Secure Data Distribution Schemes for Online Social Networks

Varsha C
Mtech, Computer Science
Nehru College of Engineering and Research Centre
Pampady, Thrissur, Kerala

Meji Jose
Mtech, Computer Science
Nehru College of Engineering and Research Centre
Pampady, Thrissur, Kerala

Abstract **- Today online social networks play an important role in daily life. There are various online social networks are there and these shows tremendous growth in recent years. These kind of social networks allow users to make social connection with others. Apart from all these there are some security issues or security violations are there. This paper secure data management system simply SDDS focusing on security of data published in social networks as well as problems related with friendship articulation. And also propose the solution for the security issues in online social networks. Along with that checking various access control methods in online social networks and their drawbacks leads to a new method to access control.**

1. INTRODUCTION

Online social networks have emerged has the new way in which people connect socially. Currently twitter, Google+, Likedln counts millions of users. The leader currently being Facebook with over 1.2 billion members. Social networks allow users to make social connection with friends, colleagues and even with the strangers and make digital interaction. All users have their own profile. From which everybody can publish information about themselves. About their likes, favorites, music, books. All these data are articulated from one profile to other profile according to users' privacy settings. A typical social network provides a virtual space like wall in facebook. In which users can upload contents in their own wall as well as in others wall [6], [7], [8].

We can create a list of friends and can create separate privacy settings for each user. Such facility may arise to ambiguous conditions that are described in this paper. All users can upload their photos and allow them to tag the persons who all are appearing in the photo. The tagging act as explicit reference to others profile. The uploaded photos can publish either private, public.

This paper mainly focuses on unauthorized access to the contents and privacy violations of users due to friendship articulation. The lack of privacy may results in malicious attack and results in spreading the content throughout the network without giving value to the original owner of the content. Moreover we discuss about how such policies could be implemented in the social networks. And also solves the problems related with friendship articulation [5].

The structure of the work is the following. After this short introduction we discuss the security issues in the social networks. Next section gives the access control methods in social networks. Afterwards gives a background details about the technique used to solve the problem. Then about the proposed solution for the problem and finally we end up with our conclusions and ideas for future works.

2. THE PROBLEM

Apart from the advantages of social networks there are some disadvantages. The main problem is the leakage of private information's and the violations of privacy settings. All social networks allow users to create friend list which contain number of friends in which users interested to make digital interaction. They can be colleagues, friends, co-workers even strangers. Users can make friend list hide from others. They can either set friend list private or make as public. The privacy violation starts here.

For example user A creates friend list and use a stronger policy that he hide friend list from others and set as private. On other side one of the friends of user A call B creates friend list and use weaker policy that he made his friend list as public. Consider user C common friend of user A and B can still get the relationship between user A and B by looking the profile of user B. That means the privacy settings of user A has no value [1].

Another problem arises in the case of content sharing. Suppose user A uploads a photo and tag who all are appear in the photo and publish the content. In the case of tagged persons view, he can only take a binary decision that he can either delete the photo or request the original owner to remove the photo. This kind of binary decision is either too lose or restrictive. He cannot make any access control over that photo. This paper discussing about the access control methods in online social networks and their drawbacks. And propose a new method to access control in secure way.

3. ACCESS CONTROL METHODS

There are various access control methods in social networks are there. Among all that the former one is the rule based access control for online social networks which is mainly focusing on web based access control. All the social networks can be represented by using a graph. Each node represents a user's profile. Web based social networks are quite larger and each node has a direct connection with other nodes. There is one current social network management that allow each user to state their security level as either public or private. That means specific information has to be shared by the user's with whom the

owner of such information has a direct relationship. Such simple access control methods have the advantage of being straight forward [11].

A common way to repesent a graph by means of graph. This representation can be adopted in case of social networks. Direct and indirect relationship can be represented by means of a graph. Depth of the relationship indicates the depth of the graph means the number of paths. The solution implies that if a user requests a resourse from another user the former recieves from latter a set of access rules regulating the release of requested resources. These rules basically state which type of ralationship should exist between the resource owner and the requestor , nad the maximum and minimum trust level are allowed.

To cope up with these problems, propose a solution that creats a certificate. For each direct relatioship there exist a certificate. Moreover the requestor must provide all the corresponding chains of certifiactes inorder to let him or her to verify the correctness if assertion. This solution is liable to security attacks., that the resorce owner cannot be sure that the requestor has actually provided all the possible chains of certificate or he or she intentionally omiitted some chains of certificates.

To overcome this problem semi decentralized architecture used. According to this a given trusted node referred to as central node , is in charge of managing certificates and of computing the trust level. All the certificates are preserved in a certificate repository. When a requestor requests resource from original owner the central node checks the certificate repository and retrieves the trust level based on the certificate. The system architecture consists of two nodes one central node and preferential node. Other than the central node is called preferential node. Central node in respose for certificate repository storing all the certficates generated by the user networks. In the case of larger social networks the central node become overheaded.

Another method is relationship based access control method. Here poly ralationships are also considering. For example child parent relationship are distinct than patient physician ralationship. Another method is based on public risk management. For example consider popular social network, facebook there is a tick mark on some profile for prooving the genuity of the page [12].

Along with that various access control methods are there in facebook. Among all these the first one is search listing and their reachability. All users will be having one profile and they can create their on friend lists. Sometimes the user set their visibility as either public or private. There are two means by users can reach the profile global name search and social graph traversal. Global name search means searching the profile name by browsing in the search bar in indvidual profile. Social graph traversal indicates that reaching in someones profile and searching the names there.

Currently the users can upload photos and tag the persons who all are appear in the photo. In the case of tagged persons, he or she can take only binary decision. The tagged person can delete the photo or can send a message to the original owner to remove the photo. The problem is if the owner tag more number of persons and all send a request back the owner cannot manage it.

4. THE PROPOSED SOLUTION

This paper finds solution for two problems. The first one is if some users hide friend list from others. That persons should be hidden from others profile too. Addressing to the first problem described in the problem description. For solving the privacy violation occurred due to friendship articulation a stronger protection mechanism should come [1], [5]. If any common friends looking the friend list of others profile. The persons who hide the friend list should be hidden from everyone's profile even though the person is mutual friend of user A and user B. While browsing the public friend list of user B, a mutual friend won't get any relationship about user

TABLE 1. ACCESS CONTROL METHODS

Method	Advantage	Disadvantage
Role based access control mechanism	Data management is done based on relationship type and the depth of the relationship.	Resource owner cannot be sure that the requestor has actually provided all the possible certificates
Enforcing access control in web based social networks	There is central node managing certificates. Each node is free from creating the certificate. These are all done by the central node.	Social networks are growing day by day. And such increase cannot managed by the central node it becomes over headed.
Relationship based access control	Types of relations are identified very clearly and according to this data accessing is done.	Identifying the type of each and every relation makes the system more complicated.
Privacy preservation model for facebook style social networks.	Can list the number of persons restricting from seeing the content to the original owner.	Still the system not providing access control over the shared data for tagged person..

B. That means user B's policy should protect by hiding that person in everyone's profile.

Addressing to the second problem all the photos uploaded in the social network is entering into a gallery where the gallery classifies the photo as tagged or owned photos. A person can upload photo in different style. Figure 1 describes the cases. A user can upload photo as either public or private. By setting the policy as private and given the names of the persons, the original owner and that

person can only view the photo. In the tagged persons part the person can use the access control that he or she can delete the photo.

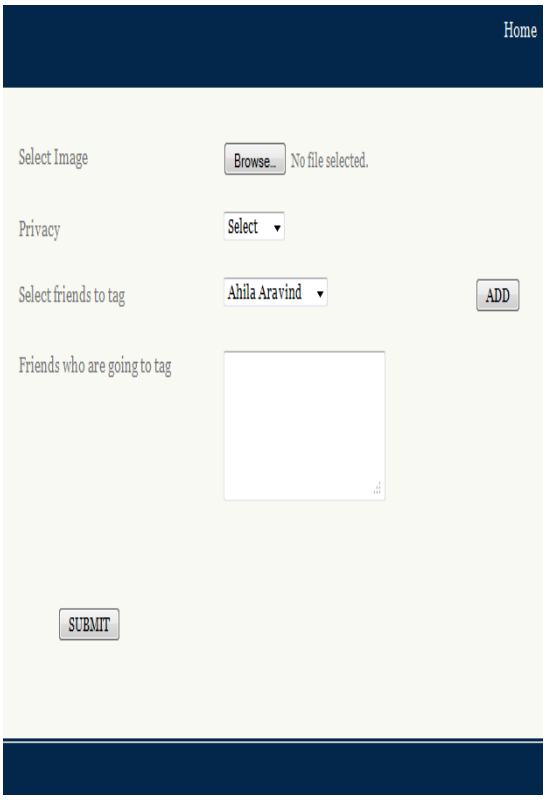

Figure 1. Photo uploading window

By setting the policy as pubic and tag the names of the persons. The photo can view by all the friends of the original owner and the tagged person. In this case the tagged person gets more access control over that photo. Figure 2 gives the access control for the tagged person. In which the first case is untag myself. Which simply delete the photo from the user's wall. Second case is groups to view. In that tagged person can give the name of the groups in which he or she is interested to view the photo. Third case is common friends to remove. In which it groups the common friends of the original owner and the tagged person. By giving the names of the person the tagged person can remove the common friends. The last case is select friends to remove. By selecting the names of the person's the tagged person can remove them from viewing the photo.

By providing such window for tagged person's secure data sharing is possible. The tagged persons can provide their own security policies over that photo.

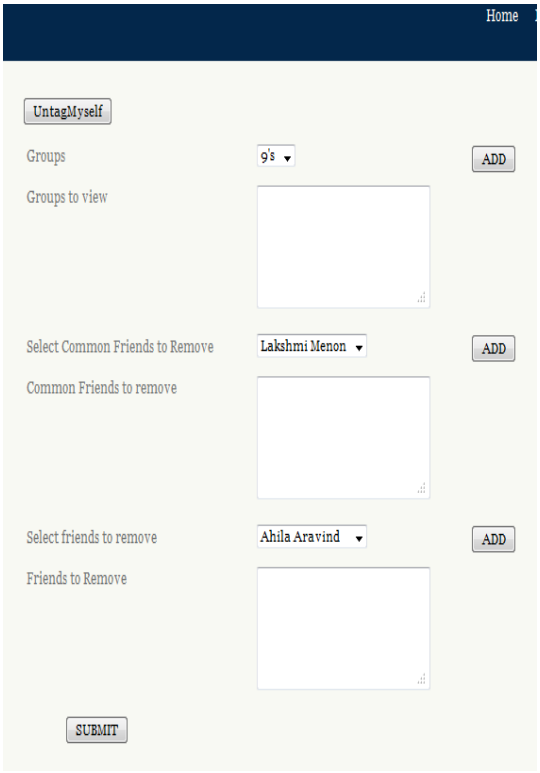

Figure 2. Tagged persons interface

7. CONCLUSION

SDDS is a complete secure sharing scheme for online social networks. Currently the users can only take binary decision over the tagged photo. This kind of binary decisions are either too lose or restrictive. The system SDDS solves such problem by providing access control for the tagged person over that shared data. Thus the tagged persons can set their own access control and security policies over the photo. Thus protect all the privacy policies and makes the system trustworthy. The system provides a collaborative management of shared data.

A wider view on the subject is that focusing more on other security issues and policy violations in the social networks. In future focuses more security issues related with online social networks and also finds a solution to connect two or more social networks by creating a global relation without accessing the database.

10. REFERENCES

1. Gail-Joon Ahn, and Jan Jorgensen "Multiparty Access Control for Online Social Networks: Model and Mechanisms".
2. Athanasios Zigomitros1, Achilleas Papageorgiou "Social Network Content Management through Watermarking". *Proc. International conference*,2012.
3. William Stallings, "Cryptography and Network Security".
4. R. Rives, "The MD5 Message Digest Algorithm", MIT laboratory of Computer Science and RSA Data Security, Inc. April 1992.
5. Philip.W.l.Fong, Mohd Anwar, "A privacy Preservation Model for Facebook Style Social Network Systems".

6. Facebook Developers, http://developers.facebook.com/, 2013.
7. Facebook privacy Policyhttp://www.facebook.com/policy.php/,2013.
8. Facebook statistics,http://www.facebook.com/press/info php?,2013.
9. Ramez *Elmasri*, B. *Navathe*, "Database Management Systems".
10. R.g. Healey,"Database Management Systems".
11. Barbara Carminati, Elena Ferrari, and Andrea Perego, "Rule Based Access Control for Online Social Networks".
12. Philip W. L. Fong, "Relationship Based access Control: Protection Model and Policy Language".
13. Philip W. L. Fong, "Privacy Preservation Model for Facebook Style Social Network Systems".