Multiple user Authority Framework for Data Sharing in OSN'S

Mrunalini Pratap Shitole
M.E (Computer Network)
Dr. D. Y. Patil School of Engineering & Technology
Affiliated to Savitribai Phule Pune University, India

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

ABSTRACT
Today all the peoples are using the social websites for the interaction and creating profile and many more purposes. In this paper, Focused on the restriction access of information which is handling by social websites. All people knows, Social Network (OSNs) have much more growth in the current year and having the facility for hundreds of millions of internet users. When user use the Social websites that provides the attractive means for communication and the information sharing purpose but it will increase the number of conflict. 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, here formulate an control model to get intrinsic nature of multiparty authorization requirement along with the condition and a conditional mechanisms. Here present a logical representation of our control model which performs many analysis tasks on our model. Here also discuss the proof of concept prototype which is the part of an application in face book.

Keywords: - AMF, OSNs, MPAC, AS, MController.

1. INTRODUCTION
Recently most of the people using the online social network for the purpose of communication between to users smoothly. There are many online social network web sites are available on the internet such as face book, Google+, twitter, linked in, what's app etc. These web sites or application is used by user to communicate with other party to make the relation. With help of this web site user get the information of other party so it will handle the problem of them. In recently, there are millions of people shared there data or information on this website. And through that web sites it will handle many business very easily. But if you says the security purpose many of the website are failed and few web sites are gives security but not 100 percent. So here the security of shared data of many user which is use this social network.

In Proposed System performed a proof-of-concept operation for the collective management of shared information, known as Multiple Controller. A proof-of-concept operation of our solution called MController has been explain and proceed by the usability study and system evaluation of our method. Here using the classifier which is classifying the message post on users profile, name of the classifier is RBFN. Categories of these messages are like hate, volatile, offensive, vulgar. A extensile access control structure in a multiple user environment should allow multiple controllers, who are associated with the shared information, to specify access control scheme. As detected previously in the mutual sharing patterns in addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, need to allow the access of the shared data as well. In our multiparty authority framework, a group of users could collide with one another so as to accommodate the final access control agreement. Although OSNs really provide simple access control architecture allowing users to gain access to information included in their own spaces, users, unfortunately, have no control over content residing outside their spaces. For instance, if a user posts a comment in a friends space, she/he cannot identify which users can see the comment. The existing work could model and evaluate access control requirements with respect to collective authorization framework of shared data in online network. The need of attached management for information sharing, especially photo sharing, in network has been implemented by the recent work provided a efficient output for collective privacy management in OSNs. Their work considered access control schemes of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately identify her/his own security preference for the shared data.

Our prototype software enables multiple associated users to specify their authorization scheme and privacy preferences to co-controller shared data item. It is worth noting that our recently implementation was restricted to handle image sharing in social network. Obversely, our approach can be recommended to deal with other kinds of information sharing and comments, in OSNs as long as the stakeholder of shared information are recognized with effective instruction like tagging, comments or searching. The proposed system shows a novel solution for collective management of shared information in network. A multiparty access control architecture was created, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, defined an approach for representing and reasoning about our proposed model.

Proposed system will perform access over shared information with the security from multiple users. Also prevent the attack scenario and collision activity. It will introduce the other controller like contributor, stakeholder and disseminator of information to manipulate data securely. The remaining of the paper is organized as follows: In Section 2, present multiparty authorization requirements and Access control patterns for OSNs. Articulate our propose MPAC model, including multiparty authorization specification and multiparty policy evaluation in Section 3. Section 4 addresses the logical representation and analysis of MPAC. The details about prototype implementation and experimental results are described in Section 5. Section 6 discusses how to tackle collusion attacks followed by the related work in Section 7. Section 8 conclusions of paper and discuses our future scope.

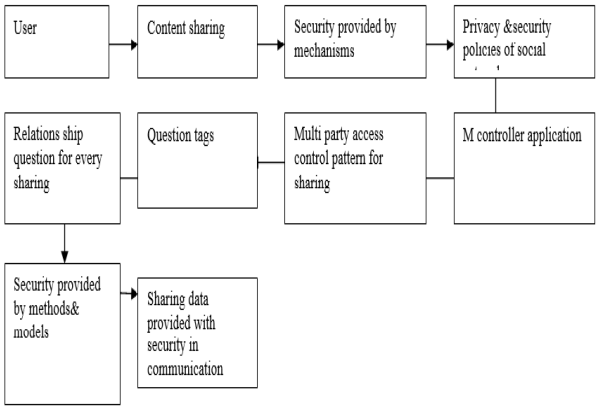

Fig. 1. Process of providing security to shared data

2. REQUIREMENT ANALYSIS OF AUTHORISATION ARCH. IN OSN'S

In this section, we explain a requirement analysis of authority model in social network. Meanwhile, discuss several typical contribution patterns happening in social network where many users may have different authority requirements to a contribute data. So specifically analyze three scenarios profile sharing, relationship sharing, and content sharing to understand the critical situation posted by the lack of collective control in OSNs.

2.1. Profile sharing

To provide useful and reprehensive services, social applications having user profile parameter. To make condition more complex, social applications on current area can also gain the profile parameter of a users friends. When users can select same contents of profile parameter they are willing to contribute with the application when the friends use the applications. Simultaneously, the users who are using the applications may also want to control what data of their friends is available to the applications because it is possible for the applications to contained their private profile parameter through their friends profile parameter. This means that when an application uses the profile parameter of a users friend, both the user and her friend want to gain access over the profile parameter.

2.2. Relationship sharing

Second contributing feature of social web is that users can mutual their relationships with other friends. Relationships are having two directions and carry very careful data that sends by users may not want to displayed. Most social web provides regulation that users can regulate the display of their friend lists. A user can only control one direction of a relationship.

2.3. Content sharing

Social network provide built-in rules enabling users to interact and contribute contents with other members. Social web users can post data in their own area, tag others to their contents, and share the contents with their friends. On the other hand, users can also post data in their friends area.

3. PROPOSED SYSTEM WITH MOTIVATION

3.1 Problem Definition

Study of multiparty authorization architecture, MPAC model for content sharing, MPAC model for profile sharing, MPAC model for relationship sharing. Also study of policy evaluation mechanism and policy scheme. In the policy specification study the access specification and data specification. Here pursue a analytical solution to make easy collective management of mutual data in social network. Also begin by analyzing how the deficiency of multiparty access control for data ingression in OSNs can examine the protection of user information. MPAC model is created to catch the kernel feature of multiparty authorization requirement that have not defined by current access control systems and models for social network. Proposed system will perform access over shared information with the security from multiple users. Also prevent the attack scenario and collision activity. It will introduce the other controller like contributor, shakeholder and disseminator of information to manipulate data securely.

3.2 Proposed system

MPAC is Multiparty access control model. It is valid because it proved the security regarding the social network. To enable a collective authorization architecture of information sharing in Social Network, it is very essential for multiple user to control access through the policies. It is in the place to always access over shared information, defining authorization requirements from associated users. A social web provides the conversation on different things. It is Attractive, i.e. social interactions raise the number of security with multiple online users. The existing system of this paper shows the simple access control model.

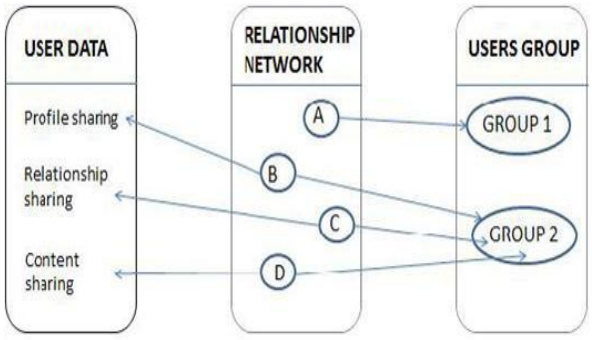

Fig. 2. Relationship between data user and users groups

That model not recognized the trusted person and untrusted persons in online social web sites. Also not given the more flexibility and privacy regarding the shared information but also many peaple use the social network for sharing information.The efficiency of attached management for information sharing in social network has been recognized by current work. So here the authorization architecture model used. A authorization framework is for-mulated to catch the importance of multiparty authorization requirements in network. Also show how Assurance Management architecture (AMF) can be applied to OSNs for identifying and resolving privacy collision, and representing and reasoning about MPAC model and policy. In this paper, MPAC model evaluation parts consist of access and control specification, multiparty policy evaluation and MPAC model. In this

architecture we are focusing on the privacy issues of shared data like a identification of fake user photo from the information also many more issues handle by this system architecture so it is more efficient than the current architecture of authorization framework.

4. MATHEMATICAL MODELLING

1. S=Set of whole system consist of
   S=U, G, P, RT, R, C, D, CT
2. U=set of N number of Users.
   U=u1, u2,....,uN.
3. G=Set of N number of groups like g1, g2, gN.
   G=g1, g2,…. gN
4. P=collection of N number of user profile like p1, p2, pN.
   P=p1, p2 ,.....pN
5. RT=Set of relationship.
6. R=set of user relationship like r1, r2, rN.
   R=r1,r2,.....rN
7. D=set of Dataset.
8. CT=set of controller type like
   Owner, Contributor, Stakeholder, Disseminator.
   CT=OW, CB, ST, DS
9. UU=set of unidirectional user to user relations
   UU=U*U
10. UG=set of user to group relations
    UG=U*G
11. UD=set of user to data relations
    UD=U*D

5. AUTHORITY ARCHITECTURE WITH PROTOTYPE

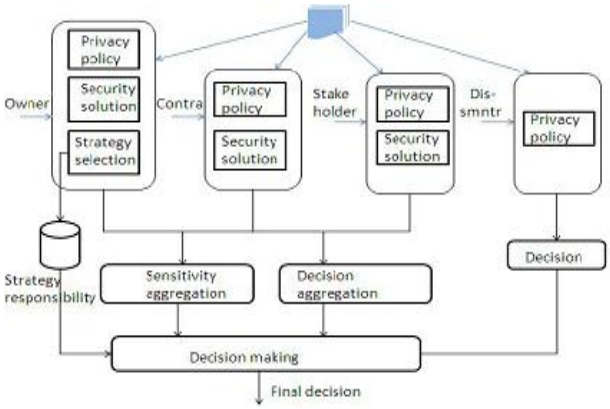

Fig.3. System Architecture

The first step to checks the input request against the policy specified by each controller and takes a decision for the controller. The accessor element in a rules decides whether the rule is applicable to a request. If the user who sends the request belongs to the user set derived from the accessor of a rule, the rule is applicable and the evaluation process returns a response with the decision (either permit or deny) indicated by the effect element in the rule. Otherwise, the re- sponse yields deny decision if the rule 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.

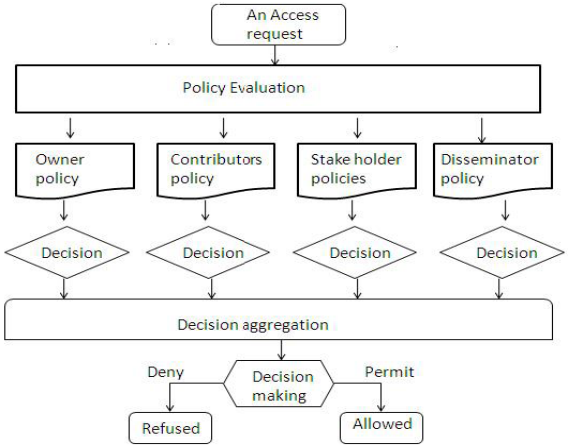

Fig.4 Decision procedure

6. POLICY SPECIFICATION AND POLICY MANAGEMENT

Our specification scheme is built upon the created MPAC structure .

6.1Accessible Specification

Assessors are a set of users who are granted to access the shared data. Assessors can be represented with a set of user names, asset of relationship names or a set of group names in OSNs .

6.2Data Specification

Policy schemes are applied over the access control model .The data specification define in three ways; profile, relationship and content sharing.

6.2.1Owner

In Owner is a data item in the space O of a user ur in the network. The user ur is called the owner of D. The user ur is called the contributor of D. We specifically defined three scenarios profile sharing, relationship sharing and content sharing to understand the risks posted by the lack of collective control in online social network.

6.2.2Contributor

In Contributor D be a data item published by a user ur in someone else's space in the network. The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor D.

6.2.3Stakeholder

In Stakeholder is a data item in the space of a user in the social network. Let Tg be the set of tagged users associated with D. A user ur is called a stakeholder of D, if ur 2 Tg who has a relationship with another called stake holder stakeholder, shares the relationship with an access.

6.2.4Disseminator

In Disseminator D be a data item shared by a user ur from someone else's space to his/her space in the social network. The user UR is called a disseminator of D. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator's space.

6.3Policy management

Multi party Authorization framework is consist of two steps. In step-1, i just make the cluster of each controller and give

the appropriate naming to that cluster.step-2,in this step we are basically decide the rules and regulation of the specific controller. step -3, if any of the user want to interact with other user then at that time it will apply the rules for it and it will take the final decision that is allowed or deny the massage. From the process of evaluation in MPAC rules, the controllers give different decision for an access request. There may be a chance of occurring conflicts. So that a mechanism is needed to resolute the conflicts for taking an unambiguous decision for each access request.

7. RESULTS

7.1. Input

When the input as a group of various field like Friend, employee etc. In the experimental result define the required parameter like likability ,simplicity ,control.

Matrix	Facebook		Mcontroller		Proposed system	
	Avg.	Upper Bound on 93% confidence interval	Avg.	Lowerbound on 95% confidence interval	Avg.	Lower bound on 93% confidence interval
Likability	0.20	0.25	0.83	0.80	0.84	0.80
Simplicity	0.38	0.44	0.72	0.64	0.80	0.72
Control	0.20	0.25	0.83	0.80	0.86	0.83

Fig. 6. Usability Evaluation for proposed system

7.2. Expected Results

In the above table representing the all things which represent the efficient result of proposed system. Logical graph of result is as follow:-

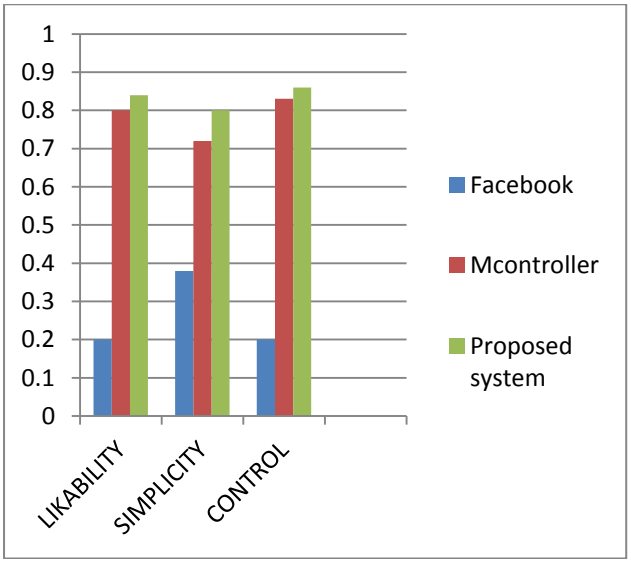

Fig. 7. Usability Evaluation for proposed system

8. CONCLUSION

Aim of base paper is to give security of collaborative information which is shared on the social network. This system is more flexible, simplest and control. In the base paper system Not using any classifier which is not given the accurate result so in the propose system take care of this thing and use the RBFN classifier so that our proposed system is more simplistic, likability and control. So here proposed system concludes that it is much better than existing system.

9. ACKNOWLEDGMENT

I would like to thank the researchers as well as publishers for making their resources available. I am also thankful to reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

10. REFERENCES

[1] 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.

[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/mpac+.pdf, Apr. 2012.

[3] B. Carminati and E. Ferrari, "Collaborative Access Control in On- Line Social Networks," Proc. Seventh Int'l 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/mpac+.pdf, 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.

[12] L. Jin, H. Takabi, and J. Joshi, "Towards Active Detection of Identity Clone Attacks on Online Social Networks," Proc. First ACMConf. Data and Application Security and Privacy, pp. 27-38, 2011.

[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.

[14] A. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3p: Adaptive Policy Prediction for Shared Images over Popular Content Sharing Sites," Proc. 22nd ACM Conf. Hypertext and Hypermedia, pp. 261-270, 2011.

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

[16] B. Viswanath, A. Post, K. Gummadi, and A. Mislove, "An Analysis of Social Network-Based Sybil Defenses," ACM SIGCOMM Computer Comm. Rev., vol. 40, pp. 363-374, 2010.

[17] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel, "A Practical Attack to De-Anonymize Social Network Users," Proc. IEEE Symp. Security and Privacy, pp. 223-238, 2010.

[18] E. Zheleva and L. Getoor, "To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles," Proc. 18th Int'l Conf. World Wide Web, pp. 531-540, 2009.

[19] Facebook Privacy Policy, http://www.facebook.com/policy. php/, 2013.

[20] Facebook Statistics, http://www.facebook.com/press/info. php?statistics, 2013.

[21] Google+ Privacy Policy, http://http://www.google.com/intl/ en/+/policy/, 2013.

[22] The Google+ Project, https://plus.google.com, 2013.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

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