情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

소셜 네트워크 서비스 환경에서 개인정보보호를 위한 OpenAPI기반 보안 프레임워크*

윤 용 석,† 김 강 석, 손 태 식‡
아주대학교 대학원 지식정보공학과

An OpenAPI based Security Framework for Privacy Protection in Social Network Service Environment*

Yongseok Yoon,† Kangseok Kim, Taeshik Shon‡
Dept. of Knowledge Information Engineering,
Graduate School of Ajou University, Suwon, Korea

요 약

모바일 디바이스의 진화와 무선 네트워크의 발전으로 스마트폰 기반 모바일 소셜 네트워크 서비스의 사용자가 증가하고 있다. 또한 실시간 의사소통과 정보공유에 따른 개인정보 유출이 심각한 사회적 문제로 대두되고 있다. 이에 본 연구에서는 먼저 OpenAPI를 이용하여 소셜 네트워크 서비스 플랫폼에 연동 가능한 프레임워크를 설계하고, 개인정보보호 강화를 위해 구현된 프레임워크에 인증과 탐지 메커니즘을 제안하였다. 인증 방식으로는 아이디와 패스워드를 사용하고 탐지 방법은 사용자가 지정한 입력패턴을 분석하여 개인정보보호 가이드라인에 해당하는지 사전에 미리 검증함으로써 소셜 네트워크 서비스 환경에서의 개인정보보안을 강화하였다. 마지막으로 성능 평가를 수행하여 본 연구의 효율성 및 타당성을 입증하였다.

ABSTRACT

With the rapid evolution of mobile devices and the development of wireless networks, users of mobile social network service on smartphone have been increasing. Also the security of personal information as a result of real-time communication and information-sharing are becoming a serious social issue. In this paper, a framework that can be linked with a social network services platform is designed using OpenAPI. In addition, we propose an authentication and detection mechanism to enhance the level of personal information security. The authentication scheme is based on an user ID and password, while the detection scheme analyzes user-designated input patterns to verify in advance whether personal information protection guidelines are met, enhancing the level of personal information security in a social network service environment. The effectiveness and validity of this study were confirmed through performance evaluations at the end.

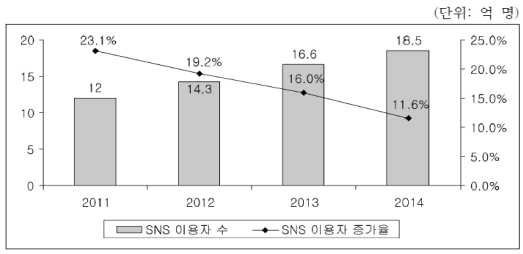
Keywords: SNS, OpenAPI, Security, Framework

I. 서 론

스마트폰 보급이 보편화되고 모바일 인터넷이 활성화됨에 따라 언제 어디서나 정보교류가 가능한 시대가 도래 하였다. 현재 인터넷 서비스는 메일, 검색, 뉴스 등 단순한 서비스를 넘어 사용자의 참여를 이끌어내고

접수일(2012년 9월 27일), 게재확정일(2012년 10월 29일)
* 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원 사업"의 연구결과로 수행되었음.
† 주저자, kaze84@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr

서로 정보를 교류하고 연결시켜주는 소셜 네트워크 서비스(SNS : Social Network Service)로 확대되어가고 있다. SNS는 미디어 매체를 대신할 정도의 상황 및 정보공유가 가능해지고, 타인과 소통할 수 있는 장점에 힘입어 점점 증가하고 있는 추세이다. 시장조사기관 eMarketer[1] 가 2012년에 발표한 자료에 의하면 [그림 1]과 같이 "2011년 12월 기준으로 한 달에 한 번 이상 SNS를 이용하는 이용자 수는 12억 명에 이르렀으며, 이러한 추세는 2014년 까지 지속될 것으로 전망하고 있다"[2].



[그림 1] 전 세계 SNS 이용자 수[2]

그러나 언제 어디서나 사용이 가능한 SNS의 특성상 사용자의 개인정보가 쉽게 노출되고 무분별하게 사용되고 있는 실정이다. 현재 SNS에서의 개인 정보보호 정책 및 기술들은 기존 인터넷 개인정보정책의 수준에서 이루어지고 있고, "사용자 자신의 개인정보에 대한 완전한 통제권을 허가하지 않아 잠재적인 개인정보 문제를 가지고 있다"[3]. 또한 위치 이동이 가능한 모바일 환경과 고정적인 환경인 PC에서의 개인정보의 노출수준이 다르기 때문에 "모바일에서 상황을 공유하는 시스템에서 개인정보보호는 중요한 문제이다"[4]. 이에 따라 기존의 환경에서 SNS보안정책이 아닌 새로운 보안 환경인 모바일 환경에 적합한 SNS에서의 개인정보보안에 대한 연구의 필요성이 요구된다. 본 연구에서는 SNS에서 제공하는 OpenAPI를 이용해 모바일 기반 SNS의 개인정보보호를 위한 프레임워크를 구현하였으며, 제안된 개인정보보호 방식은 입력패턴에 대한 탐지 및 검증이 가능해 사용자가 무의식적으로 올리는 개인정보에 대한 보호가 가능하다.

II. 관련 연구

2.1 개인정보보호 기술

개인정보보호 기술은 개인정보 침해기술인 PIT (Privacy Invading Technology)와 개인정보 강화기술인 PET(Privacy Enhancing Technology)로 분류할 수 있다.

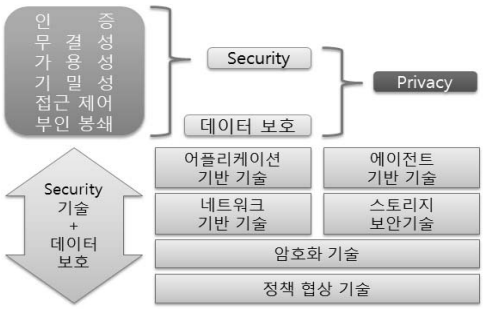
개인정보 침해기술인 PIT는 개인통신기기나 인터넷서비스에 입력한 개인정보를 [그림 2]와 같이 악의적인 목적으로 부당하게 취득하는 것으로 아이디도용, 금융거래위협 등의 제2차, 제3차 피해로 이어질 수 있다.

[그림 2] PIT유형 및 피해유형

PIT유형에는 스마트폰의 GPS를 이용한 악의적인 개인 위치정보 취득, PC와 스마트폰 같은 통신기기의 TCP/IP 주소나 쿠키정보를 이용하여 이용자 정보를 확인, 가상의 WLAN환경을 제공하여 사용자 정보취득, "인터넷 게시 글에 남겨진 개인정보를 이용해서 또 다른 정보를 얻어내는 개인정보 프로파일링 등의 여러 기법"들이 있으며, 이를 안전하게 막는 기술이 요구된다[5,6].

개인정보 강화 기술인 PET는 개인정보에 관한 수집을 최소화 시키고 개인정보의 익명화, 개인정보 데이터에 대한 접근제어 제공 및 사용자에 의한 직접적인 개인정보 통제는 물론 데이터 추적 등 다양한 개인정보 보호 기술을 말한다[7].

PET기술로는 어플리케이션 기반기술, 에이전트 기반기술, 네트워크 기반기술, 스토리지 보안기술, 암호화 기반기술, 정책협상 기반기술들이 있으며, 각각의 기반 기술에는 인증, 무결성, 가용성, 기밀성, 접근제어, 부인 봉쇄 기술과 데이터 보호와 같은 [그림 3]을 적용해야 한다. 더 나아가 PET의 7가지원칙(개인정보의 수집제한, 식별/인증/권한 부여, 개인정보보호에 사용되는 표준기술, 익명성, 암호화, 생체인식, 감사 능력)을 반영 하여 개인정보보호 기술이 설계 되어



〔그림 3〕 PET 적용전략 개념도

야 한다〔7〕.

2.2 OpenAPI

OpenAPI(Open Application Program Interface)란 "표준화된 인터페이스를 이용하여 개방형 서비스 구조를 택하여 누구나 사용 할 수 있도록 공개된 응용프로그램 인터페이스를 말한다"〔8〕. 과거 SNS서비스들은 OpenAPI를 제공하지 않아 SNS에 접근하는 것에 한계가 있었으나 현재 서비스되어지고 있는 SNS들은 OpenAPI를 제공하고 있어 SNS에 접근 및 개발이 수월해졌다. OpenAPI를 제공하는 대표적인 SNS로는 Facebook〔9〕, Twitter〔10〕, me2day〔11〕, Foursquare〔12〕 등이 있으며, 이를 활용하여 SNS에 접속하는 클라이언트 프로그램으로는 TweetDeck〔13〕, Liptwit 〔14〕, Mixero〔15〕, Seesmic〔16〕, RockMelt 〔17〕 등이 있다.

2.2.1 TweetDeck

TweetDeck은 OpenAPI를 이용한 SNS 클라이언트 프로그램으로써 Twitter에 특화되어있다. 사용자 로그인을 이용한 접속과 상대방의 글을 필터링해서 볼 수 있다는 장점과 Foursquare, Facebook등 다양한 연결을 지원하며 PC와 모바일 모두 개발되어 있다.

2.2.2 Liptwit

국내에서 제작되어진 Liptwit은 국내 사용자에 맞춰 많은 편의사항을 제공하고, TweetDeck과 비슷한 화면 분할을 가지면서 자신이 원하는 프레임을 추가하여 동시에 여러 메뉴를 볼 수 있는 것이 장점이다. Liptwit 역시 Twitter의 OpenAPI를 바탕으로 제작 되었다. 현재 Liptwit은 더 이상의 업데이트나 개발은 이루어지지 않고 있지만, 커뮤니티 사이트를 중심으로 계속 사용되고 있다.

2.2.3 Mixero

Mixero는 Twitter와 Facebook을 지원하며 윈도우 환경에서 사용자가 사용하기 편리하도록 되어있다. 사용자 그룹설정과 변경 등에 탁월하다는 것이 장점 있지만 사용자 로그인을 제외한 보안 요소는 없으며 모바일 버전은 지원하지 않는다.

2.2.4 Seesmic

TweetDeck과 더불어 PC와 모바일 둘다 개발되어있는 Seesmic은 깔끔 하게 생긴 UI와 SNS를 연결시켜주는 플러그인을 제공함으로써 OpenAPI로 이루어진 다양한 SNS를 지원한다. Seesmic역시 개인정보보안에 관한 설정이 있는 것이 아니며, OpenAPI를 이용한 사용자 로그인만 지원한다.

2.2.5 RockMelt

SNS에 특화된 웹 브라우저인 RockMelt는 Google사의 Chrome 브라우저와 생김새가 비슷하다. Facebook이나 Twitter를 연동시켜 놓으면 웹브라우저에서 메시지와 댓글의 작성이 가능하고 화면 상단을 통해 쉽게 알려주어 웹브라우저가 실행되는 동안 화면전환 없이 쉽게 SNS를 할 수 있지만 보안 부분에 있어서는 다른 SNS 클라이언트 프로그램들과 마찬가지로 사용자 로그인만 제공하고 있다.

2.3 기존의 OpenAPI를 이용하여 SNS에 접속하는 클라이언트 프로그램의 문제점

앞에 소개한 OpenAPI를 이용해서 SNS를 접속하는 프로그램들은 웹 브라우저에 접속해서 이용하는 형태를 벗어나 쉽게 SNS 접근을 도와준다. 하지만 OpenAPI를 이용해서 SNS를 접속하는 클라이언트 프로그램들 중 TweetDeck과 Seesmic만 PC와 모바일 지원하고 그 외 클라이언트 프로그램들은 PC에서만 제공된다. OpenAPI를 이용해서 SNS에 접속하는 클라이언트 프로그램들을 살펴보면 〔표 1〕과 같

〔표 1〕 기존 클라이언트 프로그램 기능

	TweetDeck	Liptwit	Mixero	Seesmic	RockMelt
로그인 방법	아이디, 페스워드	아이디, 페스워드	아이디, 페스워드	아이디, 페스워드	아이디, 페스워드
플랫폼	Android, iPhone, iPad, MAC, Windows, Chrome Browser	Windows	Windows, MAC	Android, iPhone, iPad, MAC, Windows,	Chrome Browser 기반의 Web Browser
지원하는 서비스	Twitter, Facebook, MySpace, Foursquare, Linkedin, Buzz	Twitter	Twitter, Facebook	Twitter, Facebook, Linkedin, YouTube, Foursquare Buzz	Twitter, Facebook, Gmail
특화 기능	트윗 예약, 상대방의 글 필터링	간단한 친구 추가 및 삭제 스킨제작 기능	지정된 스킨 선택, 그룹 관리	플러그인 제공을 통한 확장성	웹브라우저 형태
개인정보에 대한 접근	없음	없음	없음	없음	없음

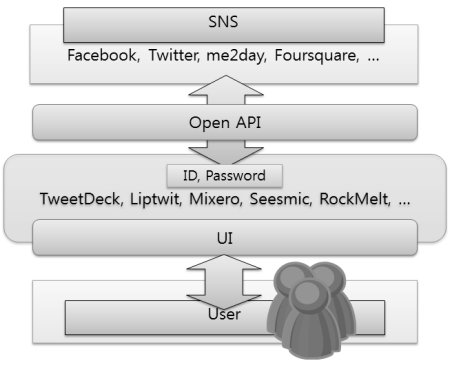
이 UI환경 개선과 그룹설정, 상대방 글 필터링 등 단순한 기능에 그치고 있고, 사용자 로그인을 제외한 개인정보 보안에 있어서는 개인정보 정책설정이나, SNS 접속 방법 등, 보안에 관련된 요소는 찾아보기가 힘들다. 따라서 사용자 로그인 외에 다른 보안들이 필요하고, OpenAPI기반 SNS 환경을 위한 개인정보보호 프레임워크를 제안한다.

III. 설계 및 구현

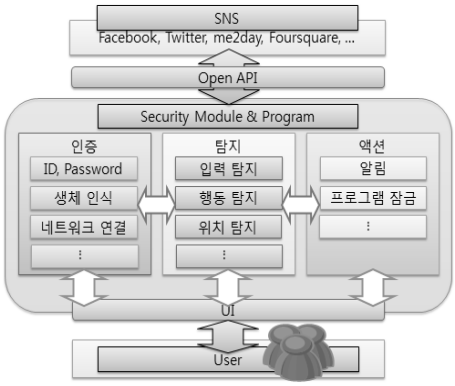
3.1 제안하는 프레임워크

기존의 OpenAPI를 이용한 클라이언트 프로그램들은 〔그림 4〕와 같이 단순히 새로 만들어진 UI에서 SNS에 접속하여 사용자 로그인과 글 작성 기능 밖에 없었다. 본 연구에서 제안하는 프레임워크는 〔그림 5〕와 같이 기존의 OpenAPI를 사용하는 클라이언트 프로그램에서의 개인정보보안의 문제를 해결하기 위해 클라이언트 프로그램에서의 보안기능을 제공하는 방식으로 프레임워크는 크게 기능을 인증, 탐지, 액션으로 구성하고, 사용자에 대한 보안을 다룸으로써 사용자 보안이 강화된 SNS접속 클라이언트 프로그램이 가능하다.

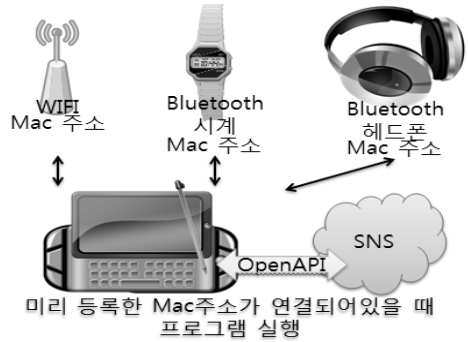
SNS에 사용자 인증을 하기 위해서는 기본적으로 아이디와 패스워드를 이용하지만 그전에 생체인식이나 〔그림 6〕과 같이 네트워크 연결 상태를 이용하여



〔그림 4〕 기존의 OpenAPI를 이용하는 클라이언트 프로그램 구조



〔그림 5〕 OpenAPI를 이용한 프레임워크 제안



〔그림 6〕 네트워크 연결을 이용한 인증 예

프레임워크에서 SNS접속을 제어할 수 있다.

제안 프레임워크 실행 시에는 사용자에 대한 탐지들과 액션들에 의해 제안하는 프레임워크가 제어가 되며, 제안하는 프레임워크의 구성인 인증, 탐지, 액션에 대한 설명은 〔표 2〕와 같다.

〔표 2〕 프레임워크 구성설명

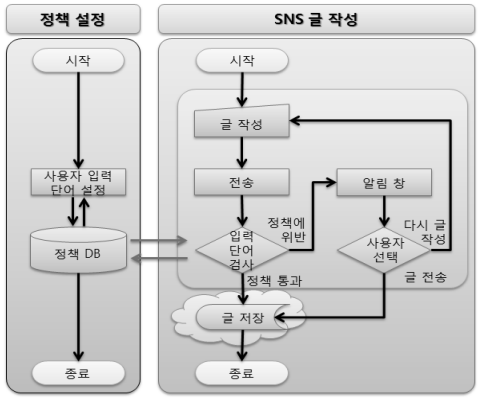
	방 법	내 용
인증	아이디와 패스워드	가장 널리 알려진 방식으로 아이디와 패스워드를 이용한 인증
	생체인식	카메라를 통한 얼굴인식이나 손금, 진동에 의한 촉감 등을 이용한 인증
	네트워크 연결	블루투스 나 Wi-Fi의 MAC 주소를 미리 등록시키고 해당 네트워크 기기 사용 시 인증
탐지	입력패턴	사용자가 작성하는 글의 입력 패턴을 가지고 탐지
	행동패턴	사용자가 지정해놓은 시간외에 사용 시 탐지나 사용자의 SNS에서의 행동인 글 작성과 사진 첨부 중의 우선순위 탐지
	위치인식	위치 기반으로 하는 SNS에 해당하는 기능으로 갑작스러운 이동이나 허용되지 않은 장소 탐지
액션	프로그램 잠금	인증실패나 부적절한 행동 패턴 감지, 인가되지 않은 위치인식시 사용자 프로그램 잠금
	알림	휴대폰 외에 이메일이나 다른 기기로 상태 알림

이외에도 보안과 관련된 요소들을 추가하여 개인정보보안에 안전한 프레임워크를 구성할 수 있다.

본 연구에서는 프레임워크 구성 중 인증 방식으로는 아이디와 패스워드를 이용한 방식과 탐지방법으로는 입력 패턴을 이용한 탐지에 대해 구현한다.

3.2 입력 패턴 탐지

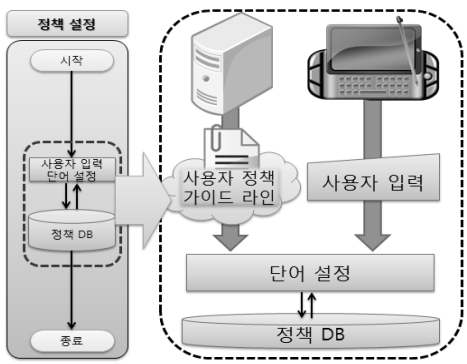
제안하는 입력패턴탐지는 〔그림 7〕과 같이 크게 정책 설정 부분과 SNS에 글을 작성하는 부분으로 나뉘어 사용자 입력에 대한 패턴을 탐지한다.



〔그림 7〕 입력 패턴 탐지 전체 흐름도

먼저 정책설정 부분은 사용자가 미리 개인정보를 입력하고, SNS에 글 작성부분은 정책설정을 바탕으로 개인정보에 해당하는 단어를 검출하는 부분으로 이루어져있다. 입력 패턴을 감지하는 SNS의 글 작성의 부분의 경우 사용자 로그인 후 글을 작성 한 뒤 전송 버튼을 누르면 사용자가 입력한 단어 정책을 가지고 해당 글을 검사하게 된다. 만약 작성한 글 중에 개인정보에 해당하는 단어가 있으면 작성한 글은 SNS에 전송되지 않고, 알림 창을 통해 검출한 단어들을 사용자에게 알려주게 된다.

입력패턴 탐지의 정책 설정의 경우 〔그림 8〕과 같이 사용자가 직접 입력하는 부분과 서버에서 정책 가



〔그림 8〕 입력패턴 탐지의 정책설정

이드라인을 받아 입력할 수 있도록 나눠진다.

사용자가 직접 개인정보를 입력할 경우 중요한 개인정보이지만 개인정보 입력 시 누락 할 수 있는 부분이 발생할 수 있다. 따라서 사용자가 누락 할 수 있는 개인정보들은 서버에서 개인정보보호 가이드라인을 받아 해당 정보를 입력하고, 그 외 정책들은 사용자가 직접 입력할 수 있게 설계하였다.

서버에서 전달되는 개인정보보호 가이드라인은 사용자가 누락할 수 있는 개인정보 형식만 알려주기 때문에 서버에서 사용자에게 전달과정 중 외부에 유출시에도 사용자 개인정보는 안전하게 보호된다.

3.3 구현 결과

본 연구에서 제안하는 프레임워크를 구현하기 위해 OpenAPI를 제공하는 SNS는 Facebook과 Twitter를 대상으로 진행하였으며, 프레임워크 구현환경은 〔표 3〕과 같다.

〔표 3〕 프레임워크 구현 환경

정책전달 서버	OS	Windows7
	Language	Java 1.7
클라이언트 단말기	OS	Android 2.3.3
	Platform	Galaxy Tab

서버의 구성은 XML파일을 전송할 수 있는 파일전송서버를 구성하였으며, 개인정보보호 가이드라인을 전송하는 서버 없이도 동작이 가능하다.

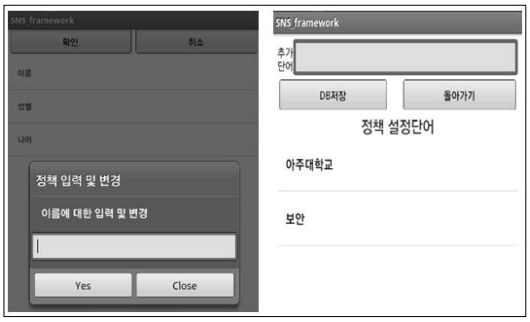
단말기에서 서버 접속 시 〔그림 9〕와 같은 XML형식으로 이루어진 개인정보보호 가이드라인을 서버로부터 전달받게 된다.

```
<?xml version="1.0" encoding="EUC-KR"?>
<POLICY>
    <P_NAME>SNS_FRAMEWORK_POLICY</P_NAME>
    <VERSION>1</VERSION>
  - <GUIDE>
        <NAME>이름</NAME>
        <SEX>성별</SEX>
        <AGE>나이</AGE>
    </GUIDE>
</POLICY>
```

〔그림 9〕 개인정보보호 가이드라인 전달 XML

서버에서 전달받은 XML형식의 개인정보보호 가이드라인 내용은 사용자가 누락할 수 있는 개인정보보호 항목에 해당하며 단말기 데이터베이스에 저장되어지고 사용자에게는 리스트 구조로 보이게 된다.

서버에서 받은 개인정보보호 가이드라인 리스트의 단어를 선택 시 〔그림 10〕 왼쪽과 같이 사용자가 자신의 개인정보를 입력하게 되고, 개인정보보호 가이드라인에 없는 항목은 〔그림 10〕 오른쪽과 같이 사용자가 직접 추가 단어를 입력한다.



〔그림 10〕 서버 및 사용자 단어설정 화면

SNS에 전송될 글을 작성 후 확인버튼을 누르게 되면 작성한 글이 바로 SNS에 전송되는 것이 아니라 단말기 데이터베이스에 들어있는 개인정보보호 가이드라인 항목과 사용자가 작성한 글을 비교하게 되고 사용자가 지정한 개인정보에 위반된 항목이 있을 경우 해당단어를 검출하게 된다.

〔그림 11〕 단어 검출 화면

검출된 내용은 〔그림 11〕과 같이 사용자에게 알려주게 되는데, 사용자 선택에 따라 Yes버튼을 누르면 SNS에 전송을 하게 되고, Close버튼을 누르면 다시 글쓰기 창으로 돌아감으로써 주요 개인정보에 대한 보호가 가능하다.

〔표 4〕 제안한 프레임워크와 클라이언트 프로그램 평가

어플리케이션 이름	로그인 방법	개인정보 접근방법	특화기능	모바일 지원
TweetDeck	아이디와 패스워드	SNS서비스별 해당 홈페이지에 접속	트윗 예약, 상대방 글 필터링	지원
Liptwit	아이디와 패스워드	SNS서비스별 해당 홈페이지에 접속	간단한 친구 추가 및 삭제, 스킨제작 기능	미지원
Mixero	아이디와 패스워드	SNS서비스별 해당 홈페이지에 접속	지정된 스킨 변경기능과 편리한 그룹관리	미지원
Seesmic	아이디와 패스워드	SNS서비스별 해당 홈페이지에 접속	플러그인을 통한 SNS 확장성 제공	지원
RockMelt	아이디와 패스워드	SNS서비스별 해당 홈페이지에 접속	웹브라우저 형태	미지원
제안한 프레임워크	아이디와 패스워드, 생체인식, 네트워크 연결 등	SNS서비스별 해당 홈페이지에 접속, 직접적인 개인정보관리	개인정보 글 탐지 및 필터링, 직접적인 개인정보관리,	지원

IV. 성능 평가

본 연구에서 구현하고 제안하는 프레임워크는 아이디와 패스워드 인증과 사용자가 지정한 입력패턴 탐지를 통해 개인정보 노출이 있는 글을 작성 시에도 사용자에게 알림으로써 직접적인 개인정보 관리가 가능해졌다. 또한, 앞에 소개한 TweetDeck, Liptwit등과 같은 OpenAPI를 이용한 SNS접속 클라이언트 프로그램 보다 사용자 개인정보 노출측면에서 효과적임을 알 수 있다. 즉, 제안하는 프레임워크를 활용하면 SNS에서 제공하는 개인정보보안이 취약할지라도 제안한 프레임워크를 통해 〔표 4〕와 같이 보안요소를 적용시킬 수 있음을 확인하였다.

본 연구에서 제안한 프레임워크 중 아이디와 패스워드를 사용하고 사용자가 지정한 입력패턴에의 한 탐지는 다음과 같은 장점을 가진다.

1) 사용자가 무의식적으로 작성할 수 있는 개인정보보안에 대해 강화되었다.
2) 개인정보를 사용자가 직접 관리가 가능해졌다.
3) 서버에서 전달되는 개인정보보호 가이드라인을 통해 사용자가 누락 할 수 있는 개인정보 항목을 줄일 수 있다.

V. 결 론

본 연구에서는 OpenAPI기반 SNS 환경에서 개인정보보안에 대한 프레임워크를 제안하였고, 사용자가 지정한 입력패턴 탐지에 대해 구현하였다. 제안한 프레임워크는 언제 어디서나 다양한 기기를 사용하는 유무선 환경에서 복합적으로 사용이 가능하다.

본 연구에서 제안한 프레임워크 중 아이디와 패스워드를 이용하는 인증방법과 사용자가 지정한 입력패턴 탐지방법은 사용자의 개인정보 노출위험이 있는 글을 작성할 경우 사용자에게 미리 알려준다. 그러므로 SNS에 올리는 글에 대한 사용자의 주요 개인정보를 최소화 시키고 개인정보를 직접관리 할 수 있는 장점이 있다. 하지만 이번 연구에서 구현한 아이디와 패스워드 인증과 사용자 지정 입력패턴 탐지는 단순히 사용자가 설정한 단어에 의해서 개인정보보안이 이루어지고 있다. SNS에 글을 작성하다 보면 같은 의미의 단어라도 다르게 쓰일 수 있고, 다른 의미라도 같은 단어로 사용될 수 있다. 따라서 사용자가 직접 지정한 단어검사 보다는 온톨로지를 기반으로 하는 자연어 검색 기술을 이용 것보다 효율적인 개인정보보호가 가능하다. 즉, 프레임워크의 보안 모듈을 구성 할 때, 현재 나와 있는 개인정보보호기술을 활용하면, 이번 연구에서 구현한 사용자지정 입력패턴 개인정보보호 보다 더 효과적인 프레임워크를 만들 수 있을 것이다.

향후 연구로는 각각의 모듈별 암호화 기법을 추가한 확장 프레임워크를 제안하고 SNS에 대한 현실적인 보안정책에 대해 연구한다.

참 고 문 헌

〔1〕 eMarketer, http://emarketer.com/
〔2〕 김희연, 오주현, “국내외 SNS의 현황과 사회적 의미,” 방송통신정책, 10(12), pp. 19-42, 2012년 7월.
〔3〕 김지혜, 이형효, “소셜 네트워크 서비스를 위한 프라이버시 보호 정책언어 및 프라이버시 보호 모듈

구현," 정보보호학회논문지, 21(1), pp. 53-63, 2011년 2월.
〔4〕 Mika Raento, Antti Oulasvirta, "Privacy management for social awareness applications," Proceedings of 1st Workshop on Context Awareness for Proactive Systems(CAPS 2005), vol.1, pp. 105-114, July. 2005.
〔5〕 최병훈, "웹 환경의 개인정보보호 시스템 설계에 관한 연구," 석사학위논문, 동국대학교 , 2010년 2월.
〔6〕 정영만, 이창훈, 정재욱, 원동호, "SNS 상에서 개인정보 보호를 위한 Paillier Encryption Scheme 적용 기술 제안," 한국정보보호학회 하계학술대회 발표집, 22(1), pp. 120-123, 2012년 6월.
〔7〕 G.W. van Blarkom, J.J. Borking, J.G.E. Olk, "Handbook of Privacy and Privacy-Enhancing Technologies : The case of Intelligent Software Agents," PISA, pp. 33-53, May. 2003.
〔8〕 김정길, 정지문, "안드로이드 기반 OpenAPI를 이용한 SNS 연동 지역정보 서비스를 위한 모바일 증강현실 시스템 설계 및 구현," 디지털 정책연구 9(2), pp. 131-140, 2011년 4월.
〔9〕 Facebook, http://www.facebook.com/
〔10〕 Twitter, http://twitter.com/
〔11〕 me2day, http://me2day.net/
〔12〕 Foursquare, http://www.foursquare.com/
〔13〕 TweetDec, http://www.tweetdeck.com/
〔14〕 Liptwit, http://liptwit.com/
〔15〕 Mixero, http://www.mixero.com/
〔16〕 Seesmic, https://seesmic.com/seesmic-social/
〔17〕 RockMelt, http://www.rockmelt.com/

〈著者紹介〉

윤 용 석 (Yongseok Yoon) 학생회원
2009년 2월: 배재대학교 정보통신공학과, 전자상거래학과, 전산전자물리학과 졸업
2009년~2011년: ㈜케이벨 정보통신연구소 연구원
2011년~현재: 아주대학교 대학원 지식정보공학과 모바일보안 석사과정
〈관심분야〉 개인정보보호, 무선 센서 네트워크, 모바일 보안, 스마트그리드, 유비쿼터스

김 강 석 (Kangseok Kim) 정회원
2007년: 인디애나 대학교 컴퓨터공학과(공학박사)
2010년~현재: 아주대학교 지식정보공학과 연구교수
〈관심분야〉 모바일 컴퓨팅, 유비쿼터스 컴퓨팅, 모바일 어플리케이션, 모바일 보안, 데이터 마이닝, 바이오 인포메틱스

손 태 식 (Taeshik Shon) 종신회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 공학사
2002년 2월: 아주대학교 컴퓨터 공학석사
2005년 8월: 고려대학교 정보보호대학원 공학박사
2004년 2월~2005년 2월: Research Scholar, University of Minnesota
2005년 8월~2011년 2월: 삼성전자 DMC 연구소 책임연구원
2011년~현재: 아주대학교 정보컴퓨터공학부 조교수
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 비정상행위탐지