ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Implementation of Access Control in Online Social Networks using Multiparty Policy Specification System

Kandi Harini
M.Tech,
Department of CSE,
Avanthi's St.Theressa College of Engineering,
Technology & Management, Garividi,
Vijayanagaram, AP.

Galinki Chinnababu, M.Tech
Associate Professor,
Department of CSE,
Avanthi's St.Theressa College of Engineering,
Technology & Management, Garividi,
Vijayanagaram, AP.

Abstract:

Online social networks (OSN) have increased become a de facto portal for billions of regular users like Face book, Twitter, Linked In world wide. These OSNs offer attractive means for social interactions and information sharing, but also raise a number of privacy and security issues. Suppose online social network allow users to restrict access to share data at present do not provide any mechanism to enforce privacy concerns over data associated with multiple users.

Our access control model which allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model, comparative study provide usability study and problems in previous and advantages of our method.

And also we create an access control model to capture the essence of multiparty authorization requirements, along with the multiparty policy specification scheme and a policy enforcement mechanism. Also, deals a security constraint, which is while sharing the information like personal photos to another one there is a chance to share the same information by the third person.

In order to overcome this problem we are generating a question tag below of the information to be shared with the other. If anyone knows the exact answer to that question they are permitted to watch those photos, videos etc., otherwise they are not eligible. Nothing is maintained secrecy in the social networks.

Keywords:

Social network, multiparty access control, security model, policy specification and management

I. INTRODUCTION:

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.

Cannot trust users place in social networks exploiting with hackers and attacks, set of threats posed to users has [1] resulted in a number of refinements to privacy controls. 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.

In our work controls the shared content can undetermined a user security analyzing the situations in Face book where [2] asymmetric privacy requirements between two friends weaken one user's privacy. We 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

ONLINE social networks (OSNs) are inherently designed to enable people to share personal and public information and make social connections with friends, colleagues, co-workers, family and even with strangers. In latest years, we have seen unprecedented growth in the application of OSNs. For example, Face book, one of representative social network sites, claims that it has additional than 800 million active users and over 30 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 typical OSN provides each user with a virtual space containing profile information, web pages and a list of the user friends. Such as wall in Face book, where users and friends can post content and leave messages. A user profile generally includes information with respect to the user's birthday, interests, gender, education and work history, and contact information.

In accumulation, users can not only upload content into their own or others' spaces but also tag other users who appear in the content. Every tag is an explicit reference that links to a user's space. For the safety of user data, current OSNs circuitously require users to be system and policy administrators for regulating their data, wherever users can restrict data sharing to a specific set of trusted users. In this paper, we pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by investigative how the lack of multiparty access control for data sharing in OSNs can undermine the protection of user data. Some typical data allocation patterns with respect to multiparty authorization in OSNs are also identified. Based on these allocation patterns, 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 and models for OSNs. Our representation also contains a multiparty policy specification scheme. Meanwhile, as conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is additional provided to deal with authorization and privacy conflicts in our model.

2. RELATED WORK:

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. For instance, if a user posts a comment in a friend's space, s/he 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 address such a critical issue, preliminary protection mechanisms have been offered by existing OSNs. For example, Face- book allows tagged users to remove the tags linked to their profiles or report violations asking Face-book managers to remove the contents that they do not want to share with the public.

However, these simple protection mechanisms suffer from several limitations. On one hand, 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. Since 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. Such a binary 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 accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively

3. MULTI PARTY POLICY EVALUATION:

Two steps are performed to evaluate an access request over multiparty access control policies. The initial step checks the access request against the policy specified by each controller and yields a decision for the controller. The accessory element in a policy decides whether the policy is applicable to a request. If the users who send the request belongs to the user set derived from the accessory of a policy, the policy is relevant 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 conclusion if the policy is not applicable to the request. In the next step, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request. Figure 1 illustrates the evaluation process of multiparty access control policies.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

While the data controllers may generate different decisions (permit and deny) for an access request, conflicts may occur. In organize to make an unambiguous decision for each access request, it is essential to accept a systematic conflict resolution mechanism to resolve those conflicts during multiparty policy evaluation.

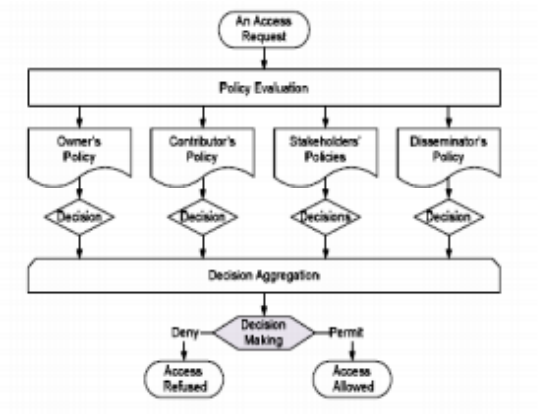

Fig. 1. Multiparty Policy Evaluation Process.

The essential reason leading to the conflicts–especially privacy conflicts–is that multiple controllers of the shared data item often have different privacy concerns over the data item.For instance, assume that Alice has three friends Bob, Carol and David in her friend list. Alice share a photo to her friends and give restrictions to them like Bob can view that photo and can share that photo. Carol only can view that photo but he cannot share that photo. David cannot view and cannot share that photo. But the problem is David is mutual friend to both Alice and Bob. So Bob can share the photo to David without asking permission from Alice. Another instance, assume that Alice and Bob are two controllers of a photo. Both of them classify their own access control policy stating only her/his friends can view this photo. Since it is approximately impossiblethat Alice and Bob have the same set of friends, privacy conflicts may forever exist when considering multiparty control over the shared data item.

A naive solution for resolving multiparty privacy conflicts is to only allow the common users of accessory sets defined by the multiple controllers to access the data item. Unfortunately, this policy is too restrictive in many cases and may not produce desirable results for resolving multiparty privacy conflicts. Consider an instance those four users Alice, Bob, Carol and Dave are the controllers of a photo, also each of them allows her/his friends to see the photo.

Assume that Alice, Bob and Carol are close friends and have many common friends, but Dave has no common friends among them and also has a pretty weak privacy concern on the photo. In this casing, adopting the naive solution for conflict resolution may turn out that no one can access this photo. Though, it is reasonable to give the view permission to the common friends of Alice, Bob and Carol. A strong disagreement resolution strategy may provide a better privacy protection. Temporarily, it may reduce the social value of data sharing in OSNs. Hence, it is important to consider the tradeoff between privacy and utility when resolving privacy conflicts. To address this problem, we introduce a simple but flexible voting scheme for resolving multiparty privacy conflicts in OSNs.

4. MPAC POLICYSPECIFICATION:

To enable a collaborative authorization management of data sharing in OSNs, it is necessary for multiparty access control policies to be in place to regulate access over mutual data, representing authorization requirements from multiple associated users. Our policy requirement scheme is built upon the proposed MPAC model.Accessory Specification: Accessory are a set of users who are granted to access the shared data. Accessors can be representing with a set of user names, a set of association names or a set of group names in OSNs. We formally define the accessory specification as follows:

Let ac U [RT [G be a user u U, a relationship type rt RT, or a group g G. Let at fUN;RN;GNg be the type of the accessor specification (user name, relationship type, and group name, respectively). The accessory specification is defined as a set, accessors = fa1; : : : ; ang, where each element is a tuple < ac, at >. Data Specification: In OSNs, user data is composed of three types of information, user relationship, user profile, and user content.

To make easy effective privacy conflict resolution for multiparty access control, we introduce sensitivity levels for data specification, which are assigned by the controller to the shared data items. A user's conclusion of the sensitivity level of the data is not binary (private/public), but multi-dimensional with changeable degrees of sensitivity. Properly, the data specification is defined as follows:

Let dt D be a data item. Let sl be a sensitivity level, which is the rational numbers in the range [0,1], assigned to dt. The data specification is defined as a tuple <dt, sl>.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Access Control Policy:

To summarize the above-mentioned policy elements, we establish the definition of a multiparty access control policy as follows:
A multiparty access control policy is a 5-tuple P =< controller, ctype, accessor, data, effect >, where
1. Controller U is a user, who can regulate the access of data,
2. ctype CT is the type of the controller,
3. accessor is a set of users to whom the authorization is approved, representing with an access specification.
4. Data is represented with a data specification, and
5. Effect {permit, deny} is the authorization effect of the policy.

Suppose a controller can control five sensitivity levels:

0.00 (none), 0.25 (low), 0.50 (medium), 0.75 (high), and 1.00 (highest) for the shared data. We show several examples of MPAC policies for OSNs as follows: The MPAC policies
(1) "Alice authorizes her friends to view her status identified by status01 with a medium sensitivity level, where Alice is the vendor of the status."
(2) "Bob authorizes users who are his colleagues or in hiking group to view a photo, summer:jpg, that he is tag with a high sensitivity level, wherever Bob is a stakeholder of the photo."
(3) "Carol disallows Dave and Edward to watch a video, play:avi, so as to she uploads to someone else's spaces with a highest sensitivity level, where Carol is the contributor of video." They are expressed as follows:
(1) p1 = (Alice,OW{<friendOf,RN>}, < status01, 0.50 >, permit)
(2) p2 = (Bob, ST, f<colleageOf;RN>, <hiking;GN>},< summer.jpg, 0.75 >, permit)
(3) p3 = (Carol,CB,{<Dave,UN>, <Edward,UN>},<play,avi, 1.00 >, deny)
(4) Carol allows David to view and share a photo and disallows Edward to view and share. But Edward is mutual friend to both Carol and David. So whenever David share that photo to Edward then he ask permission from Carol with 0.25 sensitivity level. 5.

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. 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. 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.

REFERENCES:

[1] A. T. Fiore and J. S. Donath, "Homophily in online dating: when do you like someone like yourself?" in CHI '05: CHI '05 extended abstracts on Human factors in computing systems. New York, NY, USA: ACM, 2005, pp. 1371–1374.
[2] L. Tang and H. Liu, "Scalable learning of collective behavior based on sparse social dimensions," in CIKM '09: Proceeding of the 18th ACM conference on Information and knowledge management. New York, NY, USA: ACM, 2009, pp. 1107–1116.
[3] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 1734–1744. Springer, 2006.
[4] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. ACM Transactions on Information and System Security (TISSEC), 13(1):1–38, 2009.
[5] P. Fong. Relationship-based access control: Protection model and policy language. In Proceedings of the first ACM conference on Data and application security and privacy, pages 191–202. ACM, 2011.
[6] P. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for face book-style social network systems. In Proceedings of the 14th European conference on Research in computer security, pages 303–320. Springer-Verlag, 2009. .
[7] S. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H. Choi. D-FOAF: Distributed identity management with access rights delegation. The Semantic Web–ASWC 2006, pages 140–154, 2006.