AUTHORIZATION MECHANISM FOR MULTIPARTY DATA SHARING IN SOCIAL NETWORK

Ashwajit Ramteke[1], Girish Talmale[2]

[1]*M.Tech Scholar, Department of Computer Science and Engineering, G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India*

[2]*Assistant Professor, Department of Computer Science and Engineering, G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India*

Abstract

In recent year, most popular websites are social media, it has tremendous growth take in consideration as a fast network to connect a people and thus it's give idea of overload of millions of internet user. These social network offer to carry out desirable means for digital social inter connection and information involvement, but also come again a number of security and privacy problems. 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 carry out an approach to allow the protection of shared data accompanying with multiple users in social network. We gives a stand to user to share their data in protected manner. We also discuss a proof-of-concept prototype of methodology as part of a framework on social network and provide usability study and system evaluation of our method.

Keywords: *Social network, multiple user access control, Security mode, Specification and management, Data Sharing.*

----------***----------

1. INTRODUCTION

In recent year, the peoples are come close together due to the fastest internet facility. The communication channel has play an important role to make lesser distance between the people. Networks of the internet are rapidly spread in world wide. Social networking site has more popularity than any other side, out of 100 % people, near about 60% people are login at a time with social media. 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').because these sites are more trusted sites.. These information are most of contain of user basic identity of the user. Some sites also take into consideration to allow the user for their likes and dislikes such as interests, hobbies, favorite's books or films, and even relationship status. Thus, this is not secure to expose their identity in anywhere in the untrusted web media. On the basis of literature survey on social media, we consider two social site that have more similarity identity in between their personal information and photos which is overlapping the identity of same user [9]. In recent year, study has been done on the survey of social media, we analyses near about 250-300 profile of random user , It was found that 85% profile having their real identity , and 60% profile giving their genuine photograph for identification of user via face recognition system[9][10]. Most of the user had not modify their basic information (the default setting originally agreed friends, friends of friends, and non-friends of the similar network to have full view of a user's profile). The natural human being can block the profile of the other user if he don't want, and would therefore come into the picture not to be usually used for a wide number of people. So that user can't be determine which security feature that they want to use. Facebook was disapproved due to the perceived tolerance regarding privacy in the default setting for users. Data sharing on social network is more flexible .but main important thing is that data is going to be in secure manner. there is no of feature in social media for users to partaking messages, invitations, photos, open dais applications and other applications are often the platform for others to gain access to a user's private information. A typical online social web access is give platform for each user to give up their data over the virtual space enclosing 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 photo tagging is the important feature in social media that contain link of each user which are appear in the photo. For the security of user data, existing system gives indirect security environment for each user [6]. In this paper, we create one framework that gives direct security environment for each user to protect data from such existing issue. We begin by examining how the lack of multiple random 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 know the conceptual study of two fundamental. First, we want to deep theoretical study of social media like Facebook, twitter and find out the challenges with respect to user pattern recognition. Second, we want to over simplify 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 recognizably different access control mechanism, so that Facebook is one can be best generalise model to show our derive implementation over social network.

2. RELATED WORK

Access control for OSNs is still a relatively new research area. Several access control manage models for OSNs have been presented. Early access control manage solutions for OSNs presented trust-based right to use manage encouraged 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.

S. Kruk, S. Grzonkowski introduced a technique is D_FOAF system. In recent growth of world, each person has sole identity feature including their basic information working area .Some credential information is also share via social services. But such information is more dangerous 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. Author recommended that how sensitive information can protect from malicious 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 of having unique identity having large number of data 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 (web-based social networks), where policies are expressed as constraints on the type, depth, and trust level of alive relationships [3]. The method for rule access control manage model which allows the specification of access rules for online resources. The random number of 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 data contain on social network [3]. Author modify a flexible right to use manage model and a related enforcement mechanism for controlled sharing of information in WBSNs. The model and mechanism 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 access manage that formalizes and generalizes the access control mechanism executed in Facebook, admitting arbitrary policy vocabularies that are based on theoretical graph properties [5].Gates described relationship-based access control 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 conclusions 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 examines all the possible mechanism and formulate one model and mechanism that is known as access control model for multiple user in OSNs.

3. MULTI USER ACCESS CONTROL SPECIFICATION

From base of survey of recent work, we have study the paradigm of about security challenges in social network. So that, when the number of user access their user page and wants to secure their content on profile like post ,comment, image content 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.

3.1 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 particular account. Each information and credential info are also can be access by user on the trust of owner.

3.2 Owner

We simplify the idea of owner like, if user X wants to upload an image in his account so that user X is owner of the image. Similarly concept of text, if user X 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.

3.3 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 granting the permission 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.

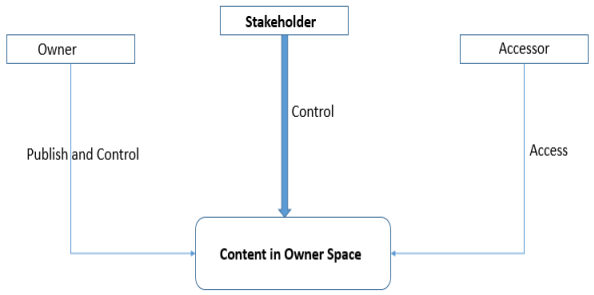

Fig-1: Multiple stakeholders can shared a content.

3.4 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 [12]. Contributor play an important role in posting wall's content.

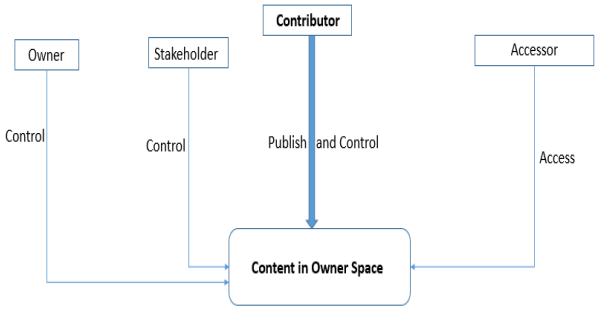

Fig-2: A shared content is published by a contributor

3.6 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].

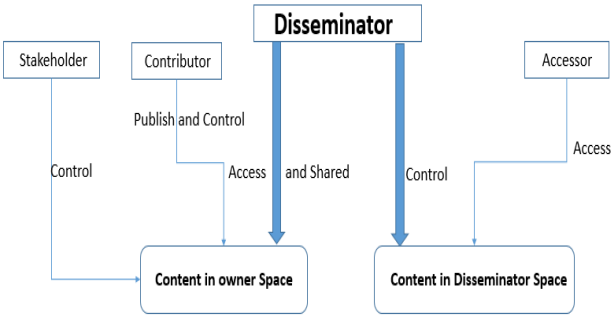

Fig-3: A desseminator Shared other's content published by a contributor

3.7 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.

4. DECISION MAKING SCHEME FOR MULTIPARTY

Voting scheme is popular concept for decision making in social media. Encouraged by such a decision-making mechanism, we recommend a voting scheme to achieve an effective multiple user conflict determination for social network. An important 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 [2]. Our voting scheme contains two voting mechanisms:
1). Decision Voting
2). Sensitivity Voting.

4.1 Decision Voting

A decision voting (DV) scheme is based on policy evaluation of social network, where evaluation (E) calculate of the basis of policy [1],

DV= {0 if evaluation (E) =Deny
DV= {1 if evaluation (E) =Permit

Consider that all controllers are equally significant, an aggregated decision value DV(agg) (choosing a range of 0.00 to 1.00) from multiple controllers with the owner DV(ow), the contributor DV(cb), and stakeholders DV(st) is calculated with following equation [1]:

$$DV\ (agg) = (DV\ (ow) + DV\ (cb) + \sum_{i=ss} DV\ (st)) \times 1/m$$

Where SS is the stakeholder set of the shared data item, and m is the number of controllers of the shared data item. Controller of shared data have some significant 1) a different trust level over the data owner and 2) a different Status value in terms of co-operative control. Thus, a simplify decision voting scheme needs to introduce weights, which can be computed by aggregating trust levels and character values, on different controllers. Different weights of controllers are essentially represented by different importance degrees on the aggregated decision.

4.2 Sensitivity Voting

Sensitivity level (SL) assign to each controller to the shared data item to reflect her/his privacy concern. Sensitivity score is more useful to calculate sensitivity level of each user. Voting decision is made on the basis of user sensitivity score. A sensitivity score (SC) (in the range from 0.00 to 1.00) for the data item can be computed based on following equation [8]:

$$Sc = (SL\ (ow) + SL\ (cb) + \sum_{i=ss} SL\ (st)) \times 1/m$$

Note that we can also use a global sensitivity voting scheme like DV (agg) to compute the Sc.

5. SECURITY ENVIRONMENT IN SOCIAL NETWORKS

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

5.1 Secure Massaging

In existing social network like a Facebook. Facebook is most popular social networking where the number of random user are online at the same time. Multiple user send a massage to one another who are in their friend list. When one user send "hello" to another user, first it received to trusted third party like Abine. But it's more harmful to our private massaging [17]. If we send any credential information to another user, any malicious user can attack on it and our information is leaks. Hence we create one secure chatting where massage directly goes to sender to receiver via admin of network only. And our content is secure [14].

5.2 Doc File Attachment

In the recent survey of social network like Facebook, Twitter, the number of images, content can upload, shared from the one user to another user .but we can't send file in this format like txt, doc, ppt, hmtl, etc. we provide platform of each user that he can share and download the file easily [11].

5.3 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]. The number of account holder in social network wants to highlight the content in their friend wall. Hence we provide automatic tag for image in which that image directly tag with all friends wall and the each user can see the wall content which are tag by their friend.

5.4 Time Control

If the user wants to post some content, upload an image and posting some blog but for some particular time period, each user set time stamp for content. When user set expiry date and time for the post.it refers only 24hrs clock time .and post content, content can automatically remove from friend's wall. This provision is only for securing credential information or any private blog in their user space.

6. IMPLEMENTATION AND EVALUATION

To inaugurate the probability 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, introduce multiple user authorization framework platform. Framework exhibit the security issue which are currently handle this issue by social network. And the security is major problem which is overcome by our model .we create one registration platform for identification of human being not robot. Then he can upload one profile photo and provide some basic information for further process. In this project, we execute total five module. They are as accessor, owner, contributor, stakeholder, and disseminator [8]. It gives fine strength of user friendly platform to make very easier to user. Multi-User access control framework model is deployed as an autonomous 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].

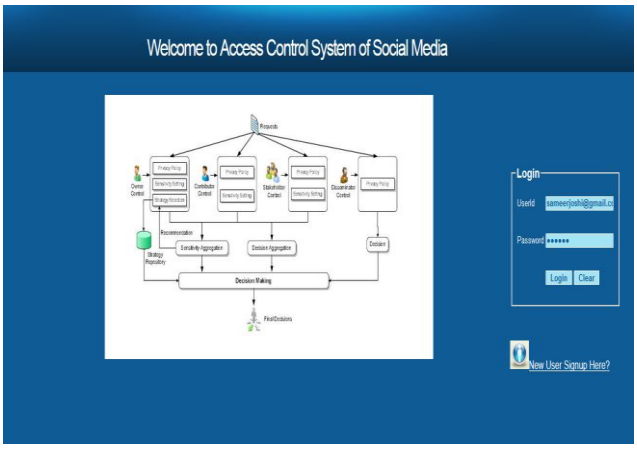

Fig-4: Control for User Authentication

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.

Fig-5: Framework for Access Control on Sharing an Image

In above figure, user can upload an image to his wall and after uploading an image we set some policy and look up to privacy concern that our image is secure from other user. Our policy management and privacy for each image is changing the total security management of the content as compare to existing system because we giving the centralise platform for each user that can sender and receiver are also used to it.

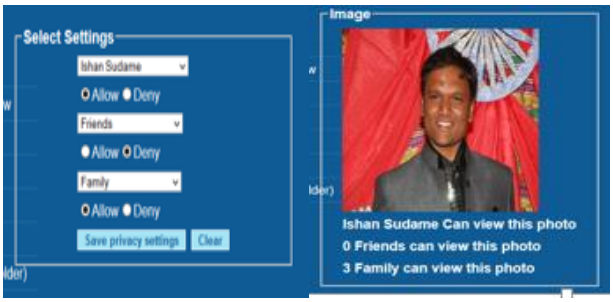

Fig-6: Policy Management and Privacy Setting for Image.

When the user register with basic information, it save the information to database MySQL. Every pattern behaviour and performance management of user is represent the activity of the live user so that data regarding user is store in database and pattern should be keep 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.

7. CONCLUSIONS AND FUTURE WORK

In this paper, we propose exclusive access control 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 and they keep their social data very private on the network. Our future work, the supervise 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.