Model For Online Social Networks A Privacy And Access Control

MS. SNEHA H. PISEY
Master of Engineering in Computer Science and Engineering, H.V.P.M, College Of Engineering & Technology, Amravati, Maharashtra, India

PROF. P. L. RAMTEKE
Associate Professor
Dept of Computer Science & Engineering, H.V.P.M, College of Engineering & Technology, Amravati, Maharashtra, India

Abstract:

Online social networks (OSNs) have experienced tremendous growth in recent years and become a de facto portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. To this end, we propose an approach to enable the protection of shared data associated with multiple users in OSNs. We formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model which allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof-of-concept prototype of our approach as part of an application in Face-book and provide usability study and system evaluation of our method.

The existence of online social networks that include person specific information creates interesting opportunities for various applications ranging from marketing to community organization. On the other hand, security and privacy concerns need to be addressed for creating such applications. Improving social network access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. To address some of the current limitations, we have created an experimental social network using synthetic data which we then use to test the efficacy of the semantic reasoning based approaches we have previously suggested.
1. Introduction

ONLINE social networks (OSNs) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs [A]. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month [C]. To protect user data, access control has become a central feature of OSNs [B], [D]. A typical OSN provides each user with a virtual space containing profile information, a list of the user’s friends, and web pages, such as wall in Facebook, where users and friends can post content and leave messages. A user profile usually includes information with respect to the user’s birthday, gender, interests, education and work history, and contact information. In addition, users can not only upload content into their own or others’ spaces but also tag other users who appear in the content. Each tag is an explicit reference that links to a user’s space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends, groups or public to access their data, depending on their personal authorization and privacy requirements [E].

2. Privacy Access control Policy and specification

The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content [F]. Past research on OSN security has mainly focused on privacy preserving techniques to allow statistical analysis on social network data without compromising OSN
members’ privacy. In contrast, access control for OSNs is a relatively new research area. Compared to existing approaches, we use semantic web technologies to represent much richer forms of relationships among users, resources and actions. Semantic web technologies have been recently used for developing various policy and access control languages for domains different from OSNs. For example, in the work by Tonti et al. (2003), authors compare various policy languages for distributed agent based systems that define authorization and obligation policies.

In most of the existing social network privacy architectures settings access control is performed via encryption, but none of the schemes focus on the issue of efficient user or attribute revocation. The existing revocation schemes have their limitations too. it is the state-of-the-art decentralized architecture for social network privacy. An architecture for OSN is a general cipher and encoding scheme that preserves the semantic properties of data such that it can be processed by the social network provider oblivious to encryption. Facebook has a similar goal, but opts to store the encrypted data on a third-party server, with fake data stored at the OSN provider. It is infeasible to apply their techniques to our problem, as a separate proxy key would be required for every possible encryption policy.

2. Analysis of Problem

Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. For instance, if a user posts a comment in a friend’s space, s/he cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. To address such a critical issue, preliminary protection mechanisms have been offered by existing OSNs [G]. For example, Face-book allows tagged users to remove the tags linked to their profiles or report violations asking Face-book managers to remove the contents that they do not want to share with the public. However, these simple protection mechanisms suffer from several limitations. On one hand, removing a tag from a photo can only prevent other members from seeing a user’s profile by means of the association link, but the user’s image is still contained in the photo. Since original access control policies cannot be changed, the user’s image continues to be revealed to all authorized users. On the other hand, reporting to OSNs only allows us to either keep or delete the content. Such a binary decision from OSN
managers is either too loose or too restrictive, relying on the OSN’s administration and requiring several people to report their request on the same content. Hence, it is essential to develop an effective and flexible access control mechanism for OSNs, accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively [H]

3. Proposed Work and Objectives:
In Proposed System we implemented a proof-of-concept Facebook application for the collaborative management of shared data, called MController. Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. It is worth noting that our current implementation was restricted to handle photo sharing in OSNs [I]. Obversely, our approach can be generalized to deal with other kinds of data sharing and comments, in OSNs as long as the stakeholder of shared data are identified with effective methods like tagging or searching. The proposed system shows a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model [J]. A proof-of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method. Indeed, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated with the shared data, to specify access control policies. As we identified previously in the sharing patterns in addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, need to regulate the access of the shared data as well. In our multiparty access control system, a group of users could collude with one another so as to manipulate the final access control decision [K].
4. **Scope & Objective**

On-line Social Networks (OSNs) are platforms that allow people to publish details about themselves and to connect to other members of the network through links. Recently, the popularity of OSNs is increasing significantly. For example, Face-book now claims to have more than a hundred million active users. The existence of OSNs that include person specific information creates both interesting opportunities and challenges. For example, social network data could be used for marketing products to the right customers. At the same time, security and privacy concerns can prevent such efforts in practice. Improving the OSN access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. However, most of current OSNs implement very basic access control systems, by simply making a user able to decide which personal information are accessible by other members by marking a given item as public, private, or accessible by their direct contacts. In order to give more flexibility, some online social networks enforce variants of these settings, but the principle is the same.

**Objectives:-**

a) Security policies.
b) Unauthorized Excess Control.
c) Provide policy and privacy for multiple user to specify there authorization.
d) Discover potential malicious activities using collaborative control
e) An Online Social Network with User-Defined Privacy
5. Desired Implications:

MODULE DESCRIPTION: Number of Modules  
After careful analysis the system has been identified to have the following modules [12]:

1. Owner Module
2. Contributor Module
3. Stakeholder Module
4. Disseminator Module
5. MPAC Module

1. Owner Module:
In Owner module let is a data item in the space m of a user u in the social network. The user u is called the owner of d. The user u is called the contributor of d. We specifically analyze three scenarios—profile sharing, relationship sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviors in collaborative systems has been addressed by the recent work.

2. Contributor Module:
In Contributor module let d be a data item published by a user u in someone else’s space in the social network. The contributor publishes content to other’s space and the content may also have multiple stakeholders (e.g., tagged users). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor

3. Stakeholder Module:
In Stakeholder module let is a data item in the space of a user in the social network. Let T
be the set of tagged users associated with d. A user u is called a stakeholder of d, if u ∈ T who has a relationship with another user called stakeholder, shares the relationship with an access or. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder’s privacy concern may be violated. A shared content has multiple stakeholders.

4. Disseminator Module:
In Disseminator module let d be a data item shared by a user u from someone else’s space to his/her space in the social network. The user u is called a disseminator of d. A content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content) publishing the content, and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator’s space. For a more complicated case, the disseminated content may be further re-disseminated by disseminator’s friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviors. Especially, regardless of how many steps the content has been re-disseminated, the original access control policies should be always enforced to protect further dissemination of the content.

5. MPAC Module:
MPAC is used to prove if our proposed access control model is valid. To enable a collaborative authorization management of data sharing in OSNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. Our policy specification scheme is built upon the proposed MPAC model. Assessors Specification: Assessors are a set of users who are granted to access the shared data. Assessors can be represented with a set of user names, asset of relationship names or a set of group names in OSNs.

6. Technical Challenges
SN sites are perfect for illegal online activities as they consist of a huge number of users with high levels of trust among them. As a result there is a high range of security risks, threats and challenges. SN sites provide some mechanisms for privacy settings to protect users, but these mechanisms are not enough to protect the users. The top and primary privacy problem is that SN sites are not informing users of the dangers of spreading their personal information. Thus
users are not aware of the extent of the risks involved. The second problem is the privacy tools in SN sites, which are not easy to use and do not offer the flexibility for users to customize their privacy policies according to their needs. The third problem is the users themselves who cannot control what other users can reveal about them such as tagging their photos or related information to other friends’ profiles.

7. Reference


