2014 Fourth International Conference on Communication Systems and Network Technologies

# Access Control Mechanism for Multi User Data Sharing in Social Networks

Ashwajit Ramteke
G. H. Raisoni College of Engineering
Nagpur (M.S.), India
aramteke.ramteke@gmail.com

Girish Talmale
G. H. Raisoni College of Engineering
Nagpur (M.S.), India
girishtalmale@gmail.com

***Abstract*—Online social networks (OSNs) have analyses large growth in recent years and become a saturation for hundreds of millions of Internet users. These OSNs offer to enforce attractive means for digital social interactions and information contribution, but also increase a number of security and privacy issues. Right to use manage mechanism is provide to restrict shared data, they currently do not provide any mechanism to minimize problem of multiuser shared data. To this end, we propose an approach to enable the protection of shared data associated with multiple users in OSNs. We gives a platform to user to share their data in secure manner. We also discuss a proof-of-concept prototype of approach as part of a framework on social network and provide usability study and system evaluation of our method.**

***Index Terms*— Social network; Multiple user access control; Security mode; Specification and management; Data Sharing**

## I. INTRODUCTION

With the growth of internet, nowadays social networking site have larger popularity than any other else. For some social networking sites like Facebook, twitter given that real names and other private information is encouraged by the site (onto a page known as a 'Profile'). These information are most of contain of user basic identity. Some sites also allow users to provide more information about themselves such as interests, hobbies, favorite's books or films, and even relationship status. Thus, it is more dangerous to user to leek their identity anywhere. Study has been done on two major social networking sites, and it is originate that by overlapping 15% of the one as the same photographs, profile images with similar pictures over multiple sites can be matched to identify the users [9]. In recent year, a study of survey was performed to analyses data of 200-300 Facebook profiles of random user. It was revealed that 89% of the users gave genuine names, and 61% gave a photograph of themselves for easier identification via face recognition [9] [10]. Most of the user had not alter their basic information (the default setting originally approved friends, friends of friends, and non-friends of the similar network to have full view of a user's profile). User are capable to block other user which are having account on Facebook, but this must be done by human being basis, and would therefore come into the picture not to be usually used for a wide number of people. The user are do not realize that which security feature they want to use. Facebook was criticized due to the perceived laxity regarding privacy in the default setting for users. It is more important for each social networking site that sharing a user data in secure manner. Features that invite users to partaking messages, invitations, photos, open dais applications and other applications are often the avenues for others to gain access to a user's private information. A typical online social network is give platform for each user to share their data over the virtual space containing user shared photos, wall post, user's friend. With the use of this feature, user not only can upload their photos but also tag the other photos in virtual space of ONSs. The tag in the photos indicate that link of the each user account which are appear on the photos. For the protection of user data, existing system gives indirect security environment for each user. In this paper, we examine issue which address privacy and security and realize multiparty right to use manage in OSNs. We begin by examining how the lack of multiple user management for data sharing in OSNs throughout the security problem can undermine the protection of user data [2]. The project work find out challenge, In particular, we have to understand the conceptual study of two fundamental. First, we want to deep theoretical study of social media like Facebook, twitter and find out the challenges regarding user pattern recognition. Second, we want to oversimplify the social media access control mechanism, by analysing the user pattern behaviour as the same network. At the end of these we have to initiate one paradigm which can generalise all user problem and give the user friendly platform to the user [4]. The model can be instantiated into a Facebook is family of social network, each with a identifiably different access control mechanism, so that Facebook is one can be best generalise model to show our derive implementation over social network.

## II. RELATED WORK

Authorization for OSNs is still a relatively new research area. Several access control manage models for OSNs have been introduced Early right to use manage solutions for OSNs introduced trust-based right to use manage inspired by the developments of trust and reputation computation in OSNs. Social networking is research area for social people who are really in search of what is new.

978-1-4799-3070-8/14 $31.00 © 2014 IEEE
DOI 10.1109/CSNT.2014.122

IEEE computer society

S. Kruk, S. Grzonkowski introduced a technique is D_FOAF system. In recent growth of world, each person has unique identity feature including their basic information working area .Some credential information is also share via social services. But such information is more risky to exploit in any where's we have not secure identity based management system. In this identity base management system, solution is based upon the social services. Structure of the social network are having access right. So access rights have some identity base management system which is explain in this paper [2]. Author suggested that how sensitive information can protect from unauthorized user and right to use manage over OSNs. Finally, the FOAF Real system that implements presented solutions and utilizes FOAF metadata to allow exchange of the profile information with other systems. But it really works on the basis only on the identity base management system.

After this analysis of identity base management, Carminati et al. gives general working of rule base system .In this system, User with large amount of data which store on web pages. Most of the user want to save their identity information on web pages and other user can access their information without any privacy concern. Author presented a right to use manage model for WBSNs, where policies are expressed as constraints on the type, depth, and trust level of alive relationships [3]. The system for rule access control manage model which allows the specification of access rules for online resources. The different tasks to be carried out to enforce right to use manage are shared among three distinguished actors—namely, the owner of the requested resource, the subject which requested it, and the social network management system.

B. Carminati, E. Ferrari, and A. Perego, were gives the method of semi decentralized mechanism for sharing contain in social network [3]. Author modify a discretionary right to use manage model and a related enforcement mechanism for controlled sharing of information in WBSNs. The model allows the specification of access rules for online wealth, where official users are denoted in terms of the relationship type, depth, and trust level alive between nodes in the network [3].

Fong et al. proposed an right to use manage that formalizes and generalizes the access control mechanism executed in Facebook, admitting random policy vocabularies that are based on theoretical graph properties [5].Gates described relationship-based right to use manage (ReBAC) as one of new security paradigms that addresses unique requirements of Web 2.0 [6]. Fong recently formulated this paradigm called a ReBAC model that bases authorization decisions on the relationships between the resource owner and the resource accessor in an OSN [7]. From the above discussion, main focus to formulate a representative ReBAC model to capture the strength of the pattern, that is, agreement decisions are based on the association between the resource owner and the resource accessor in a social network maintained by the safety system [4]. In the above discussion, we analyses all the possible mechanism and formulate one model and mechanism that is known as access control model for multiple user in OSNs.

## III. MULTIPARTY AUTHORIZATION SPECIFICATION

From base of literature survey, we have study the paradigm of about security challenges in social network. So that, when the number of user want to use their user page and wants to secure their content on profile like post ,comment, image sharing and so on , that they have some feature of access control mechanism [8]. In this project, we show some feature or characteristics, using this one can secure our predefine mechanism in social network. The module begin with their working feature as follows.

1. *Accessor*: If the user X create an account with their basic information. Now he is accessor of that account. He can access his information, sending friend request, view request, upload image and so on. Accessor have the rights to send the image to another user via request option [12]. Every user in social network is the accessor of respective account. Each information and credential info are also can be access by user.

2. *Owner***:** We generalize the idea of owner like, if any user wants to upload an image in his account so that user is owner of the image. Same likewise concept of text, if user want post any blog or comment, thus the respective user is owner of that blog or comment or text [14]. The photo containing the number of user that are tag to it, it means that all the notification are directly shown on the wall of tag user.

3. *Stakeholder:* If the any user posting an image on wall and tag some friend .so that user is the owner of that image. And the other friends are the stakeholder of that image. Any user friend can add the tag in the any photo and can remove the tag in any photo but only when authority of owner of that photo [14] [15]. Owner of the photo have the all the rights to which is right to share and formulate each user activity track to analyse the pattern behaviour of the each user.

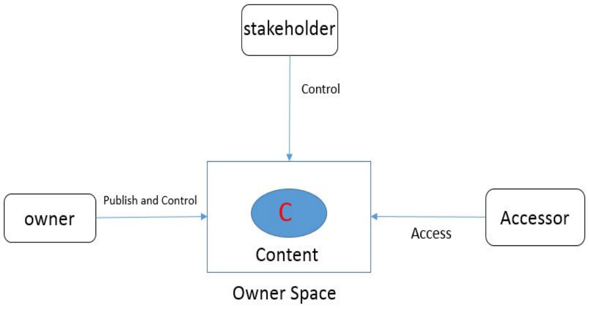


Fig. 1. A shared content has multiple stakeholders

4. *Contributor*: If any user wants to post a text or upload the image on same wall or friend's wall, so that user who are posting content is the contributor of that image, text or content. Contributor have the rights to post the image on particular user wall ,hence only respective user friend can see that post via notification to the user. Contributor play an important role in posting wall's content.

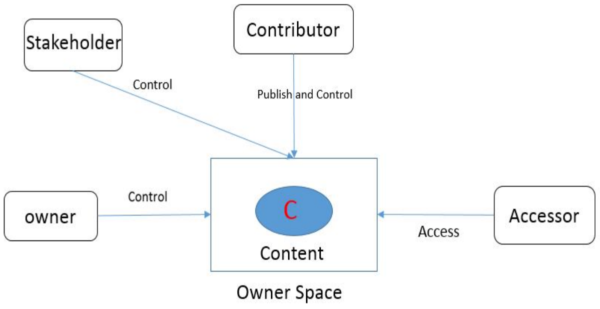


Fig. 2. A shared content is published by a contributor

5. *Disseminator:* With the help of this generalization, any user can upload the image or post the content or text in someone else space .Another owner friend can share this image or post in his space with authority of the owner of that image or post.so that this user called as disseminator of that content [15].

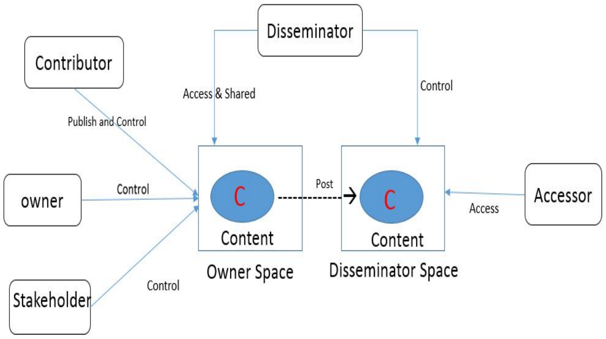


Fig. 3. A desseminator Shared other's content published by a contributor

6. *User Data:* The user data is the collection of the datasets containing information regarding profile of user friend, relationship list and content sets. User data in OSNs can be organized as a hierarchical structure, whose leaves represent the instances of data, and whose in-between nodes represent categorizations of data, *user data*, is classified into three types, *profile*, *relationship* and *content* [12]. The content is further divided into multiple categories, such as *photo*, *video*, *note*, *event*, *status*, etc.

## IV. SECURITY MEASURES IN OSN'S

On the basis of survey of social networking, we get some basic reason to short out the problem which are face by current social network. Here we discuss the propose method that we can easily implement in the platform of social network and secure user pattern behaviour that is recorded in communication between two user .The methods are likewise

1) *Secure Chat:* In existing social network like a Facebook. In the Facebook chatting option ,if user X wants to chat with the user Y .User X say "Hello" to the user During this phase ,this data is firstly encrypted in some text that goes to online privacy organization like Abine .This Abine take it and decrypted that encoded script and send to that respective user [17]. During this phase direct communication does not exist between the two users. Thus we can show that two user can communicate with each other via direct chat and encoding and decoding authority to the respective social network. In this way, we can prevent our credential information like bank account details, password, etc. [14].

2) *Doc File Attachment*: In the recent survey of social network like Facebook, Twitter, there is no provision for doc file attachment in which whenever user wants to share via social network. Except the email option, the number of user are facing a problem like file attachment. So our Framework is design the area for same problem that can resolve the problem of live user [11]. Thus, whenever any user wants to share some documents like pdf, word, power point, etc. they have option to attach any file and send to the particular user via secrete massage .Only notifying to the particular user to receive to it.

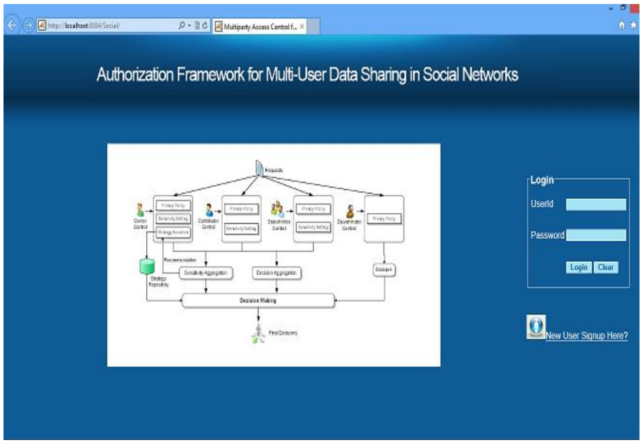
3) *Automatic Tag:* If user post some text, content, or image and want to tag all friends automatically, then there is no provision in recent social network [16]. To design the technique for automatic tag, just click on timestamp of that post and open the post containing window. Just press control + j to opening the source code window and paste some extra code in it.it showing to the user as some error massage, just ignore it and continue to it. Then user can found that post is being automatically tag to all friends. Actually it is not tag to all of friends but comment box having name of all friends so that each friends having notification of about that post. Thus each user friend can see that post.

4) *Time Control:* If the user want to post some content, upload an image and posting some blog but for some particular time period, so user need some time stamp to set that period of post and set to each post on the user wall. If the friends of user visit to user walls post then he

can easily see that post otherwise remove from the wall automatically after end of period. It is provision of security view of wall post, so that only user friend can visit that post and prevent from the malicious user on social network [13]. Time control for each wall post is more precious in the view of security control and rights in the hand of respective user walls.

## V. IMPLEMENTATION AND EVALUATION

To establish the possibility of access control model and mechanism, we implemented Social network-based model. It is implemented on another platform like Authorization framework model for supporting co-operative Supervision of shared data. In this project, established multiple user authorization framework platform. Framework exhibit the security issue which are currently facing by social network. And that problem overcome by our model .We Create one registration form to enter in the network to the user. Once the user can register with their basic information in the network, they can be one of the member of the network. Then he can upload one profile photo and needed information regarding identification of human. In this project, we have 5 module and we execute two of them [8].The result of model is fine in strength so that user can use it as user friendly. Multi-User authorization framework model is deployed as an independent platform of any social network, which is hosted in an Apache Tomcat application server supporting Java as front end and MySQL database as a backend. Multi-User authorization framework model is based on the I Frame external approach, adopting the Facebook REST-based APIs and supporting Facebook Mark-up Language (FBML), where Facebook server acts as an intermediary between users and the application server. Social network can accept the input from the user and forward to the application model. The application model server is responsible for the input process recognition and cumulative management [1].

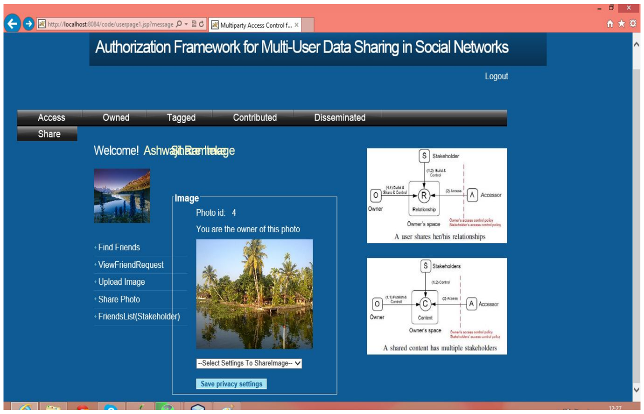

http://localhost:8084/Social/

Authorization Framework for Multi-User Data Sharing in Social Networks

Login
UserId
Password

Fig.4. Control for User Authentication

In the above figure shows that, user first create an account with basic information. Then login in it with user id and password. Login user identity and password are case sensitive .using the each information while login, are save at backend i.e. MySQL. And run on apache tomcat server.


http://localhost:8084/code/userpage1.jsp?message

Authorization Framework for Multi-User Data Sharing in Social Networks

Welcome! Ashwa[illegible]

Image
Photo id: 4
You are the owner of this photo

--Select Settings To ShareImage--

Fig. 5. Framework for Access Control on Sharing an Image

When the user register with basic information, it save the information to MySQL. Every pattern behaviour of user is represent the activity of the live user so that data regarding user is store in database and pattern should be with them on every activity log of the user [4]. The new user can send the request to the existing user, existing user can view the request for approval. User can upload the image on wall and set the timestamp to each post content. And whenever any user friends wants to share that content on wall ,the request goes to owner of the content on the wall.

## VI. CONCLUSION AND FUTURE WORK

In this paper, we propose unique authorization model for facility of collective management of share data in social network. We have given the analysis on multiple user on share data that can secure the identity information from the malicious user. We have describe here multiple user access control model on the basis of proof of concept of social network that can give secure user friendly platform to the each user.

Our future work, the effective automated face recognition model for recognize the face from photo where the photo containing image of tag user .It is use when tag remove from photo but content remain in photo , the automated face recognize the face from photo is more effective.

## REFERENCES:

1) Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen." Multiparty Access Control for Online Social Networks: Model and Mechanisms", IEEE transactions on knowledge and data engineering, vol. 25, no. 7, July 2013.

2) 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, 2006.
3) 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.
4) 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.
5) 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.
6) E. Carrie, “Access Control Requirements for Web 2.0 Security and Privacy,” Proc. Workshop Web 2.0 Security & Privacy (W2SP), 2007.
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) 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.
9) H. Hu, G.-J. Ahn, and J. Jorgensen, “Enabling Collaborative Data Sharing in Google+. Technical ReportASU-SCIDSE-12-1, http:// sefcom.asu.edu/MUC/MUC+.pdf, Apr. 2012.
10) 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.
11) Facebook developer,
http://developers.facebook.com/, 2013.
12) Facebook Privacy policy,
http://www.facebook.com/policy. Php/, 2013.
13) Facebook Statistics,
http://www.facebook.com/press/info. Php? Statistics, 2013.
14) Google+ Privacy Policy,
http://http://www.google.com/intl/ en/+/policy/, 2013.
15) The Google+ Project,
https://plus.google.com, 2013.
16) Social Network Techniques,
http://www.alltechbuzz.net/2013/11/tag-all-your-friends-in-single-click.html
17) Chat Encryption,
http://abine.com/facebookFAQ.php/,2013.