프라이

※본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.
*목원대학교 정보통신공학과 조교수
**한남대학교 멀티미디어학부 교수(교신저자)
논문접수: 2012년 11월 30일, 1차 수정을 거쳐, 심사완료: 2013년 1월 14일

버시가 노출되는 문제 또한 발생되고 있다. 소셜 네트워크 환경에서 이용자들의 프라이버시가 노출되는 것은 이용자들이 이용자의 개인 정보와 이용자간 관계 정보를 기반으로 서비스를 제공받을 때 이용자의 사용 흔적이 남기 때문이다. 또한, 소셜 네트워크 환경에서는 이용자의 개인 정보를 기업 또는 기관이 제 3자에게 광고 및 마케팅에 이용하도록 이용자의 개인정보를 제공하기 때문에 문제가 발생한다[4-6].

Zhelea et. al은 사용자의 개인정보를 보호하기 위해서 이용자간 관계 정보를 보호하는 기법을 제안하였다. 이 기법은 이용자간 관계 정보를 보호하는 장점은 있지만 개인 정보의 정점 내용 정보에 대한 익명성을 제공하지 못하는 단점이 있다[7].

Campan et. al은 소셜 네트워크의 정점 내용 정보를 k-익명성 모델을 이용하여 보안 기법을 제안하였다. 그러나, 이 기법은 구조적 공격에 의한 개인 정보 노출방지를 위해 전체 소셜 네트워크를 추상적 형태로 표현하기 때문에 전체 소셜 네트워크 구조를 왜곡하는 단점이 있다[8].

Wei et. al은 k-익명성을 만족하면서, 간선의 추가/삭제를 통한 구조적 공격 방지 기법을 제안하였지만 개인 정보가 숫자 정보인 경우에만 적용되기 때문에 원거리 정점들을 묶지 못하여 전체 소셜 네트워크 구조가 크게 손상되는 단점이 있다[9].

본 논문에서는 소셜 네트워크 환경에서 이용자간 개인 정보를 기업이 제3자에게 전달하더라도 이용자의 개인정보를 안전하게 보장할 수 있는 신뢰성이 강한 사용자 프라이버시 모델을 제안한다. 제안된 모델은 SNS에서 사용되고 있는 블록킹 대신 데이터 분리와 데이터 허위 정보를 이용하여 제3자가 이용자의 내용 정보를 수집하더라도 이용자의 정확한 정보를 추출하지 못하도록 한다. 또한, 제3자가 이용자의 정보를 불법적으로 악용하지 못하도록 소셜 네트워크 서비스 제공자가 이용자의 정보를 활용할 경우 이용자에게 사전에 동의를 구하도록 한다.

이 논문의 구성은 다음과 같다. 2장에서는 소셜 네트워크 서비스의 개념, 서비스, 특징들에 대해서 알아본다. 3장에서는 소셜 네트워크 서비스 환경에서 신뢰성이 강한 사용자 프라이버시 모델을 제안하고, 4장에서는 소셜 네트워크 환경에서 제공되고 있는 서비스를 제안 모델과 비교분석하고, 마지막으로 5장에서 결론을 맺는다

2. 관련연구

2.1 소셜 네트워크 서비스

소셜 네트워크 서비스(SNS, Social Network Service)는 특정한 관심이나 활동을 공유하는 사람들 간에 온라인 상에서 네트워크를 형성하고나 네트워크에 참여하여 교류를 할 수 있도록 제공하는 서비스를 말한다. 최근 페이스북(Facebook)과 트위터(Twitter) 등의 소셜 네트워크 서비스가 각광을 크게 받고 있어 사회적·학문적으로 관심의 대상으로 부상하고 있다[4]. 소셜 네트워크 서비스는 서비스마다 독특한 특징을 가지고 있으며, 신상 정보의 공개, 관계망의 구축과 공개, 의견이나 정보의 게시, 모바일 지원 등의 기능을 가지고 있다.

2.2 소셜 네트워크 서비스 기능

소셜 네트워크 서비스는 서비스마다 각기 다른 기능들이 구현되지만 가장 대표적인 기능으로는 첫째, 신상 정보의 등록 및 공개 둘째, 대인관계 망과 그 구조 셋째, 게시물의 글줄기 등이 있다. SNS의 신상 정보의 등록 및 공개에서는 이용자의 성별, 연령, 직업, 문화적 취향, 이데올로기, 종교 등이 전부 또는 선택적으로 공시된다. 이러한 서비스는 사용자의 프라이버 보호와 관련하여 사회적인 문제를 야기할 수 있는 단점이 있다[3]. 소셜 네트워크 서비스의 대인관계 망과 그 구조에서는 이용자 자신이 연계를 맺고 있는 또 다른 이용자들의 정보가 노출될 수 있어 다른 이용자의 네트워크를 거쳐 이용자의 신상 정보를 파악할 수 있다. 셋째, 소셜 네트워크 서비스 게시물의 글줄기는 이용자의 의견이나 정보를 이용자가 연계를 맺고 있는 이용자들이 의견이나 정보에 반응하여 또 다른 의견과 정보를 게시하는 것을 의미한다. 소셜 네트워크 서비스 서비스는 서비스별로 특화된 기능을 제공하기 때문에 사진이나 비디오를 공유하는 기능, 블로그 기능이 디폴트로 주어지는 경우, 인스턴트 메시징이나 모바일 지원 기능들이 최근 들어 대부분 이런 기능들이 포함되어 있다.

2.3 소셜 네트워크 서비스 종류

해외의 대표적인 소셜 네트워크 서비스는 트위터 페이스북 등이 있으며, 한국의 대표적인 소셜 네트워크 서비스로는 미투데이, 싸이월드 등이 있다[2,4]. 트위터는 140자의 단문메시지를 입력할 수 있어, 스마트폰과 같은

[표 1] 소셜 네트워크 서비스 종류

	미투데이	트위터	페이스북
국내이용자수	170만명	100만명	160만명
가입연령대	10-20대, 여성 이용자가 다수	30대, 얼리어답터 혹은 IT 업계 종사자가 다수를 이루고 있음	20-30대가 주이용층, 특히 25-34세 이용자가 전체 이용자의 41%를 차지하고 있음
특징	네트워크형	미디어형	인맥기반 네트워크 + 개방형
	친구 관계 속에서 컴퓨니티를 형성하고 소통	RT(ReTweet)를 통한 메시지 확산으로 정보 전달에 유리	Like 버튼으로 콘텐츠 공유 및 상호작용이 가능
기능소개	-미친 : 미투데이 친구, 친구신청 및 친구수락을 통해서 관계를 유지하며 이야기 공유 가능 -미투 : 상대방이 작성한 글에 공감할 때 '미투', 내 친구들에게 해당 글이 소개됨 -쪽지 : 네이버 웹서비스의 쪽지와 같은 개념 - 댓글달기 : 상대방이 작성한 글에 댓글달기	- Follower : 나를 따르는 사람. 내가 작성한 글, RT한 글을 읽을 수 있음 - Following : 내가 따르는 사람. 상대방이 작성, RT한 글을 읽을 수 있음 - Reply : 상대방의 글에 답변 - Retweets : 상대방의 글을 다른 팔로워들에게 알릴 때 사용 - Direct Messages : 미투데이의 쪽지와 같은 개념 - Favorites : 즐겨찾기와 같이 내가 좋아하는 글만을 한데 모아볼 수 있음	- 프로필 : 싸이월드의 미니홈피와 같이 개인 프로필 및 나와 친구들이 작성한 글을 모아둔 페이지 - 팬페이지 : 주로 기업이 마케팅을 위해 이용하는 페이지. 프로필과 UI는 비슷하지만 외부 웹사이트와 연동 가능 - wall(담벼락) : 나와 친구들이 글을 쓰고 답변 등을 주고 받는 일종의 게시판. 방명록같은 곳 - Like : 개인이 좋아하는 글. 사진 등에 Lkie 버튼을 클릭하여 그 친구들에게 해당 콘첸츠가 공유됨. 메시지 확산 가능

참조 : 정보 IT - SNS 종류와 특징, http://blog.daum.net/dourira/6825496

모바일로 쉽게 사용할 수 있고 가입절차가 간단한 장점이 있다. 트위터는 RT(ReTweets) 기능을 통해 여러 다른 팔로워들에게 전파되기 때문에 메시지의 무한 확산이 가능한 장점이 있다. 미투데이는 150자 내외의 단문 메시지를 미투데이 친구를 맺은 사람들끼리 나눌 수 있도록 서비스를 제공하며, 마음에 맞는 친구들끼리 커뮤니티를 형성하여 소통할 수 있는 장점이 있다. 페이스북은 오픈 커뮤니티 형태로 서로간의 친구 설정이 되어 있어야 컨텐츠 공유가 가능하지만 누구나 쉽게 페이지를 만들 수 있고, 누구든 개인 정보와 컨텐츠 업데이트 내용을 확인할 수 있는 것이 장점이 있다.

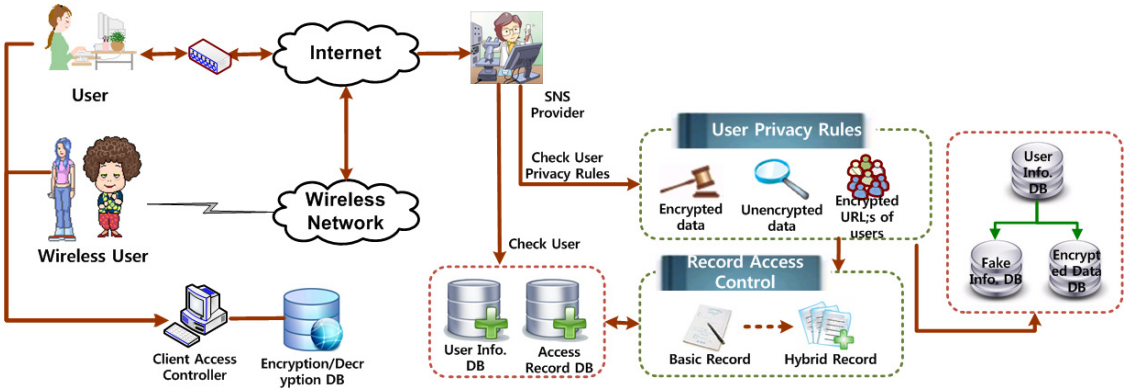
2.4 소셜 네트워크 서비스 특징

소셜 네트워크 서비스는 서비스마다 독특한 기능과 특징을 가지고 있기 때문에 특징을 포괄적으로 규정하기가 쉽지 않다. 그러나, SNS를 학문적, 사회적, 산업적 측면에서 특징을 구분하면 다음과 같이 5가지로 정의할 수 있다.

첫째, 마케팅 도구로써 소셜 네트워크 서비스를 보는 관점이다. 일반 기업은 물론 전통적 미디어나 IT 기업에서도 이런 기능적 활용을 강조한다. 둘째는 소셜 네트워크 서비스를 컴퓨터 매개 커뮤니케이션으로 보는 관점으로 커뮤니케이션 연구의 전통에서 흔히 관찰할 수 있다. 이 관점은 소셜 네트워크 서비스가 면대면 커뮤니케이션과 어떤 차별성과 유사성을 갖는가에 주목한다. 셋째는 소셜 네트워크 서비스를 사회관계망으로 보는 관점으로, 사회학 내 사회관계망 분석(Social Network Analysis, SNA)이라 불리는 영역의 관점이다. 이 관점은 네트워크 구조 자체와 구조적 특징을 보여 주는 데 일차적 관심이 있다. 넷째는 SNS를 권력관계 또는 영향력이 드러나거나 행사되는 장으로 보는 관점으로 정치학, 정치 커뮤니케이션 연구 등의 관점이다. 이 관점은 파워 이용자의 속성과 특성에 주목하여 이를 밝히려고 한다. 마지막은 SNS를 컴퓨터 활용 연구 대상으로 간주하는 관점이다. 이 관점은 대체로 컴퓨터 과학자들이 소셜 네트워크 서비스라는 사회적 현상을 대상으로 연구하면서 갖게 된 관점으로 대규모 데이터를 컴퓨터로 처리하여 그 속에서 그 어떤 규칙성을 발견하려고 한다.

3. 이용자 정보의 프라이버시 보호를 위한 신뢰성이 강한 보안 모델 설계

이 절에서는 소셜 네트워크 환경에서 이용자의 개인정보를 제3자각 악용하더라도 이용자의 프라이버시를 보호할 수 있는 보안 모델을 제안한다.



[그림 1] 사용자 프라이버시를 보장하는 제안 모델의 전체 구성도

3.1 개요

소셜 네트워크 서비스 환경에서 이용자 정보를 제3자가 악용하더라도 이용자의 개인 정보를 추출하지 못하도록 데이터 분리와 허위 정보 삽입을 개인 저보에 삽입하기 위한 제안 모델의 전체 동작 방법을 그림 1에서 보여주고 있다. 그림 1에서 제안 모델은 소셜 네트워크 서비스 관리자에게 특정 권한을 부여하여 이용자의 정보를 열람할 수 있는 기능을 부여한다. 만약 제3자가 불법적으로 접근하려고 할 경우 소셜 네트워크 서비스 관리자는 접근을 제어한다. 이 때, 소셜 네트워크 서비스 관리자는 이용자와 서로 정보를 동기화하기 위해 세션키를 사용한다.

3.2 구성요소

제안 모델은 크게 이용자, 소셜 네트워크 서비스 제공자, 이용자 프라이버시 규칙, 이용자 정보 DB 등 4가지로 구성된다. 이용자는 소셜 네트워크 서비스에 접근하기 위해서 유/무선을 통해 접근가능하며 사용자 정보를 암/복호화하여 데이터베이스에 저장한다. 소셜 네트워크 서비스 제공자는 이용자의 개인 정보를 이용자 프라이버시 규칙에 맞는지 점검하고 사용자 데이터베이스에 저장된 정보와 일치하는지 점검한다. 이용자 프라이버시 규칙은 암호화된 데이터, 비암호화된 데이터, 사용자의 암호화된 URL 정보 등으로 구성되며 사용자 정보에 대한 프라이버시 규칙을 적용하기 위한 정보이다. 이용자 정보 데이터베이스는 위조 정보 데이터베이스와 암호화된 데이터베이스로 구성되며 위조 정보 데이터베이스는 이용자 프로파일에 접근하는 비권한 이용자에게 위조 정보를 제공하기 위한 정보가 저장되어 있는 데이터베이스이다. 암호화된 데이터베이스는 권한된 사용자와 통신하기 위해 사용되는 데이터베이스이다.

3.3 이용자 정보 분할 및 위장정보 제어

제안 모델은 현재 SNS에서 사용되고 있는 블록킹 대신 이용자 정보 분리와 데이터 허위 정보를 이용하여 제3자가 이용자의 정보를 수집하더라도 이용자의 정확한 정보를 추출하지 못하도록 초기화 단계, 인증 단계, 관리자 권한정보 복구 및 조회 단계 등의 3단계로 구성한다.

3.3.1 초기화 단계

초기화 단계에서는 소셜 네트워크 서비스를 이용하는 환자의 정보를 관리자가 수집한 후 이용자의 정보에 속성을 결정하여 데이터의 허위 정보를 생성하는 단계이다.

· 1 단계 : 이용자 정보 수집 단계

1단계는 이용자가 소셜 네트워크 서비스를 사용하기 전에 관리자가 이용자의 개인 정보(이름, 직위, 주민번호, 주소 등) 또는 설문지와 관련된 정보를 요청하는 단계이다.

· 2 단계 : 이용자 권한 속성 정보 결정

2 단계는 수집된 이용자의 정보를 이용하여 관리자가 이용자의 권한 속성 정보를 결절하는 단계이다. 이 단계에서 결정된 권한 속성 정보는 이용자의 허위 정보를 생성하는데 사용된다.

· 3 단계 : 이용자의 허위 정보 생성

3단계는 관리자가 이용자의 권한 속성 정보를 이용하여 이용자의 허위 정보를 생성하는 단계이다. 이 단계는 제3자가 이용자의 정보를 추출하더라도 이용자의 정보를 이용하지 못하기 위한 단계이다.

3.3.2 접근제어 단계

인증 단계는 이용자의 권한 속성과 제3자가 이용자의 정보를 이용할 경우 이용자의 정보를 안전하게 접근하기 위해 이용자의 정보를 제어하는 단계이다.

• 1단계

관리자는 이용자의 권한 속성 정보를 식 (1)의 과정을 통해 추출한 후 (2)의 과정의 결과와 함께 이용자의 허위 정보 F를 인증 서버에 요청하여 응답을 기다린다.

$$M_l=\{M_l|M_l\in M,\ 1\le l\le L\} \quad (1)$$

$$m_l=C(M_l) \quad (2)$$

여기서 L은 분산된 이용자의 정보를 이용하려는 제 3자의 총 개수를 의미한다. 단, M은 이용자의 권한 정보이며 이용자의 권한 정보M은 $M_1\cup M_2\cup\cdots\cup M_L$이고 $\varnothing=M_1\cap M_2\cap\cdots\cap M_L$ 이라고 가정한다.

• 2단계

인증서버는 관리자에게 이용자의 권한 정보에 대한 소수 $q(q\ge n+1)$를 선택한 후 Z_q에서 임의의 랜덤 수 a_i $(1\le i<t)$를 선택하여 이진수 $k(k>1)$로 변환한다. 변환된 이진수 k를 상수항으로 하는 임의의 다항식 $a_{(n-1)(k-1)}+a_{(n-1)k}$과 같은 이용자의 허위 정보를 생성한 후 관리자에게 전달한다.

• 3단계

관리자는 이용자의 허위 정보를 a_{nk}를 전달받은 후 분할된 이용자의 정보와 XOR한다. 관리자는 이용자의 권한 정보에 따른 허위 정보를 제 3자에게 전달한다.

3.3.3 관리자 권한정보 복구 및 조회 단계

관리자 권한정보 복구 및 조회 단계에서는 최소 n명의 제3자가 이용자의 정보를 이용하기 위해서 식(3)처럼 복원하거나 행렬식으로 이용자의 정보를 복구한다.

$$(x+y)^n=$$
$$a_0x^n+a_1x^{n-1}y^1+a_2x^{n-2}y^2+\cdots+a_ny^n \quad (3)$$

식 (3)은 $a_i=\binom{n}{i}$와 같은 식이 성립되어 $(n+1)$번째 줄의 $(i+1)$번째 값과 대응되는 식이다. 식 (3)을 이용할 경우, 이용자의 개인 정보 M_l는 모든 l에 대해서 반복적으로 $m_l=C^{-1}(M_l)$ 형태로 변환 작업을 수행하고, m_l을 $M=M_1\cup M_2\cup\cdots\cup M_L$으로 만들어 이용자의 개인정보를 복구 및 조회한다.

4. 결 론

최근 소셜 네트워크 서비스로 인해 발생되는 이용자의 개인정보보호 문제가 대두되면서 이용자의 개인 정보를 안전하게 보장할 수 있는 방안에 대해서 많은 연구자들이 연구 중에 있다. 본 논문에서는 현재 SNS에서 이용자의 개인 프라이버시를 보호하기 위해 사용되고 있는 블록킹 대신 데이터 분리와 데이터 허위 정보를 이용한 SNS 사용자 프라이버시 보호 모델을 제안한다. 제안 모델은 사용자의 내용 정보를 분리하여 분리된 내용 정보에 허위 정보를 추가함으로써 제3자가 사용자의 내용 정보를 수집하여도 정확한 정보를 추출하지 못하도록 하고 있다. 또한, 제3자가 이용자의 정보를 불법적으로 악용하지 않도록 SNS 서비스 제공자가 이용자의 정보를 활용할 경우 이용자에게 사전에 동의를 구한다. 향후 연구로 소셜 네트워크 서비스를 이용하는 이용자의 프라이버시를 보호하기 위한 프로토콜를 연구할 계획이다.

참 고 문 헌

[1] 황유선(2012). 소셜미디어란 무엇인가. 소셜미디어연구포럼(저). 『소셜미디어의 이해』. 미래인.

[2] Gartner(2009), “Predict 2010: Social Software Is an Enterprise Reality”.

[3] 허진성(2010), “SNS의 개인정보 침해문제와 그 대응방안에 관한 연구”, 한국언로법학회, 언론과법 9(2),

pp.75-103.
[4] 이재현(2012). 프롤로그: 트위터란 무엇인가. 이재현(편)(2012). 『트위터란 무엇인가: 다학제적 접근』. 커뮤니케이션북스.
[5] Boyd, D. M., & Ellison, N. B.(2008). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13, 210~230.
[6] 정윤수, 이상호(2011), "클라우드 컴퓨팅에서 패스워드기반의 사용자 정보 가상화를 통한 사용자 프라이버시 보장 기법", 중소기업정보기술융합학회 논문지, 제1권 제1호, pp. 29-38.
[7] E. Zheleva, and L. Getoor(2007), "Preserving the privacy of sensitive relationships in graph data", In Proceedings of the 1st ACM SIGKDD international conference on Privacy, security, and trust in KDD, pp. 153-171.
[8] A. Campan, and T. M. Truta(2008), "A clustering approach for data and structural anonymity in social networks", In Proceedings of the 2nd ACM SIGKDD international conference on Privacy, security, and trust in KDD, pp. 33-55.
[9] Q. Wei, and Y. Lu(2008), "Preservation of Privacy in Publishing Social Network Data" , In Proceedings of the 2008 International Symposium on Electronic Commerce and Security, pp. 421-425.

정 윤 수

- 2000년 2월: 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월: 충북대학교 대학원 전자계산학 박사
- 2009년 8월~2012년 2월: 한남대학교 산업기술연구소 전임연구원
- 2012년 3월~현재: 목원대학교 정보통신공학과 조교수
- 관심분야: 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail: bukmunro@gmail.com

김 용 태

- 1984년 2월: 한남대학교 계산통계학과 학사.
- 1988년 2월: 숭실대학교 전자계산학과 석사.
- 2008년 2월: 충북대학교 전자계산학과 박사.
- 2002년 12월~2006년 2월: (주)가림정보기술이사
- 2010년 8월~현재: 한남대학교 멀티미디어 학부 교수
- 관심분야 : 모바일 웹서비스, 정보보호, 센서 웹, 모바일 통신 보안
- E-Mail: k7762@hnu.ac.kr