GIM에서 사회적 관계 속성을 이용한 ABAC에 관한 연구

서형준°, 고희동, 최윤철

ETRI 부설연구소, KIST 영상미디어센터, 연세대 컴퓨터과학과

hjseo@ensec.re.kr; ko@imrc.kist.re.kr; ycchoi@mglab.yonsei.ac.kr

A Study on ABAC Using Social Relation in GIM

H.J. Seo, Heedong Ko, Y.C. Choi

The Attached Institute of ETRI, Korea Institute of Science and Technology, YonSei Univ.

요 약

본 연구에서는 커뮤니티와 커뮤니티의 참여자가 동적으로 생성되거나 변화되는 상황에서 개인이 생성하는 정보를 안전하게 공유하는 방법을 제공하기 위하여 ABAC(Attributed Based Access Control) 개념을 도입하였고 정보주체와 자료의 속성 확장에 유연하게 대처할 수 있는 방안을 제시하였다. 대부분의 커뮤니티가 정보를 제공하는 주체와 정보를 참조하는 주체의 관계에 따라 정보를 참조하므로 이에 따라 사회적 관계 속성을 이용하여 권한을 관리하는 ABAC를 제시하였다. 본 논문에서는 사회적 관계 속성을 이용한 ABAC가 사용되는 GIM의 형태와 속성, 보안문제, 기존의 방법들이 분석되었으며 논문에서 제안하는 사회적관계 속성을 이용한 ABAC의 적용방법을 기술하였다.

1. 서 론

오늘날은 디지털 커뮤니티가 활성화된 시대로 직장, 사회, 가족, 같은 연령대, 같은 생각, 동호회 등 다양한 커뮤니티가 네트워크라는 도구를 사용하여 공간을 뛰어넘어 존재하고 있다. 디지털 커뮤니티는 관심에 따라 쉽게 모였다가 쉽게 해체되는 특성이 있고 디지털 커뮤니티에서는 개인이 습득하거나 생성한 정보가 공유되고 있다. 개인이 습득하거나 생성한 정보는 비슷한 필요를 느끼는 커뮤니티의 일원과 공개된 자료인 경우 전세계인에게 유용하게 사용될 수 있고 개개인이 원하는 정보 욕구를 만족시킬 수 있어 활성화되고 있다. 또한 개인 정보를 공유할 수 있는 도구와 환경이 마련되어 개인 정보 공유는 더욱 활성화 되리라고 생각된다.

개인정보의 공유는 개인이 관리하던 일정이나 관심사, 느낌, 생각, 사회적인 네트워크, 파일, 동영상, 지식, 관심도가 자연스럽게 공유되는 형태로 발전되었다. 개인정보관리(PIM : Personal Information Managemet)에서 발달된 GIM(Group Information Management)이라는 용어는 그룹에 대한 정보 관리라기보다는 개인정보를 그룹(커뮤니티)과 공유한다는 의미를 가진다. 개인정보를 그룹(커뮤니티)과 공유한다는 의미를 국제적으로 GIM이라는 용어를 사용하기에 본 논문에서도 GIM이라는 용어를 사용하였다.[1]

우리생활의 유무형 경험과 정보를 공유하게 됨에 따라 관리의 중요성이 점차 부각하고 있다. 관리에는 정보를 어떠한 방식으로 저장하며 어떠한 방법을 사용하여 재구성하고 검색을 효율적으로 할 것이냐는 문제를 포함하여 다양한 형태의 기술이 연구되고 있다.[2] 향후 연구가 더 필요한 기술로 개인정보 통제를 꼽고 있는데, 이러한 개인의 정보가 적절하게 관리되고 통제되지 않으면 개인 사생활에 대한 침해뿐만이 아니라 범죄에 까지도 악용될 수 있는 소지가 있기 때문이다. 따라서 원하지 않는 사람이나 대상물에 대해서 정보공유를 통제하고 동적인 상황에 따라 개인정보의 공유 범위를 쉽게 조절할 수 있는 방안이 마련되어야 한다.

본 논문에서는 커뮤니티와 커뮤니티의 참여자가 동적으로 생성되거나 변화되는 상황에서 개인이 생성하는 정보를 안전하게 공유하는 방법을 제공하기 위하여 ABAC 개념을 도입하여 확장에 유연하게 대처할 수 있는 방안을 제시하였다. 대부분의 커뮤니티가 정보를 제공하는 주체와 정보를 참조하는 주체의 관계에 따라 정보를 참조하는 권한을 관리할 수 있는 방법을 제시하기 위해 사회적 관계를 속성으로 사용하였다.

1장에서는 GIM의 형태와 속성을 살펴보고 2장에서는 GIM에서 필요한 보안문제와 기존의 방법들이 제공하는 방법의 한계를 살펴본다. 3장에서는 ABAC의 개념을 소개하고 4장에서는 논문에서 제안하는 사회적관계 속성을 이용한 ABAC를 설명한다.

2. GIM

디지털 커뮤니티가 지속되고 개인의 정보가 유용하게 되면서 개인 정보와 그룹의 정보의 연관성을 활용하려는 시도가 활발하게 전개되고 있다. GIM은 PIM의 확장에 따라 자연스럽게 일어나는 현상으로써 다음 [표 1]과 같

이 개인 일정 공유, 블로그, 사회적 네트워킹 서비스, 전자의료 기록, 파일 공유 등으로 구분할 수 있다. [3]

초기의 GIM은 모임시간을 조정하려는 의도에서 일정을 공유하는 것에서부터 시작되었다. 현재는 웹을 사용하여 일정이 공유되는 형태로 발전하여 전혀 알지 못하는 사람과도 개인의 일정을 공유할 수 있게 되었다. 개인 일정 공유 서비스는 공유할 사람과 정보를 선택할 수 있도록 하고 있다.

블로그(Blog)는 스스로가 가진 느낌이나 품어오던 생각, 알리고 싶은 견해나 주장 같은 것을 웹에다 일기(로그)처럼 적어서, 다른 사람도 보고 읽을 수 있도록 공개한 글모음 형태를 갖는다. 웹 서비스나 포털 서비스에서도 이러한 블로그 기능이 추가되면서 개인화한 블로그 서비스를 제공하고 블로그에 있는 내용이 포털에서 검색되어 제공된다. 블로그는 일반적으로 모든 정보를 공개하는 것에서부터 시작되어 정보에 대한 접근을 제한하지 않는다.

표 1. GIM과 관련된 서비스의 예

구 분	적용체계	주요 공유방법
개인 일정 공유	MS outlook 일정관리, Google 캘린더	공유 대상 지정
블로그	Google, Daum, Naver	제한없음
사회적네트워킹 서비스	싸이월드, MySpace, 피플투, 링크나우	일촌관계지정(싸이월드) 상대의 동의(링크나우)
개인 의료 기록 공유	medical/Insurance System	의료관계법에 따름
파일 공유	del.ici.ous, flickr, eVite, MeetUp	제한없음, 혹은 공개/비공개지정

사회적 네트워킹 서비스는 온라인상에서 사회적 네트워크를 형성해 주는 서비스로 같은 관심과 활동을 공유하는 사람들과 의사소통할 수 있는 서비스를 제공해 준다. 예를 들어 미니홈피를 공유하는 싸이월드, 인물검색을 통한 가치를 교환하는 피플투, 3촌(친구의 친구의 친구)까지 인맥을 형성하는 링크나우 등이 있다. 싸이월드에서는 일촌관계에 의하여 정보를 공유하는 범위를 설정하고 링크나우에서는 상대의 동의가 있을 때 연락처가 공개되는 방식을 지니고 있다.

개인 의료 기록 공유는 의료와 보험 업체계의 IT 시스템은 점차로 상호 연결되고 있어 전자 의료 기록이 GIM의 한 분야로 되어지고 있는 분야이다. 특정한 환자의 의료 기록은 다양한 사람과 기기에 의해서 생성되는 정보로 구성된다. 전자 의료 기록은 GIM에 있어서 프라이버시, 접근제어, 소유권에 관련해서 복잡한 문제를 야기하는 경우이다. 파일 공유는 북마크 공유를 지원하는 del.icio.us, 가족과 친구에서 사진을 공유하는 Flickr, Flickr는 공개와 비공개를 지정할 수 있다.

3. 접근통제기술

기존에 사용되고 있는 접근통제 기술은 임의접근통제(DAC : Discretionary Access Control), 강제접근통제(MAC : Mandatory Access Control), 역할기반 접근통제(RBAC : Role Based Access Control) 기술, 속성기반 접근통제(ABAC : Attributed Based Access Control) 등이 있다.

임의접근통제는 사용 주체에게 임의로 읽기, 쓰기, 실행 등에 관한 접근통제 정책을 부여하는 것으로 관리자 또는 권한자가 파일에 대하여 임의적으로 읽기, 쓰기, 실행을 설정할 수 있는 접근통제 방법이다. 대표적으로 UNIX 시스템에서 읽기, 쓰기, 실행의 권한을 개인과 그룹에 rw- r-- r-- 와 같은 방법으로 설정하는 것을 예로 들 수 있다. [4,5]

강제접근통제는 읽기, 쓰기, 실행 등에 대해서 강제화된 규칙에 따라 접근권한을 제공하는 것이다. 즉, 사용 주체와 객체(파일)에 등급(카테고리, 보안등급 등)을 부여하여 규칙에 따라 자동적으로 통제하는 방법을 말한다. 대표적으로 군에서 주체에 대한 비밀접근 등급을 지정하고 객체에 대한 비밀등급을 지정하여 주체의 비밀접근 등급이 객체의 비밀접근 등급보다 높거나 같아야 객체에 접근할 수 있는 방식을 예로 들 수 있다.[6]

역할기반 접근통제는 사용 주체의 개별적인 등급이 아니라 직무 및 역할에 따라 읽기, 쓰기, 실행 등에 관한 접근통제 정책을 부여하는 방법이다. 예를 들어 사용 주체 A가 내과의사 역할로 로그인할 경우 내과 진료 기록을 읽고 쓸 수 있지만 병원 직원의 역할로 로그인할 경우 진료 기록에 접근할 수 없도록 하는 것이다.[7]

속성기반 접근통제는 사용 주체와 객체, 그리고 환경에 대한 속성을 부여하여 접근을 통제하는 방법이다. 사용 주체는 사용자, 응용 프로그램, 프로세스가 될 수 있으며 ID, 이름, 직위, 역할 등이 속성으로 지정될 수 있다. 객체는 데이터, 파일, 시스템 함수, 웹 서비스 등을 말하며 일반적으로 속성기반 접근통제에서는 객체를 자원(Resource)으로 표현한다. 객체에는 비밀등급, 신규/고급 서비스 여부, 영상등급 등이 속성으로 지정될 수 있다. 환경 속성은 운영 환경, 기술 환경, 상황에 따라 접근이 가능한지 여부를 부여하는 것으로 현재 시간, 현재 위협 수준, 접근하는 네트워크의 보안 등급 등이 속성으로 지정될 수 있다.[8]

역할기반 접근통제는 주체에게 역할이라는 속성을 부여한 방법으로 속성기반 접근통제의 일종이라고 할 수 있다. 역할기반 접근통제와 속성기반 접근통제를 비교하기 위해서 고객에게 전송되는 영화의 예를 들어보자.[9]

기본적인 접근통제는 고객의 구분(어른, 청소년, 아이)과 영화의 등급구분(19세, 13세, 7세)으로 나타내어진다. 차후에 고객을 새로이 구분하게 되어 특별고객(Premium)과 일반고객(Regular)으로 나뉘게 되어 특별고객만이 새로 출시되는 영화를 볼 수 있도록 규칙이 조정되었을 때 역할기반 접근통제와 속성기반 접근통제에서는 다음과 같이 변경시켜주어야 한다.

일반적인 역할기반 접근통제는 고객에 대한 구분을 하기 위한 규칙의 수가 $\prod_{1}^{k} Range(SA_k)$ (S: 주체, A: 속성, K: 속성 수)와 같은 조합 수를 가지게 된다. 즉, 접근통

제 규칙을 주체의 구분에 따라 어른_특별(R1), 어른_일반(R2), 청소년_특별(R3), 청소년_일반(R4), 어린이_특별(R5), 어린이_일반(R6)으로 구분하여 나타내어야 한다.

속성기반 접근통제에서는 다음과 같이 기본적인 규칙 R1(기존규칙)과 향후 추가되는 규칙 R2(추가되는 규칙)로 간단히 나타낼 수 있게 된다.

R1 : can_access(고객, 영화, 환경) ←
{Age(고객) ≧ 19 ∈ 영상등급(19세, 13세, 7세)} V
{19 > Age(고객) ≧ 13 ∈ 영상등급(13세, 7세)} V
{13 > Age(고객) ≧ 7 ∈ 영상등급(7세) }
R2 : can_access(고객, 영화, 환경) ←
{MemberType(고객) = '특별'} V
{MemberType(고객) = '일반' ∧ MovieType(영화) ∉ '신규출시'}
R3 : can_access(고객, 영화, 환경) ← R1 ∧ R2

역할기반 접근통제를 확장하여 규칙기반의 RBAC 기반이 연구되었으나 여전히 이전의 규칙을 상속하는 점에서는 한계가 있다.[10] 속성기반 접근통제는 규칙이 다양하게 생성되고 적용될 수 있다는 점에서 동적인 환경에 적합한 접근통제 방법임을 알 수 있다.[11] 본 논문에서는 동적인 환경에 적합한 속성기반 접근통제를 GIM에서 사용하기 위해서 사회적 관계 속성을 이용하는 방법을 제안하였다. 다음 절은 사회적 관계 속성을 이용하는 방법에 대해서 기술하였다.

4. 사회적 관계를 이용한 ABAC

어떠한 개인이 회사, 가족, 학교, 동호회라는 사회적 관계를 가지고 있을 때 이 관계를 갖는 주체들은 관련된 자료에 접근할 수 있다. 새로운 관계가 추가되는 경우에는 [그림 1]에서 나타낸 바와 같이 사회적 관계를 통한 접근권한을 단순하게 추가하면 된다.

R1 : can_access(주체, 자료, 환경) ←
{RelationShip(주체) = '회사' ∈ 자료(회사)} V
{RelationShip(주체) = '가족' ∈ 자료(가족)} V
{RelationShip(주체) = '학교' ∈ 자료(학교)} V
{RelationShip(주체) = '동호회' ∈ 자료(동호회)}

그림 1. 사회적 관계 속성을 이용한 접근통제

사회적 관계가 포함의 관계가 생기는 경우의 접근통제는 어떻게 해야할까? 회사도 이전회사, 현재회사 등으로 추가 구분될 수 있고 가족도 1촌, 2촌, 3촌, 4촌 등으로 확장될 수 있으며 학교도 고등학교, 대학교, 대학원 등으로 나눌 수 있고 동호회도 테니스, 농구, 자전거, 바둑 등으로 나뉘어진다. 예를 들어, 고등학교 때 친구는 고등학교 자료만 볼 수 있도록 하는 규칙을 새로이 추가하면 [그림2]와 같이 된다. 단, R1은 [그림1]과 동일하고 학교는 중학교 이상으로 가정하여 표현하였다.

R3 : can_access(주체, 자료, 환경) ← R1 ∧ R2
R2 : can_access(주체, 자료, 환경) ←
{RelationShip(주체) = '고등학교' ∈ 자료(고등학교)} ∧
{RelationShip(주체) = '고등학교' ∉ 자료(중학교, 대학교, 대학원)}

그림 2. 사회적 관계 속성이 세분화 되는 경우 접근통제

사회적 관계 속서이 세분화 되는 경우의 접근통제는 [그림 2]와 같이 해결될 수 있지만, 기존에 사회적 관계 속성을 상위의 개념인 학교로만 속성을 부여한 주체와 자료의 접근권한은 어떻게 해야 할까? 규칙에 따라서 하위 개념의 자료를 전부 다 접근할 수도 있고 자료 속성이 학교로만 부여된 자료만을 접근하도록 할 수도 있다. 만약, 온톨로지 상으로 고등학교는 학교에 포함되므로 학교라는 관계가 있어 고등학교 자료도 볼 수 있다면 [그림 3]과 같이 표현된다. 단, R1은 [그림1]과 동일하고 학교는 중학교 이상으로 가정하여 표현하였다.

R3 : can_access(주체, 자료, 환경) ← R1 ∧ R2
R2 : can_access(주체, 자료, 환경) ←
{RelationShip(주체) = '학교' ∈ 자료(중학교, 고등학교, 대학교, 대학원)}

그림 3. 속성의 온톨로지에 따라 접근을 허가하는 경우

온톨로지 상으로 높은 개념을 갖는 주체는 하위의 온톨로지 개념을 갖는 자료를 접근할 수 있도록 규칙이 정해지는 것이다. 단, 이러한 개념을 사용하려면 온톨로지가 명확하게 규정되어 있어야 한다는 것을 전제로 한다.

주체의 속성이 학교로 부여된 경우에 자료의 속성이 학교로만 부여된 자료를 접근할 수 있다면 [그림 4]와 같이 표현된다. 단, R1은 [그림1]과 동일하고 학교는 중학교 이상으로 가정하여 표현하였다.

R3 : can_access(주체, 자료, 환경) ← R1 ∧ R2
R2 : can_access(주체, 자료, 환경) ←
{RelationShip(주체) = '학교' ∉ 자료(중학교, 고등학교, 대학교, 대학원)}

그림 4. 온톨로지와 관계없는 규칙에 따른 접근통제

이와 같이 접근권한 책임자에 따라 여러 규칙들이 존재하게 되면 이전 규칙과 신규 규칙의 충돌이 발생하는 경우가 생기는데 충돌 규칙에 대한 처리는 규칙이 충돌이 난다는 것을 발견할 수 있어야 하며, 충돌 규칙에 대한 처리(신규 규칙 우선, 이전 규칙 우선, 규칙관리자의 판단 등)의 과정을 통해서 해결하여야 하겠지만 본 논문에서는 충돌 규칙 처리에 대해서는 다루지 않는다.

환경에 따라서 주체의 접근권한이 달라지는 경우의 접근통제는 다음과 같이 표현할 수 있다. 가령 '2008년 4월 18일 이후에는 학교의 속성을 갖는 주체는 모든 학교자료를 볼 수 있다'고 하면 [그림 5]와 같이 표현된다.

R3 : can_access(주체, 자료, 환경) ← R1 ∧ R2
R2 : can_access(주체, 자료, 환경) ←
{RelationShip(주체) = '학교' ∧ CurrentTime(환경) >
2008년 4월 18일 ∈ 자료(중학교, 고등학교, 대학교, 대학원)}

그림 5. 환경 속성을 이용한 접근통제의 예

환경 속성이란 주체나 자료의 속성에 관계없이 어떠한 외부의 변화에 의해서 새로운 자료 접근 규칙을 갖도록 되는 경우이다.

관계에 대한 표준을 사용하여 사회적 속성을 이용한 접근통제를 사용하게 되면 호환성을 가질 수 있는 장점이 생기게 된다. 현재 XFN 1.1 프로파일에서는 관계에 대한 표준을 정의하고 있는데, 관계를 교우관계, 물리적 관계, 직업상 관계, 지리적 관계, 가족, 연애관계 등으로 분리하고 각각의 관계를 세부적으로 구분하고 있다. [12]

5. 결 론

개인의 경험과 정보가 네트워크의 발전과 활성화에 따라 더욱 많이 공유하게 됨에 따라 개인정보보호의 중요성이 더욱 중요시되고 있다. 개인의 정보가 적절하게 관리되고 통제되지 않으면 개인 사생활에 대한 침해뿐만이 아니라 범죄에 까지도 악용될 수 있는 소지가 있기 때문이다. 따라서 정보공유를 활성화 하면서 원하지 않는 사람이나 대상물에 대해서 정보공유를 통제하고 동적인 상황에 따라 개인정보의 공유 범위를 쉽게 조절할 수 있는 기술적인 방안 마련이 필요하다.

본 논문에서는 개인정보가 주로 다루어지는 GIM 환경에서 동적인 접근통제를 효율적으로 수행하기 위한 방법으로 속성기반 접근통제를 사용하였다. GIM 환경에 접근하는 대부분의 주체가 자료를 제공하는 개인과 사회적 관계 속성을 갖는다는 점에 착안하여 사회적 관계 속성을 이용한 속성기반 접근통제 방법을 제안하였다.

사회적 관계를 이용한 속성기반 접근통제는 사회적 관계의 추가, 세분화 등의 변화에 유연하게 대처할 수 있으며 사용 환경 변화에 따른 새로운 규칙의 적용도 동적으로 할 수 있는 장점이 있다. 또한, 속성기반 접근통제의 표기법(notation)을 사용하면 규칙간의 충돌을 발견하고 처리(processing)하는데도 유용할 것으로 예상되어 향후 연구에 포함하도록 할 예정이다.

본 논문에서는 사회적 관계에 대한 온톨로지 자체에 대한 논의는 다루어 지지 않았으며 이는 현재 표준화가 추진되고 있는 XFN 1.1 프로파일 등을 사용할 수 있을 것으로 판단된다.

Acknowledgement

본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 지식경제부의 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업의 08B3-B1-40S 과제와 실감형 차세대 웹 기술 개발 (Development of Tangible Web Technology) 과제로 지원된 것입니다.

참고문헌

[1]Thomas Erickson, *From PIM to GIM : Personal Information Management in Group Contexts*, Communication of the ACM, Jan. 2006

[2]Jaime Teevan et. al., *"Personal Information Management"*, Communication of the ACM Vol. 49. no. 1, Jan. 2006, pp40~43

[3]H.J Seo and Heedong Ko, *Technical Report on Personal Information Management Service*, KIST 2007

[4]Vinter S.T. *"Extended discretionary access controls Security and Privacy"*, April 18-21, 1988 pp39 ~ 49

[5]Ninghui Li, Tripunitara, M.V., *"On safety in discretionary access control, Symposium on Security and Privacy"*, May 8-11, 2005 pp 96 ~ 109

[6]Thomas T. *"A mandatory access control mechanism for the UNIX file system"*, Proceeding of the 4th IEEE Aerospace Computer Security Applications Conference Dec. 1988

[7]Heon-Man Jung, Jin-Hyun Tak, Sei-Hoon Lee, and Chang-Jong Wang, *"A Design of Role Based Access Control Manager in Distributed Virtual Environment"*, KIPS, Vol 7, No 1, 2000

[8]Keith Frikken, Mikhail Atallah, Jiangtao Li, *"Attribute-Based Access Control with Hidden Policies and Hidden Credentials,"* IEEE Transactions on Computers, vol. 55, no. 10, pp. 1259-1270, Oct., 2006

[9] Lingyu Wang, Duminda Wijesekera†, and Sushil Jajodia, *A Logic-based Framework for Attribute based Access Control,* CCS '04, October 25-29, 2004, Washington, DC, USA

[10]Al-Kahtani, M.A. and Sandhu, R., *"A Model for Attribute-Based User-Role Assignment"*, 18th Annual Computer Security Applications Conference, USA, 2002

[11]Janice Warner, Vijayalakshmi Atluri, Ravi Mukkamala , *Using Semantics for Automatic Enforcement of Access Control Policies among Dynamic Coalitions*, SACMAT '07, June 20-22, 2007, Sophia Antipolis, France pp235~244

[12]Global Multimedia Protocols Group, XFN(Xhtml Friends Network) 1.1 relationships meta data profile, http://gmpg.org/xfn/11