Protecting User Data in Profile Matching in Social Networks

GOTTUMUKKALA VENKATA GOPALAKRISHNA [#1], B.SURYANARAYANA MURTHY [#2],

[#1] MCA Student, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Associate Professor, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak user's privacy if they are allowed to post, comment, and tag a photo freely. In this paper we try to implement the security of our current OSN with three main scenarios like: An image which is uploaded in public profile will be accessed only by the direct friends or family members of that posted user, which is not allowed or accessed by friends of friends or family of family members. In the second scenario we try to give security for the private profile sharing by restricting the users not to access private content by all members who are mutually related. In the third scenario we try to give security for the comments posted for the images by several individuals. Now a day's all the comments can be viewed by each and every one who is connected with that profile, but in our proposed application we try to provide security by restricting un known persons not to access or read others comments posted on user image. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof to enable more security for the social network sites to share the data among several users.

Key Words:

Privacy, Security, Restriction, Online Social Networks, Profile Sharing

I. INTRODUCTION

Online social networks (OSNs) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, co-workers, colleagues, family and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month. To protect user data, access control has become a central feature of OSNs a typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and web pages, such as *wall* in Facebook, where users and friends can post content and leave messages.

A user profile usually includes information with respect to the user's birthday, gender, interests, education and work history, and contact information. 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 an explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs 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.

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.

II. LITERATURE SURVEY

In this section we will mainly discuss about the background work that is carried out in order to prove the performance of our proposed Method. Now let us discuss about them in detail

MOTIVATION

1) My Privacy My Decision: Control of Photo Sharing on Online Social Networks.

AUTHORS: Kaihe Xu

Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. In this paper, we attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Facebook's platform.

2. Privacy Regulation: Culturally Universal or Culturally Specific?

AUTHORS: Irwin Altman

This article examines privacy as a generic process that occurs in all cultures but that also differs among cultures in terms of the behavioral mechanisms used to regulate desired levels of privacy. Ethnographic data are examined from a variety of cultures, particularly from societies with apparently maximum and minimum privacy, and from analyses of various social relationships, such as parents and children, in-laws, husbands and wives. It is concluded that privacy is a universal process that involves culturally unique regulatory mechanisms.

3) What Anyone Can Know: The Privacy Risks of Social Networking Sites.

AUTHORS: David Rosenblum Harvard University

For the Next generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information.

4. Security Analysis of Relationship-Based Access Control Policies.

AUTHORS: Amirreza Masoumzadeh

Relationship-based access control (ReBAC) policies can express intricate protection requirements in terms of relationships among users and resources (which can be modeled as a graph). Such policies are useful in domains beyond online social networks. However, given the updating graph of user and resources in a system and expressive conditions in access control policy rules, it can be very challenging for security administrators to envision what can (or cannot) happen as the protection system evolves. In this paper, we introduce the security analysis problem for this class of policies, where we seek to answer security queries about future states of the system graph and authorizations that are decided accordingly. Towards achieving this goal, we propose a state-transition model of a ReBAC protection system, called RePM. We discuss about formulation of security analysis queries in RePM and present our initial results for a limited version of this model

III. EXISTING METHODOLOGY

In the existing system there is no proper security for the photo sharing in online social networks(OSN) especially in the public, private and comments section.Also there is no concept like M-Controller properly arranged for the photo sharing in the OSN networks.All the existing systems failed in the following things

LIMITATIONS OF THE EXISTING METHODOLOGY

The following are the limitation of existing system. They are as follows:

1. There is no Deny Access for Private Access Sharing of data in existing Access Control Methods. That is sharing option should be removed in the current OSN networks.
2. There is no M-Controller method to restrict the Multi Access in OSN networks.
3. There is no Secrecy in Maintaining Comments of One User to Other User.
4. In the public photo sharing the data is accessed for everyone i.e either for direct friends and mutual friends, which is the biggest problem in the current days OSN networks.

IV. PROPOSED METHODOLOGY

In Proposed System We implemented all the photo sharing securities on Facebook type application which is created on local server, we executed the application on tomcat server and took facebook like sample interface to show the performance of our proposed application. The proposed system mainly applied on three scenarios and if these three scenarios are implemented in current social networks like facebook or any other OSN,there will be advanced security for each and every individual user profiles.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. There is a method for Deny Access for Private Access Sharing of data in Access Control Methods.
2. There is a method for handling Multi Access Control for Storage of data or sharing the resources.

3. There is high Secrecy in Maintaining Comments of One User to Other User.
4. With this proposed Proof –of-Concept Mechanism we achieved Multi Party Access Control.
5. In the proposed system if we upload a photo in public networks,it can be only shared to direct friends not for mutual or Friend of Friends.

IV. IMPLEMENTATION STAGE

Implementation Stage is where the hypothetical structure is changed over into automatically way. In this stage we will partition the application into various modules and afterward coded for arrangement. The application is separated essentially into following 5 modules. They are as per the following:

1) USER REGISTRATION MODULE

In this module the user is registered initially with all his/her basic details and then try to get login into his account.In this module user need to fill all the valid details and all are mandatory for getting registered.

2) USER LOGIN MODULE

Once the user is registered successfully, he /she can enter into their individual accounts by substituting valid user id and password. If the user enters all his details correctly then only he/she can able to login into their account, if not the user can’t enter into their account.

3) SEND FRIEND REQUEST MODULE

In this module once the user after getting login into the system, he/she can able to send friend request to others and once if the other user accepts the request then the two users can become as friends. If the other user doesn’t accept the friend request he/she will be remained always as disseminator by waiting till he accepts the request.

4) ADD POST MODULE

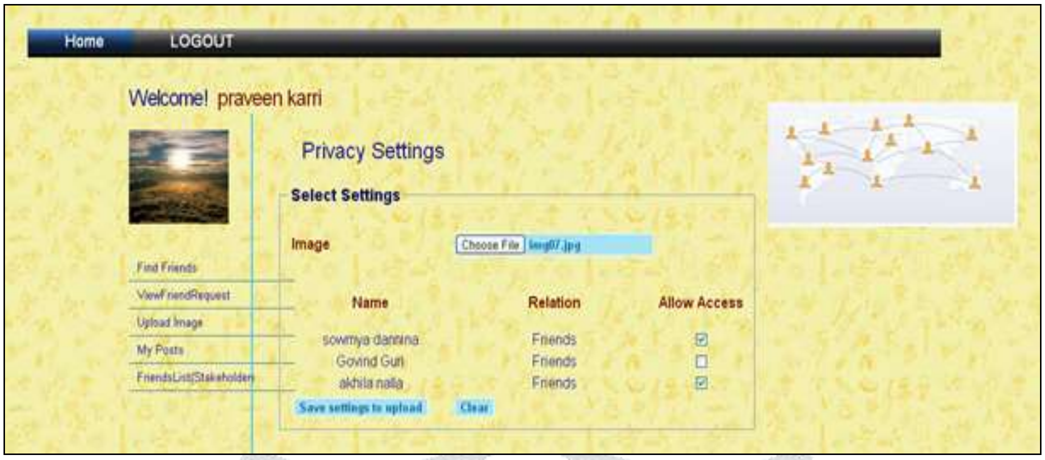
In this module user tries to post the images on his wall. The user who try to post the image or photo in his/her wall is treated as Owner and the user who got access for accessing the owners photo is known as accessor and those who are friends but don’t have access is known as stakeholder. The person who is not added as friends by the owner is treated as disseminator.

5) MULTIPARTY PRIVACY MODULE

In this module the owner can able to post his /her photo and can apply security primitives like public, private and comments

V. EXPERIMENTAL REPORTS

USER SHARE THE PHOTO IN PRIVATE ACCESS



Welcome! praveen karri

Privacy Settings

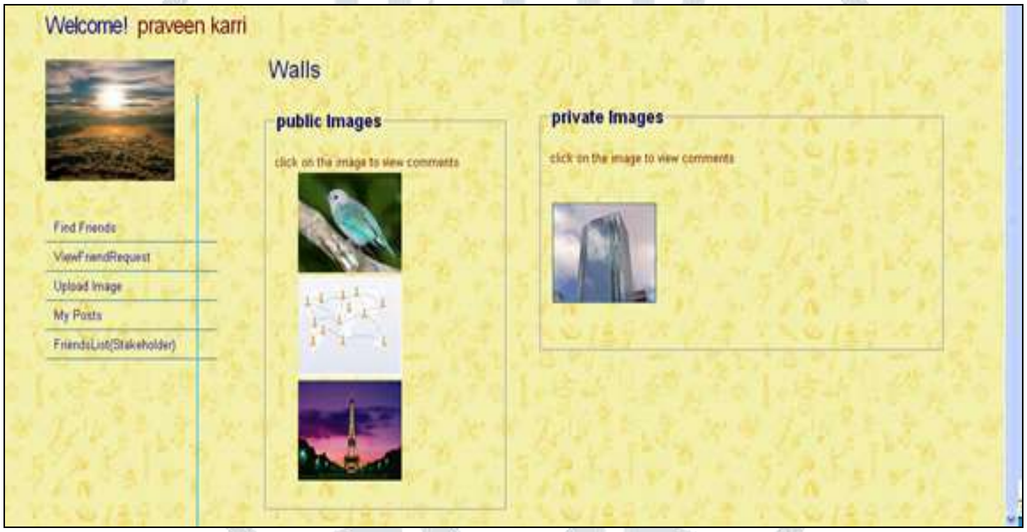
Select Settings

Image: img07.jpg

Name	Relation	Allow Access
sowmya dannina	Friends	☑
Govind Guri	Friends	□
akhila nalla	Friends	☑

Figure .Represents the User is sharing photo in Private profile

USER TRY GIVE COMMENTS ON FRIENDS DATA



Welcome! praveen karri

Walls

public Images

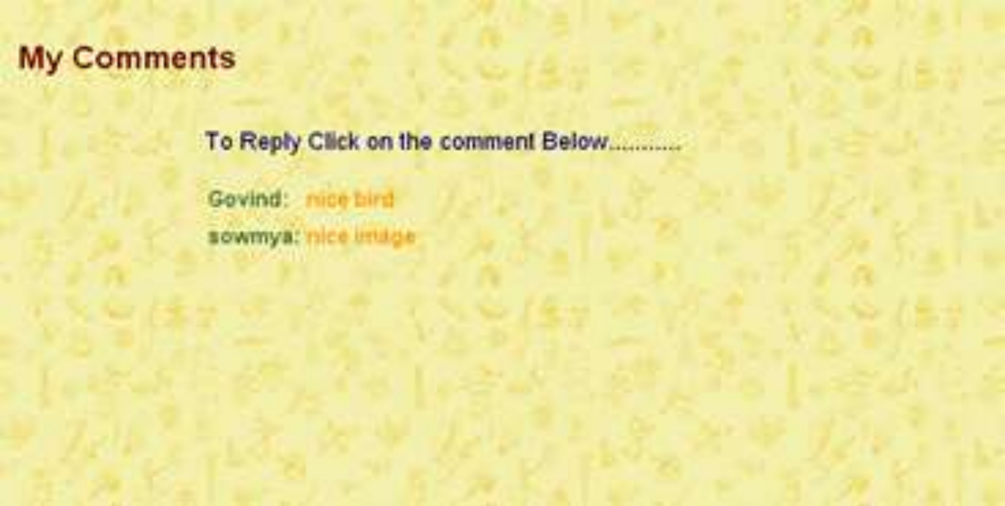
click on the image to view comments

private Images

click on the image to view comments

Figure . Represents the Comments For the Shared Images

USER CAN VIEW ALL HIS COMMENTS FOR HIS OWNER DATA



My Comments

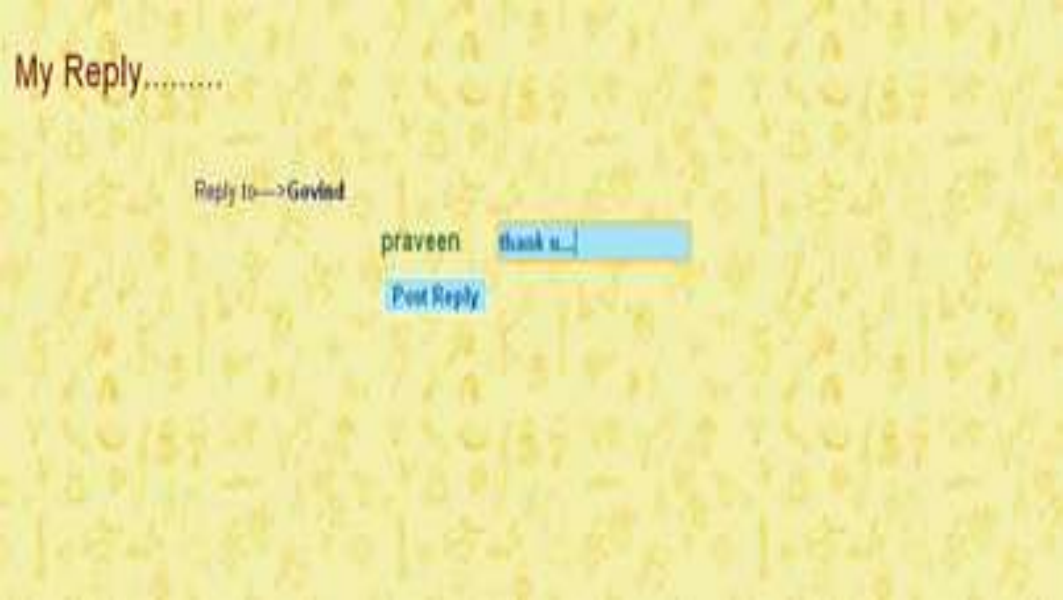
To Reply Click on the comment Below...........

Govind: nice bird

sowmya: nice image

Figure. Represents the User Personal Comments

USER CAN SHARE COMMENT REPLY INDIVIDUALLY RATHER THAN TO ALL



My Reply.........

Reply to--->Govind

praveen thank u..

Figure . Represents the User Personal Replies

VI. CONCLUSION

In our proposed application we try to provide security by restricting un known persons not to access or read others comments posted on user image. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof to enable more security for the social network sites to share the data among.

VII. REFERENCES

1. A. Besmer and H. Richter Lipford. Moving beyond untagging: Photoprivacy 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 contacts are belong 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 Worksharing (CollaborateCom)*, pages 231–240. IEEE, 2011.

4. B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, pages 1734–1744. Springer, 2006.

5. Face book Developers. http://developers.facebook.com/.
6. Face book Statistics. http://www.facebook.com/press/info.php?statistics.
7. Google+ Privacy Policy. http://http://www.google.com/intl/en/+/policy/.
8. Open Social Framework. http://code.google.com/p/opensocial-resources/.
9. The Google+ Project.
10. http://www java.sun.com
11. http://www.w3schools.com