International Journal of Computational Intelligence and Informatics, Vol. 3: No. 1, April - June 2013

Efficient and Controlled Sharing of Privacy Data in Social Network

T H Theepigaa
Department of Computer Science and Engineering
Adhiparasakthi Engineering College
Melmaruvathur, India
theepi37@gmail.com

A Bhuvaneswari
Department of Computer Science and Engineering
Adhiparasakthi Engineering College
Melmaruvathur, India
bhuvan@adhiparasakthi.in

***Abstract*-Online social Networks (OSNs) have become a successful portal for 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 the privacy over data associated with multiple users. To share the private data and content our analysis presents an approach to enable the protection of shared data associated with multiple users in social networks. We formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and enforcement mechanism. The access control model allows us to overcome the disadvantages of existing system and perform various analysis tasks on sharing privacy data and selection strategies using the multiparty access control Framework.**

Keywords-Social networks, Authorization, Multiusers, Sharing, Private data item.

I. INTRODUCTION

Online social networks sites such as Facebook, Linked In and Twitter combined to reach over billion users, the popularity of social networks continues to increase sharing information online compound. Users regularly upload personnel business and education details of revealing private details to public, to protect user information security controls have become a central feature of social networking sites but remains to users to adopt these features. Personnel data on social networks has used by employers for job searching they can communicate directly with the concern person but more sophisticated applications of social network data include tracking user behavior monitoring.

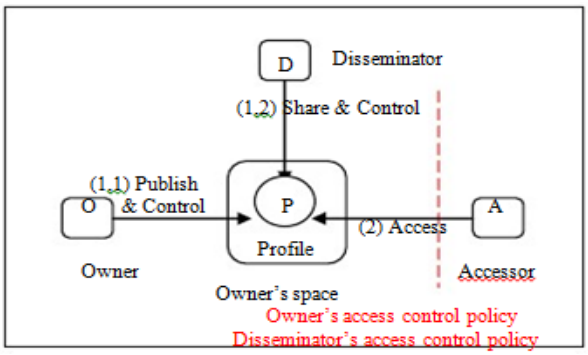
However one aspect of security remains largely unresolved friends photos stories and data are shared across the network conflicting privacy requirements between friends can result in information being unintentionally exposed to the public, while social networks allow users to restrict access to their own data currently no mechanism to enforce privacy concerns over data uploaded by other users social network content is made available to search engines and mined for information, personal privacy goes beyond what one user uploads about his/her becomes an issue of every member on the network shares.

This work controls the shared content can undetermined a user security analyzing the situations in Facebook where asymmetric privacy requirements develop authorization model to capture the core features of multiparty requirements which have not been accommodated access control systems and models for online social networks and secure networking conflict to explore both the frequency and risk of information leaked by friends whom cannot be prevented with existing privacy controls.

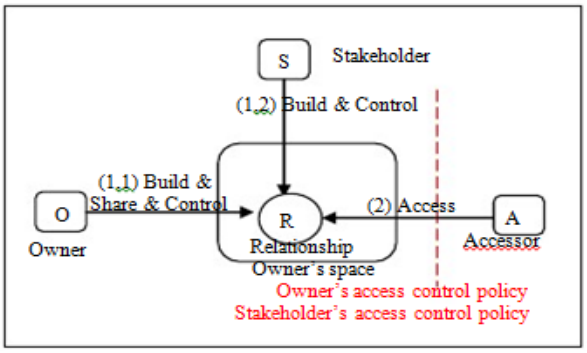
In this paper, we pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by examining how the lack of multiparty access control for data sharing in OSNs can undermine the protection of user data. A multiparty access control (MPAC) model is formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems. Our model also contains a multiparty policy specification scheme.

Another compelling feature of our solution is the support of analysis on multiparty access control model and systems. The correctness of implementation of an access control model is based on the premise that the access control model is valid. Assessing the implications of access control mechanisms traditionally relies on the security analysis technique, which has been applied in several domains (e.g., operating systems [1]). In our approach, we additionally introduce a method to represent and reason about our model in a logic program. Our experimental results demonstrate the feasibility and usability of our approach. The following figure shows the multiparty access control pattern.

ISSN: 2349 - 6363

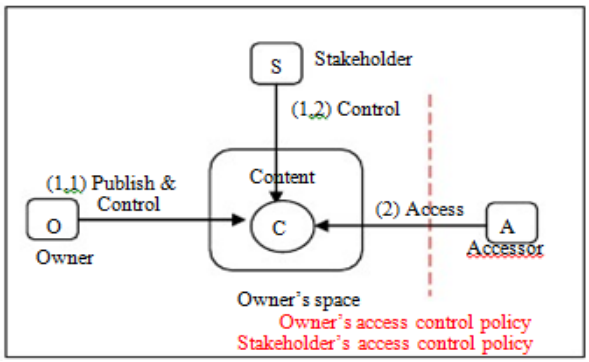


(a) A disseminator shares other's profile

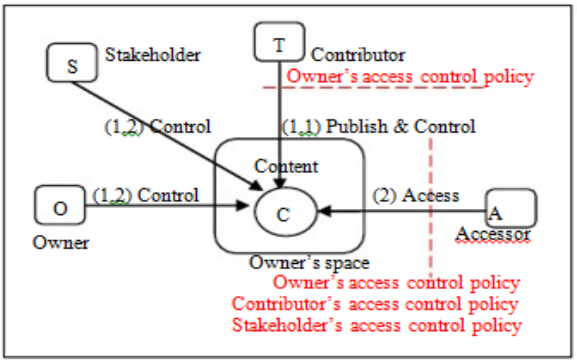


(b) A user shares his/her relationships

Figure 1. Multiparty Access Control Pattern for Profile Sharing



(a) A shared content has multiple stakeholders



(b) A shared content is published by a contributor

Figure 2. Multiparty Access Control Pattern for Content Sharing

II. Requirements And Patterns

In this section we proceed with a comprehensive requirement analysis of multiparty access control in OSNs. Meanwhile, we discuss several typical sharing patterns occurring in OSNs where multiple users may have different authorization requirements to a single resource. We specifically analyze three scenarios — profile sharing, relationship sharing and content sharing.

A. Profile Sharing and Relationship Sharing

An appealing feature of some OSNs is to support social applications written by third-party developers to create additional functionalities built on the top of users' profile for OSNs [2]. To provide meaningful and attractive services, these social applications consume user profile attributes, such as name, birthday, activities, interests, and so on. To make matters more complicated, social applications on current OSN platforms can also consume the profile attributes of a user's friends. In this case, users can select particular pieces of profile attributes they are willing to share with the applications when their friends use the applications.

At the same time, the users who are using the applications may also want to control what information of their friends is available to the applications since it is possible for the applications to infer their private profile attributes through their friends' profile attributes [3, 4]. This means that when an application accesses the profile attributes of a user's friend, both the user and her friend want to gain control over the profile attributes. If we consider the application is an accessor, the user is a disseminator and the user's friend is the owner of shared profile attributes in this scenario.

Figure 1(a) demonstrates a profile sharing pattern where a disseminator can share others' profile attributes to an accessor. Both the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Relationship sharing: Another feature of OSNs is that users can share their relationships with other members. Relationships are inherently bidirectional and carry potentially sensitive information that associated users may not want to disclose. Most OSNs provide mechanisms that users can regulate the display of their friend lists. A user, however, can only control one direction of a relationship. Figure 1(b) shows a relationship sharing pattern where a user called owner, 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.

B. Content Sharing

OSNs provide built-in mechanisms enabling users to communicate and share contents with other members. OSN users can post statuses and notes, upload photos and videos in their own spaces, tag others to their contents, and share the contents with their friends. On the other hand, users can also post contents in their friend's spaces. The shared contents may be connected with multiple users. Figure 2(b) shows a content sharing pattern reflecting this scenario where a contributor publishes content to other's space and the content may also have multiple stakeholders (e.g., tagged users). All associated users should be allowed to define access control policies for the shared content In particular, our proposed solution can also conduct various analysis tasks on access control mechanisms used.

III. ACCESS CONTROL POLICIES

A. Protection Model and Policy Language

Social Network Systems pioneer a paradigm of access control that is distinct from traditional approaches to access control. The Gates coined the term Relationship Based Access Control (ReBAC) to refer to this paradigm. Relationship-Based Access Control is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships. This work explores what it takes to widen the applicability of Relationship-Based Access Control to application domains other than social computing. We prepare an archetypical Relationship-Based Access Control model to capture the essence of the standard, that is, authorization decisions are based on the relationship between the resource owner and the resource accessor in a social network maintained by the security system. A novelty of the model is that it captures the contextual nature of associations. We work out a policy language, based on modal logic, for composing access control policies that support delegation of trust. We use a case study in the domain of Electronic Health Records to demonstrate the utility of our model and its policy language. This provides initial evidence to the feasibility and utility of Relationship-Based Access Control as a general-purpose paradigm of access control.

B. Multiparty Access Control Framework for Data Sharing

We propose a multiparty access control framework (MACF) to model and realize multiparty access control in online social networks. We begin by examining how the lack of multiparty access control for data sharing in online social networks can undermine the security of user data. A multiparty authorization model is then formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems and models for online social networks. In Meanwhile, as conflicts are inevitable in multiparty authorization specification and enforcement, systematic conflict resolution mechanism is also addressed to cope with authorization and privacy conflicts in our framework. We first examine and characterize the behaviors of ICAs. Then we propose a detection framework that is focused on discovering suspicious identities and then validating them. Towards detecting suspicious identities, we propose two approaches based on attribute similarity and similarity of friend networks. The first approach addresses a simpler scenario where mutual friends in friend networks are considered; and the second one captures the scenario where similar friend identities are concerned. We also current experimental results to demonstrate flexibility and effectiveness of the proposed approaches. Finally, Some feasible solutions to validate suspicious identities. Abbreviations and Acronyms

IV. MULTIPARTY ACCESS CONTROL MODEL

In this section, we formalize a Multi-Party Access Control (MPAC) model for OSNs, as well as a policy scheme (Section A) and a policy evaluation mechanism (Section B) for the specification and enforcement of MPAC policies in OSNs. OSN can be represented by a relationship network. OSNs provide each member a Web space where users can store and manage their personal data including profile information, friend list and content. 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. We identified previously in the sharing patterns, in addition to the other controllers, owner of data including the stakeholder, contributor and disseminator of data, need to regulate the access of the shared data as well.

A. Social Network Modules

Definition 1: (Owner): Let d be a data item in the space of a user u in the social network. The user u is called the owner of d.

Definition 2: (Contributor): Let d be a data item published by a user u in someone else's space in the social network. The user u is called the contributor of d.

Definition 3: (Stakeholder): 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 $u \in T$.

Definition 4: (Disseminator): 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.

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.

1) *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.
2) *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.
3) *Access Control Policy:* To summarize the above-mentioned policy elements, we introduce the definition of a multiparty access control policy as follows:
4) *MPAC Policy:* A multiparty access control policy (P) is a 5-tuple, they are controller, ctype, accessor, data and effect. Here
   - controller ∈U is a user who can the access of data.
   - ctype ∈ 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.
   - effect ∈ {permit, deny} is the authorization effect of the policy.

C. Multiparty Policy Evaluation

Two steps are performed to evaluate an access request over multiparty access control policies. The first step 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 the policy is applicable to a request. If the user who sends the request belongs to the user set derived from the accessor of a 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 the request. In the second step, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request.

Figure 3 illustrates the evaluation process of multiparty access control policies. Since data controllers may generate different decisions (permit and deny) for an access request, conflicts may occur. In order to make an unambiguous decision for each access request, it is essential to adopt a systematic conflict resolution mechanism to resolve those conflicts during multiparty policy evaluation. The essential reason leading to the conflicts – especially privacy conflicts.

A naive solution for resolving multiparty privacy conflicts is to only allow the common users of accessor sets defined by the multiple controllers to access the data item. Unfortunately, this strategy is too restrictive in many cases and may not produce desirable results for resolving multiparty privacy conflicts. A strong conflict resolution strategy may provide a better privacy protection. Meanwhile, it may reduce the social value of data sharing in

OSNs. Therefore, it is important to consider the tradeoff between privacy and utility when resolving privacy conflicts. To address this issue, we introduce a simple but flexible voting scheme for resolving multiparty privacy conflicts in OSNs.

1) A voting scheme for decision making of multiparty control

Majority voting is a popular mechanism for decision making [2]. Inspired by such a decision making mechanism, we propose a voting scheme to achieve an effective multiparty conflict resolution for OSNs. A notable feature of the voting mechanism for conflict resolution is that the decision from each controller is able to have an effect on the final decision. Our voting scheme contains two voting mechanisms, decision voting and sensitivity voting.

Decision Voting: A decision voting value (DV) derived from the policy evaluation is defined as follows, where Evaluation(p) returns the decision of a policy p.

$$DV = \begin{cases} 0 & if\ Evaluation\ (p)=Deny \\ 1 & If\ Evaluation\ (p)=Permit \end{cases} \quad (1)$$

Assume that all controllers are equally important, an aggregated decision value (DV_{ag}) (with a range of 0.00 to 1.00) from multiple controllers including the owner (DV_{ow}), the contributor (DV_{cb}) and stakeholders (DV_{st}), is computed with following equation.

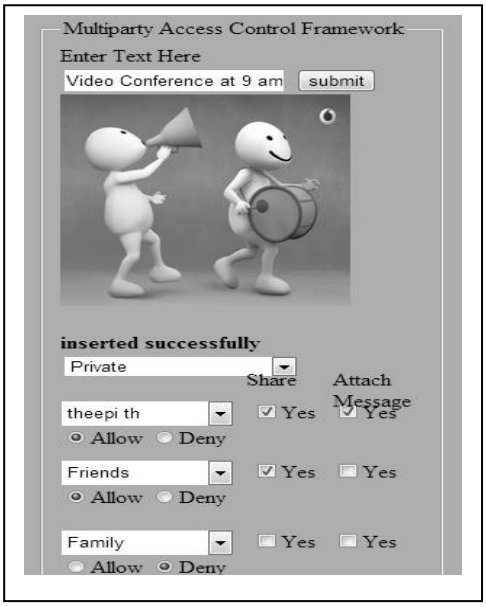


Figure 3. Multiparty Access Control Framework

$$DV_{ag} = \left(DV_{ow} + DV_{cb} + \sum_{i \in SS} DV_{st}^{i} \right) X \frac{1}{m} \quad (2)$$

where SS is the stakeholder set of the shared data item, and m is the number of controllers of the shared data item.

Sensitive Voting: Each controller assigns a sensitivity level (SL) to the shared data item to reflect her/his privacy Concern.

2) Strategy-based conflict resolution with privacy recommendation

In this conflict resolution, the sensitivity score (SC) of a data item is considered as a guideline for the owner of shared data item in selecting an appropriate strategy for conflict resolution. We introduce following strategies for the purpose of resolving multiparty privacy conflicts in OSNs.

Owner-overrides: the owner's decision has the highest priority. This strategy achieves the owner control mechanism that most OSNs are currently utilizing for data sharing. Based on the weighted decision voting scheme, the final decision can be made as follows:

$$\text{Decision} = \begin{cases} \text{Permit} & \textbf{if } \mathbf{DV_{ag}=1} \\ \text{Deny} & \textbf{if } \mathbf{DV_{ag}=0} \end{cases} \quad (3)$$

Full-consensus-permit: if any controller denies the access, the final decision is deny. This strategy can achieve the naive conflict resolution that we discussed previously. The final decision can be derived as:

$$\text{Decision} = \begin{cases} \text{Permit} & \text{if } \mathrm{DV_{ag}=1} \\ \text{Deny} & \text{otherwise} \end{cases} \quad (4)$$

Majority-permit: this strategy permits (denies, resp.) a request if the number of controllers to permit (deny, resp.) the request is greater than the number of controllers to deny (permit, resp.) the request. The final decision can be made as:

$$Decision = \begin{cases} Permit & if\ DV_{ag} \geq 1/2 \\ Deny & if\ DV_{ag} < 1/2 \end{cases} \quad (5)$$

3) Conflict resolution for dissemination control

A user can share other's contents with her/his friends in OSNs. In this case, the user is a disseminator of the content, and the content will be posted in the disseminator's space and visible to her/his friends or the public. Since a disseminator may adopt a weaker control over the disseminated content but the content may be much more sensitive from the perspective of original controllers of the content, the privacy concerns from the original controllers of the content should be always fulfilled, preventing inadvertent disclosure of sensitive contents. In other words, the original access control policies should be always enforced to restrict access to the disseminated

content. Thus, the final decision for an access request to the disseminated content is a composition of the decisions aggregated from original controllers and the decision from the current disseminator. In order to eliminate the risk of possible leakage of sensitive information from the procedure of data dissemination, we leverage a restrictive conflict resolution strategy, Deny-overrides, to resolve conflicts between original controllers' decision and the disseminator's decision. In such a context, if either of those decisions is to deny the access request, the final decision is deny. Otherwise, if both of them are permit, the final decision is permit.

V. DISCUSSIONS

In our multiparty access control system, a group of users could collude with one another so as to manipulate the final access control decision. Consider an attack scenario, where a set of malicious users may want to make a shared photo available to a wider audience. Suppose they can access the photo, and then they all tag themselves or fake their identities to the photo. In addition, they collude with each other to assign a very low sensitivity level for the photo and specify policies to grant a wider audience to access the photo. With a large number of colluding users, the photo may be disclosed to those users who are not expected to gain the access. To prevent such an attack scenario from occurring, three conditions need to be satisfied:

(1) There is no fake identity in OSNs

(2) All tagged users are real users appeared in the photo

(3) All controllers of the photo are honest to specify their privacy preferences

Regarding the first condition, two typical attacks, Sybil attacks [2] and Identity Clone attacks [1], have been introduced to OSNs and several effective approaches have been recently proposed to prevent the former [4, 5] and latter attacks [6], respectively. To guarantee the second condition, an effective tag validation mechanism is needed to verify each tagged user against the photo. In our current system, if any users tag themselves or others in a photo, the photo owner will receive a tag notification. Then, the owner can verify the correctness of the tagged users. As effective automated algorithm are being developed to recognize people accurately in contents such as photos, automatic tag validation is feasible.

Considering the third condition, our current system provides a function to indicate the potential authorization impact with respect to a controller's privacy preference. Using such a function, the photo owner can examine all users who are granted the access by the collaborative authorization and are not explicitly granted by the owner her/himself. Our future work would integrate an effective collusion detection technique into MPAC. To prevent collusion activities, our current prototype has implemented a function for owner control (keystroke control), where the photo owner can disable any controller, who is suspected to be malicious, from participating in collaborative control of the photo. In addition, we would further investigate how users reputations based on their collaboration activities can be applied to prevent and detect malicious activities in our future work.

VI. CONCLUSION

In this paper, we have proposed 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. An access control framework of our solution called Multiparty Access Control Framework has been discussed as well. As part of future work, we are planning to investigate more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs. Also, we would explore more criteria to evaluate the features of our proposed MPAC model. Besides, we plan to systematically integrate the notion of trust and reputation into our MPAC model and investigate a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in OSNs.

REFERENCES

[1] Seda Gurses and Claudia Diaz, "Two tales of privacy in online social networks", Proc. IEEE Security And Privacy, 2013.

[2] H.Hu,G.-J. Ahn, and J. Jorgensen, "Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks", Proc. 27th Ann. Computer Security Applications Conference, 2011, pp.103-112.

[3] Hongxin Hu, Gail-Joon Ahn and J. Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms", Proc. IEEE Knowledge and Data Engineering, 2013.

[4] E. Zheleva and L. Getoor, "To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles", Proc. 18th Int'l Conf. World Wide Web, pp.531-540, 2009.

[5] H.R. Lipford et al., "Visual vs. Compact: A Comparison of Privacy Policy Interfaces", Proc. 28th Int'l Conf. Human Factors in Computing Systems (CHI 10), ACM, 2010, pp.1111–1114.

[6] Anna Carreras, Eva Rodríguez and Jaime Delgado, "Using XACML for access control in Social Networks", Proc. 5th International ODRL Workshop (within Virtual Goods' 09), Nancy, France, ISBN: 978-2-9052, Sept 2009, pp.67-69.