International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017
Issue 02, Volume 08 (July 2021) www.ijiris.com

TRUST-BASED PRIVACY PRESERVING PHOTO SHARING IN ONLINE SOCIAL NETWORKS

R Padmaja,
Assistant Professor-CSE Dept
Andhra Loyola Institute of Engineering and Technology,
Jawaharlal Nehru Technological University-Kakinada
rakkisu.padmaja@aliet.ac.in
Sk.Shahnoor,N.Nikhila,L.Thanusha
Department of Computer Science and Engineering,
Andhra Loyola Institute of Engineering and Technology,
Jawaharlal Nehru Technological University-Kakinada
shahnoorshaik00@gmail.com, nnk.nikhila@gmail.com, thanushalevaku@gmail.com

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.08/Issue02/JLIS10083
Received: 13, July 2021
Accepted: 20, July 2021
Published Online: 23, July 2021
DOI: https://doi.org/10.26562/ijiris.2021.v0802.004
Citation: Padmaja, Shahnoor,Thanusha (2021).” Trust-Based Privacy Preservation photo Sharing in online social Networks. IJIRIS: International Journal of Innovative Research in Information Security, Volume VIII, 20-26.
https://doi.org/10.26562/ijiris.2021.v0802.004
Peer-review: Double-blind Peer-reviewed
Editor: Dr.A.Arul L.S, Chief Editor, IJIRIS, AM Publications, India

Abstract: In the present social media technologies, sharing photos in online social networks has now become a popular way forusers to maintain social connections with friend are others. However, the rich information contained in a photo makes it easier foramalicious viewer to infer sensitive information about those who appear in the photo. How to deal with the privacy disclosure problem incurred by photo sharing has attracted much attention in recent years. When sharing a photo that involves multiple users, the publisher of the photo should take into all related user’s privacy into account. In this paper, we propose a trust-based privacy preservingmechanism for sharing such co-owned photos. The basic idea is toanonymize the original photo so that users who may suffer a high privacy loss from the sharing of the photo cannot be identified from the anonymized photo. The privacy loss to a user depends on how much he trusts the receiver of the photo. And the user’s trust in thepublisher is affected by the privacy loss. The anonymization result of a photo is controlled by a threshold specified by the publisher. We propose a greedy method for the publisher to tune the threshold, in the purpose of balancing between the privacy preserved by anonymization and the information shared with others.
Keywords: Facial Detection, Facial Detection, Image Processing Technique, Social Media Platform

I. INTRODUCTION

The social media platforms which are we using in our day-to-day life are well equipped in terms of current trends and technology. But the major problem that arises here is with the security of the user's data (photos) so, now if we can able to address the solution for this problem. We can put a check on them is cell aneous usage of photos and this problem can be solved by detecting the faces of the people in a particular picture. And by sending a notification to the concerned person. Whether he wants to allow the picture to post or not.

II. ABOUT THE PROPOSED WORK

A. Literature Survey

The human face brings with its appearance and shape a number of clues enabling the extraction of information about person identity, gender, age, ethnicity, health, emotional state and physical wellness, to name but a few. Face recognition has a critical role in biometric systems and is attractive for numerous applications including visual surveillance and security, medical imaging, and affective computing. Though there has been a great deal of progress in face detection and recognition in the last few years, many problems remain unsolved.

- My Privacy My Decision: Control of Photo Sharing onOnline Social Networks (Kaihe Xu, Yuanxiong Guo, LinkeGuo, Yuguang Fang, Xiaolin Li)– April2017

- Privacy-Preserving Relived Experiences in VirtualReality (ChengYaoWang) –May2020
- Advantages of Having Users' Trust and ReputationValues on Data Sharing Process in Online SocialNetwork(GulsumAkkuzu,Benjamin Aziz,Mo Adda) – October2019
- Privacy-Preserving Photo Sharing based on a SecureJPEG (Lin Yuan, Pavel Korshunov, and TouradjEbrahimi) – May2015

B. Proposed Work

In this section, the proposed work is elaborate data high-level scope. Sharing one co-owned photo in an OSN may compromise multiple users' privacy. To deal with such a privacy issue, in this paper we propose a privacy-preserving photo sharing mechanism which utilizes trust values to decide how a photo should beanonymized. The photo that a user wants to share is temporarilyholden by the service provider. Based on the trust relationship between users, the service provider estimates how much privacyloss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from the photo.

Advantages:

1) Arelationship-basedaccesscontrolmechanismwithwhich userscan controlhowtheir dataare shared.
2) Builtatrustmodelto quantifyuser relationships.

SYSTEM ARCHITECTURE:

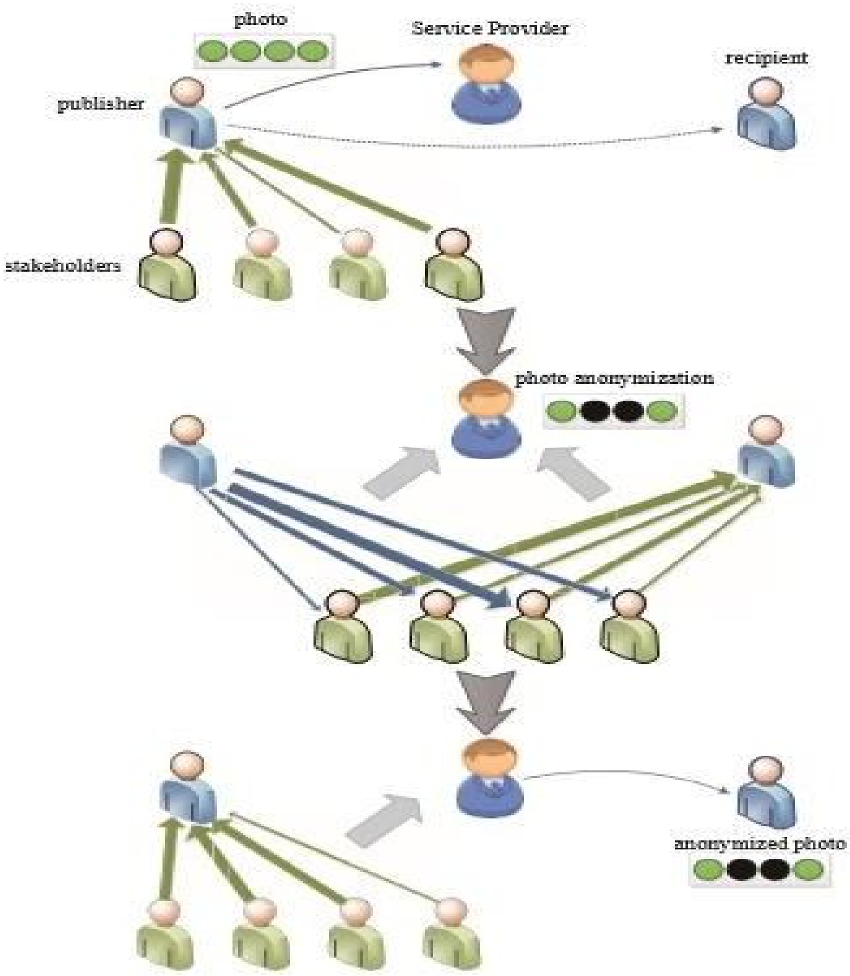


Fig.1 Architecture Model

Fig.1 Explains when a person tries to share a picture of group of members in a public social media network. The Picture is clustered by the nearest neighbours who are identical with the posting picture and send a request for Every person in the picture and ask them to respond to post in social platform or not. If the users in the picture will accept then the post will be posted in the public media if not it is sent to private and it shown that not visible to public

III. ALGORITHM

K-NEAREST NEIGHBOUR ALGORITHM (KNN):

KNN is slow supervised learning algorithm, it takes more time to get trained classification like other algorithm is divided into two step training from data and testing it on new instance. The K Nearest Neighbour working principle is based on assignment of weight to each data point which is called as neighbour. In K Nearest Neighbour distance is calculate for training dataset for each of the K Nearest data points now classification is done on basis of majority of votes there are three types of distances need to be measured in KNN Euclidian, Manhattan, Minkows ki distance in which Euclidian will be consider most one the following formula isused tocalculate theirdistance.

$$Eucledian\ Distance = D(x,y) = (x_i - y_i)_{2k_i} = 1 \qquad (1)$$

K=number of cluster

x , y=co-ordinate sample spaces

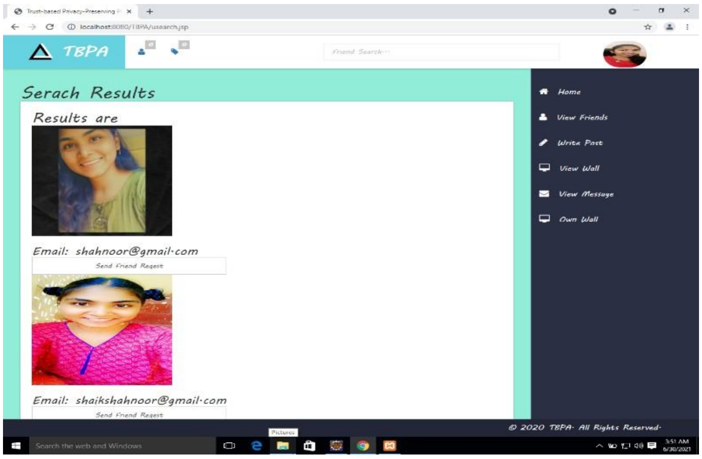
The algorithm for KNN is defined in the steps given below:

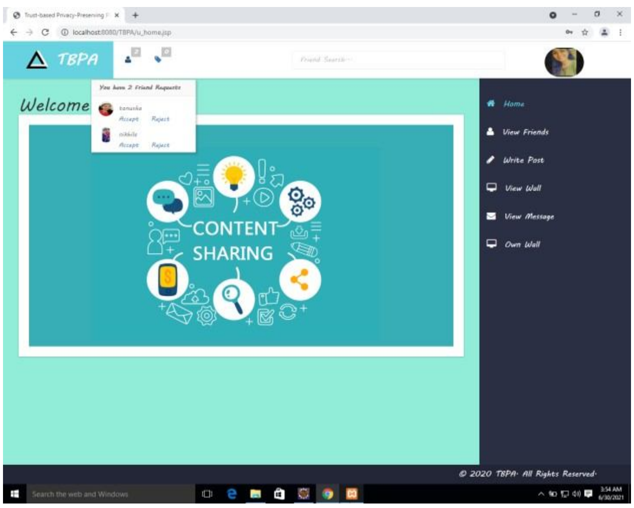
- D represents the samples used in the training and kde notes the number of nearest neighbours.
- Creates upper class for each sample class.
- Compute Euclidian distance for every training sample
- Based on majority of class in neighbour, classify the sample and perform features calling i.e., pre-processing of data

IV. RESULTS AND OBSERVATIONS

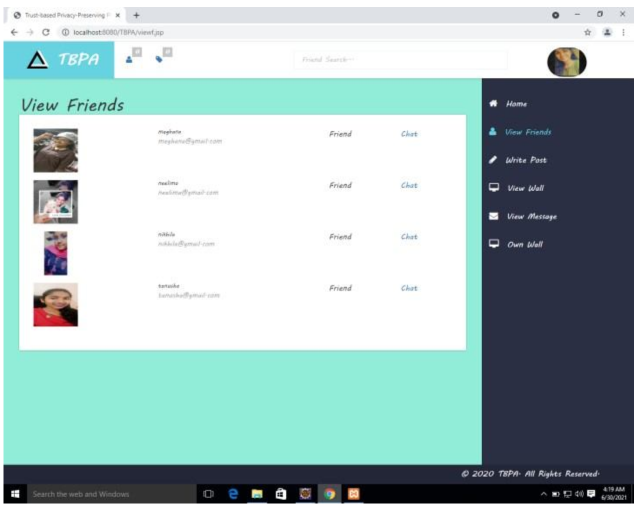
A person tries to share a picture in public sector then it recognize the person face and ask them to accept or reject the request to post the picture in public

Test Results Regarding an Online Trust Based Social Network:

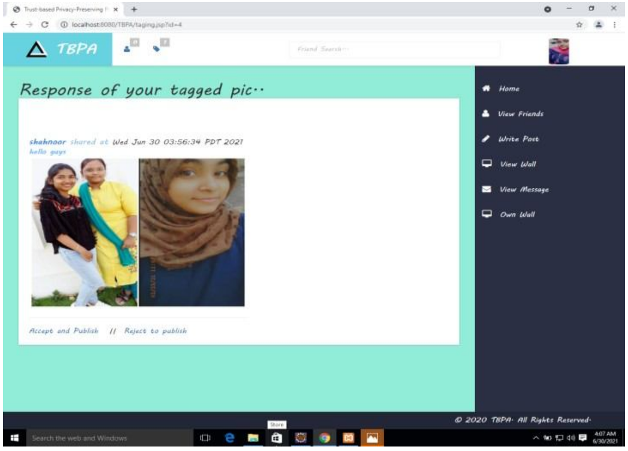




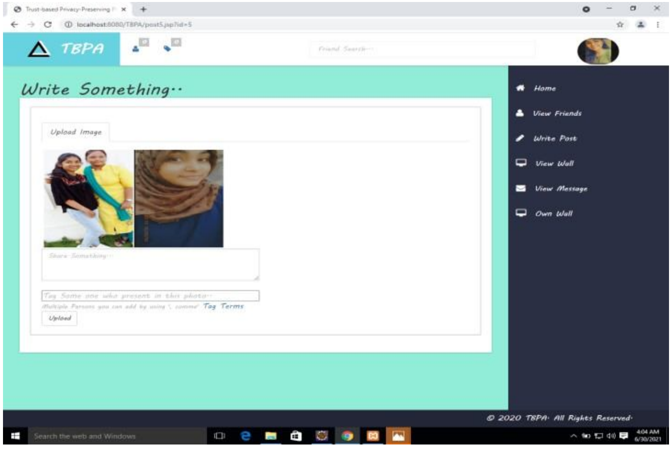
Above fig shows the Search results of a friend



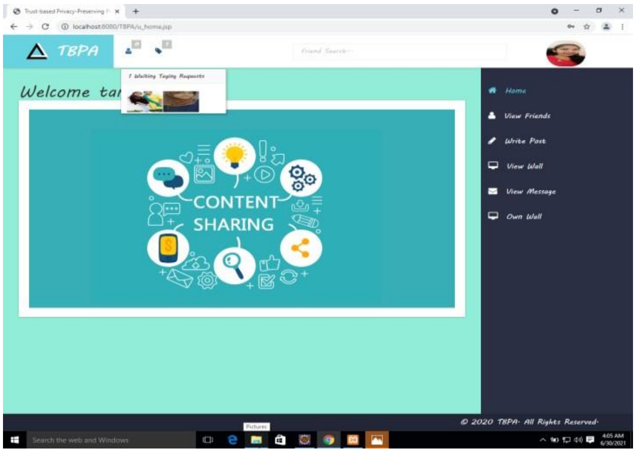
Above Fig shows the Friend Request



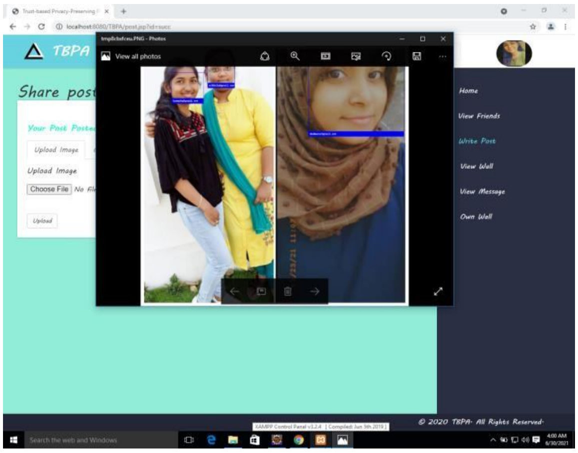
Above Fig shows Friends List



Above Fig shows Posting a Picture

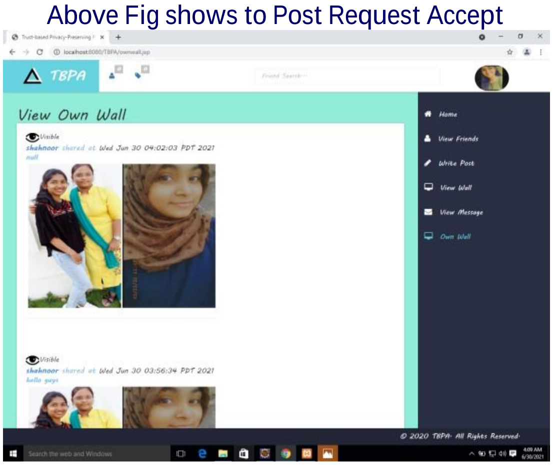


Above Fig shows Recognising People in Picture



Above Fig shows to request the person to post picture

Above Fig shows to Post Request Accept



Above Fig shows successful completion of a Post.

V. CONCLUSIONS

Sharing one co-owned photo in an OSN may compromisemultiple users' privacy. To deal with such a privacy issue, inthis paper we propose a privacy-preserving photo sharingmechanism which utilizes trust values to decide how a photo should be anonymized.

The photo that a user wants to shareis temporarily holden by the service provider. Based on the trust relationship between users, the service provider estimates how much privacy loss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from thephoto. After the photo is shared, each stakeholder evaluates the privacy loss he has really suffered, and his trust in the publisher changes accordingly. This trust-based mechanism motivates the publisher to protect the stakeholders' privacy. However, the anonymization operation leads a loss in the shared information. Considering that the threshold specified by the publisher controls the trade-off between privacy preserving and information sharing, we propose a serviceprovider assisted method to help the publisher to tune the threshold. By using synthetic network data and real-world network data, we conduct a series of simulations to verify the proposed photo sharing mechanism and the threshold tuningmethod. Simulation results demonstrate that incorporating trust values into the photo anonymization process can help to reduce user's privacy loss, and adaptively setting the threshold is necessary for the publisher to balance betweenprivacy preserving and photo sharing. In current study, wemainly focus on the sharing between one publisher and onereceiver. Considering that in practice, a user generally sharesa photo withmultiple users simultaneously,we'd like toinvestigate sucha one-to-manycase infuture work. Theproposed threshold tuning method can be seen as a greedymethod, in the sense that the publisher prefers to choose thethreshold that brings him the maximal instant payoff. Due to the correlation between privacy loss and trust values, current choice of the threshold will affect the publisher's future payoffs. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result.

ACKNOWLEDGMENT

This research project was partially supported by the Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Jawaharlal Nehru Technological University. We are grateful to Associate Professor Mrs.R.Padmaja for leading us to develop and contribute a paper to the conference.

REFERENCES

1. W.G.MangoldandD.J.Faulds,"Socialmedia: The new hybrid element of the promotion mix, "Business horizons, vol. 52, no. 4,pp. 357–365, 2009.
2. A. M. Kaplan and M. Haenlein, "Users of the world,unite!The challenges and opportunities of social media,"Business horizons, vol.53,no. 1, pp. 59–68,2010.
3. J. A. Obar and S. S. Wildman, "Social media definition and the governance challenge-an introduction to the special issue,"2015.
4. L.Xu,C.Jiang,J.Wang,J.Yuan,andY.Ren,"Information security in bigdata: Privacy and data mining, "IEEEAccess,vol.2,pp.1149–1176,2014.
5. S.K.N,S.K, and D.K,"On privacy and security in social media comprehensive study, "Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st InternationalConference on Information Security and Privacy 2015.[Online].Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211

C. C.Fiesler, M.Dye,J. L.Feuston, C.Hiruncharoenvate, Hutto, S.Morrison, P.KhanipourRoshan, U.Pavalanathan, A.S.Bruckman, M.DeChoudhury,and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing,"in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017,pp. 567–580.