ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering &Technology (IJARCET)
Volume 2, Issue 9, September 2013

PROTECTION OF SHARED DATA FOR ONLINE SOCIAL NETWORKS

A. SARATH [1], S. SRINIVASULU[2], B. SRINIVASULU[3]

1, 3, M.TECH Scholar, VEC, Kavali
2, Assistant Professor, VEC, Kavali

ABSTRACT:

Online Social Networks (OSNs) are essentially designed to facilitate people to share personal and public information and make social connections with others. These OSNs propose good-looking means for digital social communications and information distribution, but also raise a number of security and privacy issues. Whereas OSNs allow users to control access to shared data, at the moment they do not provide any mechanism to implement privacy concerns over data connected with multiple users. The proposed approach is to facilitate the defense of shared data associated with many users in OSNs. We put together an access control replica to capture the essence of multiparty agreement requirements, along with a multiparty strategy requirement scheme and a policy enforcement mechanism. Here present a logical demonstration of our access control model which allows us to influence the features of presented logic solvers to execute various analysis tasks on our model. We introduced a proof-of-concept prototype of our move toward as part of an application in Face book and make available usability study and system valuation of our method. The survival of OSNs that include person detailed information creates attractive openings for various applications ranging from advertising to group of people organization. Security and privacy concerns need to be deal with for creating such applications.

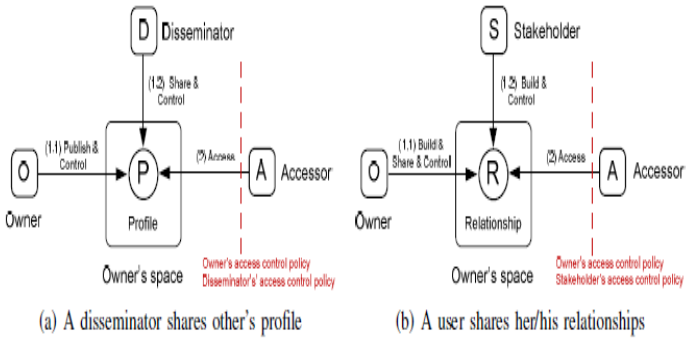
Index Terms: ***Multiparty access control, Social network, Policy specification and management, Security model***

1. INTRODUCTION

Online social networks (OSNs) such as Facebook, Twitter, and Google+ are essentially designed to facilitate people to share personal and public information and formulate social relations with friends, colleagues, family, and coworkers and even with strangers also. In current years, we have seen extraordinary growth in the application of OSNs. For example, Facebook, one of ambassador social network sites, claims that it has more than 900 million active users and over 35 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month. To protect user data, access control has become a central feature of OSNs.

A distinctive OSN provides each user with a implicit space containing profile information, a list of the user's associates, and web pages, such as fortification in Facebook, where users and friends can place content and put down messages. A user profile usually comprises information with respect to the user's gender, birthday, education, interests, work history, and contact information. In adding together, users can not only upload content into their own or others' spaces but also attach a label to other users who become visible in the content. Every tag is an explicit reference that links to a user's space. For the protection of user data, present OSNs at one remove require users to be system and policy administrators for adaptable their data, where users can control data sharing to a specific set of trusted users. OSNs often use user connection and group membership to differentiate between trusted and untrusted users. Even though OSNs currently provide simple access control methods allowing users to administer access to information controlled in their own spaces, users, regrettably, have no control over data existing *outside* their spaces. For example, if a user posts a comment in a friend's space, s/he can't specify which users can view the comment. In a different

case, when a user uploads an image and tags friends who become visible in the photo, the tagged friends cannot check who can observe this photo, even though the tagged friends may have dissimilar privacy concerns about the photo. To take in hand such a serious issue, preface protection mechanisms have been offered by existing OSNs. Suppose Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook supervisors to remove the contents that they do not want to share with the public. These simple protection mechanisms suffer from several boundaries. On one hand, removing a tag from a photo can only avoid other members from seeing a user's profile by means of the association link, but the user's image is still enclosed in the photo. Since innovative access control policies cannot be distorted, the user's image continues to be exposed to all authorized users and reporting to OSNs only allows us to either keep or remove the content. Such a binary decision from OSN managers is either too loose or too preventive, relying on the OSN's administration and requiring several people to report their request on the same content. Therefore, it is necessary to develop an effective and flexible access control mechanism for OSNs, accepting the special authorization requirements coming from multiple associated users for managing the shared data collaboratively.



(a) A disseminator shares other's profile (b) A user shares her/his relationships

Fig.1: Multiparty Access Control Pattern for Profile and Relationship Sharing

We instigate by examining how the lack of multiparty access control for data sharing in OSNs can weaken the protection of user data. Some distinctive data sharing prototypes with respect to multiparty approval in OSNs are also identified. Based on these distribution patterns, a multiparty access control (MPAC) model is put together to capture the core features of multiparty authorization requirements which have not been contained so far by existing access control systems and models for OSNs. Proposed model also contains a multiparty policy specification scheme. In the meantime, since conflicts are predictable in multiparty authorization enforcement, a voting mechanism is additional provided to deal with authorization and privacy conflicts in this model.

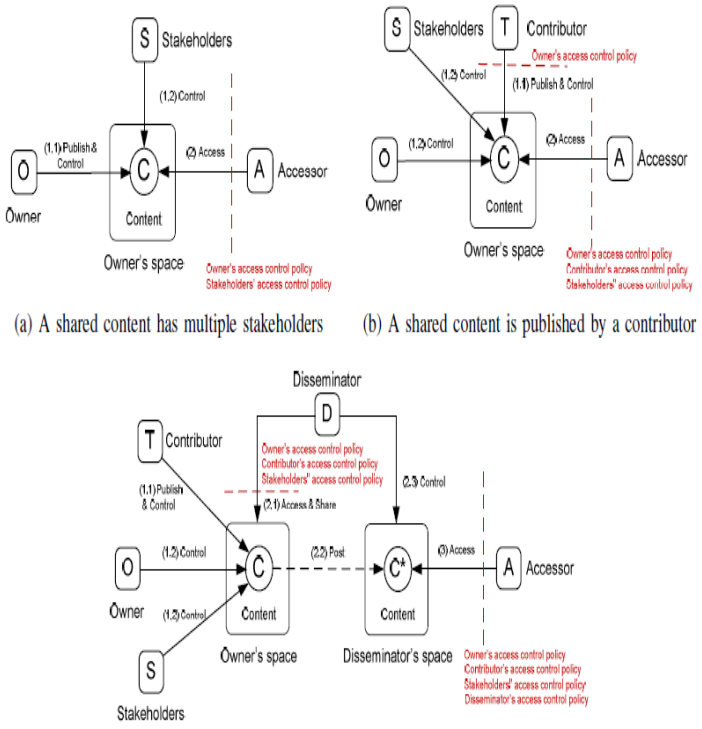
2. MULTIPARTY ACCESS CONTROL FOR OSNS: REQUIREMENTS AND PATTERNS

In this section we continue with an inclusive requirement analysis of multiparty access control in OSNs. We specifically analyze three scenarios profile sharing, content sharing and relationship sharing to understand the risks posted by the lack of collaborative control in OSNs.

***Profile sharing*:** An interesting 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. To provide significant and attractive services, these social applications munch through user profile attributes, such as name, birthday, activities, interests, and so on.

***Relationship sharing*:** Another characteristic of OSNs is that users can share their relationships with other members. Relations are essentially bidirectional and hold potentially perceptive information that associated users may not want to reveal. Most OSNs provide mechanisms that users can regulate the display of their friend lists.

***Content sharing*:** OSNs present built-in mechanisms enabling users to communicate and share contents with other members. OSN users can post statuses and notes, upload photos and tag others to their contents, videos in their own spaces and share the contents with their friends. On the other hand, users can also post contents in their friends' spaces. The shared contents may be connected with multiple users.



(a) A shared content has multiple stakeholders (b) A shared content is published by a contributor

(c) A disseminator shares other's content published by a contributor.

Fig. 2: Multiparty Access Control Pattern for Content Sharing.

3. MULTIPARTY ACCESS CONTROL MODEL FOR OSNS

3.1 MPAC Model

An Online Social Network can be represented by a connection network, a set of user groups and a group of user data. The relationship network of an Online Social Network is a directed labeled graph, where each node indicates a user and each edge indicates a relationship between two users. The label connected with each edge represents the type of the relationship. Edge path denotes that the preliminary node of an edge establishes the relationship and the terminal node of the edge accepts the relationship. The number and type of maintained relationships rely on the specific Online Social Networks and its purposes. Besides, Online Social Networks include an important feature that allows users to be organized in groups, where each group has a unique name. This feature allows users of an Online Social Network to easily find other users with whom they strength share precise interests, demographic groups, political orientation, and so on. Users can connect in groups without any approval from other group members. Furthermore, Online Social Networks provide each member a Web space where users can store up and manage their personal data as well as profile information, buddy list and content.

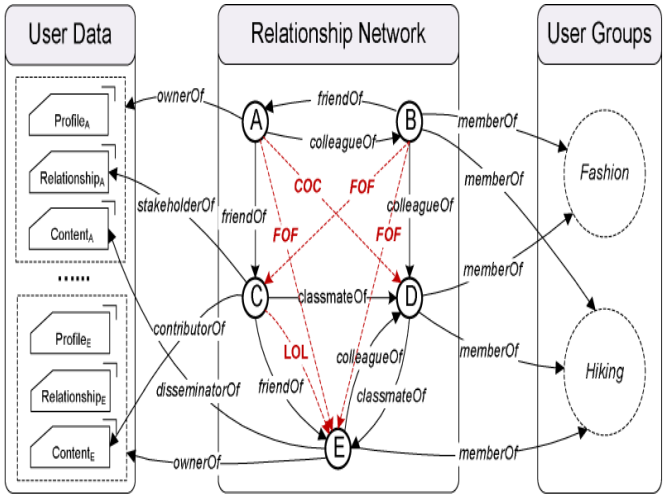


Fig. 3: An Example of Multiparty Social Network Representation.

3.2 MPAC Policy Specification

To make possible a collaborative authorization management of data sharing in OSNs, it is necessary for multiparty access control policies to be in place to control access over shared data, representing authorization necessities 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.

Access Control Policy: To summarize the above-mentioned policy elements, we introduce the meaning 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 Є U* is a user who can regulate the access of *data*;

• *ctype Є 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 Є{fpermit, deny}* is the authorization effect of the policy.

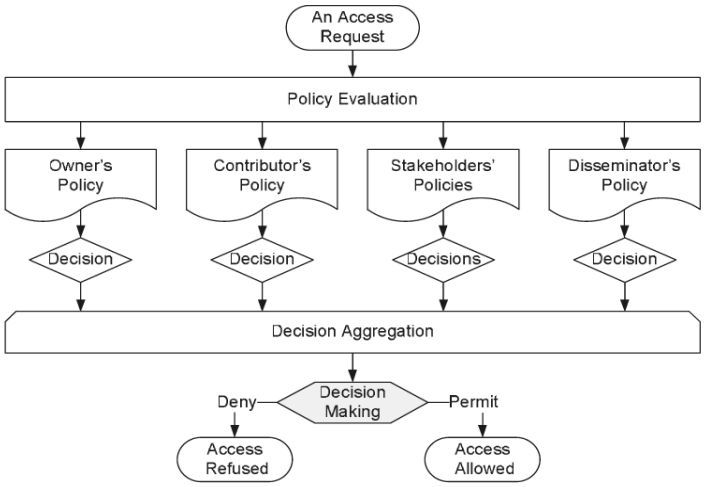


Fig.4: Multiparty Policy Evaluation Process

4. IMPLEMENTATION AND EVALUATION

4.1. Prototype Implementation

We implemented a proof-of-concept Facebook application for the two-way management of shared data, called MController . Our model application facilitates multiple associated users to identify their authorization policies and privacy preferences to co-control a collective data item. It is value noting that our current implementation was controlled to handle photo sharing in Online Social Networks. Our approach can be generalized to deal with other kinds of data sharing, such as videos and comments, in Online Social Networks as long as the stakeholder of shared data are identified with effective methods like tagging or searching

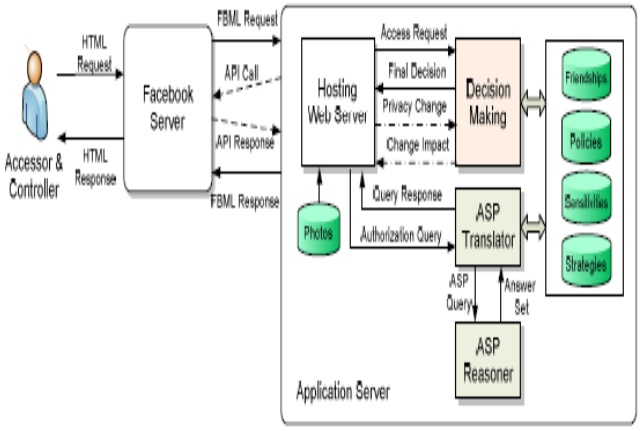


Fig.5: Architecture of MController Application.

The above figure shows the architecture of MController, which is separated into two main parts, application server and Facebook server. The Facebook server presents an entry point via the Facebook application page, and presents references to photos and feed data through API calls. Facebook server acknowledges inputs from users, and then forwards them to the application server. The application server is dependable for the input processing and mutual management of shared data. Information connected to user data such as user identifiers, user groups, friend lists, and user contents are stored in the application database. Users can admission the MController application all the way through Facebook, which provides the application in an iFrame. When access requirements are made to the decision making part in the application server, results are come back in the form of access to photos or proper information about access to photos. When privacy changes are made, the choice making segment returns change-impact information to the interface to alert the user. In addition, analysis services in MController application are grant by implementing an ASP translator, which converse with an ASP reasoner. Users can control the analysis services to perform complicated authorization queries.

A snapshot of main interface of *MController* is shown in below Fig 6 (a). All photos are loaded into a gallery style interface. To organize photo sharing, the user clicks the "Owned", "Contributed", "Tagged", or distributed" tabs, then chooses any photo to illustrate user privacy first choice by clicking the lock below the gallery. If the user is not the vendor of selected photo, user can only edit the privacy setting and sensitivity setting of the photo.3 Otherwise, as shown in Figure 6 (c), if the user is the owner of the photo, user has the option of clicking "Show Advanced Controls" to assign weight values to different types of controllers 4 and configure the conflict resolution mechanism for the shared photo. By evasion, the clash resolution is set to automatic. If the owner chooses to set a manual conflict resolution, user is informed of a sensitivity score of shared photo and receives a recommendation for choosing an appropriate conflict resolution strategy.

Fig.6: MController Interface.

5. CONCLUSION

The proposed technique is a novel solution for collaborative organization of shared data in Online Social Networks. A multiparty access control model was originated, along with a multiparty policy requirement scheme and corresponding policy assessment mechanism. In addition, we have initiated an approach for reasoning and representing about our future model. A proof-of-concept achievement of our solution called *MController* has been followed by the usability study and system assessment of our method. As part of future work, we are investigating more wide-ranging privacy conflict resolution approach and analysis services for collaborative management of shared data in Online Social Networks. Also, we would explore more criteria to evaluate the features of our proposed MPAC model. Users may be involved in the control of a larger number of shared photos and the configurations of the privacy preferences may become prolonged and dreary tasks. Therefore, we studied inference based techniques for automatically organize privacy preferences in MPAC.

6. REFERENCES

[1] Facebook Developers. http:// developers.facebook . com/.

[2] Facebook Privacy Policy. http:// www.facebook.com/policy.php/.

[3] Facebook Statistics. http://www. facebook.com/press/info.php? statistics.

[4]Google+PrivacyPolicy. http://www.google.com/intl/en/+/ policy/.

[5] The Google+ Project. https://plus.google.com.

[6] G. Ahn and H. Hu. Towards realizing a formal rbac model in real systems. In *Proceedings of the 12th ACM symposium on Access control models and technologies*, pages 215–224. ACM, 2007.

[7] G. Ahn, H. Hu, J. Lee, and Y. Meng. Representing and reasoning about web access control policies. In *Computer Software and Applications Conference (COMPSAC), 2010 IEEE 34th Annual*, pages 137–146. IEEE, 2010.

[8] J. Choi, W. De Neve, K. Plataniotis, and Y. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. *Multimedia, IEEE Transactions on*, 13(1):14–28, 2011.

[9] H. Hu, G.-J. Ahn, and J. Jorgensen. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proceedings of the 27th Annual Computer Security Applications Conference*, ACSAC '11, pages 103–112. ACM, 2011.

[10] H. Hu, G.-J. Ahn, and K. Kulkarni. Detecting and resolving firewall policy anomalies. *IEEE Transactions on Dependable and Secure Computing*, 9:318–331, 2012.

[11] L. Jin, H. Takabi, and J. Joshi. Towards active detection of identity clone attacks on online social networks. In *Proceedings of the first ACM conference on Data and application security and privacy*, pages 27–38. ACM, 2011.