International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)

International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Mechanisms of Multiparty Access Control in Online Social Network

Suvitha.D

Department of CSE, Sree Sastha Institute of Engineering and Technology, Chennai, India

suvitha19@gmail.com

***Abstract*-In this paper, Online Social Networks offers attractive interactions and information sharing, and also will raise a number of security and privacy issues. Online social networks will allow users to restrict access to shared data, and currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. Users can upload the content not only into their own or others' spaces but also tag other users who appear in the content. For the protection of user data, an approach has been proposed to enable the protection of shared data associated with multiple users in Online Social Networks. An access control model will capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. A logical representation of access control model which allows us to leverage the features of existing logic solvers to perform various analysis tasks on this model. A proof-of-concept prototype has also been implemented as part of an application in Facebook and provide usability study and system evaluation of this project.**

***Index Terms*- Social network, multiparty access control, security model, policy specification and management.**

I. INTRODUCTION

The main stay of this paper tells about Online Social Networks (OSNs) such as Facebook, Google, and Twitter are used for communicating with the people to share their personal and public information and make social connections with friends, co-workers, colleagues, family, and even with strangers. For secure purpose, simple access control mechanisms allowing users to govern access information contained in their own spaces. 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.

OSNs often use user relationship and group membership to distinguish between trusted and un-trusted users through multiparty policy specification scheme and a policy enforcement mechanism to implement user's personal authorization and privacy requirements.

For instance, if a user posts a comment in a friend's space, user cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the

photo, the tagged friends cannot restrict who can see this photo , even though the tagged friends may have different privacy concerns about the photo. To overcome this, preliminary protection mechanisms have been used by existing OSNs. For example, Facebook allows tagged users to remove the tags linked to their profiles or by asking Facebook managers to remove the contents that they do not want to share with the public.

However, these simple protection mechanisms suffer from several limitations. By removing a tag from a photo can only prevent other members from seeing a user's profile by means of the association link, but the user's image is still contained in the photo. But original access control policies cannot be changed, the user's image continues to be revealed to all authorized users. On the other hand, reporting to OSNs only allows us to either keep or delete the content. According to this example, decision from OSN managers is either too loose or too restrictive, relying on the OSN's administration and requiring several people to report their request on the same content.

Hence, it is essential to develop an effective and flexible access control mechanism for OSNs, and also authorization requirements and privacy conflicts can be resolved elegantly which comes from multiple associated users for managing the shared data collaboratively.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

II. Overview

Online social networks offers attractive 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 privacy concerns over data associated with multiple users. Users can upload a content not only into their own or others' spaces but also tag other users who appear in the content. For the protection of user data, users propose an approach to enable the protection of shared data associated with multiple users in OSNs. An access control model will capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism.

OSNs currently provide simple access control mechanisms allowing users to govern access the information contained in their own spaces, users unfortunately have no control over data residing outside their spaces. For instance, if a user posts a comment in a friend's space, she/he cannot specify which users can view the comment.

Report violations asking Facebook managers to remove the contents that the user do not want to share with the public, it will only allow us to either keep or delete the content.

III. Related Work

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. In this model multiparty policy specification scheme is used.

If a set of malicious users shares the photo which is available to a wider audience, they can access the photo, and then they tag themselves or making fake identities to the photo. So that they can assign a very low sensitivity level for the photo and also specify policies from users to access the photo. To prevent such an attack, three conditions should be satisfied: 1) There should not be any fake identity in OSNs; 2) Real user should be appeared in the photo when tagging is performed; and 3) all controllers of the photo should be honest by specifying their privacy preferences. For the first condition, Sybil attacks [10] and Identity Clone attacks [4], have been introduced to OSNs.

Regarding the second condition, an effective tag validation mechanism is used for verifying the tagged user against the photo. In this paper it tells that, if any users tag themselves or others in a photo then the photo owner will receive a tag notification. In such cases owner will come to know about the correctness of the tagged users. Facial recognition [9] is used to recognize people accurately in contents such as photos, automatic tag validation is feasible. Regarding the third condition, it tells about the potential authorization impact with respect to a controller's privacy preference. By using this function, the photo owner will examine the users who are granted to access the photo by the collaborative authorization which is not explicitly granted by the owner. Finally the owner can discover malicious activities in collaborative control.

Collusion detection in collaborative systems has been addressed by the recent work [22], [23]. Several access control models for OSNs have been introduced. Early access control solutions for OSNs introduced trust-based access control policy which is inspired by the development of trust and reputation computation in OSNs. Rule-based access control model [6] for web based social networks allows the specification of access rules for online resources where authorized subjects are denoted in terms of the relationship type, depth, and trust level existing between users in the network. This is the first proposal of an access control model for social networks. The different tasks to be carried out to enforce access control are shared among three distinguished actors namely, the owner of the requested resource, the subject which requested it, and the SNMS. This paper allows us to associate with a relationship the users participating in it, its type, depth, and trust level.

Fong [13] described a privacy preservation model for facebook-style social network systems proposed access control model that generalizes the access control mechanism implemented in Facebook, where arbitrary policy vocabularies are based on theoretical graph properties. Fong [12] recently formulated this paradigm called a Relationship-based access control model that is based on authorization decisions on the relationship between the resource owner and the resource accessor in an OSN. However, none of these existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

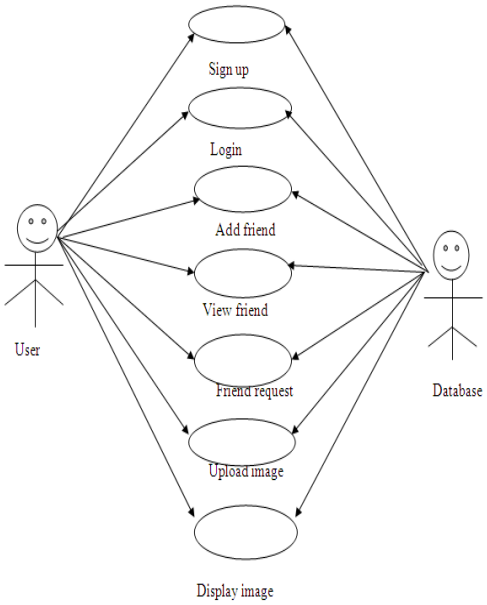
Carminati[5] introduced security policy for collaborative access control in online social networks that basically enhance topology-based access control with respect to a set of collaborative users.

In this paper, a formal model is used for addressing the multiparty access control issue in OSNs, along with policy specification scheme and flexible conflict resolution mechanism for collaborative management of shared data in OSNs. Proposed work can also conduct various analysis tasks on access control mechanisms used in OSNs, which is not addressed by prior work.

A. Processing of social networks

Users upload the photo in their own space and tags to their friends, and the owner of the photo will be the uploaded person, and stakeholders of the photo will be the tagged members. All users can specify access control policies to control over the photo and can see the photo. OSNs also enable users to share others' contents. To view a photo in friend's space and decide to share that photo with our friends, the photo will be in turn posted in their space and can specify access control policy to authorized friends to see that photo. In such cases, the person is a disseminator who shared their friend's photo.

Usecase Diagram



A use case diagram is a graph of actors, a set of use cases enclosed by a system boundary, communication (participation) association between the actors and the use cases, and generalization among the use cases. A use case diagram is a type of behavioral diagram created from a Use-case analysis. The purpose of use case is to present overview of the functionality provided by the system in terms of actors, their goals and any dependencies between those use cases.

User has to sign up his account, if he has no account before. After signing up user can login to the account. A separate profile will be displayed for him. User can add friends.

User can search friends after that he can add friends into his account. User can view friends profile and user can send friend request to his friend. In case if user wants to upload his image on his wall, he can upload the image by browsing it and he can upload the image. After uploading it, the image will be displayed on the wall.

B. Features of Online Social Network's

When user uses the social applications, they want to control what information about their friends is available in the applications. It is also possible for the social applications to infer their private profile attributes through their friends' profile attributes. When social application accesses the profile attributes of a user's friend, and also both the user and her friend want to gain control over the profile attributes. 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, a profile sharing pattern where a disseminator can share others' profile attributes to an accessor. Here the owner as well as the disseminator can specify access control policies by restricting the sharing of profile attributes.

Relationship can also be shared. Relationships are bidirectional and they carry sensitive information in OSNs which provides users to regulate the display of their friend lists. User is able to control one direction of a relationship. In relationship sharing pattern, a user is said to be owner, who has a relationship with another user called stakeholder, and shares the relationship with an accessor. In this concept, authorization requirements from both the owner and the stakeholder should be considered. Or else the stakeholder's privacy concern may be violated.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

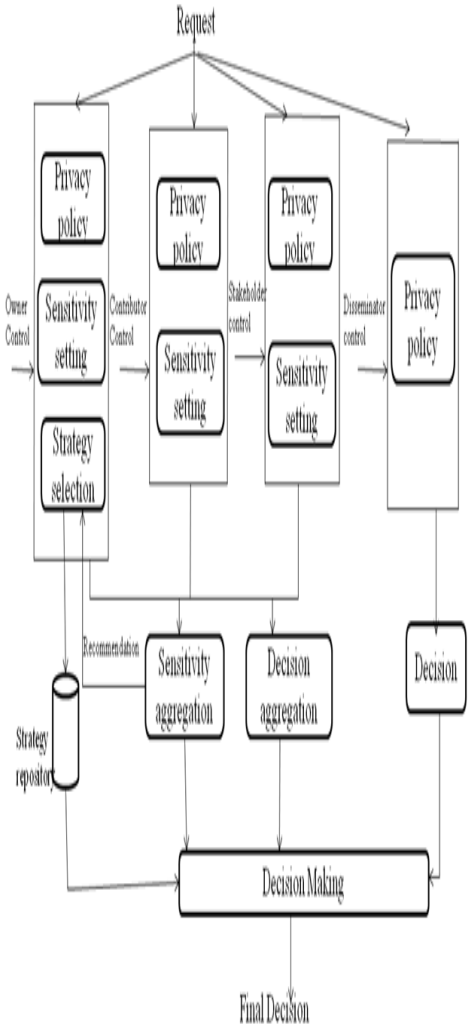
In content sharing the OSN users can post comments and statuses, and also they can upload the photos and videos in their own spaces. They tag others to their contents, and can share their contents with their friends. Users can also post contents in their friends' spaces. The shared contents can be connected with multiple users. This pattern tells about the contributor publishes content to other's space and the content can also have multiple stakeholders that is tagged users. All users who are associated should define access control policies for the shared content.

Multiparty access control 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. In this model multiparty policy specification scheme is used. Since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model. Another compelling feature of our solution is the support of analysis on the MPAC model and systems.

C. Objective

The main objective of this paper tells about Multiparty Access Control mechanisms greatly enhance the flexibility for data sharing in OSNs. It may potentially reduce the certainty of system authorization consequences so that authorization and privacy conflicts can be resolved elegantly.

Architecture Diagram



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

D. Multiparty access control model

Additionally introduce a method to represent and reason about our model in a logic program. In addition, a prototype implementation of our authorization mechanism in the context of Facebook has been introduced. Experimental results demonstrate the feasibility and usability of our approach. Multiparty authorization requirements and access control patterns for OSNs are used.

Policies

Sensitivity levels (SL) for data specification, which are assigned by the controllers to the shared data items. A user's judgement of the SL of the data is not binary (private/public), but multidimensional with varying degrees of sensitivity. Suppose a controller can leverage five SLs: 0.00 (none), 0.25 (low), 0.50 (medium), 0.75 (high), and 1.00 (highest) for the shared data.

Voting Concept

Voting is a popular mechanism for decision making. 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

- *Voting by decision*

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

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

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:

$$(DV_{ag}) = \left(DVow + DVcb + \sum_{i \in SS} DV_{st}^{i}\right) \times \frac{1}{m}$$

Where SS is the stakeholder set of the shared data item, and m is the number of controllers of the shared data item. Each controller of the shared data item may have 1) a different trust level over the data owner and 2) a different reputation value in terms of collaborative control.

Thus, a generalized decision voting scheme needs to introduce weights, which can be calculated by aggregating trust levels and reputation values, on different controllers.

Different weights of controllers are essentially represented by different importance degrees on the aggregated decision. In general, the importance degree of controller x is "weight x=sum of weights." Suppose ω_{ow},ω_{cb}, and ω_{st} are weight values for owner, contributor, and stakeholders, respectively, and n is the number of stakeholders of the shared data item. A weighted decision voting scheme is as follows:

$$DV_{ag} = \left(\omega_{ow} \times DV_{ow} + \omega_{cb} DV_{cb} + \sum_{i=1}^{n} \left(\omega_{st}^{i} \times DV_{st}^{i}\right)\right) \times \frac{1}{\omega_{ow} + \omega_{cb} + \sum_{i=1}^{n} \omega_{st}^{i}}$$

- *Voting using sensitivity level*

Each controller assigns an SL to the shared data item to reflect her/his privacy concern. A sensitivity score (Sc) (in the range from 0.00 to 1.00) for the data item can be calculated based on following equation:

$$S_c = \left(SL_{ow} + SL_{cb} + \sum_{i \in SS} SL_{st}^{i}\right) \times \frac{1}{m}$$

Threshold-based concept

A basic idea of our approach for threshold-based conflict resolution is that the Sc can be utilized as a threshold for decision making. Intuitively, if the Sc is higher, the final decision has a high chance to deny access, taking into account the privacy protection of high sensitive data.

$$Decision = \begin{cases} Permit if DV_{ag} > S_{c,} \\ Deny if DV_{ag} \leq S_c \end{cases}$$

Strategy-based concept

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, we set $\omega_{ow} = 1$,ω_{cb}=0and ω_{st}=0^1 and the final decision can be made as follows:

$$Decision = \begin{cases} Permit if DV_{ag} = 1 \\ Deny if DV_{ag} = 0 \end{cases}$$

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)

International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

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:

$$Decision = \begin{Bmatrix} Permit if\, DV_{ag} = 1 \\ Deny otherwise \end{Bmatrix}$$

Majority permit: This strategy permits (deny, 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

$$Decision = \begin{Bmatrix} Permit if\, DV_{ag} \geq {}^{1}/_{2} \\ Deny if\, DV_{ag} < {}^{1}/_{2} \end{Bmatrix}$$

IV. CONCLUSION

Multiparty Access Control Model has been formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism to provide a novel solution for collaborative management of shared data in OSNs.

REFERENCES

[1] 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.

[2] 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.

[3] A. Besmer and H.R. Lipford, "Moving beyond Untagging: Photo Privacy in a Tagged World," Proc. 28th Int'l Conf. Human Factors in Computing Systems, pp. 1563-1572, 2010.

[4] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All Your Contacts Are Belong to Us: Automated Identity theft Attacks on Social Networks," Proc. 18th Int'l Conf.World Wide Web, pp. 551-560, 2009.

[5] B. Carminati and E. Ferrari, "Collaborative Access Control in Online Social Networks," Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Worksharing (Collaborate-Com), pp. 231-240, 2011.

[6] 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, 2006.1626 IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 7, JULY 2013.

[7] 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.

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

[9] 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," IEEE Trans. Multimedia, vol. 13, no. 1, pp. 14-28, Feb. 2011.

[10] J. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, pp. 251-260, 2002.

[11] P. Fong, "Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems," Proc. IEEE Symp. Security and Privacy (SP), pp. 263-278, 2011.

[12] 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.

[13] 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, 2009.

[14] J. Golbeck, "Computing and Applying Trust in Web-Based Social Networks," PhD thesis, Univ. of Maryland at College Park, College Park, MD, USA, 2005.

[15] M. Harrison, W. Ruzzo, and J. Ullman, "Protection in Operating Systems," Comm. ACM, vol. 19, no. 8, pp. 461-471, 1976.

[16] H. Hu and G. Ahn, "Enabling Verification and Conformance Testing for Access Control Model," Proc. 13th ACM Symp.Access Control Models and Technologies, pp. 195-204, 2008.

[17] 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.

[18] 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.

[19] 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/mpac+.pdf, Apr. 2012.

[20] 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.

[21] 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.

[22] B. Qureshi, G. Min, and D. Kouvatsos, "Collusion Detection and Prevention with Fire+ Trust and Reputation Model," Proc. IEEE 10th Int'l Conf. Computer and Information Technology (CIT), pp. 2548-2555, 2010.

[23] E. Stab and T. Engel, "Collusion Detection for Grid Computing,"Proc. Ninth IEEE/ACM Int'l Symp. Cluster Computing and the Grid,pp. 412-419, 2009.