MULTIPARTY ACCESS CONTROL AND KEY AGREEMENT FRAMEWORK FOR ONLINE SOCIAL NETWORKS

G.T.Rajaganapathi[#1], D.Muthusankar[*2]

CSE-CSE Department, KSR College of Technology- KSR College of Technology
Tiruchengode, India

[1]rajaganapathi88@gmail.com

[2]muthusankar@ksrct.ac.in

[*]*Associate professor of CSE Dept*
KSR College of Technology
Tiruchengode, India

Abstract - **Social network is a network consists of many number of users and maintains the relationship between them. Social networks can be accessed from anywhere in the world. ONLINE social networks (OSNs) such as Facebook, Googleþ, and Twitter are designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family, and even with strangers. OSN experienced a tremendous growth in the recent years, with new features and application. This paper pursues a systematic solution to facilitate collaborative management of shared data in OSNs. Initially it begins 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. An MPAC model is formulated to capture the main features of multiparty authorization requirements that have not been addressed so far by existing access control systems and models for OSNs. This paper deals with the online social network security constraint, in which there is chance of sharing the information like photos, videos, to another one and it will be get shared by the third person. To overcome this issue, group key management techniques are used to authenticate the users. The proposed system supports a one-many authentication, which is the basis of batch authentication to simultaneously authenticate multiple users.**

Keywords: **Online social networks, Multiparty access control, group key management techniques.**

I INTRODUCTION:

Online social networks (OSNs) such as Facebook, Goggle+ and twitter are designed to enable people to share personal and public information with their friends, co-workers, colleagues, and family members. Recent years these online social networks made a tremendous growth. Web-based Social Networks (WBSNs) are online communities that allow users to publish resources and to record and/or establish relationships with other users. The adoption of Semantic Web technologies, such as FOAF (Friend of a Friend) has simplified information access and dissemination over multiple WBSNs. It is possible for the users to establish a user relationship and group relationship to distinguish their trusted and untrusted users. There is quite a relevant improvement towards an easier sharing of information, it is now necessary that information owners have more control over its diffusion. So far, this issue has been addressed by most of the available Social Network Management Systems (SNMSs) by allowing a user to specify whether a given piece of information should be public or accessible only by the users with whom the owner of such information has direct relationship. It provides a separate virtual space for individual users, such as wall in Facebook, so that the users can post their own contents. It is possible to tag other users who get appear in the content. OSN also provide simple access control mechanisms allowing users to govern their respective information contained in their own spaces.

OSNs provide built-in mechanisms enabling users to communicate and share contents with other members. OSN users can post statuses and notes, upload photos and videos in their own spaces, tag others to their contents, 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. OSNs currently provide simple access control mechanisms allowing users to govern their own information in their spaces, but they will not get control over data residing outside their spaces. 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, Facebook allows tagged users to remove the tags linked to their profiles or report violations 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. 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.

This paper gives a systematic solution to facilitate collaborative management of shared data in OSNs. Initially, the lack of multiparty access control (MPAC) for data sharing in OSN is examined. 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. This model also contains a multiparty policy specification scheme. Meanwhile, since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in this model.

II MULTIPARTY AUTHORIZATION REQUIREMENTS

In OSNs, for a single resource multiple users have different authorization techniques. In this, to evaluate the risk in the collaborative control in OSNs, 3 scenarios are considered – Profile sharing, relationship sharing and content sharing. For this, Facebook is taken as example because it is the popular online social network provider.

Profile sharing

It is an attracting feature of OSN, It is provided to support the social applications, which was developed by third-party developers. The Social applications provide meaningful and attractive services to their users. Because of this, users can able to select particular attributes and they can share to their friends. Also the user can able to control over his information so that other than the owner and his friends cannot access it. User's friend is the owner of shared profile, the user is disseminator and the application is an accessor. Both the owner and the disseminator can control the policies and restricts the profile contents.

Relationship sharing

OSN provide an important feature of relationship sharing. Through this relationship can be shared with their friends, families. OSN provides mechanisms so that the user can regulate their friend lists. Consider an example, a scenario where a user john specifies a policy to hide his friend list from the public. Adam one of john's friend has a weaker policy that permits his friend list visible to anyone.

Content sharing

Online social networks provide an important feature to the users to share their views to the members. Users can post their status, views, photos and videos in their respective spaces so that they can able to share it with their friends, colleagues. Also, they can able to share anything in their friend's spaces too.

IIIANALYSIS OF PROBLEM:

Now days, main problem in online social networks is that the user has the rights to control or govern the access in their own walls or spaces, but they do not have rights to gain access over the data in others spaces. For example in facebook if a user uploads a photo and share with their friends and he can tag the friends who appear in the photo. Though we can able to restrict who can view this, but the tagged friends cannot restrict because they may have different profile concerns. The security policy of the tagged friends may be different from the owner. However the facebook has some preliminary mechanisms by removing the tags of the tagged users. But it has some limitations, removing a tag only prevent other members from seeing the profile. But the photo has the image of the user, it will be revealed to all users. Reporting to online social networks will decides whether to delete the particular content or to keep with it. Managers will take the decision based on the maximum no of reports that has come from the users about the content. If majority are against that content means then it will be removed completely. It is essential for the online social networks to develop an flexible access mechanisms that will satisfy the requirements of multiple associated users for sharing the data collaboratively without any hindrance.

IVPROPOSED WORK:

In proposed system, MController is proof-of-concept introduced in the facebook application for collaborative management in shared data. It helps the multiple users to control over their policies and privacy over their shared data items. Current implementation was restricted with the photo sharing only. But the proposed implementations deals with the different data sharing such as videos, comments, tagging, etc,. It gives a systematic solution of collaborative management for data sharing in online social networks. A multiparty access control model was introduced with the multiparty policy specification and schemes. Multiuser environment is prevailed in the online social networks, it allow multiple controllers to access their policies and schemes. A group key management techniques is introduced in

the MController so that this gives a solution for the collaborative management of shared data. Also some of the conflicts are unavoidable, for such conflicts voting mechanism is provided to deal with it. Peer to peer batch authentication framework is proposed for online social networks. The hash-based protocol adopts lightweight cryptosystems to reduce the computational costs. To offer higher security properties, the proxy- and certificate based methods are based on asymmetric encryption and signature methods to fulfill the security requirements of sensitive transactions.

V. MODULE DESCRIPTION

System has the following modules

1. User module
2. MController module
3. MPAC module
4. Batch authentication framework

User module

A sample online social network is considered in this module. User is the owner of the data d in their own space. He has the full control of data d in its space. Mainly some scenarios are considered such as, content sharing, relationship sharing, profile sharing. User will specify the full access and rights of this data. No other third party will gain control over it.

MController module

MController helps the users to specify the authorization policies and privacy for a shared data item. It deals with other types pf data sharing shuch as videos,tagging and comments. Main component is the decision making module, where the requests are processed and responses will be formulated.multiparty privacy conflicts are resolved through the majority decisions of the controller. Aggreagate sensitivity value is aggregated so that the users can allow the multiple users to share the data. Contributor is the one who publish the data item in other's space. Published content may also have multiple users. Stakeholder is the one gain s control over the data and has the relationship with the other users. Disseminator are the persons where the data get shared to their own space or timeline from other users. Disseminator has no control over the data.

MPAC Module

Proposed system can be proved through MPAC module only. MPAC policies are formulated to enable a colloborative management of sharing the data. Users granting the access to the shared data are termed as accessors. For every request accessor element in the policy is considered. If the policy accepts means, it sends the response, or else it denies it. Privacy conflicts can be rsolved by voting mechanisms.

A. Title and Author Details

Title must be in 24 pt Regular font. Author name must be in 11 pt Regular font.

Batch authentication framework

Batch authebticatio framework is designed for online social networks. In this, 3 important techniques are used. Hash-based technique uses the lightweight ccryptosystems to reduce the computational cost. To offer high security properties, proxy-based methods and certificate based methods are used. These methods are based on the asymmetric encryption and signature methods are used for sensitive transactions. In most group key management techniques, group members are authenticated by the group leader "one by one." That is, n authentication messages are required to authenticate n group members. Then, these members share one common group key for the group communication. In our batch authentication techniques, users are simultaneously authenticated by the requester. That is, one authentication message is required to authenticate n session peers. Then, the requester negotiates one secret key with each user instead of sharing one group key among all users.

VI. CONCLUSION:

In this paper, we have proposed a naïve solution for the colloborative management of shard data in online social networks. It reduces the communication cost required for the users. By incorporating different trust levels, proposed techniques allow the user with a high level of trust and helps to authenticate with the other users. 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. Future work are based on the interference based techniques, in which multiple users shared large number of photos and the privacy concerns in this may be tedious and time consuming.

ACKNOWLEDGMENT

Rajaganapathi G T is a Master of Engineering Student in the Computer Science and Engineering Department, K.S.Rangasamy College of Technology. He research interests are Web Mining, software testing.

REFERENCES

[1]Facebook developers
http://developers.facebook.com/, 2013.
[2]B. Carminati, E. Ferrari, and A.Perego, "Enforcing Access Control in Web-Based Social Networks," ACM Transaction Information and System Security,
[3]P. Fong, M. Anwar, and Z. Zhao, "A Privacy Preservation Model for Facebook-Style Social Network Systems," In Proceedings of the 14th European Conference Research in Computer Security
[4]H. Hu and G. Ahn, "Multiparty Authorization Framework for Data Sharing in Online Social Networks," In Proceedings of 25th Conference on Data and Applications Security and Privacy
[5] N. Li, Q. Wang, W. Qardaji, E. Bertino, P. Rao, J. Lobo, and D. Lin, "Access Control Policy Combining: Theory Meets Practice," Proceedings of 14th ACM Symposium Access Control Models and Technologies.
[6]A. Squicciarini, M. Shehab, and F. Paci, "Collective Privacy Management in Social Networks," Proceedings of 18th International Conference World Wide Web

