Journal of Digital Contents Society Vol. 13 No. 1 Mar. 2012(pp. 101-110)

사용자를 위한 향상된 콘텐츠 및 소셜 네트워킹 서비스 제공을 위한 RCBAC 기반 분류 방법

조은애*, 문창주**, 박대하***,

요 약

최근 소셜 네트워크 사이트는 모바일 디바이스 기능과 보급의 향상과 맞물려 큰 인기를 끌고 있다. 이에 따라 사용자의 소셜 네트워크 사이트 가입도 많아지고 있고, 서비스 사용도 더욱 활발해지고 있다. 그러나 사용자들의 수요에 비해서 각각의 소셜 네트워크 사이트 벤더들은 데이터 소유자가 다양한 루트로부터 생성한 콘텐츠를 다른 사용자들과 효율적으로 공유할 수 있도록 서비스를 제공하지 못하고 있다. 또한 여러 디바이스에서 생성된 콘텐츠들을 사용자가 정책으로 정한 관계에 따라 접근할 수 있도록 할 경우, 정책을 공유하는 과정에서 개인정보가 부적절하게 노출될 수 있고 이는 프라이버시 침해 문제를 야기할 수 있는 것이 자명한데, 이러한 문제를 해결할 수 있는 소셜 네트워크들의 통합 관리 방안은 미비한 상태이다. 따라서 본 논문에서는 다양한 소셜 네트워크들이 사용자로부터 생성된 콘텐츠를 공유할 때, 이에 사용되는 정책을 암호화한 상태에서 제3자에 의해 분류하도록 하여 사용자 프라이버시를 보호하는 동시에 콘텐츠를 효율적으로 분류하여 접근 제어 권한을 부여할 수 있도록 하는 모델을 제안한다. 제안하는 모델은 여러 장치들로부터 생성된 콘텐츠를 관리하기 위하여 RCBAC 모델을 기반으로 하여 이루어질 수 있도록 하고, 정책 공유 시 관계들 간의 유사도를 암호화 한 상태에서 측정하여 공격자로부터 사용자 정책 및 컨탠츠를 보호할 수 있도록 하는데 기여할 수 있다.

A Categorization Method based on RCBAC for Enhanced Contents and Social Networking Service for User

Eun-Ae Cho*, Chang-Joo Moon**, Dae-Ha Park***

Abstract

Recently, social network sites are very popular with the enhancement of mobile device function and distribution. This gives rise to the registrations of the people on the social network sites and the usage of services on the social sites is also getting active. However, social network sites' venders do not provide services enough compared to the demand of users' to share contents from diverse roots by users effectively. In addition, the personal information can be revealed improperly in processes sharing policies and it is obvious that it raises a privacy invasion problem when users access the contents created from diverse devices according to the relationship by policies. However, the existing methods for the integration management of social network are weak to solve this problem. Thus, we propose a model to preserve user privacy, categorize contents efficiently, and give the access control permissions at the same time. In this paper, we encrypt policies and the trusted third party classifies the encrypted policies when the social network sites share the generated contents by users. In addition, the proposed model uses the RCBAC model to manage the contents generated by various devices and measures the similarity between relationships after encrypting when the user policies are shared. So, this paper can contribute to preserve user policies and contents from malicious attackers.

Keywords : Web Contents, RCBAC((Relationship-Contents based Access Control), Social Network, Privacy, Access Control

※ 제일저자(First Author) : 조은애
접수일:2012년 03월 01일, 수정일:2012년 03월 20일
완료일:2012년 3월 24일
* 삼성전자
ea.cho@samsung.com

1. 서론

최근 여러 가지 유무선 네트워크를 기반으로 한 클라우드 컴퓨팅 환경의 발전과 스마트 장치(Smart Device)의 개발 및 보급이 디지털을 통한 커뮤니케이션을 가능하게 하고 세상을 변화시키고 있다[1]. 특히 최근 각광받고 있는 클라우드 컴퓨팅과 같이 데이터 통합과 분산 처리가 가능한 환경에서는 사용자들이 개인 데이터를 자유롭게 활용할 수 있다. 뿐만 아니라 웹 2.0 환경에서는 애플리케이션의 가상화도 발달하고 있으므로 현재 서비스되고 있는 애플리케이션들의 통합적인 서비스의 제공이 가능하다[2]. 따라서 사용자들은 이제 PC, 스마트 디바이스를 통해 단순히 웹을 검색하고 이메일(e-mail)을 주고, 받기만 하는 것이 아니라 게임을 하거나 TV를 볼 수도 있고, 또 다양한 소비 활동도 할 수 있다[3].

또한, 사용자들은 이와 같은 디지털 환경에서 발전된 디바이스들을 통해 소셜 활동(social activity)을 시작하게 되었다. 이는 최근 몇 년 사이에 페이스북(Facebook), 트위터(Twitter)와 같은 소셜 네트워크 사이트(Social Network Sites, SNSs)가 크게 성장할 수 있는 기반이 되었다[4]. 이 같은 성장은 SNS 상에서 여러 가지 서비스의 제공이 가능한 환경을 조성하였으며, 모바일 및 웹 관련 기업에서는 개인화(personalization), 소셜 네트워킹(Social Networking), 위치기반서비스(Location-based Services, LBSs) 등의 기술들을 이용하여 이메일, 주소록, 일정관리, 가계부 등 개인관리 정보 연동 서비스를 제공하게 되었다 [5][6].

위와 같은 사실들은 여러 가지 웹 기술들을 기반으로 웹 공간에서의 사회화가 점점 빠르게 진행되고 있는 것을 보여준다. 따라서 서로 다른 환경들 간 정보와 지식들의 공유가 이슈화되고 있으며[7], 소셜 네트워크(social network) 관리의 필요성이 점차 높아지고 있는 상태이다.

그러나 발전된 커뮤니케이션 기술과 환경은 소셜 네트워킹(Social Networking) 능력의 증가를 제공하는 반면에 개인 정보의 많은 노출로 인하여 프라이버시 침해 문제를 야기하고 있다.

이 문제를 해결하기 위해서 최근 소셜 네트워크(social network) 관련 사용자 프라이버시(privacy) 보호 연구가 활발히 진행되고 있으며[8][9][10][11], 특히 각 SNS들은 프라이버시 관련 문제의 발생을 막기 위해서 그룹(Group) 혹은 관계(Relationship)를 설정함으로써 게시물에 대한 접근 권한을 부여할 수 있도록 시도하고 있지만, 서로 다른 SNS로부터 생성된 콘텐츠 통합 시 일어날 수 있는 정보의 노출에 대한 연구는 아직 이루어지지 않고 있는 상태이다. 콘텐츠의 노출은 개인적인 성향(가치관, 집안 또는 직장 상황, 정치적 또는 종교적 성향 등)에 대한 추론을 가능하게 하므로 보호되어야 할 분명한 개인 프라이버시이지만, 기하급수적으로 늘어난 SNS들은 이것들이 만족스럽게 보호하지 못하고 있다[12]. 뿐만 아니라 각 SNS들도 자신들의 관계 구성 정책을 공식적으로 공개하고 싶지 않아 할 수 있으므로 이들에 대한 프라이버시 보호의 필요성도 많아지고 있다.

따라서 본 논문에서는 소셜 네트워크를 여러 가지 디바이스들 혹은 애플리케이션에서 정의한 관계와 SNSs에서 정의한 소셜 관계(social relationship)를 통합하고, SNS에 접근하는 모든 사용자에 대하여 사용 레벨과 그에 맞는 접근 권한을 부여할 수 있도록 정책(Policy)을 정의하여 사용자들의 프라이버시를 보호하는 동시에 편의성과 만족도를 높일 수 있는 방법을 제안하고자 한다.

제안하는 모델은 프라이버시를 보호하는 동시에 효율적으로 관계들을 분류하기 위하여 숫자형 데이터(numerical data)를 위해서는 ASPE 암호화 방법[2]을 사용하고, 범주형 데이터(categorical data)를 위해서는 식별자를 암호화하는 방법을 사용하여 분류를 수행한다. 또 사용자 프라이버시 보호를 위해서 정책 통합 및 공유 시 제3자에 의해 분류를 수행하도록 한다.

본 논문에서 쓰이는 정책은 관계 관리에 효율적인 RCBAC(Relationship-Contents based

* 건국대학교 항공우주정보시스템공학과
cjmoon@konkuk.ac.kr
* 고려사이버대학교 IT학부
summer69@cyberkorea.ac.kr
▣ 이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임.[NRF-2009-352-D00283]

Access Control)을 기반으로 표현하며, 사용자의 소셜 네트워크를 구축하는데 편의성을 높이기 위하여 스마트 장치들의 주소록(address book)의 정보를 메타데이터(metadata)와 태그(tag)로 구성할 수 있도록 한다. 이 때, 사용자 개인의 장치 정보 및 콘텐츠(contents)와 관련된 정책 혹은 각 SNS들의 정책들은 암호화하여 사용자 프라이버시를 보호하면서 분류를 수행할 수 있도록 한다.

본 논문 나머지 부분의 구성은 다음과 같다. 2장에서는 관련 연구인 RCBAC 정책과 ASPE (Asymmetric scalar product preserving encryption)[13], 식별자 암호화 방법 등 사용자 정책을 암호화하는 방법들에 대해서 간단히 설명하고, 3장에서는 제안한 모델을 적용한 전체 프레임워크에 대해 자세히 설명한다. 4장에서는 시나리오를 바탕으로 한 수학적인 검증을 보이고, 5장에서 기존 연구와의 비교 및 평가를 수행한다. 마지막으로, 6장에서 본 연구의 결론 및 향후 연구 과제에 대해 서술한다.

2. 관련 연구

소셜 네트워크에 대한 연구와 웹 환경에서 콘텐츠 사용자의 프라이버시를 보호하기 위한 방법은 다음과 같이 RCBAC, ASPE, 식별자를 사용한 암호화 방법이 있다.

2.1 RCBAC

RCBAC은 사용자가 나(I)를 중심으로 관계(relationship)를 정의하고, 접근 주체에 대한 자연스럽고 다양한 표현과 소셜 네트워크의 확장을 가능하도록 하기 위해 제안된 접근 통제 모델이다 [7][14][15]. 이 모델에서는 관계를 주체(subject)로 하고 주제별 분류를 객체(object)로 하여 이 둘을 연산(operation)으로 매핑한 권한(permission)을 정의한다. 주체로써 사용자는 자신의 개성에 따라 그룹의 종류와 이름, 구성원 등을 설정할 수 있고, 객체는 웹 콘텐츠와 그것들을 분류하여 정리한 시맨틱 웹으로 구성한다. 이 둘을 생성(create), 읽기(read), 연결(link), 덧쓰기(rewrite) 등과 같은 연산(operation)으로 권한(permission)을 매핑하여 객체에 대한 내용 의미(content semantic)를 표현하였다.

간단히 표현된 권한의 예를 들면 다음과 같다.

$$Subject \xrightarrow{operations} G(\ Object\ )$$

위 식과 같이, 주체 Subject가 소셜 네트워크 그룹 G 에 포함될 때, 분류를 거친 객체 Object에 대한 접근 권한에 대한 연산 Operation이 표현될 수 있다. 본 논문에서는 콘텐츠의 내용과 사용자의 관계를 모두 중요 시 생각하여 반영하기 위하여 이 접근제어 방법을 사용하도록 한다.

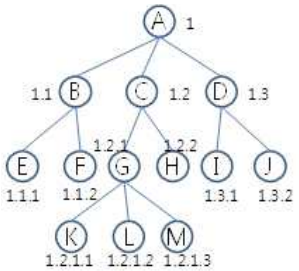
2.2 ASPE

ASPE[13]은 암호화된 데이터베이스에서 kNN 질의의 안전한 계산을 하기 위해 설계된 방법이다. 복구 가능한 거리 정보를 포함한 DRE와 달리 ASPE는 거리에 대한 순서만을 가지기 때문에 데이터가 노출되는 상황에서도 거리에 대한 정보를 보호할 수 있다.

예를 들어, p_1와 p_2를 데이터베이스에 있는 데이터라고 하고, q를 질의(query)라고 하자. 이 방법은 p_1, p_2, q를 p_1', p_2', q'로 암호화 했을 때, p_1과 p_2 두 데이터 중 무엇이 더 q에 가까운지를 판별할 수 있다는 것을 증명한다. ASPE는 가장 가까운 이웃 질의를 찾기 위한 거리 순서를 보존할 뿐 직접수치적인 결과를 나타내지는 않는다. 따라서 데이터의 내용을 보호할 수 있으며 동시에 어떤 데이터가 더 유사도가 높은지를 판단할 수 있다. 본 논문에서도 이러한 방법을 사용하여 서비스 제공자의 가까운 순서만을 판별하도록 한다.

2.3 식별자를 사용한 암호화 방법

유사도 계산 시 식별자를 사용하는 암호화 방법[16]은 범주형 데이터의 계산을 할 때 유용하게 사용되며, 특히 다음 그림과 같은 시맨틱 트리의 노드 번호와 같이 일정한 규칙을 가지고 있다면 다양한 형태의 정보에 적용할 수 있다.



(그림 1) 식별자를 사용한 노드의 예

식별자를 사용하여 암호화를 하는 목적은 데이터 내용의 노출을 최소화하기 위한 것이다. 암호화 방법은 크게 1) 같은 레벨의 노드 간 거리를 구하는 경우, 2) 레벨이 다르고 낮은 레벨을 기준으로 식별자가 같은 경우, 3)레벨이 다르고 다른 식별자가 있는 경우와 같이 세 가지로 나누어 계산한다.

위의 방법에 따라 룰(rule) 간의 거리를 계산한 후 이들을 더하여 유사도를 구하면 가까운 식별자는 1에 가깝게 먼 거리는 0에 가깝게 표현된다.

3. 제안 모델

본 절에서는 여러 디바이스를 통하여 생성된 콘텐츠를 안전하고 효율적으로 공유하기 위해서 각 SNSs에서의 정책을 보호할 수 있도록 통합 및 관리할 수 있는 방법을 제안한다.

3.1 요구 사항 및 사전 정의

먼저, 본 논문에서 제안하는 방법을 적용하기 위해 기존 연구[17]를 기반으로 하여 도출한 요구 사항은 다음과 같다.

- *요구사항 1.* SNS들은 사용자의 관계 정보를 통합하고 분류하여 사용자의 서비스 이용 및 활동에 편의를 제공해야 한다.
- *요구사항 2.* 사용자 프라이버시 보호를 위해서 자신의 정보는 사용자가 원하는 대로 자신이 제어할 수 있도록 해야 한다.
- *요구사항 3.* 제 3자는 신뢰할 만한 기관이어야 한다.

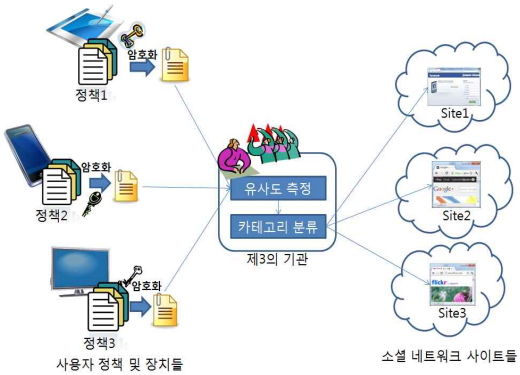
앞서 언급한 바와 같이 현재 사용자들은 다양한 장치를 통한 소셜 네트워킹 활동이 가능하다. 따라서 SNS들은 사용자의 편의를 위해서 관계 정보들을 통합해서 사용할 수 있어야 하며, 이때, 사용자 프라이버시의 침해가 발생하지 않으면서 자신의 정보는 자신이 관리할 수 있도록 해야 한다.

이와 같은 요구사항 1과 2를 위해서 본 논문에서는 RCBAC을 통하여 콘텐츠에 대한 정보들을 좀 더 편리하고 자동적(automatic)으로 처리할 수 있도록 하고, 나(I)를 중심으로 사용자가 직접 세부적인 관계를 정의할 수 있도록 한다.

또한 요구사항 3은 믿을 만 한 제 3자의 기관을 가정하고 사용자 정책에 대한 연산이 여기에서 수행되도록 한다.

3.2 전체 구성

앞의 요구 사항에서 언급한 내용을 적용하여 본 논문에서 제안한 전체 구조는 다음 (그림 2)와 같다. 전체 구조는 크게 사용자, SNS들, 그리고 신뢰할 수 있는 제 3의 기관으로 구성된다.



(그림 2) 전체 구조도

먼저, 사용자는 자신의 스마트 장치 및 PC를 이용하여 정책을 작성한 후 암호화하여 제 3의 기관으로 전송하고, 제3의 기관에서는 암호화되어 있는 정책의 유사도를 측정하여 카테고리를 분류한다. 분류된 카테고리는 각각의 소셜 네트워크 사이트로 전송되어 사용자가 콘텐츠에 접속 시 각각의 목적에 맞는 서비스를 제공할 수 있도록 한다.

각각의 사용자는 여러 가지 종류의 장치들 및 PC를 소유할 수 있으며, 유사도를 측정하는 제3

의 기관은 암호화된 데이터들을 다루므로 비교적 안전하지만, 여러 사용자의 정책을 관리해야 하기 때문에 신뢰성을 갖추고 있어야 한다. 이러한 연산 및 분류 과정을 거치면, 각각의 SNS들은 어느 장치에서 어떻게 생성된 정책인지는 알지 못한 채, 사용자에 맞게 커스터마이징되고 더 나아가 통합된 관계를 통해 분류 별로 서비스를 제공할 수 있다.

3.3 RCBAC기반 분류 방법

접근 제어 기본 구성인 주체(subject), 객체(object), 권한(permission)에 해당하는 부분은 다음 <표 1>과 같다.

<표 1> 접근 제어의 구성

주체	소셜 네트워크를 포함한 사용자 부분 (스마트 장치 등 포함)
객체	주제별로 분류된 콘텐츠 부분,
권한	주체와 객체들을 관리하기 위해 연산(operation)으로 매핑한 부분

앞에서 언급한 바와 같이 사용자 정보의 노출을 막기 위해서 주체에 해당되는 스마트 장치에서 정의한 관계에 대한 정책은 암호화하여 전송한다. 이 때, 관계는 SNS의 정책을 따르는 것이 아니라 사용자의 임의대로 작성되므로 사용자가 정의해 놓은 정책들 간의 유사도를 측정하여 가장 가까운 카테고리로 분류(assign)할 수 있도록 RCBAC을 기반으로 각각의 객체들 간의 매핑을 수행한다. 유사도의 계산은 XML을 기반으로 거리를 계산하는 방법[16][18]을 응용하여 적용하도록 한다. 사용자가 작성하는 정책의 스키마는 다음 (그림 3)과 같다.

```
<xs:schema elementFormDefault="qualified"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">
   <xs:element name="UserPolicy">
     <xs:complexType>
        <xs:sequence>
          <xs:element ref="UserInfo"/>
          <xs:element ref="Relationships"/>
        </xs:sequence>
     </xs:complexType>
   </xs:element>
   <xs:element name="UserInfo">
     <xs:complexType>
       <xs:sequence>
         <xs:element name="id" type="xs:string"/>
         <xs:element name="name" type="xs:string"/>
         <xs:element name="email" type="xs:string"/>
       </xs:sequence>
     </xs:complexType>
   </xs:element>
   <xs:element name="Relationships">
     <xs:complexType>
       <xs:sequence>
         <xs:element ref="group_name"/>
         <xs:element ref="subgroup"/>
         <xs:element ref="permissions"/>
       </xs:sequence>
     </xs:complexType>
   </xs:element>
   <xs:element name="group_name" type="xs:string"/>
   <xs:element name="subgroup" type="xs:string"/>
   <xs:element name="permissions"/>
     <xs:complexType>
       <xs:sequence>
          <xs:element ref="read"/>
          <xs:element ref="write"/>
          <xs:element ref="link"/>
       </xs:sequence>
     </xs:complexType>
   </xs:element>
   <xs:element name="read" type="xs:boolean"/>
   <xs:element name="write" type="xs:boolean"/>
   <xs:element name="link" type="xs:boolean"/>
</xs:schema>
```

(그림 3) 관계 정책 XML 스키마의 예

(그림 3)과 같이 관계 정책은 나(I)를 기준으로 관계를 정의할 수 있고, 관계 별로 소셜 네트워크의 관계를 표현하는 'Relationships'와 권한 'permissions' 등은 속성(attributes)을 이용하여 간단히 표현하고 추가 및 수정할 수 있다.

객체에 해당되는 콘텐츠는 각 사용자의 장치에서 생성되고 그 때 함께 붙여지는 태그에는 콘텐츠의 분류, 스마트 장치에 대한 정보, 소셜 네트워크 구조 등이 포함될 수 있다. 이 데이터들의 스키마에 대한 예는 다음 (그림 4)와 같이 나타낼 수 있다.

```
<xs:schema elementFormDefault="qualified"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">
   <xs:element name="MobileContentsInfo">
     <xs:complexType>
        <xs:sequence>
          <xs:element ref="type"/>
```

```
        <xs:element ref="contents"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="type" type="xs:string"/>
  <xs:element name="contents">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="name" type="xs:string"/>
        <xs:element name="location" type="xs:string"/>
        <xs:element name="time" type="xs:string"/>
        <xs:element name="tag" type="xs:string"/>
        <xs:element name="policy">
          <xs:complexType>
            <xs:sequence>
              <xs:element ref="group"/>
              <xs:element ref="read"/>
              <xs:element ref="write"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="group" type="xs:string"/>
  <xs:element name="read" type="xs:boolean"/>
  <xs:element name="write" type="xs:boolean"/>
</xs:schema>
```

(그림 4) 상황 정보에 대한 XML 스키마의 예

(그림 4)에서 언급된 메타데이터(metadata)는 콘텐츠의 생성 위치/장소, 시간, 이벤트, 사용자 달력, 사용자 메모, 날씨, 소셜 네트워크 데이터 등의 상황(context) 정보가 포함될 수 있다.

사용자의 관계 정보는 OWL(Web Ontology Language)을 기반으로 하는 FOAF(Friend of a Friend)[19] 혹은 하이퍼링크(HyperLink)를 기반으로 하는 XFN(XHTML Friends Network)[20]을 이용하는 것도 가능하다. 이 두 가지 방법은 중앙집중식 데이터베이스가 아닌 자기 자신을 기준으로 소셜 네트워크를 구성할 수 있도록 해주며, 개인 관계 정의에 대한 공개(publish) 및 다른 사람의 관계와의 연결(link)가 가능하다. 따라서 이와 같이 설계를 하면, 제안한 모델은 개인 프라이버시를 보호하고 소셜 네트워크를 편리하고 세부적으로 정의할 수 있을 뿐만 아니라 다른 SNS으로까지 확장할 수도 있게 된다.

각 주체로부터 객체에 해당하는 권한을 부여하는 매핑이 끝나면, 유사도를 계산하여 관계들을 통합한다. 권한을 부여하는 과정과 유사도를 계산하기까지 과정은 다음 '4. 사례 연구'절에서 더욱 자세히 설명하도록 한다.

4. 사례 연구

4.1 시나리오

앞서 언급한 바와 같이 사용자는 다양한 장치들 혹은 애플리케이션을 통하여 생성된 콘텐츠에 태그 정보를 삽입할 수 있고, 이러한 태그 정보를 이용하여 콘텐츠에 대한 메타데이터를 구성할 수 있다.

콘텐츠 생성 시, 스마트 장치들은 위의 (그림 3)과 (그림 4)에서 언급한 바와 같이 상황 정보(위치/장소, 시간, 이벤트, 사용자 달력, 사용자 메모, 날씨, 소셜 네트워크 데이터, 사용자 정의 태그 등)를 수집하여 수동 또는 자동적으로 콘텐츠에 태그 정보로 삽입시키는 기능을 제공한다고 가정한다.

위와 같은 가정을 바탕으로 하여 다음과 같은 시나리오에 따라 본 논문에서 제안한 방법을 적용할 수 있다.

- Alice는 SNS들을 이용하면서 그룹이나 게시물에 대한 권한을 설정하여 이용한다.
- Alice는 휴대폰 주소록에 그룹을 만들어 지인들을 분류해 놓았다.
- Alice는 레스토랑에서 휴대폰으로 사진을 찍고, 그 사진을 지인들과 공유하기 위해 태그를 붙여 자신의 공간에 업로드 시킨다.
- Alice의 친구 Bob이 그 사진을 보기 위해 사이트에 접속하면, Bob이 해당 SNS 사이트에 가입하지 않았다 하더라도 SNS 서버는 Bob을 인증하고, policy를 검토한 후, 권한에 해당하는 사진들을 볼 수 있게 해준다.

이때, 사용자는 사용자 정의 태그만을 사진에 추가 시키지만 앞에서 언급한 바와 같이 이미 사진 파일에는 컨텍스트 정보가 태깅 되어 정보들이 메타데이터로 구성되어 있는 상태이다. 왜냐하면 가정한 바와 같이 사진 촬영 시에 기기 자체에서 자동적으로 컨텍스트 정보들을 수집하여 태깅하기 때문이다.

그리고, SNS는 사용자들의 정의들을 수집하

고 정리하여 콘텐츠 공유를 위해 메타데이터를 정의하게 되는데, 이것은 콘텐츠가 가지고 있는 태그 정보를 통해 구성될 수 있다. Alice가 관리하고 있는 SNS 혹은 스마트 휴대폰 주소록의 관계 정책 그리고 그 장치에서 만들어진 콘텐츠에 대한 정책의 예는 다음 (그림 5, 6)과 같다.

```
<?xml version="1.0" encoding="UTF-8"?>
<Addressbook_group_policy userID = "#me">
   <Group Group_name = "friends">
      <member>
         <name> Bob Lee</name>
         <subgroup>Best Friends </subgroup>
         <email> bob@aaa.edu </email>
      </member>
   </Group>
   <Group Group_name = "family">
      <member>
         <name> Charlie Kim </name>
         <email> Charlie@bbb.edu </email>
      </member>
      <member>
         <name> David Kim </name>
         <subgroup>CS dept </subgroup>
         <email> david@ccc.edu </email>
      </member>
   </Group>
</Addressbook_group_policy>
```

(그림 5) 스마트 장치에 정의된 관계 정책의 예

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileContentsInfo
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
 "xsi:noNamespaceSchemaLocation="MCIschema.xsd">
    <type>cellphone</type>
    <contents>
        <name>Alice</name>
        <location> West Lafayette, IN</location>
        <time>11/11/11 17:30:00</time>
        <tag>foods</tag>
        <Policy>
            <group>friends</group>
            <read>ture</read>
            <write>false</write>
        </Policy>
    </contents>
</MobileContentsInfo>
```

(그림 6) 스마트 장치에 작성된 콘텐츠 정책의 예

(그림 5)는 사용자의 스마트 장치에 있는 관계 정책의 예제이다. 이 그림에서 Bob은 friends로, 그리고 Charlie와 David는 family로 분류되어 있으며 각 멤버(member)는 관련 정보(information)를 포함한다. (그림 6)은 인디애나(Indiana) 주의 한 레스토랑에서 휴대폰을 이용하여 촬영한 사진 콘텐츠에 대한 정책의 예제이다. 자동적인 콘텐츠의 메타데이터 이외에 <tag>를 이용하여 사용자가 태그를 정책에 추가할 수 있다.

4.2 유사도 측정

본 논문에서 제안하는 유사도 측정은 프라이버시를 보장하는 동시에 정책 통합을 위한 매핑을 하기 위한 것이다. XML을 기반으로 한 암호화된 관계 정책 간의 유사도 측정을 위하여, 제안하는 방법은 계산된 결과 값을 바탕으로 가장 가까운 분류(category)로 관계들을 매핑한다. 정책의 유사도를 측정하는 자세한 방법 및 순서는 다음과 같다.

먼저, 정책에서 숫자로 나타나는 데이터는 ASPE 방법[13][16]을 적용하여 유사도를 구한다. 속성의 수에 따라 차원(dimension)을 구성하여 가깝고 먼 정도를 파악할 수 있다.

다음으로 관계 정보를 나타내는 분류 데이터들은 트리(tree)형태의 온톨로지(ontology)를 바탕으로 구성되어 있다고 가정한다. 각 장치 혹은 애플리케이션에서 정의되고 사용되는 관계들은 온톨로지의 일부의 노드로 구성될 수 있다.

본 논문에서 제안하는 방법은 사용자 정책의 내용을 노출하지 않으면서 분류를 수행하는 것이다. 정책 내용을 감추기 위해서 트리의 노드는 번호로 대체하는 방법을 사용하며, 그 번호를 기준으로 거리를 계산한다면, 데이터를 숨길 수 있다[16]. 그러나 번호가 노출된다면 이를 통하여 충분히 원본 데이터들 간의 상하좌우 관계를 도출할 수 있으며 내용 역시 결국 유추될 수 있다. 따라서 정보의 노출을 최소화하기 위해서 본 논문에서는 한 단계 더 나아가 번호로 대체한 노드 값을 암호화하여 유사도를 측정한 다음 분류를 수행한다. 여기에서 유사도는 각 노드 사이의 거리로 정의하며 유사도가 높은 노드끼리 같은 분류로 묶어서 나눌 수 있다.

5. 비교 평가

본 절에서는 환경 별 소셜 네트워크에 대한 프라이버시 보호 정도를 비교한다.

소셜 네트워크 시스템의 사용자들은 SNS들이 어떻게 그들 자신의 프라이버시와 보안 문제를 보호 할 수 있는지 아는 것이 중요하다. 예를 들면 사용자들은 자신들이 공개한 정보에 개인의 위치나 활동 정보와 같은 개인 정보가 포함될 경우 어떤 방식과 수위로 노출이 되는지 각별한 주의를 기울여야 한다.

<표 2> 환경별 SNS들의 프라이버시 보호 정도 비교

	제안 모델	프라이버시 보호 친구 관계 설정 연구 [8]	사용자 결정을 지원하는 연구 [9]
사용자 정보 노출 방지	가능	가능	가능
관계 정의	가능	부분적 가능	불가능
다양한 권한과 정책의 작성	가능	불가능	부분적 가능
사용자 콘텐츠 보호	가능	불가능	부분적 가능

하지만 위의 <표 2>에서 볼 수 있듯이 프라이버시 보호 측면에서 모바일 소셜 네트워크에 대하여 다룬 기존의 선행 연구들[8][9]은 사용자들의 프로파일(profile) 및 관계(relationship) 정보 또는 공개, 비공개와 같은 정책에 대한 프라이버시 보호를 고려하고 있지만 관계의 다양성이나 혹은 사용자가 만들고 공유하는 콘텐츠(객체)에 대한 고려는 미흡한 실정이다.

또, 기존에는 세부적인 관계의 정의나 관리가 불가능하여 컨텐트의 수집, 요약으로부터 개인의 정보 및 관심사가 추론될 수 있었고, 정보의 소유자만의 소셜 네트워크 구축이 어려웠다. 그러나 제안 모델을 사용한 접근제어 기법으로 이러한 문제점들을 해결하고 프라이버시 등을 보호할 수 있다.

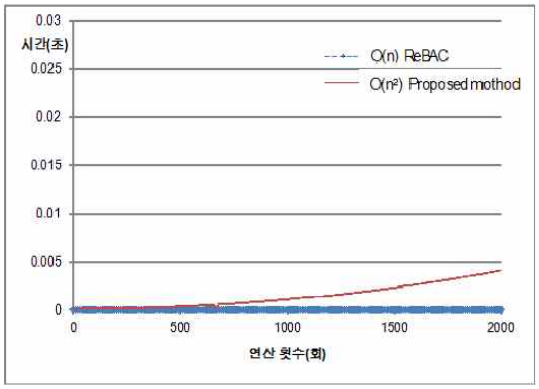
최근에 인기가 있었던 ReBAC의 일종인 친구 기반 접근 제어(Friend-based access control)는 사용자가 관계들을 정의할 때, 오퍼레이터(operator)에서 제공하는 관계의 종류에 따라 private, friend, public 등으로 구분하며 비교적 쉽게 관계를 정의할 수 있다. 그러나 이러한 방식은 친밀함의 단계를 세분화하지 못한다. 또한 기존에는 엔터프라이즈 환경이나 관리자 중심으로 관계가 정의되었지만, 현재 클라우드 컴퓨팅 환경에서는 다양한 장치를 통해 개인 사용자를 중심으로 콘텐츠가 모아지고 재생산된다. 따라서 사용자 중심의 관계의 정의가 어렵고, 다른 사용자 및 SNS로의 소셜 네트워크 확장이 쉽지 않다.

그러나 본 논문에서 제안한 모델은 사용자 중심의 상세한 접근제어의 정의가 가능하고, 콘텐츠 분류를 바탕으로 한 사용자 간의 권한 부여가 가능하기 때문에 사용자 프라이버시의 노출을 막는 동시에 소셜 네트워크를 위한 관계의 확장이 가능하다. 위와 같이 정성적인 분석은 본 연구가 기존의 연구들보다 사용자들에게 향상된 프라이버시를 제공하는 것을 볼 수 있다. 뿐만 아니라 동시에 정량적으로는 큰 지연이 생기지 않은 것을 다음 <표 3>과 같이 볼 수 있다.

<표 3> 시간 복잡도의 정량적 비교

	제안 모델	ReBAC
빅오 표기법	$O(n^2)$	O(n)

위의 <표 3>은 본 연구와 기존 방법 ReBAC을 시간 복잡도 표현 방법인 빅오표기법(big-oh notation)으로 나타낸 것이다. 먼저, 본 연구는 식별자 부분과 ASPE 방법의 합으로 나타낼 수 있는데, 식별자 부분은 역시 트리로 구성되고, ASPE 방법은 두 행렬의 곱으로 최종 표현될 수 있으므로 빅오표기법으로는 $O(n^2)$이다. ReBAC은 트리 형태로 이루어져 있지만 사용자에 따라 이진 트리가 아니라 한쪽으로 치우친 트리가 될 경우 O(n)의 복잡도를 가진다.



(그림 7) 연산으로 인한 시간 지연에 대한 비교

위의 (그림 7)은 ReBAC 방법과 제안 모델에서 지연 시간을 표현한 그래프이다. 가정에서 보통 쓰는 PC가 초당 10억 개 연산을 한다고 가정했을 때, 한 사용자가 500개 이하의 데이터를 처리한다면 시간 지연은 0.00025초 미만이므로 거의 느낄 수 없을 정도이다. 따라서 시간적인 부분에서 생길 수 있는 지연은 크지 않다고 말할 수 있다.

6. 결론 및 향후연구

본 연구는 최근 스마트 장치와 웹 애플리케이션에서 그 필요성이 증가하고 있는 소셜 네트워크의 편리한 정의 및 설정과 사용자 콘텐츠의 통합적인 관리로 프라이버시 보호를 수행하고자 하였다. 또한 SNS들에서 쓰이고 있는 여러 가지 기술을 기반으로 하여 사용자의 스마트 장치들에서 생성된 콘텐츠들을 자동 분류하여 사용자의 편의성을 극대화 시켰다.

본 연구의 프라이버시 보호 정책의 개발은 이 모델을 바탕으로 확장될 수 있는 소셜 네트워크를 통해서 더욱 다양한 형태로 제공될 수 있다. 또한, 기존의 DRM 기술과 접목하여 P2P 환경을 통해 공유되는 콘텐츠(영상, 음반, e-book 등) 또는 UCC에 대한 저작권 보호 정책으로 사용 가능하다. 뿐만 아니라 방송, 게임, 출판 산업에도 새로운 비즈니스 모델이 창출될 수 있다.

결국 본 논문은 스마트 장치 사용자들의 요구에 대한 만족도를 높이고 프라이버시 보호를 위한 접근 제어 기술들을 도입함으로써 차후 가치의 중요성이 더 높아질 개인 정보 및 개인 관계들을 보호하는 모델들의 가이드라인을 제시해 줄 수 있으며 클라우드 컴퓨팅 환경에서의 접근 통제 및 프라이버시 보호로 확장을 도울 수 있을 것이다.

향후 연구로는 제안한 모델의 정형적인 정의와 발생할 수 있는 관계의 충돌 검출 및 해결 방안, 정의된 관계들의 관리 방법 등 제안한 방법들을 더욱 향상시킬 수 있도록 관련 제약 조건 해결 및 발전된 사용자 UI(User Interface) 모델을 제시하는 것이 필요하다.

참 고 문 헌

[1] Jari Porras, Petri Hiirsalmi and Ari Valtaoja, “Peer-to-Peer Communication Approach for a Mobile Environment,” Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS'04), Vol.9, 2004.

[2] Winnie Cheng, Jun Li, Keith Moore, Alan H. Karp, “MUPPET: Mobile Ubiquitous Privacy Protection for Electronic Transactions, In Hewlett-Packard Laboratories Technical Report HPL-2006-141R1, 2006.

[3] L. Aaronson, “Your cell phone is so money,” Popular Science, 2006.

[4] Bishal Raj Karki, Arto Hämäläinen, and Jari Porras, "Social networking on mobile environment," Proceedings of the ACM/IFIP/USENIX Middleware '08 Conference Companion (Companion '08), pp.93-94, 2008.

[5] NHN Corporation, http:// www.nhncorp.com/, 2009.

[6] W3C Mobile Web Initiative, http://www.w3.org/Mobile/, 2009.

[7] Eun-Ae Cho, Chang-Joo Moon, Dae-Ha Park, Doo-Kwon Baik, “An Approach to Privacy Enhancement for Access Control Model in Web 3.0,” Proceedings of the 3rd International Conference on Convergence and Hybrid Information Technology (ICCIT), Vol.2, pp.1046-1051, 2008.

[8] Sören Preibusch, Alastair R. Beresford, “Privacy-Preserving Friendship Relations for Mobile Social Networking,” W3C Workshop on the Future of Social Networking, 2009.

[9] Giuseppe Lugano, Pertti Saariluoma, “To Share or Not to Share: Supporting the User Decision in Mobile Social Software Applications,” Proceedings

of the User Modelling 2007 (UM2007), pp.440-444, 2007.
[10] Leucio Antonio Cutillo, et al., Privacy Preserving Social Networking Through Decentralization
[11] Elena Zheleva, et al., Preserving the Privacy of Sensitive Relationships in Graph Data
[12] Blog, http://en.wikipedia.org/wiki/Blog, Wikipedia, 2012.
[13] W. K.Wong, D.W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," Proceedings of the 35th ACM SIGMOD international conference on Management of data (SIGMOD '09), pp.139 - 152, 2009.
[14] "웹 2.0 환경에서 사용되는 디지털 콘텐츠의 사용자 프라이버시 보호를 위한 RCBAC 모델," 조은애, 문창주, 박대하, 김정동, 강동수, 백두권, 한국디지털콘텐츠학회 논문지 : 제9권 제4호, pp.697~705, 2008.12.
[15] Eun-Ae Cho, Chang-Joo Moon, Dae-Ha Park, Doo-Kwon Baik, "User Privacy Enhanced Access Control Model in Social Network Environment," Proceedings of the 2009 International Conference on Semantic Web and Web Services (SWWS), pp.128-133, Jul. 2009.
[16] Eun-Ae Cho, Gabriel Ghinita, Elisa Bertino, "Privacy-Preserving Similarity Measurement for Access Control Policies," Proceedings of the ACM CCS2010 Workshop on Digital Identity Management (DIM '10), pp. 3 - 11, 2010.
[17] 조은애, 박대하, 문창주, "모바일 서비스 환경에서 정책의 프라이버시 보호를 위한 서비스 제공자 선택 프레임워크", 한국정보과학회 논문지 : 정보통신 제38권 제5호, pp.331-416, 2011.10.
[18] D. Lin and et al, "An approach to Evaluate Policy Similarity," Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT'07), pp.1-10, 2007.
[19] Dan Brickley and Libby Miller, "FOAF Vocabulary Specification 0.9," http://xmlns.com/foaf/0.1/, 2007.
[20] XFN(XHTML Friends Network), http://en.wikipedia.org/wiki/XHTML_Friends_Network, Wikipedia, 2012.

조 은 애

2003년 : 고려대학교 컴퓨터학과 (학사)
2005년 : 고려대학교 컴퓨터학과 (석사)
2009년 : 고려대학교 컴퓨터학과 (박사)
2009년~2011년 : Purdue University 박사후연구원
2012년~현 재 : 삼성전자 책임연구원
관심분야 : 접근제어(Access Control), 권한부여, RBAC(Role-based Access Control), 홈 네트워크, 프라이버시, 데이터베이스 보안

문 창 주

1997년 : 고려대학교 컴퓨터학과 (학사)
1999년 : 고려대학교 컴퓨터학과 (석사)
2004년 : 고려대학교 컴퓨터학과 (박사)
2004년~2005년:고려대학교 정보보호대학원 연구교수
2005년~2006년:건국대학교 컴퓨터응용과학부 컴퓨터시스템전공 조교수
2006년~2008년 : 건국대학교 공과대학 항공우주정보시스템공학과 조교수
2008년~현 재 : 건국대학교 공과대학 항공우주정보시스템공학과 부교수
관심분야 : 접근제어, 권한부여, RBAC, 프라이버시, 유비쿼터스 보안, 임베디드 시스템

박 대 하

1992년 : 고려대학교 컴퓨터학과 (학사)
1994년 : 고려대학교 컴퓨터학과 (석사)
2004년 : 고려대학교 컴퓨터학과 (박사)
1999년~2004년 : (주)시큐리티테크놀로지스연구소장
2004년~현 재 : 고려사이버대학교 정보관리보안학과 교수
관심분야 : 정보보안 정책, 프라이버시 보호, 보안 프로토콜, 이동코드 보안, 클라우드컴퓨팅 보안