



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년07월30일
(11) 등록번호 10-1420639
(24) 등록일자 2014년07월11일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) G06Q 50/30 (2012.01)
G06F 17/00 (2006.01)
(21) 출원번호 10-2012-0157249
(22) 출원일자 2012년12월28일
심사청구일자 2012년12월28일
(56) 선행기술조사문헌
KR1020100054303 A

(73) 특허권자
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
박석
서울 종로구 평창12길 16-6, 2동 202호 (평창동, 평창삼호빌라)
김청하
서울 은평구 가좌로7나길 35, 101동 1205호 (응암동, 강남아파트)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 11 항

심사관 : 박진아

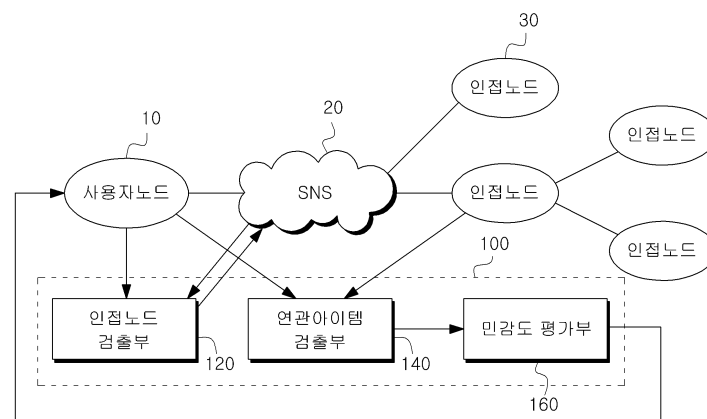
(54) 발명의 명칭 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법

(57) 요약

본 발명은 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법에 관한 것으로, 보다 구체적으로는 사용자노드로부터 아이디정보를 입력받아, 입력받은 아이디정보를 SNS(Social Network Service)를 통해 검색하여 상기 사용자노드와 연관관계가 존재하는 적어도 하나의 인접노드를 검출하는 인접노드검출부; 상기 사용자노드와 검출된 인접노드간 존재하는 적어도 하나의 연관아이템을 검출하는 연관아이템검출부; 및 검출된 상기 연관아이템에 대한 민감도를 연산하고, 그 연산결과에 기초하여 민감도아이템을 검출하는 민감도평가부;를 포함한다.

이러한 구성에 의해, 본 발명의 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법은 SNS를 통해 상호 연관있는 사용자노드와 인접노드로부터 연관아이템을 검출하고, 이에 대한 민감도를 연산하여, 그 연산결과 민감도가 높은 상위 연관아이템을 민감도아이템으로 검출하여, SNS를 통해 사용자노드의 프라이버시정보가 외부로 유출되는 것을 미연에 방지할 수 있는 효과가 있다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	1415123332
부처명	지식경제부
연구사업명	대학IT연구센터 육성지원
연구과제명	융합 소프트웨어를 위한 요구 및 품질검증 기술 개발
기 여 율	1/1
주관기관	서강대학교 산학협력단
연구기간	2012.01.01 ~ 2012.12.31

특허청구의 범위

청구항 1

사용자노드로부터 아이디정보를 입력받아, 입력받은 아이디정보를 SNS(Social Network Service)를 통해 검색하여 상기 사용자노드와 연관관계가 존재하는 적어도 하나의 인접노드를 검출하는 인접노드검출부;

상기 사용자노드와 검출된 인접노드간 존재하는 적어도 하나의 연관아이템을 검출하는 연관아이템검출부; 및

검출된 상기 연관아이템에 대한 민감도를 민감도 평가함수를 이용하여 연산하고, 그 연산결과에 기초하여 민감아이템을 검출하는 민감도평가부;

를 포함하며,

상기 민감도 평가함수는

상기 사용자노드와 연관관계가 존재하는 인접노드 리스트, 상기 인접노드의 연관아이템 리스트, 상기 사용자노드와 인접노드간 유사도, 상기 연관아이템 및 상기 연관아이템이 네트워크 내 관계를 맺은 사용자 수에 기초하여 연산되는 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템.

청구항 2

제1항에 있어서,

상기 인접노드는

상기 사용자노드와 SNS 내 일촌, 친구 또는 팔로어와 같은 연관관계를 허용하는 노드를 나타내는 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템.

청구항 3

제1항에 있어서,

상기 민감도평가부는

상기 연관아이템이 상기 사용자노드 및 인접노드에서 검출된 횟수에 따라 해당 연관아이템에 가중치를 차등적으로 부여하는 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템.

청구항 4

제1항에 있어서,

상기 민감도평가부는

상기 민감도 평가함수는 하기의 수학식으로 이루어지며,

$$\begin{aligned} \text{sensitivity function } s(T_u, T_{adj}, S_u, I) \\ = \sum_{I \in T_{adj}^i} S_u^i \times \frac{\max(\text{popularity}(I))}{\text{popularity}(I)} \end{aligned}$$

이때, 상기 T_u 는 사용자노드와 연관관계가 있는 인접노드 리스트를 나타내고,

상기 Tadj는 상기 인접노드들의 연관아이템 리스트를 나타내며,

상기 Su는 상기 사용자노드와 인접노드간 유사도를 나타내고,

상기 I는 연관아이템을 나타내며,

상기 popularity(I)는 연관아이템 I가 네트워크 내 얼마나 많은 사용자와 관계를 맺고 있는지 여부를 나타내는 함수인 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템.

청구항 5

제4항에 있어서,

상기 사용자노드와 인접노드간 유사도는 하기의 수학식에 의해 연산되며,

$$S_{uv} = \text{similarity}(u, v) = \frac{|t_u \cup t_v| + 1}{|t_u \cup t_v| - |t_u \cap t_v| + 1}$$

이때, 상기 u는 사용자노드를 나타내고,

상기 v는 인접노드를 나타내며,

상기 tu는 상기 사용자노드의 연관아이템을 나타내고,

상기 tv는 상기 인접노드의 연관아이템을 나타내는 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템.

청구항 6

사용자노드로부터 아이디정보를 입력받아, 입력받은 아이디정보를 SNS(Social Network Service)를 통해 검색하여 상기 사용자노드와 연관관계가 존재하는 적어도 하나의 인접노드를 검출하는 단계;

상기 사용자노드와 검출된 인접노드간 존재하는 적어도 하나의 연관아이템을 검출하는 단계; 및

검출된 상기 연관아이템에 대한 민감도를 민감도 평가함수를 이용하여 연산하고, 그 연산결과에 기초하여 민감도 연관아이템을 검출하는 단계;

를 포함하며,

상기 민감도 평가함수는

상기 사용자노드와 연관관계가 존재하는 인접노드 리스트, 상기 인접노드의 연관아이템 리스트, 상기 사용자노드와 인접노드간 유사도, 상기 연관아이템 및 상기 연관아이템이 네트워크 내 관계를 맺은 사용자 수에 기초하여 연산되는 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법.

청구항 7

제6항에 있어서,

상기 인접노드를 검출하는 단계는

상기 사용자노드와 SNS 내 일촌, 친구 또는 팔로우와 같은 연관관계를 허용하는 노드를 검출하는 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법.

청구항 8

제6항에 있어서,

상기 민감도를 연산하는 단계는

상기 연관아이템 중 상기 사용자노드 및 인접노드에서 검출된 횟수에 따라 해당 연관아이템에 가중치를 차등적으로 부여하는 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법.

청구항 9

제6항에 있어서,

상기 민감도를 연산하는 단계는

상기 민감도 평가함수는 하기의 수학식으로 이루어지며,

$$\text{sensitivity function } s(T_u, T_{adj}, S_u, I) = \sum_{I \in T_{adj}^i} S_u^i \times \frac{\max(\text{popularity}(I))}{\text{popularity}(I)}$$

이때, 상기 T_u 는 사용자노드와 연관관계가 있는 인접노드 리스트를 나타내고,

상기 T_{adj} 는 상기 인접노드들의 연관아이템 리스트를 나타내며,

상기 S_u 는 상기 사용자노드와 인접노드간 유사도를 나타내고,

상기 I 는 연관아이템을 나타내며,

상기 $\text{popularity}(I)$ 는 연관아이템 I 가 네트워크 내 얼마나 많은 사용자와 관계를 맺고 있는지 여부를 나타내는 함수인 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법.

청구항 10

제9항에 있어서,

상기 사용자노드와 인접노드간 유사도는 하기의 수학식에 의해 연산되며,

$$S_{uv} = \text{similarity}(u, v) = \frac{|t_u \cup t_v| + 1}{|t_u \cup t_v| - |t_u \cap t_v| + 1}$$

이때, 상기 u 는 사용자노드를 나타내고,

상기 v 는 인접노드를 나타내며,

상기 t_u 는 상기 사용자노드의 연관아이템을 나타내고,

상기 t_v 는 상기 인접노드의 연관아이템을 나타내는 것을 특징으로 하는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법.

청구항 11

제6항 내지 제10항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명세서

기술분야

[0001] 본 발명은 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법에 관한 것으로, 특히 SNS를 사용하는 사용자의 프로필 또는 프라이버시 정보가 사용자의 동의없이 유출되는 방지할 수 있는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법에 관한 것이다.

배경기술

[0002] 소셜 네트워크 서비스(Social Network Service; SNS)는 사용자들이 정보를 공유하고, 다른 사용자와 의사 소통할 수 있는 온라인 서비스이다. SNS의 사용자 수는 지속적으로 증가해왔으며, 특히 스마트폰과 무선인터넷 서비스의 등장은 더욱 폭발적인 사용자 수 증가를 가져왔다.

[0003] 도 1은 인접노드에 의해 사용자정보의 프라이버시정보가 유출되는 과정을 나타낸 도면이다.

[0004] 도 1에 도시된 바와 같이, 하나의 사용자 노드 A와 상기 사용자 노드A와 SNS를 통해 연관관계를 갖는 인접노드 B, C, D가 존재한다. 이러한 상기 사용자노드 A는 아이템 x와 연관되어 있다. 이때, 아이템 x는 사용자노드 A를 사용하는 사용자의 프로필정보, 종교정보, 정치정보 중 적어도 하나를 포함한다. 또한, 상기 인접노드 B, C, D는 연관아이템으로 x,y와 x,z 및 x를 각각 포함한다. 이러한 경우, 악의를 가지고 SNS를 통해 노드에 접근하고자 하는 공격자노드는 상기 사용자 노드 A가 아이템 x를 포함하는 것을 알지 못하고, 상기 인접노드 B, C, D의 정보를 알고 있는 경우, 상기 공격자노드는 상기 사용자노드 A와 아이템 x에 대한 명확한 연결정보를 알지 못하더라도 사용자노드 A는 인접노드 B, C, D와 연관관계가 있으므로, 연관 아이템 x와 연관될 거라고 유추할 수 있다. 이러한 유추과정은 인접노드에 의한 프라이버시 정보가 유출되었다고 할 수 있다.

[0005] 예를 들어, 특정한 성적, 정치적, 종교적 지향을 갖고 있는 사용자의 경우에는 해당 분야의 아이템에 대한 선호를 SNS 상에서 직접적으로 밝히지 않았더라도, 이러한 경향성을 갖고 다른 사용자와 관계를 맺었다면 이를 통해 밝히고 싶지 않은 부분이 공격자에게 알려지는 문제점이 발생했다.

[0006] 상술한 바와 같이, SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법을 살펴보면 다음과 같다.

[0007] 선행기술 1은 한국등록특허공보 제1045928호(2011.06.27)로서, 소셜 네트워크 서비스 제공 시스템에 관한 것이다. 이러한 선행기술 1은 웹서버, 가입회원별로 해당 가입회원의 정보를 저장하고 있는 프로필 데이터베이스, 가입회원의 온라인 친구들에 대해서 연락처를 각각 저장한 온라인 인맥카드들과, 가입회원의 오프라인 친구들의 연락처를 각각 저장한 오프라인 인맥카드들을 가입회원별로 저장하고 있는 인맥 데이터베이스, 인맥 데이터베이스에 저장되는 연락처 정보를 관리하는 연락처 관리모듈, 가입회원의 온라인 친구가 올린 벽보글을 가입회원의 벽보글 화면에 표시하도록 제어하는 벽보글 처리모듈을 구비함으로써, 소셜네트워크 서비스 제공 사이트에 가입된 온라인 친구들의 연락처 이외에도 사용자의 오프라인 친구들의 연락처 및 개인정보를 통합적으로 관리하고 활용할 수 있다.

[0008] 또한, 선행기술 2는 한국공개특허공보 제2012-0087210호(2012.08.07)로서, 소셜 네트워크 서비스 제공 단말, 서버 및 방법에 관한 것이다. 이러한 선행기술 2는 복수의 지인에 관계되는 정보를 저장하는 지인 목록 저장부, 지인에 각각 대응하는 복수의 노드를 3차원에 배치하고 연결하여 3차원 소셜 네트워크 트리를 생성하는 지인 관계 처리부, 그리고 소셜 네트워크 서비스를 제공하는 서버로부터 수신한 정보를 상기 지인 목록 저장부와 상기 지인 관계 처리부로 전달하는 서버 연동부를 포함한다. 소셜 네트워크 서비스를 제공하는 서버는 단말로부터 소셜 네트워크 트리 정보를 수신하여 저장하는 데이터베이스, 소셜 네트워크 트리 정보에 포함된 지인 정보를 이용하여 수신한 소셜 네트워크 트리와 관계있는 지인 정보를 추론하는 추론부, 그리고 단말과 연동하여 추론한 지인 정보를 단말로 전송하는 단말 연동부를 포함하여, 소셜 네트워크 서비스 이용자와 지인 간의 관계를 시각적으로 나타내는 3차원 소셜 네트워크 트리를 제공하고, 소셜 네트워크 서비스 제공 서버에서 지인 간의 관계 정보에 기초하여 추론한 지인 정보를 소셜 네트워크 서비스 이용자에게 제공하여 소셜 네트워크 트리를 확장하

도록 지원한다.

발명의 내용

해결하려는 과제

- [0009] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 SNS를 이용하는 사용자노드의 프로필정보 및 개인 프라이버시 정보가 SNS를 통해 연관관계를 맺고 있는 인접노드에 의해 외부로 유출되는 것을 방지하여 사용자 보안을 향상시킬 수 있는 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법을 제공하고자 한다.

과제의 해결 수단

- [0010] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템은 사용자노드로부터 아이디정보를 입력받아, 입력받은 아이디정보를 SNS(Social Network Service)를 통해 검색하여 상기 사용자노드와 연관관계가 존재하는 적어도 하나의 인접노드를 검출하는 인접노드검출부; 상기 사용자노드와 검출된 인접노드간 존재하는 적어도 하나의 연관아이템을 검출하는 연관아이템검출부; 및 검출된 상기 연관아이템에 대한 민감도를 연산하고, 그 연산결과에 기초하여 민감도아이템을 검출하는 민감도평가부; 를 포함한다.
- [0011] 특히, 상기 사용자노드와 SNS 내 일촌, 친구 또는 팔로어와 같은 연관관계를 허용하는 노드를 나타내는 인접노드를 포함할 수 있다.
- [0012] 보다 바람직하게는 상기 연관아이템이 상기 사용자노드 및 인접노드에서 검출된 횟수에 따라 해당 연관아이템에 가중치를 차등적으로 부여하는 민감도평가부를 포함할 수 있다.
- [0013] 보다 바람직하게는 검출된 상기 연관아이템에 대하여 민감도 평가함수를 이용하여 민감도를 연산하되, 상기 민감도 평가함수는 하기의 수학식으로 이루어지며,

$$\text{sensitivity function } s(T_u, T_{adj}, S_u, I) = \sum_{I \in T_{adj}^i} S_u^i \times \frac{\max(\text{popularity}(I))}{\text{popularity}(I)}$$

- [0014]
- [0015] 이때, 상기 T_u 는 사용자노드와 연관관계가 있는 인접노드 리스트를 나타내고, 상기 T_{adj} 는 상기 인접노드들의 연관아이템 리스트를 나타내며, 상기 S_u 는 상기 사용자노드와 인접노드간 유사도를 나타내고, 상기 I 는 연관아이템을 나타내며, 상기 $\text{popularity}(I)$ 는 연관아이템 I 가 네트워크 내 얼마나 많은 사용자와 관계를 맺고 있는지 여부를 나타내는 함수인 민감도평가부를 포함할 수 있다.
- [0016] 보다 바람직하게는 상기 사용자노드와 인접노드간 유사도는 하기의 수학식으로 이루어지며,

$$S_{uv} = \text{similarity}(u, v) = \frac{|t_u \cup t_v| + 1}{|t_u \cup t_v| - |t_u \cap t_v| + 1}$$

- [0017]
- [0018] 이때, 상기 u 는 사용자노드를 나타내고, 상기 v 는 인접노드를 나타내며, 상기 t_u 는 상기 사용자노드의 연관아이템을 나타내고, 상기 t_v 는 상기 인접노드의 연관아이템을 나타낼 수 있다.
- [0019] 위와 같은 과제를 해결하기 위한 본 발명의 다른 실시 예에 따른 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법은 사용자노드로부터 아이디정보를 입력받아, 입력받은 아이디정보를 SNS(Social Network Service)를 통

해 검색하여 상기 사용자노드와 연관관계가 존재하는 적어도 하나의 인접노드를 검출하는 단계; 상기 사용자노드와 검출된 인접노드간 존재하는 적어도 하나의 연관아이템을 검출하는 단계; 및 검출된 상기 연관아이템에 대한 민감도를 연산하고, 그 연산결과에 기초하여 민감아이템을 검출하는 단계;를 포함한다.

[0020] 상기 연관아이템 중 상기 사용자노드 및 인접노드에서 검출된 횟수에 따라 해당 연관아이템에 가중치를 차등적으로 부여하는 상기 민감도를 연산하는 단계를 포함할 수 있다.

[0021] 보다 바람직하게는 추출된 상기 연관아이템에 대하여 민감도 평가함수를 이용하여 민감도를 연산하되, 상기 민감도 평가함수는 하기의 수학식으로 이루어지며,

$$\text{sensitivity function } s(T_u, T_{adj}, S_u, I) = \sum_{I \in T_{adj}^i} S_u^i \times \frac{\max(\text{popularity}(I))}{\text{popularity}(I)}$$

[0022]

[0023] 이때, 상기 T_u 는 사용자노드와 연관관계가 있는 인접노드 리스트를 나타내고, 상기 T_{adj} 는 상기 인접노드들의 연관아이템 리스트를 나타내며, 상기 S_u 는 상기 사용자노드와 인접노드간 유사도를 나타내고, 상기 I 는 연관아이템을 나타내며, 상기 $\text{popularity}(I)$ 는 연관아이템 I 가 네트워크 내 얼마나 많은 사용자와 관계를 맺고 있는지 여부를 나타내는 함수인 민감도를 연산하는 단계를 포함할 수 있다.

[0024] 보다 바람직하게는 상기 사용자노드와 인접노드간 유사도는 하기의 수학식으로 이루어지며,

$$S_{uv} = \text{similarity}(u, v) = \frac{|t_u \cup t_v| + 1}{|t_u \cup t_v| - |t_u \cap t_v| + 1}$$

[0025]

[0026] 이때, 상기 u 는 사용자노드를 나타내고, 상기 v 는 인접노드를 나타내며, 상기 t_u 는 상기 사용자노드의 연관아이템을 나타내고, 상기 t_v 는 상기 인접노드의 연관아이템을 나타낼 수 있다.

발명의 효과

[0027] 본 발명의 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법은 SNS를 통해 상호 연관있는 사용자노드와 인접노드로부터 연관아이템을 검출하고, 이에 대한 민감도를 연산하여, 그 연산결과 민감도가 높은 상위 연관아이템을 민감아이템으로 검출하여, SNS를 통해 사용자노드의 프라이버시정보가 외부로 유출되는 것을 미연에 방지할 수 있는 효과가 있다.

[0028] 또한, 본 발명의 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법은 사용자노드의 정보를 알지 못하는 공격자노드가 인접노드의 정보만을 이용하여 사용자노드의 정보를 유추하지 못하도록 하여, 사용자노드가 공격자노드에 의해 공격받는 것을 방지할 수 있는 효과가 있다.

도면의 간단한 설명

[0029] 도 1은 인접노드에 의해 사용자정보의 프라이버시정보가 유출되는 과정을 나타낸 도면이다.

도 2는 본 발명의 일 실시 예에 따른 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템을 나타낸 개념도이다.

도 3은 본 발명의 다른 실시 예에 따른 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법을 나타낸 순서도이다.

도 4는 도 3의 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법을 알고리즘으로 구현한 도면이다.

도 5는 본 발명이 구현되는 소셜 네트워크를 나타낸 도면이다.

도 6은 본 발명을 실제 SNS 상에서 구현한 화면을 나타낸 도면이다.

도 7은 개별 아이템별 응답민감도를 나타낸 그래프이다.

도 8은 종래기술과 본 발명간 민감아이템 차이를 나타낸 도면이다.

도 9는 사용자별 민감아이템 비율을 나타낸 그래프이다.

도 10은 사용자별 비공개를 원하는 아이템의 비율을 나타낸 그래프이다.

도 11은 사용자노드의 친구 수에 따른 평균 응답민감도를 나타낸 그래프이다.

발명을 실시하기 위한 구체적인 내용

- [0030] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.
- [0031] 먼저, 본 발명이 구현되는 SNS에 대하여 간략히 살펴보도록 한다.
- [0032] 소셜 네트워크 서비스(Social Network Service)는 사용자들이 자신의 단말(이하, 노드라고 한다.)을 통해 정보를 공유하고, 다른 사용자와 의사소통을 할 수 있는 온라인 서비스를 나타낸다. 최근에는 페이스북, 트위터 등이 주로 사용되고 있다.
- [0033] 이하, 도 2를 참조하여, 본 발명의 일 실시 예에 따른 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템에 대하여 보다 자세히 살펴보도록 한다.
- [0034] 도 2는 본 발명의 일 실시 예에 따른 SNS를 통한 사용자의 프라이버시 정보 누출 탐지 시스템을 나타낸 개념도이다.
- [0035] 도 2에 도시된 바와 같이, 본 발명의 SNS를 통한 사용자의 프라이버시 정보 누출 탐지 시스템(100)은 인접노드검출부(120), 연관아이템검출부(140) 및 민감도평가부(160)를 포함한다.
- [0036] 인접노드검출부(120)는 사용자노드(10)로부터 아이디정보를 입력받아, 입력받은 아이디정보를 SNS(Social Network Service, 20)를 통해 검색하여 상기 사용자노드(10)와 연관관계가 존재하는 적어도 하나의 인접노드(30)를 검출한다. 이와 같이 검출된 상기 인접노드(30)는 상기 사용자노드(10)와 SNS(20)를 통해 일촌, 친구 또는 팔로어와 같은 연관관계를 허용하는 노드를 나타낸다.
- [0037] 연관아이템검출부(140)는 상기 사용자노드(10)와 검출된 인접노드(30)간 존재하는 적어도 하나의 연관아이템을 검출한다.
- [0038] 민감도평가부(160)는 검출된 상기 연관아이템에 대한 민감도를 연산하고, 그 연산결과에 따라 상기 사용자노드(10)에 대한 민감아이템을 검출한다. 이러한 민감도평가부(160)는 상기 연관아이템이 상기 사용자노드(10) 및 인접노드(30)에서 검출된 횟수에 따라 해당 연관아이템에 가중치를 차등적으로 부여한다.
- [0039] 예를 들어, 상기 사용자노드와 인접노드에서 검출된 횟수가 상대적으로 더 높은 연관아이템 x에 대하여 가중치를 5를 부여했다면, 검출횟수가 낮은 연관아이템 y에 대해서는 가중치를 2를 부여할 수 있다. 이에 더하여, 상기 사용자노드와 인접노드가 아닌 SNS 즉, 네트워크 내 검색된 횟수가 높은 경우에는 사용자노드의 프라이버시 정보에 해당한다고 보기 어려움으로 비교적 낮은 가중치를 부여할 수 있다. 또한, 상기 민감도평가부(160)는 검출된 상기 연관아이템에 대하여 민감도를 연산하기 위해, 민감도 평가함수를 이용하는데, 이러한 민감도 평가함수는 하기의 수학식 1과 같이 이루어진다.

[0040] [수학식 1]

$$\text{sensitivity function } s(T_u, T_{adj}, S_u, I) = \sum_{I \in T_{adj}^i} S_u^i \times \frac{\max(\text{popularity}(I))}{\text{popularity}(I)}$$

[0041]

[0042] 이때, 상기 T_u 는 사용자노드와 연관관계가 있는 인접노드 리스트를 나타내고, 상기 T_{adj} 는 상기 인접노드들의 연관아이템 리스트를 나타내며, 상기 S_u 는 상기 사용자노드와 인접노드간 유사도를 나타내고, 상기 I 는 연관아이템을 나타내며, 상기 $\text{popularity}(I)$ 는 연관아이템 I 가 네트워크 내 얼마나 많은 사용자와 관계를 맺고 있는지 여부를 나타내는 함수이다.

[0043] 이때, 상기 사용자노드와 인접노드간 유사도는 하기의 수학식 2와 같이 연산된다.

[0044] [수학식 2]

$$S_{uv} = \text{similarity}(u, v) = \frac{|t_u \cup t_v| + 1}{|t_u \cup t_v| - |t_u \cap t_v| + 1}$$

[0045]

[0046] 이때, 상기 u 는 사용자노드를 나타내고, 상기 v 는 인접노드를 나타내며, 상기 t_u 는 상기 사용자노드의 연관아이템을 나타내고, 상기 t_v 는 상기 인접노드의 연관아이템을 나타낸다.

[0047] 이하, 도 3을 참조하여, 본 발명의 다른 실시 예에 따른 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법에 대하여 자세히 살펴보도록 한다.

[0048] 도 3은 본 발명의 다른 실시 예에 따른 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 방법을 나타낸 순서도이다.

[0049] 도 3에 도시된 바와 같이, 사용자노드로부터 아이디정보를 입력받아, 입력받은 인접노드 검출부가 아이디정보를 SNS(Social Network Service)를 통해 검색하여 상기 사용자노드와 연관관계가 존재하는 적어도 하나의 인접노드를 검출한다(S210).

[0050] 연관아이템 검출부가 상기 사용자노드와 검출된 인접노드간 존재하는 적어도 하나의 연관아이템을 검출한다(S220). 이러한 연관아이템 검출과정은 SNS를 통해 서로 연관관계가 있는 사용자노드와 인접노드는 서로 유사한 성향 및 특징을 보이는 가능성이 높으므로, 상기 사용자노드의 민감아이템을 추출하기 위해, 상기 민감아이템의 후보가 되는 연관아이템을 먼저 검출하는 것이 바람직하다.

[0051] 민감도 평가부가 검출된 상기 연관아이템에 대한 민감도를 연산하고, 그 연산결과에 기초하여 민감아이템을 검출한다(S230). 이러한 연관아이템에 대한 민감도 연산과정에 있어서, 상기 연관아이템 중 상기 사용자노드 및 인접노드에서 검출된 횟수에 따라 해당 연관아이템에 가중치를 차등적으로 부여한다. 예를 들어, 상기 사용자노드와 인접노드에서 검출된 횟수가 상대적으로 더 높은 연관아이템 x 에 대하여 가중치를 5를 부여했다면, 검출횟수가 낮은 연관아이템 y 에 대해서는 가중치를 2를 부여할 수 있다. 이에 더하여, 상기 사용자노드와 인접노드가 아닌 SNS 즉, 네트워크 내 검색된 횟수가 높은 경우에는 사용자노드의 프라이버시 정보에 해당한다고 보기 어려움으로 비교적 낮은 가중치를 부여할 수 있다.

[0052] 특히, 민감도평가부가 추출된 상기 연관아이템에 대하여 민감도 평가함수를 이용하여 민감도를 연산하는데, 이러한 상기 민감도 평가함수는 하기의 수학식 1로 이루어진다.

[0053] [수학식 1]

$$\text{sensitivity function } s(T_u, T_{adj}, S_u, I) = \sum_{I \in T_{adj}^i} S_u^i \times \frac{\max(\text{popularity}(I))}{\text{popularity}(I)}$$

[0054]

[0055] 이때, 상기 T_u 는 사용자노드와 연관관계가 있는 인접노드 리스트를 나타내고, 상기 T_{adj} 는 상기 인접노드들의 연관아이템 리스트를 나타내며, 상기 S_u 는 상기 사용자노드와 인접노드간 유사도를 나타내고, 상기 I 는 연관아이템을 나타내며, 상기 $\text{popularity}(I)$ 는 연관아이템 I 가 네트워크 내 얼마나 많은 사용자와 관계를 맺고 있는지 여부를 나타내는 함수인 것을 나타낸다.

[0056] 또한, 상기 사용자노드와 인접노드간 유사도는 하기의 수학식 2와 같이 연산된다.

[0057] [수학식 2]

$$S_{uv} = \text{similarity}(u, v) = \frac{|t_u \cup t_v| + 1}{|t_u \cup t_v| - |t_u \cap t_v| + 1}$$

[0058]

[0059] 이때, 상기 u 는 사용자노드를 나타내고, 상기 v 는 인접노드를 나타내며, 상기 t_u 는 상기 사용자노드의 연관아이템을 나타내고, 상기 t_v 는 상기 인접노드의 연관아이템을 나타낸다.

[0060] 상술한 일련의 과정을 의사코드로 나타내면 도 4와 같이 나타낼 수 있다.

[0061] 도 4는 도 3의 SNS를 통한 사용자의 프라이버시 정보 누출 탐지 방법을 알고리즘으로 구현한 도면이다.

[0062] 도 4에서 사용되는 각 함수의 기능에 대하여 살펴보면 다음과 같다. $|X|$ 는 리스트 X 의 원소의 개수를 반환하는 함수를 나타낸다. $\text{read_related_items}(x)$ 는 노드 x 의 연관아이템을 읽어 아이템 리스트(t_u)의 형태로 반환하는 함수이다. 실제로는 SNS를 통해 연관아이템을 추출한다. $\text{read_adjacent_users}(x)$ 는 노드 x 의 인접노드들을 리스트 형태로 반환하는 함수를 나타낸다. $\text{similarity}(T_u, T_v)$ 는 아이템 리스트 T_u 와 아이템 리스트 T_v 를 읽어, 이들 간의 유사도를 계산하여 반환하는 함수를 나타낸다. $\text{sensitivity}(T_u, T_{adj}, S_u, I)$ 는 연관아이템 리스트 t_u 와 연관아이템 리스트 t_{adj} , 노드 u 와의 유사도 리스트 S_u 를 기반으로 하여 연관아이템 I 의 민감도를 반환하는 함수를 나타낸다.

[0063] 이처럼 도 4에 도시된 알고리즘에서의 유사도는 사용자 노드 u 와 인접노드들의 연관아이템을 사용하여 각 노드 간의 유사도 S_u 를 결정한다. 또한, 민감도는 사용자가 미리 지정하여 각각의 연관아이템들이 지닌 민감도를 평가한 수치를 나타내는 것으로, 민감도 수치가 높은 연관아이템들이 노출되는 것은 사용자의 프라이버시에 위협이 된다는 것을 의미한다.

[0064] 이하, 민감도 평가 알고리즘에 대하여 보다 자세히 설명하도록 한다.

[0065] 사용자노드의 아이템 리스트와 인접노드의 아이템 리스트를 입력받아 연관아이템 리스트를 출력한다. 이러한 민감도 평가 알고리즘은 기본적으로 $tf \times idf$ 모델을 응용하여, 상대적으로 많은 인접노드에서 추출되는 연관아이템에 대해서는 가중치를 증가시키고, 전체 네트워크에 걸쳐 일반적으로 많이 추출되는 연관아이템에 대해서는 가중치를 감소시키는 방식을 이용한다.

[0066] 또한, 주변의 인접노드를 평가하기 위해 자카드 계수(Jaccard Coefficient)를 응용한 수학식을 이용하여 사용자노드와의 유사도를 분석할 수 있다. 사용자노드의 인접노드 리스트를 T_u , 인접노드들의 연관아이템 리스트를 T_{adj} 로 나타내고, 사용자노드와 인접노드와의 유사도를 S_u , 그리고 연관아이템 I 를 입력값으로 하여, 민감도 함수 $\text{sensitivity function } s(T_u, T_{adj}, S_u, I)$ 는 하기의 수학식 1과 같이 이루어지며, 이때의 출력값은 사용자노드에 대한 연관아이템 I 의 민감도 값이 된다.

[0067] [수학식 1]

$$\text{sensitivity function } s(T_u, T_{adj}, S_u, I) = \sum_{I \in T_{adj}^i} S_u^i \times \frac{\max(\text{popularity}(I))}{\text{popularity}(I)}$$

[0068]

[0069] 상기 popularity(x)함수는 연관아이템 x의 네트워크 전체에 걸쳐 얼마나 많은 사용자와 관계를 맺고 있는지를 나타낸 것으로, 대부분의 SNS에서 일반적으로 공개되어 있는 수치를 나타낸다. 예를 들어, 페이스북의 경우에는 like 버튼을 누른 사용자의 수, Last.fm의 경우에는 listener의 수로 나타낼 수 있다. 여기서, popularity 값을 계산하는 이유는 (tf × idf 모델에서와 같이) 많은 인접 노드에서 발견되는 연관아이템이라고 해도 일반적으로 많은 사용자들에게 연관아이템으로서 받아들여지는 아이템이라면 그만큼 사용자에게 있어서는 민감아이템이라고 판단할 가능성이 낮아 민감도 계산에 있어서 부여되는 가중치를 축소해야 하기 때문이다.

[0070] 이때, max(popularity(I))는 상기 민감도평가 알고리즘에 입력값으로 입력된 모든 아이템 집합에서 가장 높은 popularity 값을 나타낸다. 분모에 max(popularity(I))를 두는 것은 단순히 popularity 값으로만 나타냈을 때 popularity 값에 의해서만 민감도가 평가되는 것을 방지하기 위한 것이다.

[0071] 여기에서, 민감도평가 함수의 입력값인 유사도 similarity는 사용자 노드와 개별 인접노드와 관계를 맺은 연관아이템을 기준으로 얼마나 높은 유사성을 보이는지를 계산한 것이다. 이 때, 임의의 노드 u와 v, 그리고 이들의 연관아이템 집합이 각각 tu와 tv일 때, 노드 u와 v의 유사도를 구하는 공식은 하기의 수학식 2와 같이 구성할 수 있다.

[0072] 이때, 노드 u와 v 간 유사도는 Suv로 표기한다.

[0073] [수학식 2]

$$S_{uv} = \text{similarity}(u, v) = \frac{|t_u \cup t_v| + 1}{|t_u \cup t_v| - |t_u \cap t_v| + 1}$$

[0074]

[0075] 여기서 |x|는 리스트 x의 원소의 개수를 나타낸다.

[0076] 이러한 유사도 계산은 두 아이템 집합 간의 차이를 나타낼 때 이용되는 자카드 계수(Jaccard Coefficient)의 역수를 취한 후, 분모와 분자에 각각 1을 더한 것이다. 이때, 자카드 계수의 역수를 취한 이유는 유사도를 계산해야 하기 때문이며, 분모와 분자에 1을 더한 것은

$$t_u \cap t_v = t_u \cup t_v$$

일 때, 분모가 0이 되는 것을 방지하기 위해서이다.

[0077] 이하, 도 5를 이용하여 본 발명이 실제 소셜 네트워크 서비스 상에서 구현되는 과정에 대하여 자세히 살펴볼도록 한다.

[0078] 도 5는 본 발명이 구현되는 소셜 네트워크를 나타낸 도면이다.

[0079] 도 5에 도시된 바와 같이, A와 B, C, D는 각각 노드를 나타내며, A는 사용자노드를 나타내고, B, C, D는 상기 사용자노드 A의 인접 노드이다. 또한, 사용자노드 A는 j, k아이템과 연결을 갖고 있으며, 사용자노드 B는 j, k, l에, 사용자노드 C는 k, l, m에, 사용자노드 D는 l, m, n과 연결을 각각 갖고 있다. 이때, 상기 아이템들의 popularity 값은 하기의 표 1과 같이 나타났다고 가정한다. 또한, l이 가장 높은 popularity 값을 갖고 있으므로, max(popularity(I)) 값은 12인 것을 알 수 있다.

표 1

아이템	j	k	l	m	n
Popularity	3	4	12	4	8

이에 따라, 본 발명을 적용하여 개별 아이템이 A 와 얼마나 연관을 가지고 있는지, 즉 얼마나 프라이버시 위험도가 높은지를 판단한다.

이를 위해, 먼저 노드 B, C, D 의 A 와의 유사도를 판단할 필요가 있는데, 개별 사용자와의 유사도는 관계를 맺은 아이템의 유사성을 통해 하기와 같이 계산할 수 있다.

A 와 B 의 유사도

$$\text{similarity}(A, B) = \frac{|\{j, k, l\}| + 1}{|\{j, k, l\}| - |\{j, k\}| + 1} = \frac{3 + 1}{3 - 2 + 1} = \frac{4}{2} = 2.0$$

A와 C의 유사도

$$\text{similarity}(A, C) = \frac{|\{j, k, l, m\}| + 1}{|\{j, k, l, m\}| - |\{k\}| + 1} = \frac{4 + 1}{4 - 1 + 1} = \frac{5}{4} = 1.25$$

A와 D의 유사도

$$\text{similarity}(A, D) = \frac{|\{j, k, l, m, n\}| + 1}{|\{j, k, l, m, n\}| - |\emptyset| + 1} = \frac{5 + 1}{5 - 0 + 1} = \frac{5}{5} = 1.0$$

이때, A 와 D 의 유사도는 1.0으로, 두 관계를 맺은 아이템 집합 간에 교집합의 원소 수가 0 일 때 나타나는 것으로, 본 발명에서 나올 수 있는 유사도의 최저치이다. 또한, 계산된 유사도 수치를 이용하여 아이템별 민감도를 구하게 되는데, 아이템 1 의 민감도를 하기와 같이 연산할 수 있다.

$$\text{sensitivity}(A, l) = (2.0 + 1.25 + 1.2) \times \frac{12}{12} = 4.45$$

또한, 아이템 m 의 민감도는 하기와 같이 연산할 수 있다.

$$\text{sensitivity}(A, m) = (1.25 + 1.2) \times \frac{12}{4} = 7.35$$

개별 아이템의 민감도를 표에 나타내면(소수점 셋째 자리에서 반올림) 하기의 표 2와 같이 나타낼 수 있다.

표 2

아이템	j	k	l	m	n
민감도	8.00	9.75	4.45	7.35	1.5

- [0095] 여기서 가장 높은 민감도 값을 가진 아이템은 j 와 k 이지만, 이미 사용자노드 A 와 연결을 가지고 있으므로, 결과값에서는 제외된다. 여기서 가장 높은 민감도 값을 가지고 있는 아이템은 m 으로서, 본 기법은 해당 아이템 이 사용자에게 있어서 민감한 아이템일 가능성이 가장 높을 것으로 예측한다. 이때, 아이템 1 의 경우에는 사용자 A 와 관계를 맺은 모든 사용자에게서 나타나지만, 민감도 값이 가장 높지 않은 것을 알 수 있다. 해당 아이템에 많은 인접 사용자에게서 나타난다고 해도 일반적으로 많은 흥미를 얻어 대중성이 높은 아이템이라면, 사용자노드의 정보와는 크게 관련이 없을 가능성이 높으며, 또한 민감한 아이템이기도 어렵기 때문이다. 결과적으로, 사용자노드 A 는 아이템 m 과 연관을 갖고 있을 가능성이 가장 높으며, 특히 아이템 m 이 사용자 A 에게 민감한 종류의 아이템일 경우에 중대한 프라이버시 위협이 될 수 있다.
- [0096] 이하에서는 본 발명의 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 및 방법을 대표적인 SNS인 페이스북에서 서드 파티 어플리케이션으로서 실제 구현하는 과정에 대하여 자세히 살펴보도록 한다.
- [0097] 도 6은 본 발명을 실제 SNS 상에서 구현한 화면을 나타낸 도면이다.
- [0098] 본 실험을 위해, 실제 사용자들을 대상으로 데이터를 수집하고 추출된 데이터에 대한 질문에 응답하게 하였다. 사용자가 얼마나 수집된 아이템에 대하여 민감하며, 프라이버시 위협을 느끼는지는 사용자에게 대한 설문 이외의 방식으로 측정하기 어렵기 때문에, 실제 사용자에게 대하여, 실제 서드파티 애플리케이션과 동일한 방식으로 동작하는 실험을 구현하여 추출될 수 있는 아이템들에 대한 반응을 설문으로 응답하도록 하였다.
- [0099] 본 실험의 비교를 위해, 종래기술로서 소셜 네트워크의 연결 정보와 사용자 간의 신뢰도를 이용하여 개별 사용자의 영화 평점을 예측하는 기법인 협업 필터링 기법 FilmTrust를 이용하였다. 설문을 위하여 구현한 서드 파티 애플리케이션은 자원자를 대상으로 필요한 정보를 수집하고, 추출된 아이템 중 민감도에 따라 상위 10 개씩을 노출하여 사용자가 해당 아이템의 민감도를 질문하여 1 이상 5 이하의 정수로 응답하게 하였다.
- [0100] 질문지는 다음과 같다.
- [0101] 1) 이 아이템은 당신을 얼마나 잘 설명합니까?
- [0102] 2) 이 아이템과의 관계가 일반에 공개되어도 무방합니까?
- [0103] 페이스북 서버와의 통신을 위해서, 페이스북의 REST-like API 를 이용하였으며, 기법의 계산과 적용을 위하여 javascript 와 PHP, Twitter Bootstrap Library 를 이용하였고, 데이터의 저장과 관리를 위하여 mongoDB 를 이용하였다.
- [0104] 본 실험을 통해, 사용자들이 느끼는 프라이버시 위협의 정도를 분석하고 종래기술과 비교하였다.
- [0105] 약, 11 일간 10대부터 30대까지 연령별 사용자 16 명을 대상으로 데이터를 수집하였고, 추가적으로 아이템의 비공개 여부를 묻기 위해 동일한 사용자들을 대상으로 3 일간 다시 설문을 수행하였다.
- [0106] 이하에서는 개별 아이템에 대하여 사용자들이 얼마나 민감하게 느끼는지 여부를 직접 응답하게 하고, 이에 따른 결과값을 도 7로 표시하였다.
- [0107] 도 7은 개별 아이템별 응답민감도를 나타낸 그래프이다.
- [0108] 도 7에 도시된 바와 같이, 본 그래프는 사용자별 추출한 아이템들에 대하여 응답한 평점의 평균을 표시하고, 평점을 오름차순으로 정렬한 것이다. 평점이 높을수록 추출된 아이템들이 높은 프라이버시 민감도를 가진다고 볼 수 있다. 본 발명과 종래기술을 통해 추출한 아이템들이 실제 사용자가 생각하는 ‘민감한 아이템’ 과 어떠한 차이가 있는지를 비교하기 위하여 RMSE(Root Mean Square Error)를 이용하였다. 상기 RMSE 는 일반적으로 협업 필터링 시스템의 성능을 평가하는데 쓰이는 방법으로서, 기법들 간에 예측값과 실제값 사이의 오차를 비교하는데 이용되며, false-positive 에 대한 검정 방식이라고 볼 수 있다. n 개의 샘플에 대하여 p_i 를 i 번째 아이템
- $$\sqrt{\left(\frac{\sum_{i=1}^n (p_i - r_i)}{n}\right)^2}$$
- 의 예측값, r_i 를 i 번째 아이템의 실제값이라고 할 때, $RMSE =$ 로 나타낼 수 있다.
- [0109] 이처럼, 본 발명과 종래기술에 따른 RMSE 값의 비교는 도 8과 같이 알 수 있다.
- [0110] 도 8은 종래기술과 본 발명간 민감아이템 차이를 나타낸 도면이다.

- [0111] 도 8에 도시된 바와 같이, RMSE 값을 계산하기 위해서, 본 발명과 종래기술에 따라 추출한 상위 10 개의 아이템에 대하여 모두 최대의 민감도인 5 를 예측했다고 가정하고(즉, $p? = 5$), 실제로 사용자가 응답한 값과의 차이를 에러로 두고 계산하였다.
- [0112] 사용자가 민감도 2 이하로 응답한 아이템의 경우, 사용자가 실제로 민감함을 느끼지 않는다는 점에서, 소셜 네트워크의 정보를 통하여 민감한 아이템을 추출해낼 수 있다는 것을 보이는 본 발명과 큰 연관관계가 없다고 볼 수 있으며, 사용자가 추출된 아이템들에 대하여 평균적으로 느끼는 민감도와는 별개로 분석되어야 한다. 따라서, 본 발명에서는 사용자가 응답한 아이템 중 민감도 3 이상을 보인 아이템의 숫자를 분석하고 그 분석결과를 도 9와 같이 나타내었다.
- [0113] 도 9는 사용자별 민감아이템 비율을 나타낸 그래프이다.
- [0114] 도 9에 도시된 바와 같이, 본 그래프는 각각의 사용자에게 대하여, 본 발명과 종래기술에 의해 추출하여 노출한 10 개의 아이템에 대하여 민감도 3 이상을 보인 아이템의 비율을 표시하였다.
- [0115] 예를 들어, 사용자 15 는 민감도 3 이상으로 응답한 아이템의 수가 본 발명에서 5 개, 종래 기술에서 2 개인 것이다. 실험군 내에서는 모든 사용자가 본 발명이 더 낮거나 동일한 결과를 보였으며, 평균적으로 10.6% (신뢰도 95% 구간 [0.3811, 1.7439]) 더 많은 ‘민감한 아이템’ 을 찾아내는 것을 알 수 있다.
- [0116] 개별적인 아이템의 민감도에 대한 설문 결과와 더불어, 상기 아이템이 실제로 사용자들이 일반에 감추고 싶어하는 아이템인지를 좀 더 정확하게 분석하기 위해 설문지의 두 번째 질문을 좀 더 직접적으로 구성하였다.
- [0117] 동일한 아이템들에 대하여 공개여부를 원하지 않는지 문의하여 그 답변을 도 10과 같이 나타내었다.
- [0118] 도 10은 사용자별 비공개를 원하는 아이템의 비율을 나타낸 그래프이다.
- [0119] 도 10에 도시된 바와 같이, 평균적으로 사용자들은 26.875%의 아이템에 대하여 공개를 원하지 않는다고 응답하였다. 이러한 결과는 종래기술에 대한 응답인 14.375%에 비해 향상된 값으로서, 종래기술에 비하여 ‘공개를 원하지 않는’ 아이템을 더 많이 찾아낸 것을 알 수 있다.
- [0120] 즉, 이러한 결과를 통해 본 발명으로 사용자가 공개를 원하지 않으면서 관련 있는 아이템을 찾아내는 것이 실제로 가능하며, 이는 곧 인접 노드에 의한 프라이버시 유출이 실제로 일어날 수 있음을 보인 것이다.
- [0121] 또한, 도 11을 통해 사용자가 응답한 민감도를 친구의 숫자에 따라 표시하였다.
- [0122] 도 11은 사용자노드의 친구 수에 따른 평균 응답민감도를 나타낸 그래프이다.
- [0123] 도 11에 도시된 바와 같이, 각각의 점은 개별 사용자의 친구 숫자(가로축)와 제시한 아이템들에 대해 응답한 민감도의 평균(세로축)을 나타낸다.
- [0124] 친구의 숫자에 따라 표시해본 결과, 친구의 숫자가 많을수록 정확도가 떨어지는 경향을 확인할 수 있다. 친구의 숫자가 많을 경우, 사용자와 밀접한 연관이 있는 사용자의 비율이 낮아지기 때문으로 분석할 수 있다. 조사 대상의 성별이나 연령, 사용자가 응답한 ‘프라이버시 감수성’ 과는 뚜렷한 경향성을 발견할 수 없으며, 친구의 숫자가 비교적 고르게 분포한 본 실험의 실험군은 모집단에 대한 대표성을 획득하였다고 볼 수 있다.
- [0125] 본 발명의 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법은 SNS를 통해 상호 연관있는 사용자노드와 인접노드로부터 연관아이템을 검출하고, 이에 대한 민감도를 연산하여, 그 연산결과 민감도가 높은 상위 연관아이템을 민감아이템으로 검출하여, SNS를 통해 사용자노드의 프라이버시정보가 외부로 유출되는 것을 미연에 방지할 수 있는 효과가 있다.
- [0126] 또한, 본 발명의 SNS를 통한 사용자의 프라이버시 정보 유출 탐지 시스템 및 방법은 사용자노드의 정보를 알지 못하는 공격자노드가 인접노드의 정보만을 이용하여 사용자노드의 정보를 유추하지 못하도록 하여, 사용자노드가 공격자노드에 의해 공격받는 것을 방지할 수 있는 효과가 있다.
- [0127] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

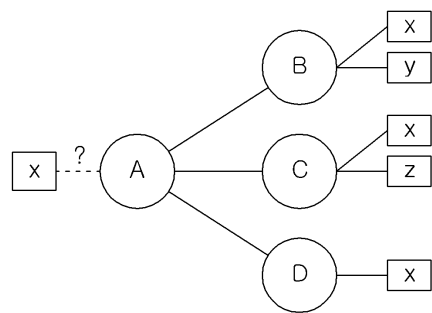
- [0128]
- 120: 인접노드검출부

140: 연관아이템검출부

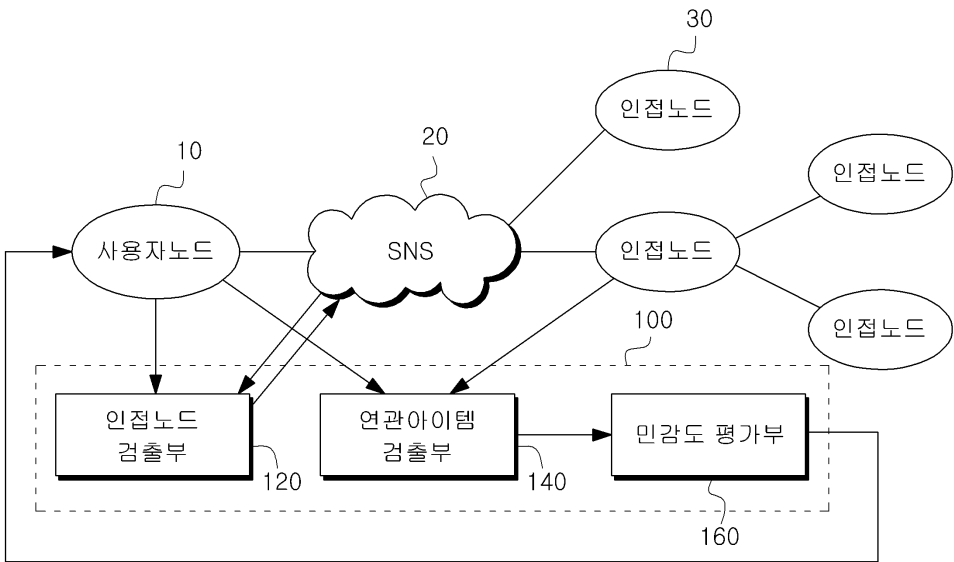
160: 민감도평가부

도면

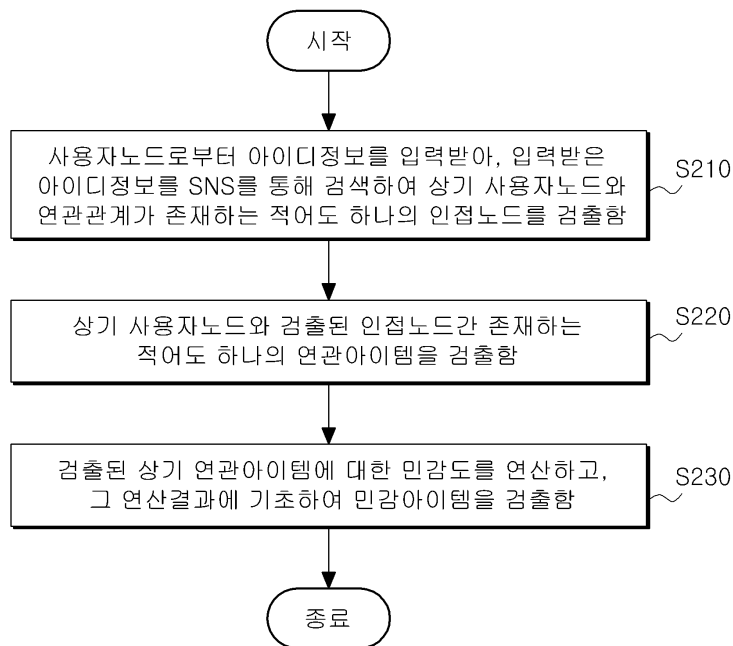
도면1



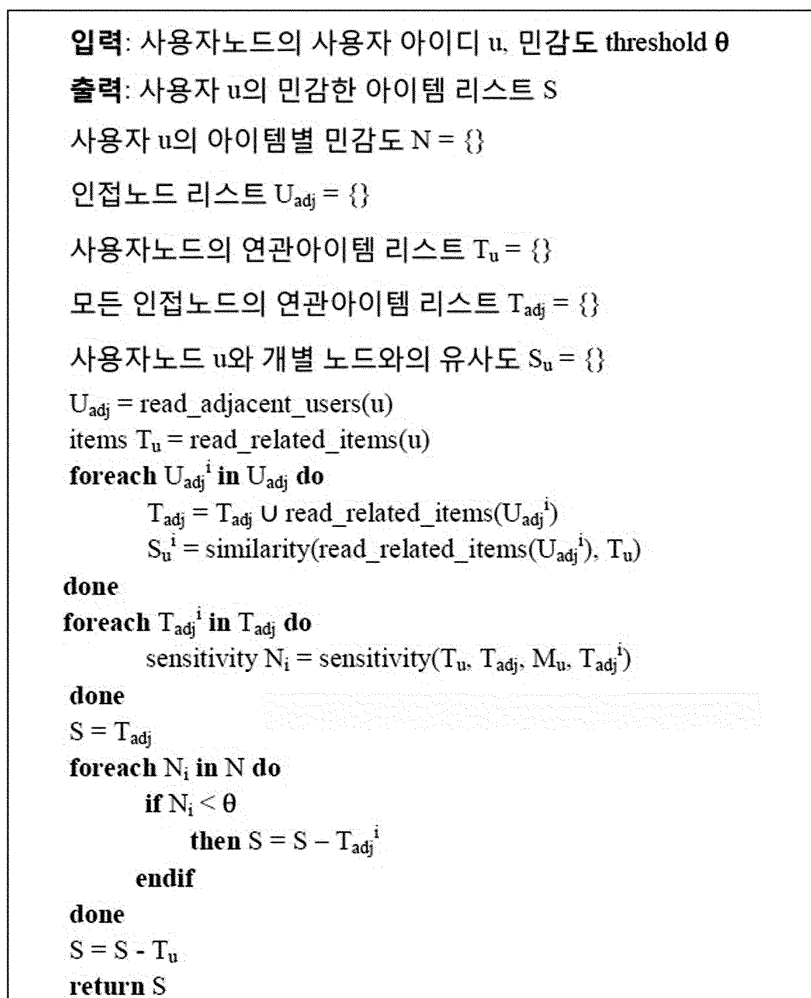
도면2



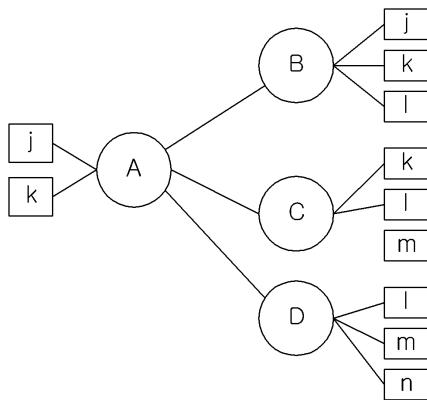
도면3



도면4



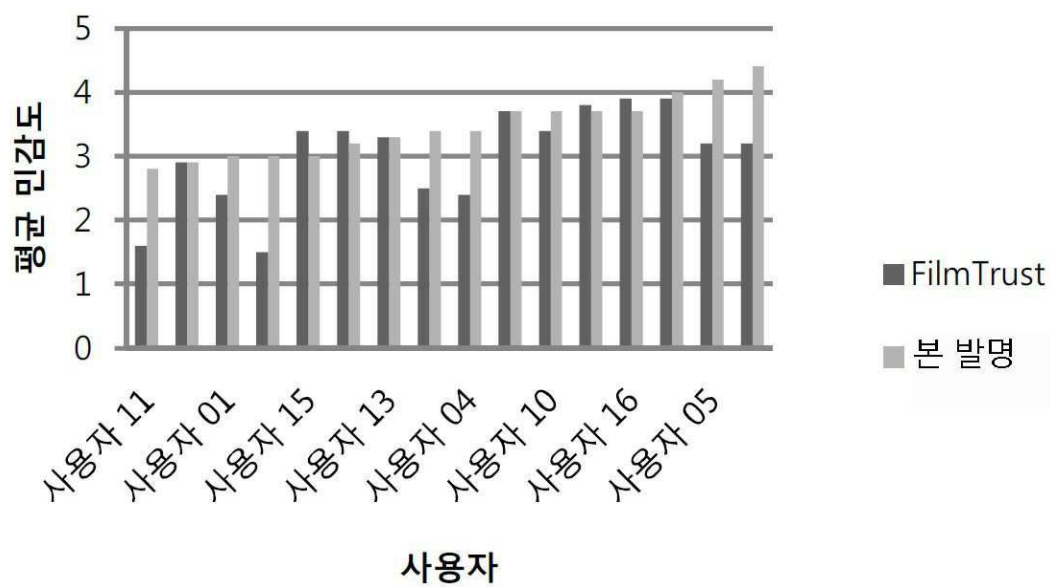
도면5



도면6



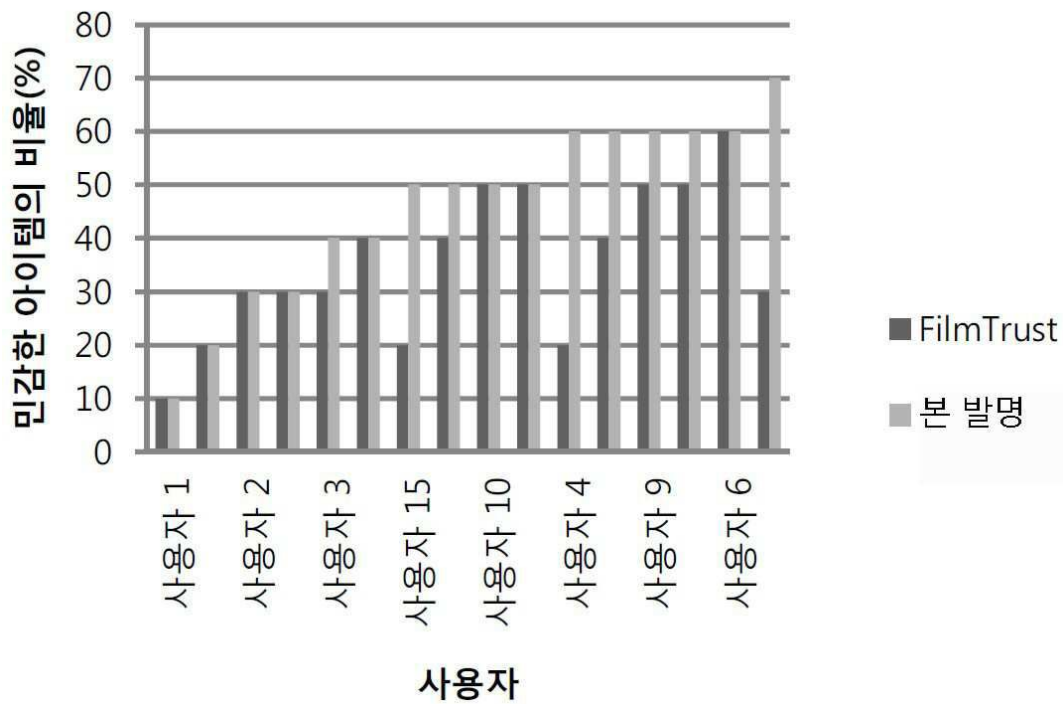
도면7



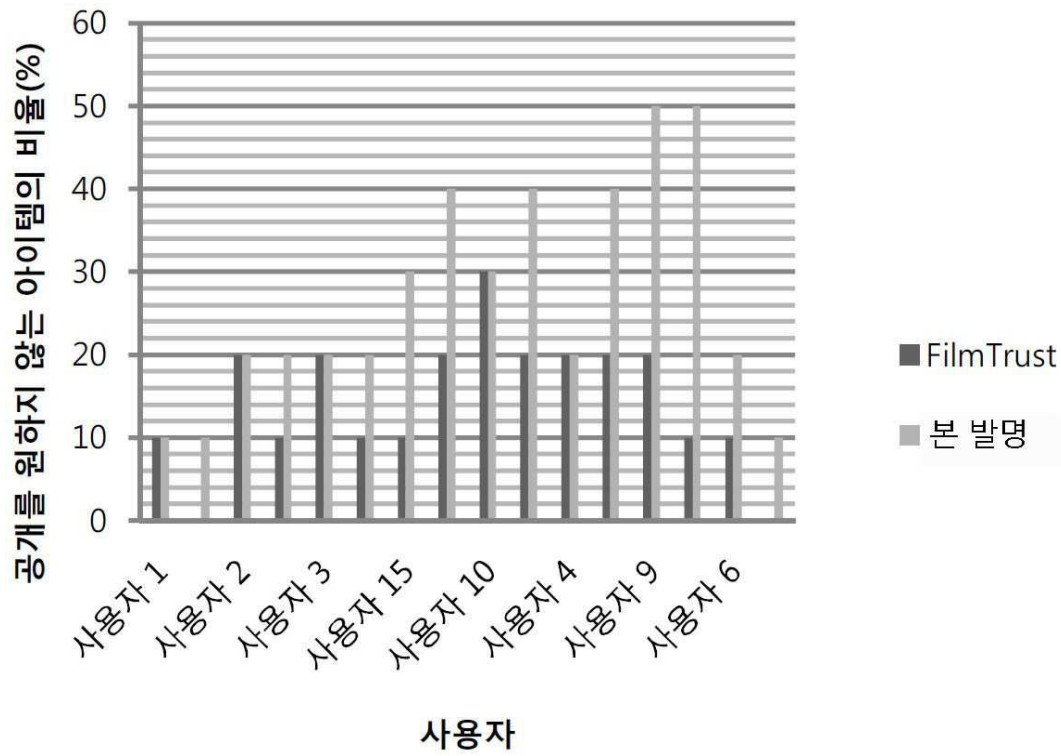
도면8

	RMSE
FilmTrust	1.96875 (95% 신뢰구간 [1.310, 1.764])
본 발명	1.5375 (95% 신뢰구간 [1.610, 2.327])

도면9



도면10



도면11

