Users Privacy on Sharing of Photos on Online Social Networks

[1]Janak Chetri, [2]Ankit Sinha, [3]Suresh Kumar S

[1]Student, Dept of CSE, [2]Student, Dept of CSE, [3]Asst.Prof,Dept of CSE
Computer Science and Engineering,
Vivekananada Institute of Technology, Bengaluru, India
[1]jchetri26@gmail.com, [2]ankitsinha.vkit@gmail.com, [3]sureshkatte89@gmail.com

Abstract: Photo sharing refers to the transfer or publishing of a user's digital photos online and the website which provides such acquaintances over services such as hosting, uploading, sharing and managing of photos through online system. This function provides the upload and display of images through both websites and applications. The photo sharing term can be set up and managed by individual users for the usage of online photo galleries including photo blogs. It means that other users can view but not essentially download the photos, users being able to select different copy-right options for their photos. Unfortunately, it may reveal users privacy if they are permitted to post, comment, and tag a photo liberally. To address this problem, this project proposes an efficient facial recognition system that can recognize everyone in the photo. Online photo sharing applications have become popular as it provides users various new and innovative alternatives to share photos with a range of people. The photo sharing feature is incorporated in many social networking sites which allow users to post photo for their loving ones, families and friends. For users of social networking sites such as Facebook, this system focuses on the privacy concerns and needs of the users, at the same time explores ideas for privacy protection mechanisms. By considering users current concerns and behaviors, the tool can be designed as per the user's desire which they can adopt and then can be motivated to use.

Index Terms **– Social network, photo privacy, secure multi-party computation**

I. INTRODUCTION

With the huge popularity of sharing and the vast usage of social networking sites users unknowingly reveal certain kinds of personal information. Social-networking users may or may not have the idea of getting their personal information will be leaked or could protect the malicious attackers and may perpetrate significant privacy breaches. The rest decade of 21st century has seen the extreme popularization of Internet and the growth of web services which facilitate participatory information sharing and collaboration. Social Networking Sites (SNSs) have become a boundless communication media to keep in touch beyond boundaries. SNSs are a part of human culture than just a web application. Use of SNSs has out spaced in almost every fields as news agencies, big and small companies, governments, and famous personalities etc. to interact with each other. With the adoration of sharing, Facebook has stood out as the most renown SNSs in the world where people hangout for hours. With the extravagancy of technology and services sharing of news, photos, personal taste and information with friends and family has led to an ease. But along with this user privacy should also be taken into consideration. An issue related to privacy with Facebook users has been constantly appearing on international press either because of the companies privacy policy or because of users unaware-ness of content sharing consequences. As a research says the simple disclosure of date and place of birth of a profile in Facebook can be used to predict the Social Security Number (SSN) of a citizen in the U.S. Many a times just by simply publishing their friends list, users might be revealing a large amount of information. For example, through the use of prediction algorithms it is possible to infer private information that was previously undisclosed. Sometimes sensitive information even comes embedded in the photo as metadata and may identify people on the photo by accompanying more information that could be exploited, like captions, comments and photo tags; marked regions.

II. PROBLEM DEFINITION

To address the issue of photo sharing vulnerabilities and study the situation when a client shares a photograph containing people other than himself/herself(termed co- photograph)and provide privacy protection to photo being shared.

III. PROPOSED SOLUTION

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, we proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We 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. We expect that our proposed scheme be very careful in protecting user's privacy in photo/image sharing over online social networks. Our prototype application is implemented. We use OpenCV Library 2.4.6 to carry out the face detection and Eigen face method to carry out the FR. Fig.1 shows the graphical user interface (GUI). A log in/out button could be used for log in/out with Facebook. After logging in, a greeting message and the profile picture will be shown. Our prototype works in three modes: a setup, sleeping and working mode.

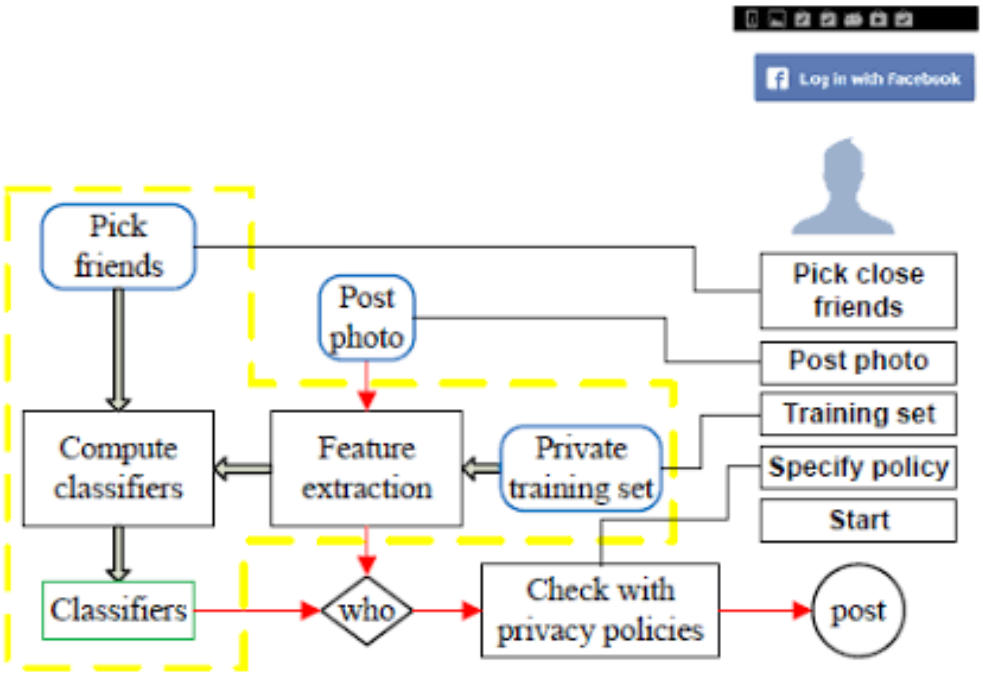

Fig 1 System Architecture of our Application

A mechanism has been designed to make users aware of the posting activity and make them actively take part in the photo posting and decision making paradigm for which a facial recognition (FR) system is recommended which can recognize everyone present in the photo. If more privacy setting is done then it may limit the number of photos which will be utilized as the training set for FR system. In order to overcome this problem and for training set for FR system we would utilize the private photos of users which would differentiate the photo co-owners without affecting their privacy. A distributed consensus based method is developed which would protect the private training set and even reduce the computational complexity.
Our contributions to this work when compared with previous work are mentioned below:

1. We can find the potential owners of shared photos automatically even when the use of generated tags is kept as an option in our paper.
2. Private photos in a privacy-preserving manner and social contexts to derive a personal FR engine for any particular user is proposed in our paper.
3. We propose a consensus-based method to achieve privacy and efficiency.

A privacy-preserving FR system is used to identify individuals in a co-photo. The owners present in the shared photos can be automatically recognized and identified with or without user-generated tags. The FR engine is derived from the private photos and social contexts. The privacy is protected by providing users facility to restrict others from seeing their photos. Each user is able to deny his/her policy which are privacy policy and exposure policy. Computation cost is very low. FR system provides privacy by notifying the subject about the posting activity and thus leading the other subjects to take active part in it. To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual present in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, an efficient facial recognition (FR) system is needed which recognizes everyone in the photo. However, if more privacy settings are done then it may bind the number of photos necessary to train the FR system. So in order to solve this problem, private photos of users is utilized to train the FR system and thus prevent the leakage of the privacy of the individuals.

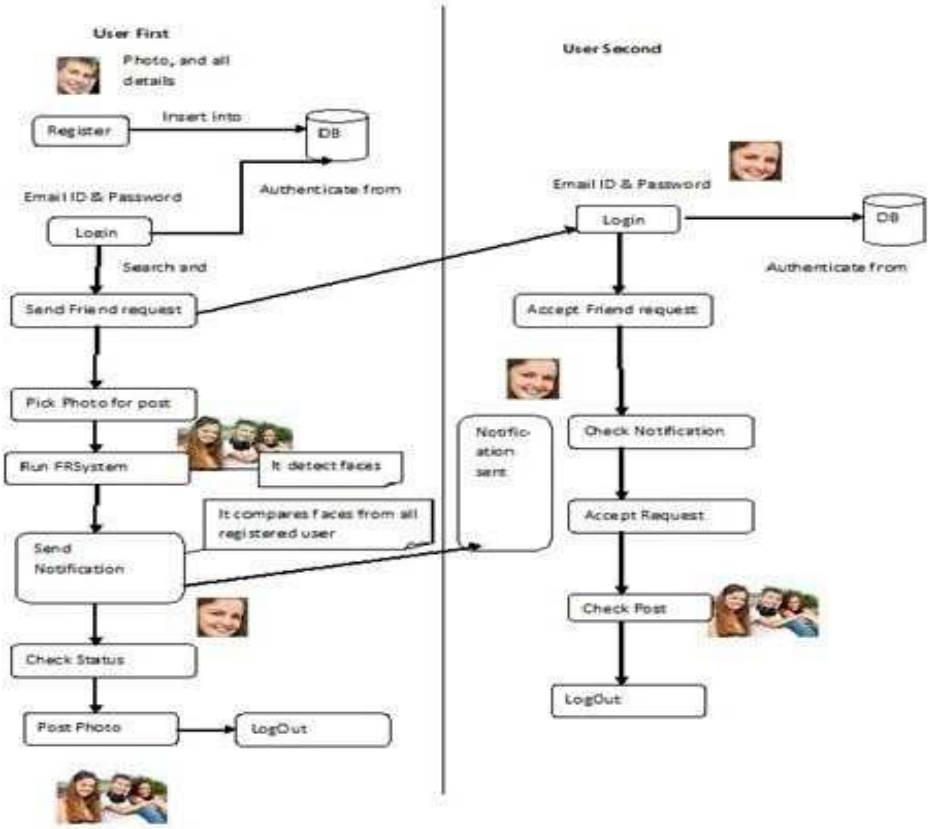

Fig 2 Flowchart of the system workflow

A. MODULE DESCRIPTION

Set up: This module will setup basic framework to accept user profiles and their face pictures. Has different tabs based on project description, new user registration, login page.

Face Recognition: In this subsection, we study the recognition ratio against the number of friends and the number of strangers. Standard face detection in [23] is used for face detection and eigen face [22] is used to extract features and vectorize the training image. However, the standard eigen face method is a centralized approach, it may not be applicable to our distributed case. To address this, we assume principle components have already been extract to form a vector space S. User's facial photos are projected into this space as feature vectors. Based on our simulation results, we find that this modification is reasonable due to the fact that the important features on human face lie on only a few directions. Facial feature extraction is beyond the scope of this paper. Better facial feature extraction method can be applied to our system to obtain a better recognition ratio.

Privacy policy and Face Matching: After registration from user, he/she can send the friend request to anybody to become friends and other requested person can accept friend request if he wishes to become friend. Whenever user wants to upload picture he can use "Post "option given in the system. Once photo is uploaded then and there itself the face gets recognized and checks anybody in the system has similar face or not. Nearest neighbour algorithm is used to find the best match.

Control decision for privacy: Once any user uploads photo then requests is being sent to the other person, he can either allow or deny him from uploading the photo. Before proceeding to vote for permission he needs to recheck the photo whether he/ she are looking inappropriate or not.

IV. RESULTS

The objective of designing a secure photo sharing on Online Social Networks using Face Reorganization is being achieved. This project has ended up in helping achieve separate secured single privacy for each of the user's which is completely under their control. It would help reduce various cyber security crimes, frauds which happen very frequently. The proposed scheme is very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade between

privacy and utility. Preserving user privacy and making them actively participate in the photo posting activity is a very prime concern in OSNs. The co-photo can be posted only with the permission of the co-owner and if the privacy and exposure policy gets satisfies. To make the system more secured the notification is sent to the co-owner and only with his/her acceptance the photo is posted. In addition random OTP is generated while uploading photo to verify the user who is posting it as someone may access his account to upload photos which are in actual not to be posted by the concerned account holder. The result of the system is shown with the help of the comparison table where it reacts the difference between the existing system and the system proposed. The result of the system depends on the number of the train images. As the number of train images increases the recognition of the owners and co-owners photo is done more easily and quickly.

V. ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of our guide Asst.Prof Suresh Kumar S who made it possible because “Success is the abstract of hard work and perseverance, but steadfast of is encouraging guidance.” Also provided with all the resources and great platform to accomplish my target. I also express my special thanks to my friends and to the organization in particular and everybody who have supported me in for supporting me in my research work.

VI. CONCLUSION AND FUTURE ENHANCEMENT

Photograph sharing is a standout amongst the most prevalent elements in online informal organizations, for example Facebook. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, we proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We 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. These functions provided by websites and applications facilitate the upload and display of images. The term may even be useful for online photo galleries that are positioned up and managed by individual users, including photo blogs. The system used a toy system with two users to demonstrate the principle of the design. The system that is built has proven that how to build a general personal FR with more than two users. The system can reduce the privacy leakage by using this design as it provides intimation to the co-owners and even to the owners through random OTP generation. Theoretical analysis and experiments were conducted to show effectiveness and efficiency of the proposed scheme. We expect that our 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 our 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. Our future work could be how to move the proposed training schemes to personal clouds like Dropbox and/or icloud.

REFERENCES

[1] Kaihe Xu, Yuanxiong Guo, Linke Guo, Yuguang Fan g, Xiaolin Li, ”My Privacy My Decision: Control of Photo Sharing on Online Social Networks”, IEEE Transaction on Dependable and Secure Computing, Volume: PP , Issue: 99, pp-1-1, 2015

[2] Z. Stone, T. Zickler, and T. Darrell, “Auto tagging Facebook: Social network context improves photo annotation”, IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 1-8, 2008.

[3] Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang,”Social circles: Tackling privacy in social networks”, in Proc. Sympsable Privacy Security, 2008.

[4] J. Bonneau, J. Anderson, and L. Church, ”Privacy suites: Shared privacy for social networks”, in Proc. Symp. Usable Privacy Security, 2009.

[5] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, ”Providing access control to online photo albums based on tags and linked data”, pp. 9-14, 2009.

[6] A. Besmer and H. Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1563-1572, 2010.

[7] Barbara Carminati, Elena Ferrari, Raymond Heatherly, Mu-rat Kantarcioglu, Bhavani Thuraisingham, ”Semantic web-based social network access control”, pp. 108-115, 2011.

[8] Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demi-dova , "I Know What You Did Last Summer! Privacy-Aware Image Classification and Search", Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012.

[9] Kambiz Ghazinour, Stan Matwin and Marina Sokolova , "Your privacy protector: A Recommender System For Privacy Settings In Social Networks", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.

[10]Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantar-cioglu, Bhavani Thuraisingham, Semantic web-based social network access control 2011.

[11] 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, 2011.

[12] Anna Cinzia Squicciarini, Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites, IEEE Transactions On Knowledge And Data Engineering, vol. 27, no. 1, January 2015.