ISSN: 2321-7782 (Online)

Volume 2, Issue 12, December 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Multiparty Authorization Architecture for Collabrative Data Sharing in OSNs

Mrunalini Pratap Shitole[1]
M.E (CSE)
Dr.D.Y.Patil School of Engg. & Technology,
Charholi (Bk), Lohgaon, Pune.
India

Madhuri Patil[2]
Prof.
Dr.D.Y.Patil School of Engineering & Technology
Affiliated to Savitribai Phule, Pune University, Pune
India

Abstract: Today all the peoples are using the online social network for the communication and creating profile information and many more purposes. In this paper I mainly concentrate on the security of all the information which is handling by online social network. All people knows, Online Social Network (OSNs) have experienced much more growth in the current year and having the separate portal for hundreds of millions of internet users. When we use the Online Social Network that provides the attractive means for interaction and the information sharing purpose but it will increase the number of security and privacy issues. Because of this issues Online Social Network allow user to restrict access to shared information. They do not provide any mechanism for same security and privacy issues with multiple users which is happened in the Online Social Network. So propose an approach to enable the security of shared information associated with multiple users in Online Social Network. For that purpose we formulate an access control model to capture intrinsic nature of multiparty authorization requirement along with the policy specification scheme and a policy enforcement mechanism. Here we present a logical representation of our access control model which performs many analysis tasks on our model. Here I also discuss the proof of concept prototype which is the part of an application in face book.

Keywords: Online Social Network, multiparty access control, security model, policy specification scheme and policy management, policy enforcement.

I. Introduction

Online social networks (OSNs) such as Face book, 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 Face book, 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 Face book allows tagged users to remove the tags linked to their profiles or report violations asking Face book 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.

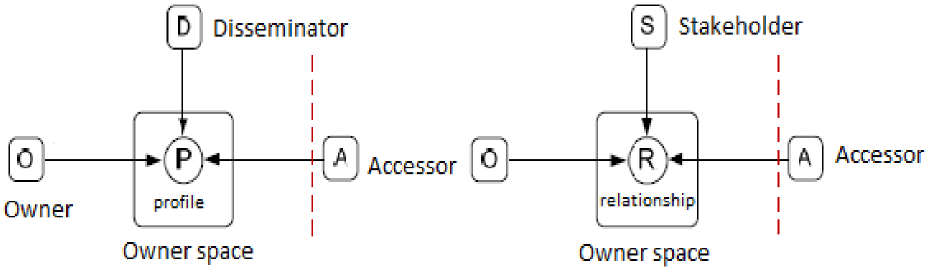

Fig.1 Multiparty Access Control Pattern for Profile and Relationship Sharing

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.

II. Related Work

The existing system of this paper shows the simple access control model. That model not recognized the trusted person and untrusted persons in OSNs. Also not given the more flexibility and privacy regarding the shared information. So here the MPAC model used. A Multiparty Access Control (MPAC) model is formulated to capture the essence of multiparty authorization requirements in OSNs. In particular, I show how Assurance Management Framework (AMF) can be applied to OSNs for identifying and resolving privacy conflicts, and representing and reasoning about MPAC model and policy. In this paper, MPAC model evaluation parts consist of MPAC policy specification, multiparty policy evaluation and MPAC model.

Multi user access control is introduced for secure network access, existing access control solutions for online social networks trust based access control inspired by the developments of trust and reputation in online social networks. The friend of friend ontology based distributed identity management system for online social network where relationships are associated with a trust level which indicates the level of friendship between the users participating in a given relationship. This model allows the specification access rules for online resource where authorized users are denoted in terms of the relationship type depth and trust level between users in online social networks. Semi-decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in online social network. Fong et al proposed an access control mechanism in

Face book admitting arbitrary policy vocabularies that are based on theoretical graph properties described relationship based access control as one of new security paradigms that addresses unique requirements of Web 2.0 then Fong (Ahn , 2010) (Ahn , 2007)recently formulated this paradigm called a relationship based access control model that bases authorization decisions on the relationship between the resource owner and the resource access or in an online. The data sharing specially photo sharing in online social network provided a solution for collective privacy management in online social networks. Their work considered access control policies of a content that is co-owned by multiple users in online social networks such that each co-owner may separately specify his or her own privacy preference for the shared content. Carminative et al. (Choitet al,2011)(Hutet al , 2011) recently introduced a new class of security policies, called collaborative security policies that basically enhance topology-based access control with respect to a set of collaborative users. In contrast, our work proposes a formal model to address the multiparty access control issue in OSNs, along with a general policy specification scheme and a simple but flexible conflict resolution mechanism for collaborative management of shared data in OSNs. In particular, our proposed solution can also conduct various analysis tasks on access control mechanisms used.

III. Problem Defination

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 (MPAC) for data sharing in OSNs can undermine the protection of user data. Some typical data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, an MPAC model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs. Proposed Multiuser Access Control Mechanism is shown in below figure:-

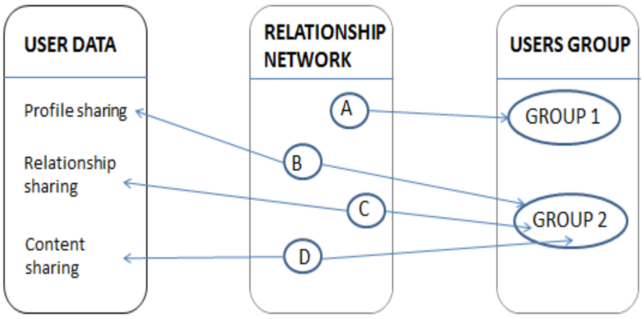

Fig. 2 Proposed multiuser access control mechanism

IV. Mcontroller

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.

OSN represented with directed labeled graph where each node represents user and edge denotes relationship between two users. The edge direction denotes the relationship from initial to terminal node. The profile space of the user managed himself with his privacy data and content. For that privacy data to maintain security several schemes are introduced. But no scheme gives totally security, mainly all those schemes have only one controller that is owner. By this single controller security and privacy issues may be raised on data which was personal to the owner.

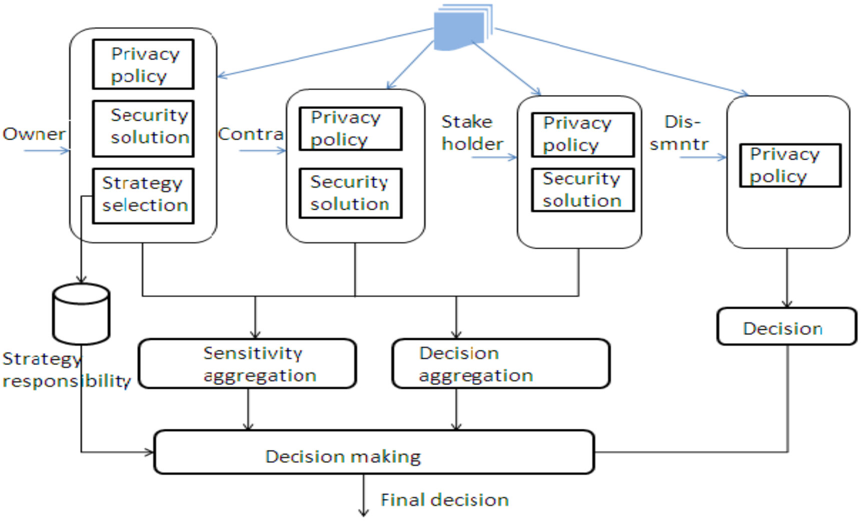

Fig. 3 System architecture of decision making in MController

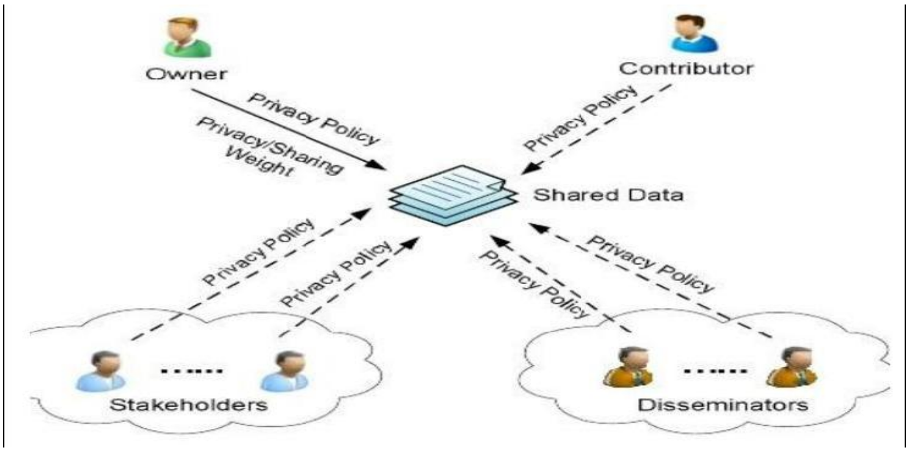

Fig.4 Mcontroller Architecture

So that rather than the owner controlling additional controllers are need for the flexible privacy mechanisms in OSN. The additional controllers are contributor, stakeholder and disseminator which provide their own privacy policies on shared data by giving the permission either permit or deny to unauthorized user on shared data. Figure 3 illustrates different controllers providing their privacy policies on shared data. We define multi controllers as follows:

» Owner (O): In the social network the user u is called the owner of the data item d, if d presents in the space m of user u. The user u is also called as contributor of d, when that user share data item d. The owner share data in three types, they are profile sharing, content sharing and relationship sharing. It enables the owner to discover potential malicious activities in collaborative control.

» Contributor (C): In the social network the user u is called the contributor of the data item d, if d published by user u in someone else’s space. The contributor tags 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.

» Stakeholder (S): In the social network the user u is called a stakeholder of the data item d, if user u is tagged user T for d. A shared content has multiple stakeholders.

» Disseminator (D): In the social network, let d be a data item shared by a user u from someone else’s space to his/her space. The user u is called a disseminator of d. the real content sharing starts with the owner, then disseminator views the content and shares with others. This disseminated content may be re-disseminated again and again by others.

»

V. Multiparty Access Control Model

a) MPAC Specification

It is very essential for MPAC policies to regulate access and representing authorization requirements from multiple associated users to enable a collaborative authorization management of data sharing in OSNs.

» **Accessor Specification:** Accessor is the set of users who granted to access the shared data. Accessor can be represented with a set of user names, relationship names and group names in OSNs. The accessor specification is defined as a set, accessors = {a1, a2. . . , an}, where each element is a tuple < ac,at >. where ac ∈ U ∪ RT ∪ G be a user u ∈ U, a relationship type rt ∈ RT, or a group g ∈ G. at ∈ {UN,RN,GN} be the type of the accessor specification, where UN,RN,GN represents user name, relationship name, and group name.

» **Data Specification:** The data specification represented in three ways; profile, relationship and content sharing. For effective privacy the different controllers provide sensitivity levels on data. Let dt ∈ D be a data item, sl be a sensitivity level (range 0.00 to 1.00) for data item dt. The data specification is defined as a tuple < dt, sl >.

b) MPAC Policy

To summarize the above-mentioned specification elements, we introduce the definition of a Multiparty access control policy as follows:

The multi party access control policy is a 5 - tuple P = < controller, Ctype, accessor, data, effect > where Controller is a user who can regulate the access of data.

» Ctype is the type of the controller.

» Accessor is the set of users who granted to access the shared data.

» Data is represents a data specification.

» Effect ∈ {permit, deny} is the authorization effect of the policy. Suppose a controller can leverage five sensitivity levels: 0.00 (none), 0.25 (low), 0.50 (medium), 0.75 (high), and 1.00 (highest) for the shared data.

c) MPAC Evaluation

Multi party access control is evaluated in two steps. In step-1, the individual decision are collected from different controllers, and in step-2, individual decision are aggregated and makes final decision for the access request. Figure 5 illustrates that how MPAC evaluated in step by step. Initially an access request goes to under policy evaluation, which is done under four controllers. The four controllers provide their own privacy policies in the form of decision either permit or deny in step-1 process. After giving decisions by individual controllers, they are aggregated and make final decision by using decision voting schemes in step-2 process. The final decision making decides whether the access request is allowed or refused.

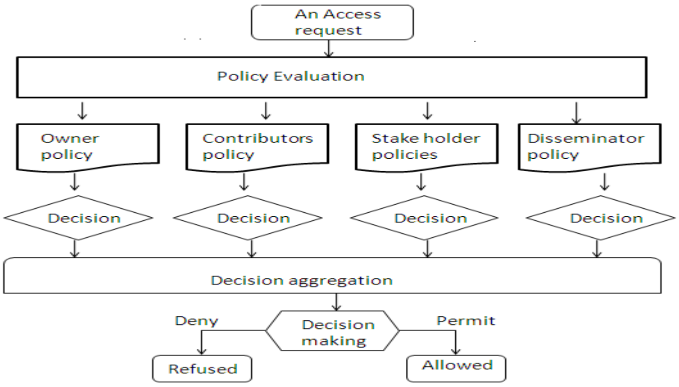

Fig. 5 Multiparty policy evaluation process

From the process of evaluation in MPAC policies, the controllers give different decision for an access resolute the conflicts for taking an unambiguous decision for each access request. For the better privacy, a strong resolution for conflict may need. So it is better to consider tradeoff between privacy and utility in resolution of conflict. For this conflict issue, we introduce decision voting schemes resolving the MPAC conflicts which is simple and flexible.

VI. Conclusion

The proposed a novel solution for collaborative management of shared data in OSNs. An MPAC 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. In our multiparty access control system for model and mechanism, a group of users could collude with one another so as to manipulate the final access control decision. An attack scenarios, anywhere 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; and (3) all controllers of the photo are honest to specify their privacy preferences.

Acknowledgement

It gives me a great pleasure and immense satisfaction to present this special topic seminar report on Multiparty Access Control for Online Social Networks : Model and Mechanisms, The success of this seminar has throughout depended upon an exact blend of hard work and unending co-operation and guidance, extended to me.

References

1. J.Choi, W. De Neve, K. Plataniotis, and Y. Ro, Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared onOnline Social Networks, IEEE Trans. Multimedia, vol. 13, no. 1, pp. 14-28, Feb.2011.
2. H. Hu, G.-J. Ahn, and J. Jorgensen, Enabling Collaborative Data Sharing in Google+., Technical Report ASU-SCIDSE-12-1, http:// sefcom.asu.edu/mpac, Apr. 2012.
3. B. Carminati and E. Ferrari, Collaborative Access Control in On- Line Social Networks, Proc. Seventh Intl Conf. Collaborative Computing: Networking, Applications and Worksharing (Collaborate- Com), pp. 231-240, 2011.
4. H. Hu, G.-J. Ahn, and K. Kulkarni, Detecting and Resolving Firewall Policy Anomalies, IEEE Trans. Dependable and Secure Computing, vol. 9, no. 3,pp. 318-331, May 2012.
5. N. Li, Q. Wang, W. Qardaji, E. Bertino, P. Rao, J. Lobo, and D. Lin, Access Control Policy Combining: Theory Meets Practice, Proc. 14th ACM Symp. Access Control Models and Technologies, pp. 135- 144, 2009.
6. N. Li, Q. Wang, W. Qardaji, E. Bertino, P. Rao, J. Lobo, and D. Lin, Access Control Policy Combining: Theory Meets Practice, Proc. 14th ACM Symp.Access Control Models and Technologies, pp. 135- 144, 2009.
7. H. Hu and G. Ahn, Multiparty Authorization Framework for Data Sharing in Online Social Networks, Proc. 25th Ann. IFIP WG 11.3 Conf. Data and Applications Security and Privacy, pp. 29-43, 2011.
8. H. Hu, G. Ahn, and K. Kulkarni, Anomaly Discovery and Resolution in Web Access Control Policies, Proc. 16th ACM Symp. Access Control Models and Technologies, pp. 165-174, 2011.
9. H. Hu, G.-J. Ahn, and J. Jorgensen, Enabling Collaborative Data Sharing in Google+., Technical Report ASU-SCIDSE-12-1, http:// sefcom.asu.edu/mpac, Apr. 2012.
10. 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 Conf., pp. 103-112, 2011
11. H. Hu, G.-J. Ahn, and K. Kulkarni, Detecting and Resolving Firewall Policy Anomalies, IEEE Trans. Dependable and Secure Computing, vol. 9, no. 3,pp. 318-331, May 2012.

AUTHOR(S) PROFILE

Mrunalini Shitole, pursuing the M.E degree in Computer Science from Dr.D.Y.Patil School of Engg. & Technology, Charholi (Bk), Lohgaon, Pune in 2013-2015.

Mrs. Madhuri Patil, I am Assistant Professor of Department of Computer Engineering in Dr. D. Y. Patil School of Engineering & Technology at Dr. D. Y. Patil Knowledge City, Charholi (Bk.), Via. Lohgaon, Pune - 412105, Maharashtra, India