MULTIPARTY ACCESS CONTROL FOR ONLINE SOCIAL NETWORKS: MODEL AND MECHANISMS

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 Facebook and provide usability study and system evaluation of our method.

EXISTING SYSTEM

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.
PROPOSED SYSTEM

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. 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. 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.

MODULE DESCRIPTION:

Number of Modules

After careful analysis the system has been identified to have the following modules:

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

In Owner module let \( d \) be 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 \( d \) be 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 \( u \in T \) who has a relationship with another user called stakeholder, shares the relationship with an accessor. 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. Accessor Specification: Accessors are a set of users who are granted to access the shared data. Accessors can be represented with a set of user names, asset of relationship names or a set of group names in OSNs.

PROCESS FLOW:
SOFTWARE REQUIREMENTS:

Operating System: Windows
Technology: Java and J2EE
Web Technologies: Html, JavaScript, CSS
IDE: My Eclipse
Web Server: Tomcat
Tool kit: Android Phone
Database: My SQL
Java Version: J2SDK1.5

**HARDWARE REQUIREMENTS:**

- **Hardware**: Pentium
- **Speed**: 1.1 GHz
- **RAM**: 1GB
- **Hard Disk**: 20 GB
- **Floppy Drive**: 1.44 MB
- **Keyboard**: Standard Windows Keyboard
- **Mouse**: Two or Three Button Mouse
- **Monitor**: SVGA