ISSN No. 0976-5697

Volume 4, No. 11, Nov-Dec 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Anonymization for Social Network Data using Multi-Party Access Control Mechanism

N.Madhuri
Student, CSE, Vignan's Institute of Engineering for Women, AP, India,
madhuri.natha@gmail.com

S.Ram Prasad Reddy
Associate Professor, CSE, Vignan's Institute of Engineering for Women, AP, India,
reddysadi@gmail.com

S.Kalyani
Asst Professor, IT,
Vignan's Institute of Engineering for Women, AP, India,
vishal_mohi@yahoo.co.in

Abstract: Social Networking sites at present have recorded phenomenal growth rates, as they offer attractive means for digital social interactions and image sharing, but also raise a number of security and privacy issues. While Social Networks allows users to restrict access to shared content, right away they do not provide any mechanism to enforce privacy concerns over images associated with multiple users. In this paper, we present an approach for assessing the privacy risk of sharing anonymized images in network giving access to the trusted users. This leads us to show how effectively anonymization is done providing privacy for images and comments posted in public and private. To attain our approach we originate an access control model to capture the essence of multiparty authorization requirements, along with a Multi-party Access Control Mechanism. Friends in an online community designed to make social life more active and stimulating. They share images among themselves and friends comment the images, this has become the fastest growing travel and lifestyle social networking community portal and to keep your friends and family informed of your where about movements and activities. We have used the MPAC model to achieve our goal by providing anonymization for the images posted in the Social Network by individual users and also providing high level privacy for the comments below the images posted.

Keywords: Social Network, Anonymization, Multi-party access control, privacy, Comments.

I. INTRODUCTION

Social Networks such as Facebook, Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, colleagues, family and even with strangers. In recent years, we have seen unrivalled growth in the application of Social Network [4].Users publish their information publicly without any consideration and most users are not aware of the Social Networks features. In a small thesis study, it has been found that none of the 10 study participants used social Networks to control their privacy settings. To protect user information, access control has become a central feature. A typical social network provides each user with a virtual space that contains profile information, a list of the user's friends, and web pages, such as a Facebook wall, where users and friends can post content and leave messages. A user profile generally includes information with respect to the user's date of birth, gender, education and work history, and contact information. Furthermore, users can not only upload images into their own or others spaces. For the protection of user data, current social network indirectly require users to be system and policy administrators for regulating their images, where users can restrict image sharing to a specific set of trusted users. Social Networks often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends, groups or public to access their data, depending on their personal authorization and privacy requirements.

Although social network currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, woefully, have no control over images residing outside their spaces [3]. For example, if a user posts a comment in his friend's space, she/he cannot specify which users can view the comment. In another case, when a user uploads a photo with his friends, who also appearing in that photo, the friends in the image cannot restrict who can see this photo, even though the friends of him may have different privacy concerns about the photo. To address such a critical issue, prior protection mechanisms have been offered by existing social network. For instance, Facebook allows users to remove the images 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 methods 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 exists in the photo. Since normal access control mechanisms cannot be changed, the user's image continues to be revealed to all authorized users. On the other hand, reporting to Social Network only allows us to either keep or remove the content. Such a binary decision from Social Network managers is either too loose or too restrictive, depending on the Social Network's administration and requiring several people to report their request on the same content. Hence, it is essential to develop an effective flexible access control mechanism for Social Network, accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively.

The social networks we study here exist within the databases of on-line social networking sites. However, different online social networks are enforced as overlay networks. Social Network has gradually expanded the idea of social graph to so-called Open Graph as it launches new services such as photos and places, and includes these in the graph over time [5]. For instance, the graph formed by people who exchange email, or the graph formed by a network users who include each other in their friends list can be viewed as another social network on top of the Internet. Understanding the structure of on-line social networks is not only critical to understanding the strength and security of distributed on-line social networks, however additionally understanding their impact on the long run Internet.

II. RELATED WORK

A social network describes entities and connections between them. The entities are often individuals; they are connected by personal relationships, interactions, or flows of information. Social network analysis is concerned with uncovering patterns in the connections between entities. It has been widely applied to organizational networks to classify the influence or popularity of individuals and to detect collusion and fraud [2]**.** Most Social networking users share large amount of private information in their Social Network space. This information ranges from contact details, images, comments etc. Hence Social Networks contains a large pool of sensitive data. Anonymization is the most privacy issue in Social Networks. The study of techniques to allow better anonymization of sensitive data has been ongoing for many years. This has a long history in statistical areas, since census, survey, Social Network data should not reveal personal information about the participants. Methods based on cryptography give strong privacy guarantees, but have not been shown to be sufficiently scalable for the content publishing scenario in social Networks [1]. Due to the popularity of social networking services, there has been great interest in studying the structures and features of users interaction, and implications this has for the transmission of information and users ideas. This led many to ask how best to post content without compromising the privacy of the individuals who intended their details to be shared only with their social network friends.

Considering these issues 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 Social Network. Our model also contains a multiparty policy specification scheme [6]. The correctness of implementation of an access control model is based on the premise that the access control model is valid. Moreover, while the use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in Social Networks, it may potentially reduce the certainty of system authorization consequences due to the reason that authorization and privacy conflicts need to be resolved elegantly. Assessing the implications of access control mechanisms traditionally relies on the security analysis technique, which has been applied in several domains (e.g., operating systems, trust management, and role-based access control). In our approach, we additionally introduce a method to represent and reason about our model in a logic program. In addition, we provide a prototype implementation of our authorization mechanism in the context of Facebook. Our experimental results demonstrate the feasibility and usability of our approach.

III. OBJECTIVE

Our application allows multiple associated users to specify their authorization policies and privacy preferences to manage a shared image. It is worth noting that our current implementation was restricted to handle photo sharing in Social Network. Our approach will be generalized to deal with other kinds of data sharing and comments, in Social Network as long as the users of shared data are identified with effective methods. The proposed system shows a novel solution for management of shared data in Social Network. A multiparty access control model was developed, in conjunction with a multiparty policy specification scheme. There is a method for deny Access for Private Access Sharing of data in Access Control Methods and also a method for handling Multi Access Control for Storage of data or sharing the resources. Our goal is to enable the useful analysis of social network data while protecting the privacy of individuals. There is high secrecy in maintaining comments of one user to other user. Our implementation predominantly focuses on the subsequent features.

a. No one can view other's profile until he/she accept the friend request with none privacy settings applied i.e.by default.
b. Images posted on user's wall can be viewed by his/her friends only but not by their friend's friends.
c. Limiting the comments access to individual users by not permitting others to View Ones Comments, However image is viewed to all his/her friends
d. Deny Access to view data for whom we don't like to show our data in Private Access Control i.e., choosing specific person to whom we wish to relinquish access to view the image.
e. Providing a facility for requesting multiple persons in our site to join as a friend or Family relations at the time of acceptance.

These features are associated with different modules to attain anonymization for social network data using multi party access control mechanism. The Modules in our approach are Authentication i.e., Login and Registration, Finding People on network, Uploading Images in Private and Public, My posts, My Friends List and we concentrate on the comments related to images posted by the user and the reply to the comment.

IV. MULTIPARTY ACCESS CONTROL MODEL

We formalize a Multiparty Access Control (MPAC) model for Social Network, as well as a policy scheme and a policy evaluation mechanism for the specification and enforcement of MPAC policies in Social Network.

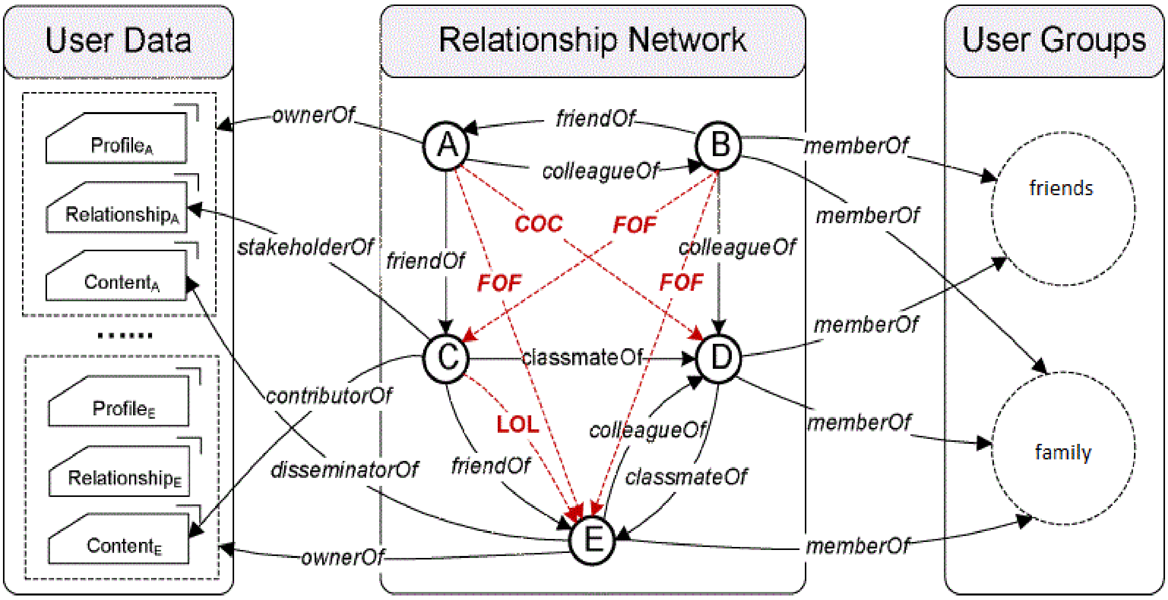

Figure 1: Representation of a Multiparty Social Network

Fig.1 shows a Social Network that can be represented by a relationship network, a set of user groups and a collection of user data. The relationship network of a social network is a directed labeled graph, where every node denotes a user and every edge represents a relationship between two users [4]. The label related with every edge indicates the sort of the relationship. Edge direction denotes that the initial node of an edge establishes the relationship and the terminal node of the edge accepts the relationship. The number and type of supported relationships rely on the specific social network and its purposes. Besides, Social Networks include an important feature that allows users to be organized as a list of friends. This feature enables users of a Social Network to easily find other users with whom they might share specific interests, demographic groups (e.g., studying at the same schools), political orientation, and so on. Furthermore, Social Network provides each member a Web space where users can store and manage their personal data including profile information, friend list and content. Recently, many access control schemes have been projected to support fine-grained authorization speci fications for Social Networks. Unfortunately, these schemes can only permit a single controller, the resource owner, to specify access control policies. Indeed, flexible access control mechanism in a multi-user environment like Social Network should allow multiple controllers, who are associated with the shared data, to specify access control policies. As we identified previously in the sharing patterns, in addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, ought to regulate the access of the shared data as well. We define these controllers as follows:

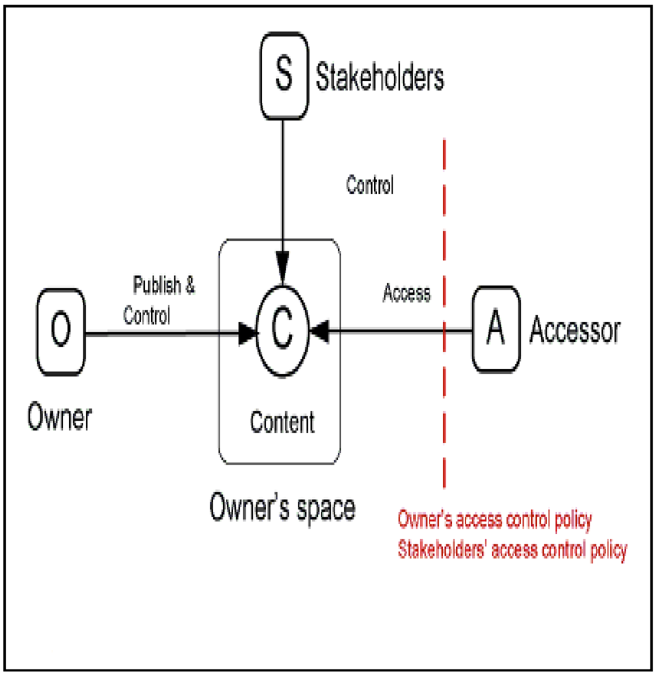

Figure 2: A shared data item with multiple Stakeholders

a. ***Owner:*** Let d be a data item in the space of the user u in the social network. The user u is called as the owner of d.
b. ***Contributor***: Let d be data item published by the user u in someone else's space in the social network. The user u is called the contributor of d.
c. ***Stake Holder:*** Let d be the data item in the space of the user u in the social network. Let t be the set of users associated with d. A user u is called the stake holder of d. if u Є t [7].

A. MPAC Policy Specification:

To enable an authorized management of data sharing in social network, it is essential for multiparty access control policies to be in place to regulate access over shared data and images, representing authorization requirements from multiple associated users [3].

a. Accessor Specification: Accessors are a set of users who are granted to access the shared data. Accessors can be represented with a set of user names, a set of relationship names or a set of group names in Social Networks [6].

b. Data Specification: In Social Networks, user data is composed of three types of information, user profile, and user relationship and user posts [6]. To facilitate effective privacy conflict resolution for multiparty access control, we introduce sensitivity levels for data specification, which are assigned by the controllers to the shared data items.

c. Relationship sharing: Relationships are inherently bidirectional and carry potentially sensitive information that associated users may not want to disclose [6]. Most Social Networks provide mechanisms that users can regulate the display of their friend lists. A user, however, can only control one direction of a relationship.

B. Multiparty Policy Implementation and Evaluation:

A concept of social networking application is implemented here for the collective management of shared images and content known as MController. This application allows multiple associated users to specify their authorization policies and privacy preferences to control a published data item. MController architecture is divided into two major parts, Social Network Server and application server, The Social Network server provides an entry point via its application page, and provides references to photos, friends, and feed data through API calls. Social Network server accepts input from users, then forwards them to the application server [6] .The application server is responsible for the input processing and collaborative management of shared data. Information related to users such as friend lists, groups, posts, are stored in the application database. When a request to access is made to the decision making portion in the application server, results are returned in the form of access to photos or proper information about access to photos and comments.

MController is developed as third party application, which is hosted in an Apache Tomcat application server supporting HTML, JavaScript and MySQL database. MController application relies on the iFrame external approach. Using the JavaScript and HTML, it accesses user's data through the Graph API and query Language [6]. It can retrieve the list of photos, which are owned or uploaded by the user. Once the information is imported, the user accesses MController through its application page, where she/he can query access information, set privacy for photos that he/she ia a controller or view which are allowed to access.

The core component of MController is the decision making module, which processes access requests and returns responses for the requests. To evaluate an access request, the policies of each controller of the targeted image are enforced first to generate a decision for the controller. Then the decisions of all the controllers are aggregated to yield a final decision as the response of the request.

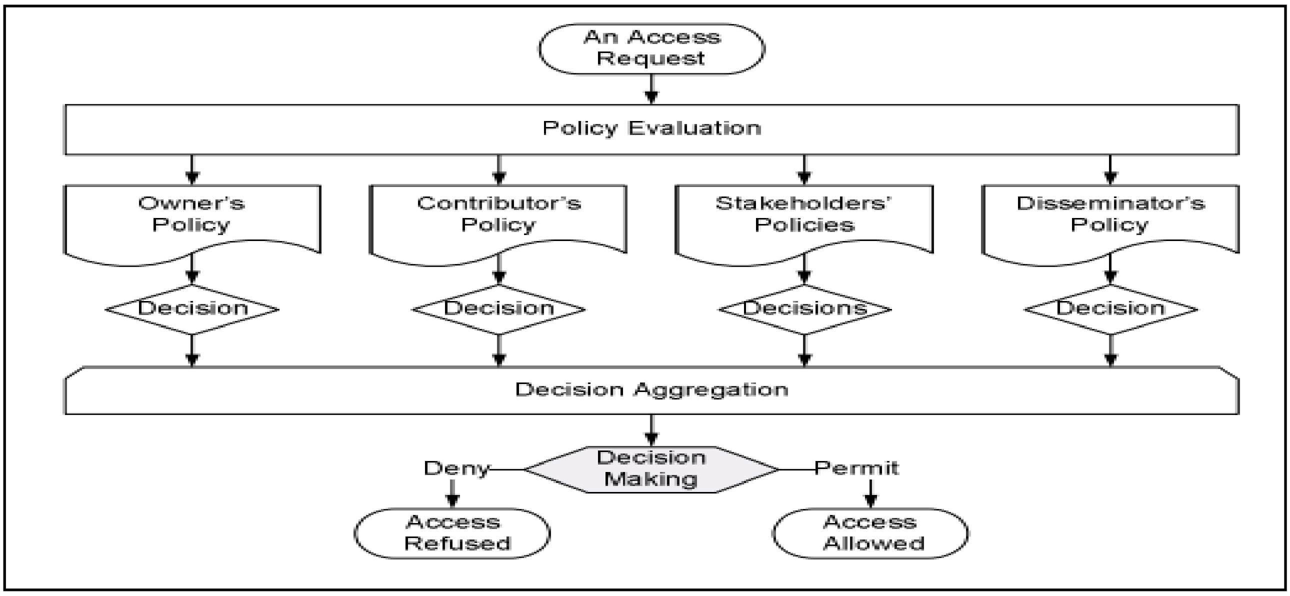

Figure 3: System architecture of Decision making in MPAC

Two steps are performed to evaluate an access request over multiparty access control policies as shown in Fig.3. The first step checks the access request against the policy specified by each controller and yields a decision for the controller. The accessor element in a policy decides whether the policy is applicable to a request. If the user who sends the request belongs to the user set derived from the accessor of a policy, the policy is applicable and the evaluation process returns a response with the decision (either permit or deny) indicated by the effect element in the policy[6]. Otherwise, the response yields deny decision if the policy 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.

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

We present the following components in our approach A *user* represents a human being registered in a Social Network system to whom authorization may be granted. Users maintain relationships with each other, own a number of resources, and perform various kinds of actions against resources and users in the system and *Session* is an active instance of a user who has logged into the OSN. Accessing users perform access through sessions [5].*Authentication* of the users is the primary factor in social network. It is done by filling the registration form with his/her details like name, email id, date of birth, gender, school, college, and occupation which are stored in the database. After submitting the form, user is said to be a member in the network. User registered in the network should be logged in and logged out to access his account.

Finding people in network is our next modules where we can search our friends and in this module user select friend to send request. Users who logged in can view request and accept to add them into their list. User can`not enter into his/her friend profile until it is approved. Friend Request is a module where users can find his/her requests sent by his friends they can accept them if he wishes or ignore them if they don’t want to add them. Immediately after confirming the request we need to choose the relation with the user who had sent you the request.

Posting the image on the wall is one of the modules, where it can be done in two ways public and private. Everyone can view the images posted in public, but private images can be viewed by the specific users to whom the access is given. And most important is limiting the accessibility of comments posted to the image, no one other than the owner of the image and user who posted the comment can view them.

Friends List is the list where all the user friends are placed whom we like to add and give access. By clicking on the profile picture we can view the details of the user like date of birth, school, college information etc.

Privacy for Comments this is the main module where our paper focuses. Users in the network can view the images posted by their friends in public and comment them, here we are limiting the access control i.e., only the owner of the picture can view his comments and can reply to the user individually. Only the user to whom the reply is sent can view the reply.

In our multiparty access control approach we guarantee the privacy for the comments and their replies. We can say that the anonymization is done when the users interact with each other. Communication between the users is said to be end to end, i.e., authenticated users cannot view the comments posted about the image, even though there is a relationship among users.

V. CONCLUSION

Social Networks have necessary implications for our daily life. Privacy and Security issues are increasing day by day and many of the privacy concerned issues are to be resolved. In our paper we have come up with multiparty access control approach to resolve a problem associated with the privacy of the images posted by each individual in their Social network space and their comments posted below the image. We have focused exclusively on the user image and comments. Many of the sites allow these comments to be posted in public where there is no privacy to comments. Limiting the access to the users by giving control only to specific users is one major feature.

VI. FUTURE ENHANCEMENTS

Online social networks are websites that permits users to build connections and relationships to other Internet users. Social networks store information remotely, rather than on a user’s personal computer. Social networking can be used to keep in touch with friends, create new contacts and find people with similar interests and ideas. For the further development of Social Networking sites we can also provide the privacy to documents and videos that are shared among users securely. There is lot of scope to work on the privacy of social networking sites as they are playing lead role in present generation.

VII. REFERENCES

[1]. Bhagat, Smriti, Graham Cormode, Balachander Krishnamurthy, and Divesh Srivastava. "Class-based graph anonymization for social network data.", Proceedings of the VLDB Endowment 2, no. 1 (2009): 766-777.

[2]. Hay, Michael, Gerome Miklau, David Jensen, Philipp Weis, and Siddharth Srivastava, "Anonymizing social networks." , Computer Science Department Faculty Publication Series (2007): 180.

[3]. Hu, Hongxin, and Gail-Joon Ahn. "Multiparty authorization framework for data sharing in online social networks.", In Data and Applications Security and Privacy XXV, pp. 29-43. Springer, Berlin Heidelberg, 2011.

[4]. Kun Liu, Kamalika Das, Tyrone Grandison, Hillol Kargupta, “Privacy-Preserving Data Analysis on Graphs and Social Networks”-2008, qbic.almaden.ibm.com.

[5]. Cheng, Yuan, Jaehong Park, and Ravi Sandhu. "Relationship-based access control for online social networks: Beyond user-to-user relationships.", Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom), IEEE, 2012.

[6]. Hu, Hongxin, G. Ahn, and Jan Jorgensen. "Multiparty access control for online social networks: model and mechanisms." (2012): 1-1, ieeexplore.ieee.org.

[7]. Rao, N. Venkateswara, K. Mehar Prasad, and Y. Ramesh Kumar, "Analysis of Online Social Networks–Study on Multiparty Access Control Mechanism."Analysis-2, no.11, (2013).