Security Strategies for Online Social Networks

M.Ebinezer [#1], *B.Suresh* [*2]

[#] *Student & CSE Department*
Mother Theresa College of Engineering, Nunna, India

[*]Professor & CSE Department
Mother Theresa College of Engineering, Nunna, India

***Abstract*— In this decade online social networks (OSNs) have marvelous enlargement per hundred of millions of users on the internet. The internet users are more good-looking about OSNs for information sharing and social interactions. Here a number of security and privacy issues are raised. The online social networks (OSNs) currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. We proposed a comprehensive approach to increase the privacy of shared data associated with multiple users. To increase the privacy the policy is going to use multiparty access control model and policies**.

***Keywords*—** Social networks, PAC model, MPAC policies

I. INTRODUCTION

Online social networks have marvelous growth in recent years. These online social networks offer attractive means for digital social interactions and information sharing. Online social networks such as Face book, Google+ and Twitter These social networks are used to share personal and public information and Make social connection .Face book is a one of the representative social network .And claims that it has 30 billion of users. a list of the user's friends, and web pages, such as wall in Face book, where users and friends can post content and leave messages. A user profile generally include information with respect to the user's birthday, gender, interests, education and work history . In addition, users can not only upload content into their own or others spaces but also tag other users who appear in the content. Each tag is in explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly need users to be system and policy administrators for regulating their data, where users can limit data sharing to a exact set of trusted users. OSNs often use user association and group membership to differentiate between trust and un trust users.

II. PROBLEM DEFINITION

The existing work could model and analyse access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing. In OSNs has been recognized by the recent work provided a solution for collective isolation management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content.

DRAW BACKS OF EXISTING SYSTEM:

For instance if a user posts a comment in a friends spaces she/he can not specify which users can view the comment .When user uploads a photo and tags friends who appear in the photo. The tagged friends cannot restrict who can this photo To address such a problem a critical issue, preliminary protection mechanisms have been offers by existing OSNs.

III. FOR EXAMPLE

Face book allows label users to remove the tags linked to their profiles or report violations asking Face book managers to remove the contents that they do not want to share with the public.However, these simple protection mechanisms suffer from several limitations.On one hand, Removing a tag from a photo can only put a stop to other members from seeing a user's profile by means of the association link, But the user's image is still contained in the photo. Since original access control policies cannot be changed, the user's image continues to be revealed to all authorized users. The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their

work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co- owner may separately specify her/his own privacy preference for the shared content.

IV.OBJECTIVE

In Proposed System we put into practice a proof-of-concept Face book application for the collaborative management of shared data, called MController. Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. Our current implementation was restricted to handle photo sharing in OSNs. Our approach can be generalized to deal with other kinds of data sharing and comments.The proposed system shows a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method. Indeed, a flexible access control mechanism in a multi-user environment like OSNs 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, need to regulate the access of the shared data as well. In our multiparty access control system, a group of users could collude with one another so as to manipulate the final access control decision.

V. ANALYSIS

- **A.** Profile sharing
- **B.** Relationship sharing
- **C.** Content sharing
- **D.** Owner
- **E.** Contributor
- **F.** Stakeholder
- **G.** Disseminator

A. Profile sharing

To provide meaningful and attractive services, these social applications consume user profile attributes, such as name, birthday, activities,and so on. In this case, users can select particular pieces of profile attributes they are willing to share with the applications. At the same time, the users who are using the applications may also want to control what information of their friends is available to the applications

- Since it is possible for the applications to infer their private profile attributes through their friends' profile attributes.
- This means that when an application accesses the profile attributes of a user's friend,
- Both the user and her friend want to gain control over the profile

B. Relationship sharing

Another feature of OSNs is that users can share their relationships with other members. Relationships are inherently bidirectional. Most OSNs provide mechanisms that users can regulate the display of their friend lists. A user however can only control one direction of a relationship. A scenario where a user Alice specifies a policy to hide her friend list from the public.

C. Content sharing

OSNs provide built-in mechanisms enabling users to communicate and share contents with other members. OSN users can post statuses and notes, upload photos and videos in their own spaces, tag others to their contents, and share the contents with their friends. On the other hand, users can also post contents in their friends' spaces. The shared contents may be connected with multiple users.

D. Owner

Let d be a data item in the space of a user u in the social network. The user u is called the owner of d.

E. Contributor

Let d be a data item published by a user u in someone else's space in the social network. The user u is called the contributor of d.

F. Stakeholder

Let d be a data item in the space of a user in the social network. Let T be the set of tagged users associated with d. A user u is called a stakeholder of d, if u 2 T who has a relationship with another user called stakeholder, shares the relationship with an accessor. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated. A shared content has multiple stakeholders.

G. Disseminator

Let d be a data item shared by a user u from someone else's space to his/her space in the social network. The user u is called a disseminator of d.

VI .NEW MPAC MODE

Assessors are a set of users who are granted to access the shared data. Assessors can be represented with a set of user names, a set of relationship names or a set of group names in OSNs. We formally define the access or specification as follows:

• U = {u1…u2} funting is a set of users of the OSN. Each user has a unique identifier;

• G = {g1; : : : ; gn} is a set of groups to which the users can belong. Each group also has a unique identifier;

• P = {p1….p2} is a collection of user profile sets, where pi ={qi1…..qim}; is the profile of a user . Each profile entry is a <attribute: profile-value> pair, qij =< attrj : pvaluej >, where attrj is an attribute identifier and pvaluej is the attribute value;

• RT is a set of relationship types supported by the OSN. Each user in an OSN may be connected with others by relationships of different types;

• R = {r1……rn}; is a collection of user relationship sets, where ri = {si1; : : : ; sim} is the relationship list of a user . Each relationship entry is a <user: relationship- type> pair, sij =< uj : rtj >, where U, 2 RT;

• C = {c1; : : : ; cn} is a collection of user content sets, where ci = fei1; : : : ; eimg is a set of contents of a user i 2 U, where eij is acontent identifier;

• D = {d1; : : : ; dn} is a collection of data sets, where di = pi, ri, ci is a set of data of a user i 2 U;

• CT = {OW,CB,ST,DS} is a set of controller types, indicating owner, contributor, stakeholder, and disseminator, respectively;

• UU = {UUrt1 ; : : : ;UUrtn} is a collection of uni-directional binary user-to-user relations, where Uri _ U _ U specifies the pairs of users having relationship type rti 2 RT;

• UG _ U _ G is a set of binary user-to- group membership relations;

• UD = {UDct1….UDctn} is a collection of binary user-to-data relations, where UDcti _ U_D specifies a set of < user; data > pairs having controller type cti 2 CT;

• Relation members : U->2U a function mapping each user u £ U to a set of users with whom s/he has a relationship
rt€ RT: relation members
(u : U; rt : RT) = {u′ £ U | (u; u′) € UUrt};
• ROR members : a function mapping each user to a set of users with whom s/he has a transitive relation of a relationship RT, denoted as relationships-of-relationships (ROR). For example, if a relationship is friend, then its transitive relation is friends- of-friends (FOF):
ROR members(u : U; rt : RT) = {u′ £ U € relation members(u; rt) _ (£u′ ′ 2 U[u′ ′ 2 ROR members(u; rt)) ^ u′ ROR members;

• Controllers : D->U; a function mapping each date item to a set of users who are the controller with the controller type
ct 2 CT: controllers(d : D; ct : CT) = { 2 U 2UDct};

• Group members : G->2U; a function mapping each group g € G to a set of users who belong to the group: group members
(g : G) = {u £ U j (u; g) € UG};
groups(u : U) = { g€G | (u; g) £ UG};

PRIVACY SURVEYS

Beginning in 1974, Westin conducted over 30 privacy surveys to measure privacy attitudes. Three general categories were used: fundamentalist (high concern), pragmatist (medium concern), and unconcerned (low) . The majority of the participants were either fundamentalists or pragmatists, each year only a small portion of the participants were unconcerned. The most important factor was typically reported to be the ability to control one's own data. The Westin surveys were conducted before OSNs were popular. A more recent study of reputation management (n = 2253) provides additional data about how OSN users manage the data they share. The salient results in regard to our research include the data collected from participants in the 18-29 age group. 44% of participants in this group report they take steps to limit the amount of personal information about them online 71% report they have changed the privacy settings on their pro_le to limit what they share, and 47% delete unwanted comments. These results are in contrast to the long-held belief that users do not act on their privacy concerns.

VII. MODULE DESCRIPTION:

Number of Modules
After careful analysis the system has been identified to have the following modules:
1. Owner Module
2. Contributor Module
3. Stakeholder Module
4. Disseminator Module
5. MPAC Module

1. OwnerModule:

In Owner module let d be a data item in the space m of a user u in the social network. The user u is called the owner of d. The user u is called the contributor of d. We specifically analyze three scenarios—profile sharing, relationship sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviors in collaborative systems has been addressed by the recent work.

2 .ContributorModule

In Contributor module let d be a data item published by a user u in someone else's space in the social network. The contributor publishes content to other's space and the content may also have multiple stakeholders (e.g., tagged users). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor.

3. StakeholderModule:

In Stakeholder module let d be a data item in the space of a user in the social network. Let T be the set of tagged users associated with d. A user u is called a stakeholder of d, if u 2 T who has a relationship with another user called stakeholder, shares the relationship with an accessor. In this scenario, authorization requirements from both the owner and thestakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated. A shared content has multiple stakeholders.

4. Disseminator Module:

In Disseminator module let d be a data item shared by a user u from someone else's space to his/her space in the social network. The user u is called a disseminator of d. A content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content) publishing the content, and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator's space. For a more complicated case, the disseminated content may be further re-disseminated by disseminator's friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviors. Especially, regardless of how many steps the content has been redisseminated, the original access control policies should be always enforced to protect further dissemination of the content.

5. MPAC Module:

MPAC is used to prove if our proposed access control model is valid. To enable a collaborative authorization management control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. Our policy specification scheme is built upon the proposed MPAC model. 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, asset of relationship names or a set of group names in OSNs.

VIII. CONCLUSIONS

To develop secure mechanism to enforce privacy concerns over data associated with multiple users. By using this mechanism contributor share the photo to the particular stakeholders only. And it has another advantage as comments sharing Hence it is essential to develop an effective and flexible access control mechanism for OSNs. Multiparty access model is used for the accessing the users. Multiparty Policy Evaluation Process is used for controlling the access.

REFERENCES

[1] A. Besmear and H. Richter Lip ford. Moving beyond untangling: Photo privacy in a tagged world. In Proceedings of the 28th international conference on Human factors in computing systems, pages 1563–1572. ACM, 2010.

[2] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your ontacts are belonging to us: automated identity theft attacks on social networks. In Proceedings of the 18th international conference on World Wide Web, pages 551–560. ACM, 2009.

[3] B. Carminati and E. Ferrari. Collaborative access control in online social networks. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing (Collaboration), pages 231– 240. IEEE, 2011.