Special Issue on Proceedings of International Conference on Newer Trends and Innovation in Nanotechnology, Materials Science, Science and Technology March 2021. International Journal of Aquatic Science, Vol 12, Issue

# ONLINE MODEL ACCESS THROUGH USER DECISION AND SOCIAL NETWORK

**Dr.S.PathurNisha ,**Professor , Department of CSE, Nehru Institute of Technology

**Mrs. Beaulah David,** Assistant Professor, Department of CSE, Nehru Institute of Technology

**R. Vijaya,** Assistant Professor, Department of CSE, Nehru Institute of Technology

nitcsehod@nehrucolleges.com

Abstract:

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, coworkers, colleagues, family, and even with strangers. A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and webpages, such as wall in Facebook, where users and friends can post content and leave messages. In addition, users can not only upload content into their own or others' spaces but also tag other users who appear in the content. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. To overcome the problem based on Online Social Networks, a systematic solution to facilitate multiparty access control (MPAC) of shared data in OSNs is introduced. The user can share their data or images to their friends. When the user is tried to share other user's data, the request will be send to the owner of the data. After receiving the request, the owner of the data has rights to accept or reject the request. The User can only share other data after getting the approval from the data owner; otherwise the user cannot share that data to others.

## I.Introduction:

Networking is a process that fosters the exchange of information and ideas among individuals or groups that share a common interest. It may be for social or business purposes. Professionals connect their business network through a series of symbolic ties and contacts. Business connections may form due to an individual's education, employer, industry or colleagues. For instance, a business network of Harvard Business School alumni may develop. Networking may also refer to the setting up and operation of a physical computer network.

Social networking is the use of internet-based social media programs to make connections with friends, family, classmates, customers and clients. Social networking can occur for social purposes, business purposes or both through sites such as Facebook, Twitter, LinkedIn, Classmates.com and Yelp. Social networking is also a significant target area for marketers seeking to engage users.

### 1.2 Online Social Network

Online Social Networks have become integral part of our daily life and has profoundly changed the way we interact with each other, fulfilling our social needs–the needs for social interactions, information sharing, appreciation and respect. It is also this very nature of social media that makes people put more content, including photos, over OSNs without too much thought on the content. However, once something, such as a photo, is posted online, it becomes a permanent record, which may be used for purposes we never expect. For example, a posted photo in a party may reveal a connection of a celebrity to a mafia world. Because OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue. When more functions such as photo sharing and tagging are added, the situation becomes more complicated.

## II. Literature Survey

Altman (1977) presented that privacy as a generic process which occurs in all cultures but that also differs among cultures in terms of the behavioral mechanisms used to regulate desired levels of privacy.This article addresses the question posed in the title, namely, is privacy regulation a culturally universal process or is it a culturally specific phenomenon?. A. Besmear and H. Richter Lipford (2010) identified the social tensions that tagging generates, and the needs of privacy tools to address the social implications of photo privacy management. S. Boyd, et. al (2011) argued that the alternating direction method of multipliers is well suited to distributed convex optimization, and in particular to large-scale problems arising in statistics, machine learning, and related areas.Carminati et al (2006) aims to understand the impact of security, trust and privacy concerns on the willingness of sharing information in social networking sites. Using an online questionnaire, empirical data were collected from 250 Facebook users of different age group over the time period of 4 months.J. Y. Choi et al (2011) demonstrated that the proposed collaborative FR method is able to significantly improve the accuracy of face annotation, compared to conventional FR approaches that only make use of a single FR engine. Further, the collaborative FR framework has a low computational cost and comes with a design that is suited for deployment in a decentralized OSN.

## III .Existing System:

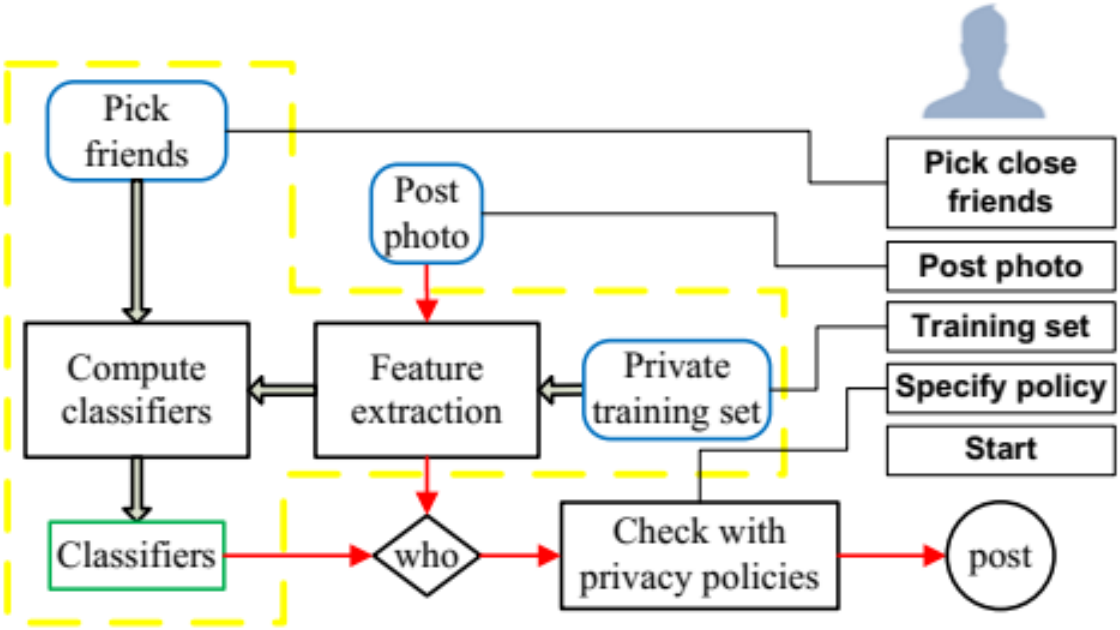
A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and webpages, such as wall in Facebook, where users and friends can post content and leave messages. In addition, users can not only upload content into their own or others' spaces but also tag other users who appear in the content.

**Disadvantages**

- 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 contained in the photo.
- Since original access control policies cannot be changed, the user's image continues to be revealed to all authorized users.
- On the other hand, reporting to OSNs only allows us to either keep or delete the content.

IV. Proposed System:

To overcome the problem based on Online Social Networks, a systematic solution to facilitate conflict detection of shared data in OSNs is introduced. The user can share their data or images to their friends. When the user is tried to share other user's data, the request will be send to the owner of the data. After receiving the request, the owner of the data has rights to accept or reject the request. The User can only share other data after getting the approval from the data owner, otherwise the user cannot share that data to others. To pursue a systematic solution to facilitate collaborative management of shared data in OSN's. We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data.




System Architecture

**MODULES**

- User Interface
- Policy Evaluation
- Image Classification
- Sharing Image
- Secure Sharing and Block image access right
- Recommended List

**User Interface**

This module can be also used to register users for custom modules that support personalization and user specific handling. If the users wish to create their own user accounts, i.e. register, then registration checks for the username availability and assign unique ID. It provides functionality to register viewers of the learning site in order to get access to

personalized content that the site using this module provides to its users. After registration and login, there is option to form the friends list. The friend suggestions will be there to add a new friend. Accept/ Reject option will be there for accept or reject the friend request. Through this process, friend circle are formed for each user.

**Policy Evaluation**

This module evaluates the policy each user which are currently in communication. Policy means identifies which users are owner, accessor and disseminator. The user who makes the profile updation, sharing, are considered as owners. The accessor are users who have a right to access the owner shared data. Disseminator are users who not have rights for viewing the owner images. This module evaluates the policy of the users based on the above contents.

**Sharing Images**

The user views all details of these group details, if want to connect with other group of friends, the user send request for with another groups via image owner approval. These group is already created with different groups means of request such as friends, family, staff, company etc., After that created group wise then send for interested groups of these details. After if want to send images content and metadata content you can share this via securely.

**Classification Approach**

User will first make a list for desired classifiers use private set operations in to request against friend's neighbor's classifiers lists one by one. we propose an image classification which classifies images first based on their friend list and then refine each category into sub categories based on their classifier. one-against-one strategy a user needs to establish classifiers between {self, friend} and {friend, friend} also known as the two loops in Algorithm. During the first loop, there is no privacy concerns of user1 friend list because friendship graph is undirected. However, in the second loop, user1 need to coordinate all user1 friends to build classifiers between them. According to our protocol, user1 friends only communicate with user1 and they have no idea of what they are computing

**Secure Sharing and Block image access rights**

This module is for sharing of resources, it gets the policy of the users and the contents what want to share. As per the policy of each data sharing, the data will share for only the users who all have the access rights. This module is to block the download rights and

**5.3.6 Recommended List**

In this module to share the images to particular friend list, create domain groups for each friend in particular categories (for ex college, family, native. etc.,) with his friend request. After connecting with different group of We now introduce the policy recommendation process based on the social groups obtained from the previous step. Suppose that a user uploaded new images then proposed method will invoked the images for user policy decision.

## V. Results and Discussion

### Multiparty access control (MPAC)

To pursue a systematic solution to facilitate collaborative management of shared data in OSNs.We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data. Some typical data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, aMPAC model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs.

This system analyze three scenarios—profile sharing, relationship sharing, and con tent sharing—to understand the risks posted by the lack of collaborative control in OSNs. We leverage Facebook as the running example in our discussion because it is currently the most popular and representative social network provider. In the meantime, we reiterate that our discussion could be easily extended to other existing social network platforms, such as Google++.

### Conflict Detection

We need a way to compare the individual privacy preferences of each negotiating user in order to detect conflicts among them. However, each user is likely to have defined different groups of users, so privacy policies from different users may not be directly comparable. To compare privacy policies from different negotiating users for the same item, we consider the effects that each particular privacy policy has on the set of target users T . Privacy policies dictate a particular action to be performed when a user in T tries to access the item. In particular, we assume that the availableactions are either 0 (denying access) or 1 (granting access).

## CONCLUSION

Photo sharing on social network sites has grown tremendously to over a billion new photos a month. Yet the tagging of photos on social network sites such as Facebook has caused users to lose control over their identity and information disclosures. Users have very few controls to manage socially appropriate photo sharing across their many overlapping social spheres. Users are forced to accept the resulting problems because of a strong desire to participate in photo sharing. Our findings reveal a number of important design considerations for photo privacy tools around the importance of identity and impression management and the tensions of ownership

To overcome the problem based on Online Social Networks, a systematic solution to facilitate conflict detection of shared data in OSNs is introduced. The user can share their data or images to their friends. When the user is tried to share other user's data, the request will be send to the owner of the data. After receiving the request, the owner of the data has rights to accept or reject the request. The User can only share other data after getting the approval from the data owner, otherwise the user cannot share that data to others. To pursue a systematic solution to facilitate collaborative management of shared data in OSN's.We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data.

## REFERENCES

[1] I. Altman. Privacy regulation: Culturally universal or culturallyspecific? Journal of Social Issues, 33(3):66–84, 1977.

[2] A. Besmear and H. Richter Lipford. Moving beyond untagging:photo privacy in a tagged world. In Proceedings of the SIGCHIConference on Human Factors in Computing Systems, CHI '10, pages1563–1572, New York, NY, USA, 2010. ACM.

[3] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein. Distributedoptimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn., 3(1):1–122, Jan.2011.

[4] B. Carminati, E. Ferrari, and A. Perego. Rule-based access controlfor social networks. In R. Meersman, Z. Tari, and P. Herrero,editors, On the Move to Meaningful Internet Systems 2006: OTM2006 Workshops, volume 4278 of Lecture Notes in Computer Science,pages 1734–1744. Springer Berlin Heidelberg, 2006.

[5] J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborativeface recognition for improved face annotation in personal photocollections shared on online social networks. Multimedia, IEEETransactions on, 13(1):14–28, 2011.

[6] K. Choi, H. Byun, and K.-A. Toh. A collaborative face recognitionframework on a social network platform. In Automatic Face GestureRecognition, 2008. FG '08. 8th IEEE International Conference on,pages 1–6, 2008.

[7] K.-B. Duan and S. S. Keerthi. Which is the best multiclass svmmethod? an empirical study. In Proceedings of the 6th internationalconference on Multiple Classifier Systems, MCS'05, pages 278–285,Berlin, Heidelberg, 2005. Springer-Verlag.

[8] P. A. Forero, A. Cano, and G. B. Giannakis. Consensus-baseddistributed support vector machines. J. Mach. Learn. Res., 99:1663–1707, August 2010.

[9] B. Goethals, S. Laur, H. Lipmaa, and T. Mielikinen. On privatescalar product computation for privacy-preserving data mining.In Proceedings of the 7th Annual International Conference in Information Security and Cryptology, pages 104–120. Springer-Verlag,2004.

[10] L. Kissner and D. Song. Privacy-preserving set operations. InIN ADVANCES IN CRYPTOLOGY - CRYPTO 2005, LNCS, pages241–257. Springer, 2005.

[11] L. Kissner and D. X. Song. Privacy-preserving set operations.In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes inComputer Science, pages 241–257. Springer, 2005.

[12] N. Mavridis, W. Kazmi, and P. Toulis. Friends with faces: Howsocial networks can enhance face recognition and vice versa. InComputational Social Network Analysis, Computer Communicationsand Networks, pages 453–482. Springer London, 2010.

[13] R. J. Michael Hart and A. Stent. More content - less control: Accesscontrol in the web 2.0. In Proceedings of the Workshop on Web 2.0Security and Privacy at the IEEE Symposium on Security and Privacy,2007.

[14] M. E. Newman. The structure and function of complex networks.SIAM review, 45(2):167–256, 2003.

[15] L. Palen. Unpacking privacy for a networked world. pages 129–136. Press, 2003.