IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Secure Data Access and Empowerment of Life in Online Social Networks Using MPAC Mechanisms

Mrs. Vijayachithra[1], Mr.P.Balamurugan[2]

[1]PG Scholar, Computer Science and Engineering Department, DR. Pauls Engineering College, Villupuram, Tamil Nadu-605 109

[2]Assistant Professor, Computer Science and Engineering Department, DR. Pauls Engineering College, Villupuram, Tamil Nadu-605 109

Abstract

Theft of personal privacy is sometimes loss of life .The Online Social Network currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. To this end, it proposes an approach to enable the protection of shared data associated with multiple users in OSNs. In this project, we need to analyze and implement Multi Party Access Control Mechanism by which the Users are allowed to share data based on the following Criteria with the relationships between the Users: 1. Data Sensitivity, 2.Decision Mechanisms, 3. Threshold Mechanisms. Also we implement to share the data based on the Majority Permit mechanism.

Index Terms *–online social networks (OSNs), multiparty access control, security model, policy specification and management, web security, collaborative control.*

1. INTRODUCTION

Theft of personal privacy is sometimes loss of life. In Online social networks (OSNs) such as Facebook, Twitter, and Google+ are inherently designed to enable people to share personal and public information and make social connections with coworkers, family, friends, colleagues, and even with strangers. In Facebook users can allow groups, friends, and friends of friends or public to right to use their data, depending on their personal authorization and privacy requirements. Although online social networks presently provide simple access control mechanisms [1] [2] allowing users to govern access to information contained in their own spaces, [3] users, unfortunately, have no power over data residing outside their spaces. Such as, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. The Internet itself, content can easily be disclosed to a wider audience than the user intended. This thesis aims to provide (MPAC) and insight into privacy issues and needs faced by users of OSNs and their origins. The insights gained help plot a course for future work. . 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 (e.g., [4], [5], [6], [7], and [8]). Since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model. The correctness of implementation of an access control model is based on the premise that the access control model is valid. Moreover, while the use of an MPAC mechanism can greatly enhance the flexibility for regulating data sharing in OSNs.

2. EXISTING SYSTEM

The Online Social Networks offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. They currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces.

Limitations on Existing System

1. Every user in the group can access the shared content.
2. Not give any mechanism to enforce privacy concerns over data associated with multiple users.
3. If a user posts a comment in a friend's space, he/she cannot specify which users can view the comment.
4. While a user uploads a photo and tags friends who appear in the photograph, the tagged friends cannot restrict who can see this photograph.

3. PROPOSED SYSTEMS

To overcome this drawback we are implementing a Multi Party Access Control Mechanism by which the user can restrict the data shared with their friends and other. If a user posts a comment in a friend's space, he/she can specify which users can view the comment. For this purpose, Multi Party Access Control Mechanism, the content will be shared based on the following techniques.

1. Decision Based Voting in which based on the Users decision the data will be shared and accessed.
2. Data Sensitivity: Based on the sensitivities, the data will be shared with the users.
3. Threshold Based Conflict Resolution in which based on the threshold values, the data will be shared between the Users.
4. Strategy Based Conflict Resolution in which the data is shared between the Users based on the strategies.

3.1 MPAC Model

An OSN can be represented by a relationship network, a set of user groups, and a collection of user data. The relationship network of an OSN 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 indicates the type of the relationship. The number and type of supported relationships rely on the specific OSNs and its purposes. Besides, OSNs include an important feature that allows users to be organized in groups (or called circles in Google+ [5]), where each group has a unique name. This feature enables users of an OSN to easily find other users with whom they might share specific interests (e.g., same hobbies), demographic groups (e.g., studying at the same schools), political orientation, and so on. Users can join in groups without any approval from other group members.

Furthermore, OSNs provide each member a web space where users can store and manage their personal data including profile information, friend list and content. Recently, several access control schemes (e.g., [4], [5], [6], and [7]) have been proposed to support fine-grained authorization specifications for OSNs. Unfortunately, these schemes can only allow a single controller, the resource owner, to specify access control policies. Indeed, a flexible access control mechanism in a multiuser 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, needs to regulate the access of the shared data as well.

We define these controllers as follows:

(**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.

(**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.

(**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 $u \in T$.

(**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.

3.2 MPAC Policy Specification

To enable a collaborative authorization management of data sharing in OSNs, it is essential for MPAC 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. Accessor can be represented with a set of user names, a set of

relationship names (RNs) or a set of group names (GNs) in OSNs.

We formally define the Data specification as follows:

Data specification: In OSNs, user data are composed of three types of information: user profile, user relationship, and user content. To facilitate effective privacy conflict resolution for MPAC, we introduce sensitivity levels (SL) for data specification, which are assigned by the controllers to the shared data items. A user's judgment of the SL of the data is not binary (private/public), but multidimensional with varying degrees of sensitivity. Formally, the data specification is defined as follows:

(Data Specification): Let dt ∈ D be a data item.Let sl be an SL, which is a rational number in the range [0, 1], assigned to dt. The data specification is defined as a tuple <dt; sl>.

4. MULTIPARTY POLICY EVALUATION

Two steps are performed to evaluate an access request over MPAC policies. The first checks the access request against the policy specified by each controller and yields a decision for the controller.

MPAC evaluation process is have five steps to implement our proposed schemes

4.1 Voting Scheme for Decision Making

We are implementing the Decision Voting and Sensitivity Voting Scheme. In the decision based voting scheme, we are getting the decision from the user's of the network and based on the average value the data will be shared among the Users. In the Sensitivity based voting we are calculating the sensitivity value of the data, so that based on the sensitivity the data will be shared.

4.2 Thresholds Based Conflict Resolution

In this mechanism, we are setting a threshold value. Based on the threshold value the data will be shared among the users. If the Decision voting value is high then that sensitivity value, then the data will be shared among the Users. If the Sensitivity value is greater than the Decision Value, then the data will not be shared among the Users.

4.3 Strategy Based Conflict Resolution

In this resolution technique we are implementing two mechanisms, namely, Owner Overrides and User Overrides. In the Owner Overrides mechanism, the Owner's decision is finalized to share the data. If the Owner not allows the data to be shared, then the data will not be shared. User Overrides, in this process if one the user is not allowed to access the data, then the data will not be shared among their networks.

4.4 Conflict Resolution Based On The Dissemination Control

In this resolution scheme, best on the Data Owner's sensitivity level, the data will be shared among the User rather than User's Sensitivity level. For an example if 'A' be the data owner and shared the data to B with high sensitivity. If 'B' wants to share the data to 'C' with low sensitivity, then 'B' is not allowed to share the data among the other Users.

5. SYSTEM MODEL

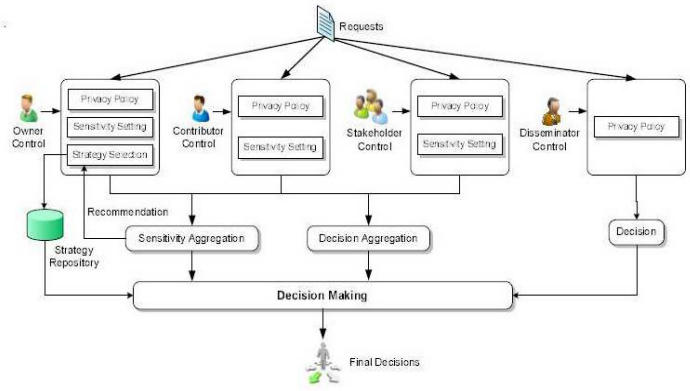

Fig.1: System architecture for Multiparty Access Control for OSN (MController)

6. MPAC TECHNIQUE PROPOSED MECHANISMS

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. Assessors Specification: Assessors are a set of users who are granted to access the shared data.

7. RELATED WORK

Access control for OSNs is still a relatively new research area. Several access control models for OSNs have been introduced (e.g., [9] [4], [5], [6], [7], [8]). Early access developments of trust and reputation computation in OSNs. The D-FOAF system [8] is primarily a friend of a friend ontology-based distributed identity management system for OSNs, where relationships are associated with a trust level, which indicates the level of friendship between the users participating in a given relationship. Carminati et al. [4] introduced a conceptually similar but more comprehensive trust-based access control model. This model allows the specification of access rules for online resources, where authorized users are denoted in terms of the relationship type, depth, and trust level between users in OSNs. The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. Compared to a few existing approaches to formalizing XACML policies [7]. This formal representation is more straightforward and can cover more XACML features. Furthermore, translating XACML to ASP allows us to leverage off-the-shelf ASP solvers for a variety of analysis services such as policy verification, comparison and querying.

MITM attack makes the users difficult to understand that whether they are connected to original secured connection or not. Fong et al. [7] proposed an access control model that formalizes and generalizes the Access control mechanism implemented in Facebook. Gates [11] described relationship-based access control (ReBAC) as one of new security paradigms that addresses unique requirements of Web 2.0. The increased social networking capabilities provided by Web 2.0 technologies requires a examination of what consider "private" and what consider "personal" information. Then, Fong [6] recently formulated this paradigm called a ReBAC [4] model that bases authorization decisions on the relationships between the resource owner and the resource accessor in an OSN. However, none of these existing works 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 MAF and , in OSNs has been recognized by the recent work [9], [10], [11] and Squicciarini et al. [12] 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, Our work proposes a formal model to address the MPAC 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.

8. CONCLUSION

In this paper, it has 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. A proof-of-concept implementation of our solution called MController 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 privacy content (information's) are honest to specify their privacy preferences.

In the proposed goal of this Project is, User can post any data and can specify it is Sensitive, Then the data sharing to a Particular Category. If unshared Person wants to see the Unshared Data then him / she has to get Permission from the Data Owner, then only the Data is shared.

REFERENCES

[1] Facebook Privacy Policy, http://www.facebook.com / policy.php/, 2013.
[2] Google+ Privacy Policy, http://http://www.google.com/intl/en/+/policy/, 2013.
[3] G. Ahn and H. Hu, "Towards Realizing a Formal RBAC Model in Real Systems," Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 215-224, 2007.
[4] G. Ahn, H. Hu, J. Lee, and Y. Meng, "Representing and Reasoning about Web Access Control Policies," Proc. IEEE 34th Ann. Computer Software and Applications Conf. OMPSAC), pp. 137-146, 2010. [1] Facebook Developers, http://developers.facebook.com/, 2013.
[5] B. Carminati, E. Ferrari, and A. Perego, "Rule-Based Access Control for Social Networks," Proc. Int'l Conf. On the Move to Meaningful Internet Systems, pp. 1734-1744, 2006.
[6] B. Carminati, E. Ferrari, and A. Perego, "Enforcing Access Control in Web-Based Social Networks," ACM

Trans. Information and System Security, vol. 13, no. 1, pp. 1-38, 2009.

[7] P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 191-202, 2011.

[8] P. Fong, M. Anwar, and Z. Zhao, "A Privacy Preservation Model for Facebook-Style Social [Network Systems," Proc. 14th European Conf. Research in Computer Security, pp. 303-320, 009

[9] S. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H. Choi, "D-FOAF: Distributed Identity Management with Access Rights Delegation," Proc. Asian Semantic Web Conf. (ASWC), pp. 140-154,

[10] G. Ahn, H. Hu, J. Lee, and Y. Meng, "Representing and Reasoning about Web Access Control Policies," Proc. IEEE 34th Ann. Computer Software and Applications Conf. (COMPSAC), pp. 137-146, 2010.

[11] Hu .H and. Ahn .G.Multiparty authorization framework for data sharing in online social networks, in Proceedings of the 25th annual IFIP WG 11.3 conference on Data and applications security and privacy, Springer-Verlag , 2011.

[12] Pushpendra Kumar, Pateriya, Srijith Kumar.S. Analysis on Man in the Middle Attack on SSL, International Journal of Computer Applications (0975 – 8887) Volume 45– No.23, May 2012.

[13] A. Squicciarini, M. Shehab, and F. Paci, "Collective Privacy Management in Social Networks," Proc. 18th Int'l Conf. World Wide Web, pp. 521-530, 2009.