International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Online Social Network

Mrs. K. Gomathi[1], Hari Nitheesh[2], M, Ramesh. R[2], Haridharsan. D[2], Vijaya Ragavan. S[2]

[1]Assistant Professor, Department of CSE, Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatore Tamil Nadu, India

[2]UG Scholar, Department of CSE, Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatore Tamil Nadu, India

ARTICLEINFO

Article History:

Accepted: 01 June 2023
Published: 06 June 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
724-727

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 web pages, 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 others data after getting the approval from the data owner, otherwise the user cannot share that data to others.

Keywords: Social Network, Privacy Preservation, multiparty access control, Photo Sharing

I. INTRODUCTION

Online Social Networks have become integral part of the daily life and has profoundly changed the way to interact with each other, fulfilling the 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 can 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. For instance, nowadays it can share any photo as that like on OSNs, regardless of whether this photo contains other people (is a co-photo) or not. Currently there is no restriction with sharing of co-photos, on the contrary, social network service providers like Facebook are encouraging users to post co-photos and tag their friends in order to get more people involved. However, what if the co-owners of a photo are not willing to share this photo? Is it a privacy violation to share this co photo without permission of the co-owners? Should the co-owners have some control over the co-photos? To answer these questions, this need to elaborate on the privacy issues over OSNs. Traditionally, privacy is regarded as a state of social withdrawal.

According to Altman's privacy regulation theory, privacy is a dialectic and dynamic boundary regulation process where privacy is not static but "a selective control of access to the self or to one group". In this theory, "dialectic" refers to the openness and closeness of self to others and "dynamic" means the desired privacy level changes with time according to environment. During the process of privacy regulation, it strives to match the achieved privacy level to the desired one. At the optimum privacy level, this can experience the desired confidence when user wants to hide or enjoy the desired attention when user want to show. However, if the actual level of privacy is greater than the desired one, user will feel lonely or isolated; on the other hand, if the actual level of privacy is smaller than the desired one, user will feel over-exposed and vulnerable.

II. 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 others 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 OSNs.User begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data.

III. MODULES & DESCRIPTION

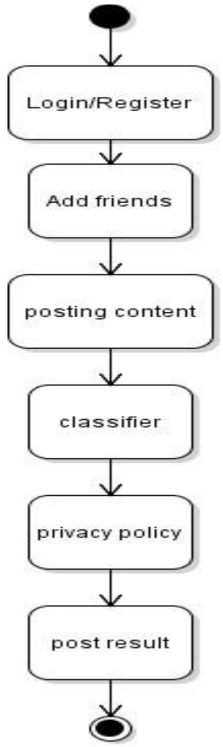

Figure 1. Block diagram

1. 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.

2. **Policy** Evaluation

This module evaluates the policy the each users 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 rights 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.

3. Sharing Images

The user view 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 and etc., After that created group wise then send for interested groups of these details. After if want to send images content and metadata content can share this via securely.

4. Classification Approach

This module evaluates the policy the each users 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 rights 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.

IV. ADVANTAGES

1. Advantages for USERS:

- Secure Profile sharing
- Cannot share or tag without owner's permission
- Available only to Friends of the user

V. APPLICATIONS

- This platform offers a range of exciting features that cater to different interests and preferences. I am particularly drawn to [mention specific features that interest you, such as groups, events, live streaming, or photo sharing]. I believe these features would enhance my online social experience and allow me to express myself creatively.
- They highly value my privacy and online security. I appreciate that your social network has implemented robust measures to protect user data and maintain a safe environment. Knowing that my personal information and online interactions are secure gives me peace of mind.
- As an avid social media user, I appreciate a platform that is intuitive, responsive, and aesthetically pleasing. Based on my research, your network prioritizes user experience, which is a significant factor in my decision to join. I am eager to explore the user interface and discover the various features your platform offers.

VI. CONCLUSION

Photo sharing is one of the most popular features in online social networks such as Facebook. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, this project is proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. In this, the project is designed a privacy preserving FR system to identify individuals in a co-photo. The proposed system is featured with low computation cost and confidentiality of the training set. Theoretical analysis and experiments were conducted to show effectiveness and efficiency of the proposed scheme. This can expect to that proposed scheme be very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-off between privacy and utility. For example, In current Android application, the co-photo could only be post with permission of all the co-owners. Latency introduced in this process will greatly impact user experience of OSNs. Moreover, local FR training will drain battery quickly. Future work could be how to move the proposed training schemes to personal clouds like Dropbox and/or icloud.

VII. REFERENCES

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

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

[3]. J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011

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

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

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

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

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

[9]. N. Mavridis, W. Kazmi, and P. Toulis. Friends with faces: How social networks can enhance face recognition and vice versa. In Computational Social Network Analysis, Computer Communications and Networks, pages 453–482. Springer London, 2010.

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

Cite this article as :

Mrs. K. Gomathi, Hari Nitheesh, M, Ramesh. R, Haridharsan. D, Vijaya Ragavan. S, "Online Social Network", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 3, pp. 724-727, May-June 2023.
Journal URL : https://ijsrst.com/IJSRST523103136