Journal of Engineering Sciences

Vol 11, Issue 7,July/2020

ISSN NO:0377-9254

PHOTO SHARING AND STORING OVER ONLINE SOCIAL NETWORKS BASED TRUST & PRIVACY

[1]VATSAVAI SRIJA & [2]T SAI DURGA

M-Tech, Dept of CSE kakinada institute of engineering and technology for women, Korangi,

Mail Id: - vsrija529@gmail.com

Assistant Professor, Dept of CSE kakinada institute of engineering and technology for women, Korangi.

Abstract

In online web world, social networking sites are playing major role with various advantages. The main advantages of social network are creation of the social circle virtually and share data to friends and public. Sharing data like photos and videos in online social applications has now become a common behavior for sharing their status, mood and activity with their social associations or public. While sharing these data like pictures may consists of other user's information, publisher may tag to the other users who are present in the data or tag to the users who relative that post, this process is called Tagging. This tagging may damage the tagged user's privacy that may express data of user's location, presence or sexual content etc. It is a privacy loophole for the user's who are taking space in the photo with publisher of the picture. Privacy preserving in social networks in sharing data is current hot research topic in Social Networking. For this we are proposing a system called Privacy Preserving Framework for sharing data in social networks. Our System will identify the co-owner faces from the sharing data and tag to the co-owner's accounts for taking permission from the co-owners. For this we are using Machine Learning methods of K-Neighbours Classifier algorithm for detection of users in shared data.

Keywords: - Share Photo, Publisher Tag to Friends, Face Detection, KNN,

1. INTRODUCTION

In current generation we are living in online social world, most of the humans are connect with others through social networking apps virtually by compare to live. In this way people all also habituated to share the data of their status, mood or activity in social networking sites. The data can share in three formats; one is through micro-blogs or text, with multimedia data like images and videos [2]. While sharing images in social networking sites, most of the scenarios share images of events which consist of the other user presence. When we share those images to the online world it may leak the some information which other user does not want to share. This is the reason few survey's proposed and some social networking apps deployed concept called Tagging. In this Tagging process when we share a data if it's may contain the other user's data then the publisher should inform to the users by applying tag, so that tagged users may get chance to know of the shared data. But this concept now using for getting more audience for shared data. In social networking apps a user can share images which consist of other user information like user's location, user's presence, user's sexual content etc. In current social networking apps there no authority to stop the published data even if tagged users does not want to share his/her information to the world. For Example in a social networking sites Alice and Bob are friends. Bob share an image to his wall which consists of Alice presence. Here there are two scenarios, in first case Bob tag the Alice. In this case Alice get notification of the tagging, and that image also shares Alice wall, if Alice does not want share that image she can un-tag to the image so it won't share on the Alice's wall but it's still sharing on the Bob's wall. In second scenario Bob not tag to the Alice for sharing image but Alice present in the picture, in this can Alice never known about the photo sharing of her own picture in the image. In this scenario Alice security information like location, activity or sexual content may lead to the public. For these reasons we required a system that automatically identifies the users from the images and automatically tag to the user's who are sharing by the others.

By considering these security loopholes we are proposing a system called Privacy Preserving Framework for sharing data in social networks. Our System will identify the faces from the sharing image

and tag to users who are other than the publisher. But in our system if user tag the user or tagged by the system by face matching that image will share to wall after taking permission from tagged users. For identification of users we are using Machine Learning methods of K-Neighbours Classifier algorithm for detection of users in shared data.

2. RELATED WORK

Existing System

In current generation we are very much habituated to connect with others through social networking apps. Now day's people used to share the data of their status, mood or activity in social networking sites. In social networking application for sharing data focused the security of publisher only. For example if user x want to share a data to the wall, the user x can customize the privacy setting like to whom it will visible, to set hide for certain user or group user's. In the current system there is no privacy for users who are present in the images. In social networking apps a user can share images which consist of other user information like user's location, user's presence, user's sexual content etc. In current social networking apps there no authority to stop the published data even if tagged users does not want to share his/her information to the world.

Proposed System

In current social networking applications we have no authority to preserving security to the published other users, and for tagged users. The tagged users or co-owner of data user does not want to share his/her information to the world system cannot restrict the sharing of the image. We can complain/report about the data which are threatening to us but that results we can't expect soon. Based on these situations we are proposing a system called Privacy Preserving Framework for sharing data in social networks. Our architecture will match the co-owner faces from the sharing data and tag to the co-owner's accounts for taking permission from the co-owners. For this we are using Machine Learning methods of K-Neighbours Classifier algorithm for detection of users in shared data.

3. IMPLEMENTATION

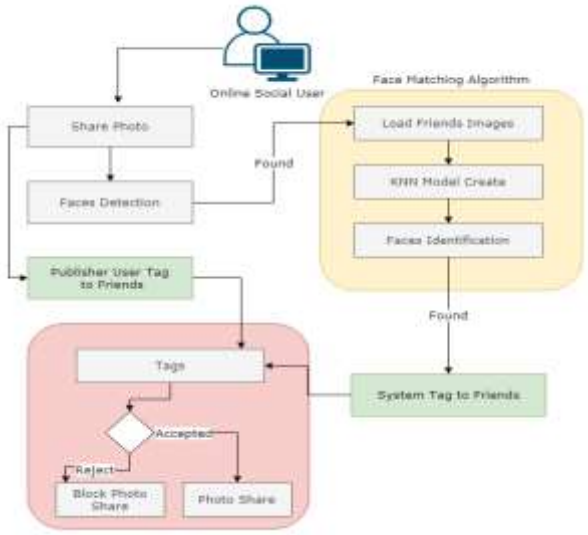

Fig:-1 System Architecture

Architecture

In this architecture I describe the flow of the process of the project. This architecture will describe the online social user process of the photo sharing process, in this flow there is a manual procedure and another one is system procedure in the tagging process. Let's describe the architecture modules.

Share Photo

This module starts with when user uploads image for photo sharing, this is the initial step of our main flow of the execution. For this option user need to register in our application and create a social circle of his/her own. In this option user need to upload an image which s/he wants to share to his/her wall.

Publisher Tag to Friends

In this module user/publisher only tag the other users/friends. When publisher mention any user/friend for uploading image as tag then user will get the tag notification. If any user tagged by the publisher then the tagged user direct continue to tag option.

Face Detection

- pip install face-recognition

In the following image face-recognition API identified the multiple face in the image.

Journal of Engineering Sciences

Vol 11, Issue 7,July/2020

ISSN NO:0377-9254

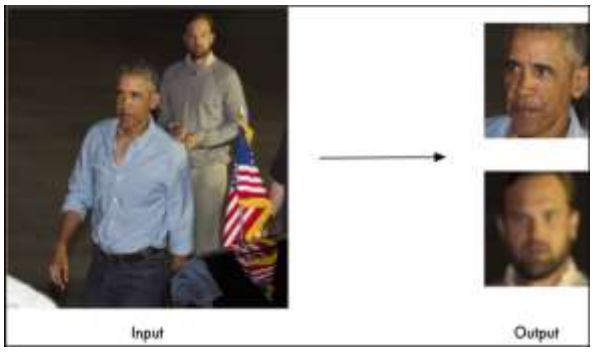

Fig 2: Face-recognition example
[Source: https://pypi.org/project/face-recognition/]

```
import face_recognition
image = face_recognition.load_image_file("test.jpg")
face_locations = face_recognition.face_locations(image)
print(face_locations)
```

```
[(96, 494, 186, 404), (68, 378, 175, 270)]
[Finished in 3.3s]
```

Fig 3: Sample code of the Face recognition

In above sample code I have shown the face_recognition module. In the output we have two faces co-ordinates.

KNN Model Create

For face matching concept we are using the K-Nearest Neighbors algorithm. In the KNN algorithms there are multiple sub methods are there, in our project we are using Ball-Tree algorithm. Ball-Tree algorithm also called as Binary Tree algorithm. In this algorithm each and every node creates a D-dimensional hypersphere, containing a subset of the points to be searched. After constructing the B–Tree we save the prediction parameters in clf file. Here we are taking three persons images as my train data. In the fig 4, we can find the train images.

4. EXPERIMENTAL RESULTS

Fig 4: Home Screen

Fig 5: Tag Notification

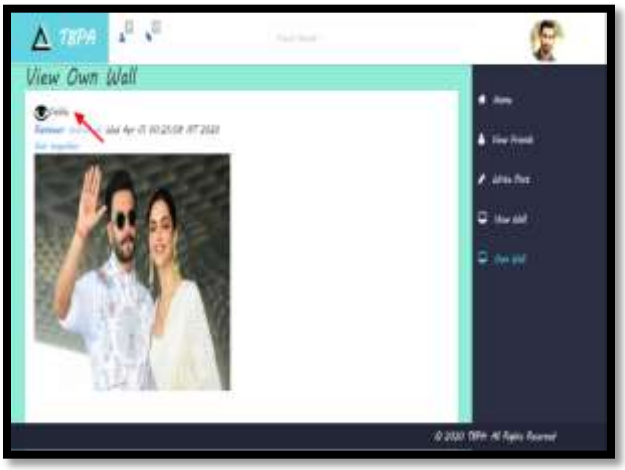

Fig 6: Post Visible after permission

5. CONCLUSION

We come to a conclusion from over application that In current social networking applications we have no authority to preserving security to the published other users, and for tagged users. The tagged users or co-

owner of data user does not want to share his/her information to the world system cannot restrict the sharing of the image. For this we are using Machine Learning methods of K-Neighbours Classifier algorithm for detection of users in shared data. Based on these situations we are proposing a system called Privacy Preserving Framework for sharing data in social networks. Our architecture will match the co-owner faces from the sharing data and tag to the co-owner's accounts for taking permission from the co-owners. We can complain/report about the data which are threatening to us but that results we can't expect soon.

6. REFERENCES

[1] L. Yuan, P. Korshunov, and T. Ebrahimi, "Privacy-preserving photo sharing based on a secure jpeg," in Computer Communications Workshops, 2015, pp. 185–190

[2] M. Duggan and J. Brenner, "The demographics of social media users 2012," 2013

[3] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 2, pp. 199–210, March 2017

[4] C. Ma, Z. Yan, and C. W. Chen, "Scalable access control for privacyaware media sharing," IEEE Transactions on Multimedia, pp. 1–1, 2018.

[5] P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '15, 2015, pp. 781–792.