# An Access Control Model for Collaborative Management of Shared Data in OSNS

Ch. Aruna[1], G. Minni[2]

[1]M.Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.
[2]Asst. Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India.

***ABSTRACT:*** *Online social networks (OSNs) have attracted a large amount of users to regularly connect, interact and share information with each other for various purposes. Users share a tremendous amount of content with other users in social networks using various services. The recent growth of social network sites such as Twitter, Facebook and MySpace has created many interesting and challenging security and privacy problems. In OSNs, users manage their profile, interact with other users, and selforganize into different communities. Users profiles usually include information such as the user's name, address, birthdate, contact information, emails, education, interests, photos, music, videos, blogs and many other attributes The explosive growth of private or sensitive user data that are readily available in OSNs has raised an urgent expectation for effective access control that can protect these data from unauthorized users in OSNs. This paper presents an access control model for the protection of shared data associated with multiple users in online social networks.*

***Keywords:*** *Access control, MController, OSN, Privacy.*

## I. INTRODUCTION

Online social networks (OSNs) serve a number of purposes, but three primary roles stand out as common across all sites. First, OSNs are used to maintain and strengthen existing social ties, or make new social connections. The sites allow users to "articulate and make visible their online social networks", thereby "communicating with people who are already a part of their extended social network" [1]. Second, OSNs are used by each member to upload her own content. Note that the content shared often varies from site to site, and sometimes is only the user's profile itself. Third, OSNs are used to find new, interesting content by filtering, recommending, and organizing the content uploaded by users.

Full participation in OSNs requires users to register a (pseudo) identity with the network, though some sites do allow browsing public data without explicit sign-on. Users may volunteer information about themselves, for example their birthday, place of residence, interests, etc., all of which constitutes the user's profile. The online social network itself is composed of links between users. Some sites allow users to link to any other user, without consent from the link recipient, while other sites follow a two-phase procedure that only allows a link to be established when both parties agree. Certain sites, such as Flickr, have social networks with directed links- meaning a link from A to B does not imply the presence of a reverse link, whereas others, such as Orkut, have social networks with undirected links. Most sites also enable users to create special interest groups, which are akin to Usenet [2] newsgroups. Users can post messages to groups (visible to all group members) and even upload shared content to that group. Certain groups are moderated, and admission to the group is controlled by a single group administrator, while other groups are open for any member to join. All sites today require explicit group declaration by the users; users must manually create groups, appoint administrators (if necessary), and declare which groups they are a member of.

Once an identity is built, users of content sharing sites can upload content onto their account. Many such online sites enable users to mark content as public (visible to anyone) or private (visible only to their immediate "friends"), and to tag content with labels. Many sites, such as YouTube, allow users to upload an unlimited amount of video content, while other sites, such as Flickr, require that users either pay a subscription fee or be subject to an upload limit. All of the content uploaded by a given user is listed in their user's profile, allowing other users to browse through the social network to discover new content. Typically, the content is automatically indexed, and, if publicly available, made accessible though a textual search. An example is Flickr's photo search, which allows the users to locate photos by searching based on tags and comments.

## II. RELATED WORK

Several studies have examined the interface design to support user awareness of the privacy risks and algorithms for relationship-based access-control scheme. In [3], the authors presented a social-networking-based access-control scheme for online information sharing by considering identities as key pairs and identifying the social relationship based on social attestations. Under this approach, a simple access-control list is employed to manage user access. A more sophisticated mechanism to manage access controls in [4], is rule- based and follows complex policies that are expressed as constraints on the type, depth, and trust level of existing relationships. This control methods is further extended by making access-control decisions completely decentralized and collaborative [5].

In [6], the authors introduced a conceptually-similar but more comprehensive trust-based access control model. This model allows the specification of access rules for online resources, where legitimate users are denoted in terms of the relationship type, depth, and trust level between users in OSNs. In [7], the authors proposed an access control model that formalizes and generalizes the access control mechanism implemented in Facebook, admitting arbitrary policy vocabularies that are based on theoretical graph properties. In [8], the authors described relationship-based access control as one of new security paradigms that addresses unique requirements of Web 2.0. In [9], the authors provided a solution for collective privacy management in OSNs. Their work considered access control policies of a data 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.

## III. MULTIPARTY ACCESS CONTROL MODEL FOR OSNS

### A. Multi party Access Control Model

A social network can be represented by a relationship network, a set of user groups and a collection of user data (Figure 1). The relationship network of a social network is a directed labeled graph, where each node denotes a user and each edge represents a relationship between two users. The label associated with each edge represents the type of the relationship. Edge direction denotes that the initial node of an edge establishes the relationship and the terminal node of the edge accepts that relationship. The number and type of supported relationships rely on the specific social network and its purposes. Social network should allow multiple controllers, who are associated with the shared data, to specify access control policies. In addition to the owner of data, other controllers, including the stakeholder, contributor and disseminator of data, need to regulate the access of the shared data as well.

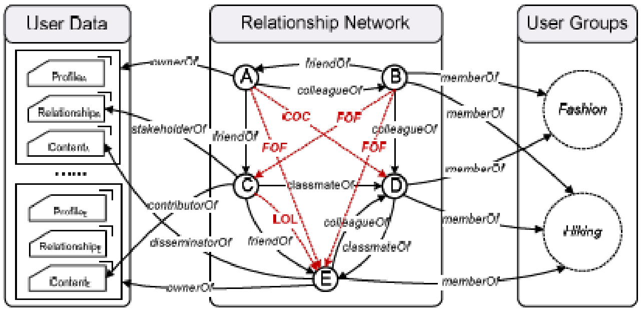

Figure 1: An Example of Multiparty Social Network Representation

### B. MPAC Policy specification

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, a set of relationship names or a set of group names in OSNs.

**Data Specification:** In OSNs, user data is composed of three types of information, user profile, user relationship and user content. To facilitate effective privacy conflict resolution for multiparty access control, we introduce sensitivity levels for data specification, which are assigned by the controllers to the shared data items. A user's judgment of the sensitivity level of the data is not binary (private/public), but multi-dimensional with varying degrees of sensitivity.

**Access Control Policy:** To summarize the above-mentioned policy elements, we introduce the definition of a multiparty access control policy as follows:

A multiparty access control policy is a 5-tuple P =< controller; ctype; accessor; data; effect >, where

- controller $\in$ U is a user who can regulate the access
- of data;
- ctype $\in$ CT is the type of the controller;
- accessor is a set of users to whom the authorization
- is granted, representing with an access specification.
- data is represented with a data specification and
- effect $\in$ {permit; deny} is the authorization effect of the policy.

### C. Multiparty Policy Evaluation

Two steps are performed to evaluate an access request over multi- party access control policies. The first one checks the access request against the policy specified by each controller and yields a decision for the controller. The accessor element in a policy decides whether that policy is applicable to a request. If the user who sends the request belongs to the user set derived from the accessor of the policy, the policy is applicable and the evaluation process returns a response with the decision (either permit or deny) indicated by the effect element in the policy. Otherwise, the response yields deny decision if the policy is not applicable to that request. In the second one, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request. Figure 2 illustrates the evaluation process of multi- party access control policies.

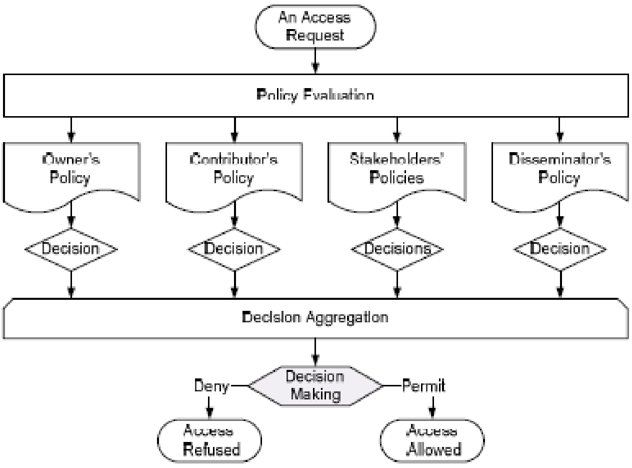

Figure 2: Multiparty Policy Evaluation Process

## IV. IMPLEMENTATION OF MCONTROLLER

In our proposed work, we present an application called "MController" for supporting collaborative management of shared data. It enables multiple associated users to specify their access control policies and privacy preferences to co-control a shared data item. Consider the social network "Facebook". Facebook server accepts inputs from the users, and then forwards them to the application server. The application server is responsible for the input processing and the collaborative management of the shared data. Information related to the user data such as friend lists, user identifiers, user groups, and user contents are stored in the MySQL database. Once the user installs MController in his/her Facebook space, MController can access user's basic information and contents. In particular, MController can retrieve and list all the uploaded photos, which are owned or uploaded by the user, or where the user was tagged. Then, the user can select any photo to specify his/hery preference. If the user is not the owner of the selected photo, then he/she only edit the privacy setting and sensitivity setting of the photo. Otherwise, if the user is an owner of the photo, then he/she can further configure the conflict resolution mechanism for the shared photo.

The core component of MController is the decision making module, which processes access requests and then returns responses (either permit or deny) for the requests. Figure 3 depicts the system architecture of the decision making module in MController. To evaluate an access request, the control policies of each controller of the targeted content are enforced first to generate a decision for the Mcontroller. Then, the decisions of all of the controllers are aggregated to yield a final decision as the response to that request. During the process of decision making, policy conflicts are resolved when evaluating the controllers' policies by adopting a strategy chain pre-defined by the controllers.

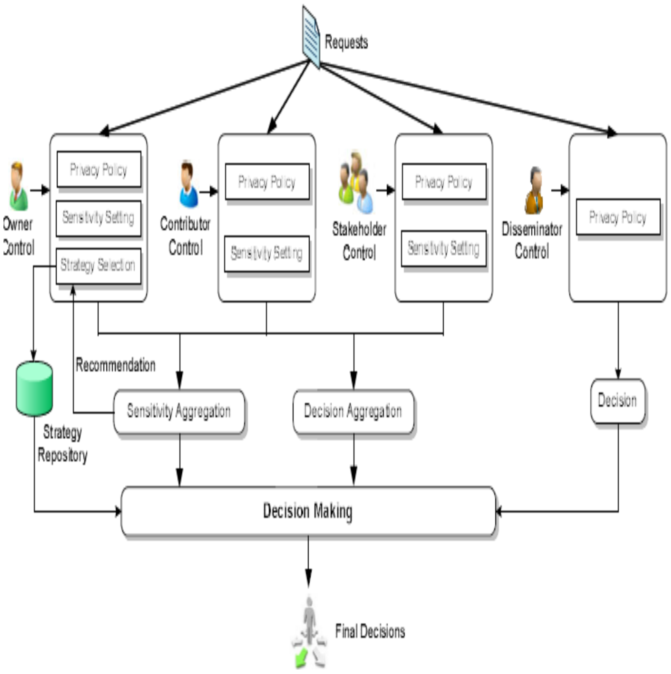

Figure 3: System Architecture of Decision Making in MController

In addition, multi- party privacy conflicts are also resolved based on the configured conflict resolution method when aggregating the decisions of controllers. If the owner of the content chooses the automatic conflict resolution, then the aggregated sensitivity value is utilized as a threshold for making a decision. Otherwise, multi- party privacy conflicts are resolved by applying the strategy selected by the owner, and the aggregated sensitivity score is considered as the recommendation for that strategy selection. Regarding access requests to the disseminated contents, the final decision is made by combining the disseminator's decision and the original controllers' decision through a deny-overrides combination mechanism.

## V. SYSTEM USABILITY AND PERFORMANCE EVALUATION

### A. Participants and Procedure

MController is a functional proof-of-concept implementation of collaborative privacy management. To measure the practicality and usability of our mechanism, we conducted a survey study (n=35) to explore the factors surrounding users' desires for privacy and discover how we might improve those implemented in MController. Specifically, we were interested in users' perspectives on the current Facebook privacy system and their desires for more control over photos they do not own. Users were given the opportunity to share our application and play with their friends. While this is not a random sampling, recruiting using the natural dissemination features of Facebook arguably gives an accurate profile of the ecosystem. Before Using MController. Prior to using MController, users were asked a few questions about their usage of Facebook to determine the user's perceived usability of the current Facebook privacy controls. Since we were interested in the maximum average perception of Facebook, we looked at the upper bound of the confidence interval. An average user asserts at most 25% positively about the likability and control of Facebook's privacy management mechanism, and at most 44% on Facebook's simplicity as shown in Table 1. This demonstrates an average negative opinion of the Facebook's privacy controls that users currently must use.

TABLE 1
Usability Evaluation for Facebook and MController Privacy Controls

| Metric | Facebook | | MController | |
|---|---|---|---|---|
| | Average | Upper bound on 95% confidence interval | Average | Lower bound on 95% confidence interval |
| Linkability | 0.20 | 0.25 | 0.83 | 0.80 |
| Simplicity | 0.38 | 0.44 | 0.72 | 0.64 |
| Control | 0.20 | 0.25 | 0.83 | 0.80 |

After Using MController, users were then asked to perform a few tasks in MController. Since we were interested in the average minimum opinion of MController, we looked at the lower bound of the confidence interval. An average user asserts at least 80% positively about the likability and control, and at least 67% positively on MController's simplicity as shown in Table 1. This demonstrates an average positive opinion of the controls and ideas presented to users in MController.

### B. Performance Evaluation

To evaluate the performance of the policy evaluation mechanism in MController, we changed the number of the controllers of a shared photo from 1 to 20, and assigned each controller with the average number of friends, 130, which is claimed by Facebook statistics. Also, we considered two cases for our evaluation. In the first case, each controller allows "friends" to access the shared photo. In the second case, controllers specify "friends of friends" as the accessors instead of "friends". In our experiments, we performed 1,000 independent trials and measured the performance of each trial. Since the system performance depends on other There are O(n) MySQL calls and data fetching operations and O(1) for additional operations. Moreover, we could observe there was no significant overhead when we run MController in Facebook.

## VI. CONCLUSION

Although social networks attempt to improve security and privacy, they have not achieved the complete or ideal access control mechanisms that users actually demand. In current social networks, individual users can choose different preferences, causing privacy conflicts in shared information that multiple users co- own. In this paper, we have proposed an optimal solution for collaborative management of shared data in OSNs. A multi- party access control model was formulated, along with a multi- party policy specification scheme and corresponding policy evaluation method. In addition, we have introduced an approach for representing and reasoning about our proposed method. 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 proposed method.

## REFERENCES

[1] Danah boyd and Nicole B. Ellison. Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 2007.

[2] Bryan Pfaffenberger. The USENET Book: Finding, Using, and Surviving News- groups on the Internet. Addison Wesley, New York, NY, USA, 2004.

[3] Kiran K. Gollu, Stefan Saroiu, & Alec Wolman. (2007, October). A Social Networking-Based Access Control Scheme for Personal Content Proc. 21st ACM Symposium on Operating Systems Principles (SOSP '07), Stevenson,Washington. (WIP)

[4] Carminati, B., Ferrari, E., & Perego, A. (2006, October). Rule-based access control for social networks. Paper presented at the On the Move to Meaningful Internet SystemsWorkshops.

[5] Carminati, B., & Ferrari, E. (2008, October). Privacy-aware collaborative access control in Web-based social networks. Paper presented at the 22nd annual IFIPWorking Group 11.3Working Conference on Data and Applications Security, London, UK.

[6] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 1734–1744. Springer, 2006.

[7] P. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for facebook-style social network systems. In Proceedings of the 14th European conference on Research in computer security, pages 303–320. Springer-Verlag, 2009.

[8] E. Carrie. Access Control Requirements for Web 2.0 Security and Privacy. In Proc. of Workshop on Web 2.0 Security & Privacy (W2SP). Citeseer, 2007.

[9] A. Squicciarini, M. Shehab, and F. Paci. Collective privacy management in social networks. In Proceedings of the 18th international conference on World wide web, pages 521–530. ACM, 2009.