International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Selective Control of Photo Sharing on Online Social Network

Dr.K.V Subbiah # Surendra kumar #2

#1 Professor,Dept of CSE, PBR Visvodaya Institute Of Technology And Science ,Kavali,India.Email id:kvsubbaiah72@gmail.com

#2Studnet,Dept of Master of Computer Application (MCA), PBR Visvodaya Institute Of Technology And Science ,Kavali,India.Email id: onterusurendra225143@gmail.com

Abstract: *Online social networks provides facilities such as sharing, hosting , uploading and photo management which are shared and transferred online on social network. Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. In this paper, we attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system[1]. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of privacy using encryption algorithm and opensource. Our mechanism is implemented as a proof of concept Android application on Face book's platform.*

Keywords— **online social networks, FR system, open social, privacy**

1. INTRODUCTION

Photo sharing is an interesting component of Online Social Networks (OSNs)[6]. Users have no control over data residing outside their spaces. Each user has a different privacy concerns about the photos related to them. Each user can tag/share contents to his/her friends. OSNs only allows us to keep or delete the content. A large proportion of photographs contain face images which are associated with the daily lives of the photographers who captured them. Currently, online social networks (OSNs) such as Facebook ,Instagram, Twitter, and Snapchat are prevailing platforms on which people communicate with their social connections such as friends, family members, and colleagues in the real world. Social networks, due to many unfavorable incidents, have been blame for breaching the privacy of their users. Both in academia and in the media, the importance of a user's confidentiality has been rarely discussed.

In addition to some proposed technical solutions, there have been a huge number of initiatives to educate users so that they do not provide an excessive amount of personal information. Privacy issue is one of the main concerns, since many social network user are not careful about what they expose on their social network space. The second issue is identity theft; attackers make use of social networks account to steal victim's identities. The third is the spam issue. Attackers make use of social networks to increase spam click through rate, which is more effective than the traditional email spam.

In the past, there was a buzz regarding the privacy settings of Facebook as it was very complicated but later they have simplified it for better understanding and easy access to common people. Due to lack of knowledge and understanding of privacy features of Facebook, people make many mistakes. Another important thing which should be controlled is the availability of the personal information which should be prevented from leakage as it may reveal personal information of an individual in the form of videos, images or any data. As the popularity of social networks continues to grow, concerns surrounding sharing information online compound. Users regularly upload personal stories, photos, videos, and lists of friends revealing private details to the public. To protect user data, privacy controls have become a central feature of social networking sites but it remains up to users to adopt these features.

Privacy restrictions form a spectrum between public and private data[5].On the public end, users can allow every Facebook member to view their personal content. On the private end, users can restrict access to a specific set of trusted users. Facebook uses friendship to distinguish between trusted and untrusted parties. Users can allow friends, friends of friends, or everyone to access their profile data, depending on their personal requirements for privacy. We proposed a system where photo can be shared in a secure way. Proposed framework can help clients to effortlessly and appropriately design security settings.

2. MOTIVATION

Despite the spectrum of available privacy settings, users have no control over information appearing outside their immediate profile page. When a user posts a comment to a friend's wall, he cannot restrict who sees the message. Similarly, if a user posts a photo and indicates the name of a friend in the photo, the friend cannot specify which users can view the photo. For both of these cases, Facebook currently lacks a mechanism to satisfy privacy constraints when more than one user is involved. This leads to privacy conflicts, where asymmetric privacy requirements result in one user's privacy being violated. Privacy conflicts publicly expose personal information, slowly eroding a user's privacy.

3. LITERATURE SURVEY

There are several systems proposed for privacy preserving of photos on online social network. These systems preserve the privacy of the photo.

In 2008, Z. Stone, T. Zickler, and T. Darrell [2], described that the sensitive and private user attributes can be revealed by the act of tagging pictures on the social-networking site of Facebook. Through Facebook lots of data is being shared which may even be private and very sensitive so a prime concern is given to user privacy. Even it is been revealed that even the date and place of birth of a profile can be used to predict the Social Security Number (SSN) of a Facebook user and additional to that much more can be revealed through users friends list.

People may be identified on the photo through sensitive information which may be embedded in the photo as metadata by accompanying much more information that could be exploited like comments, captions marked regions and photo tags. Even if through the photo tags [2], if the individual is not identified, it is possible to infer someone's identity through the combination of face recognition software and publicly available data. So it is preferred that the users should be able to hide their tags rather than deleting it and thus keep a high degree of interaction by keeping track of the photos they have online with the album owner but the photos shouldn't be linked directly to their profiles.

In 2008, A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang [3] , developed privacy settings based on the concept of social circles which protects personal information through a web based solution. The friend's lists are automatically generated through Social Circles Finder that identifies the intensities of the relation by analyzing the social circle of the person which in turn helps in categorizing of friends for privacy policy setting. The social circle of the subject will be identified by the application but won't be revealed to the subject. The subject's interest of sharing the information will be considered by interrogating the subject and based on that the piece of personal information will be shared in the form of visual graphs.

In 2009, J. Bonneau, J. Anderson, and L. Church explains privacy suites [4] which allows users to easily choose "suites" of privacy settings that can be created by an expert using privacy programming or can be created through exporting them to the abstract format or through existing configuration UIs. A Privacy suite can be verified by a good practice, a high level language and motivated users which then can be then distributed to the members of the social sites through existing distribution channels.

In 2009, JaeYoung Choi', Wesley De Nevel, Yong Man Ro l, and Konstantinos N Plataniotis [5], made use of available multiple and distributed database and also FR engine on OSN to improve accuracy of face annotation. This system utilized the real-world personal photos which were available on web and the standard MPEG-7VCE-3 data set to form a collaborative FR method [5] which improved the accuracy of face annotation by considering the annotation results obtained from individual FR engines. Social relationship among community members and social context in personal photographs are used to form FR databases and engines to annotate faces in a collaborative way rather than considering individual FR on which fusion techniques are applied to combine results from multiple FR engine and give a single result. The collaborative system thus used the face annotation method to improve the accuracy of the system which was done through the set of database.

In 2011, Alessandra Mazzia Kristen LeFevre and Eytan Adar [10], explains how users apply privacy policies to their networks. It [10] is an interface and system that allows the user to recognize its profile based on different factors such as natural sub-groupings of friends that is build up at different stages of granularity. The automatically constructed group can be automatically recognized and distinguished with the help of group labels.

This tool is better than other tools like Facebook's Audience View and Custom Settings page.

In 2012, Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova developed a technique [11] which enables privacy-oriented image search for automatically detecting private images. The security policies are provided by combination of textual metadata images with variety of visual features. In this the selected image features (edges, faces, color histograms) which can help distinguish between natural and man-made objects/scenes can be done through image features like edges, faces or color histogram through which the presence or absence of object can be determined. The classification models which are trained on large scale dataset are utilized in which social annotation game is used to obtain privacy assignments.

In 2012, Sergej Zerr developed a technique [12] which enables privacy-oriented image search for automatically detecting private images. The security policies are provided by combination of textual metadata images with variety of visual features. In this the selected image features (edges, faces, color histograms) which can help distinguish between natural and man-made objects/scenes can be done through image features like edges, faces or color histogram through which the presence or absence of object can be determined. It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game.

In 2015, Anna Cinzia Squicciarini represented A3P system [10] which automatically generates personalized policies as it is a free privacy settings system. Based on the images content, person's personal characteristics and metadata, the user uploaded image can be handled by A3P system. It consists of two components: A3P Core and A3P Social. The A3P core receives the image uploaded by the user, which it classifies and decides whether there is a need to call upon the A3P-social. If the metadata is unavailable or if it is created manually then it may cause inaccurate classification, violation policy and even may cause inaccurate privacy policy generation.

4.PROPOSED SYSTEM

Photograph sharing is an alluring component which advances Online Social Networks (OSNs). Sadly, it may release client's security on the off chance that they are permitted to post, remark, and label a photograph openly. In this paper, we endeavor to address this issue and study the situation when a client shares a photograph containing people other than himself/herself (termed co-photograph for short). We are proposing a system where photo can be shared in a secure way.

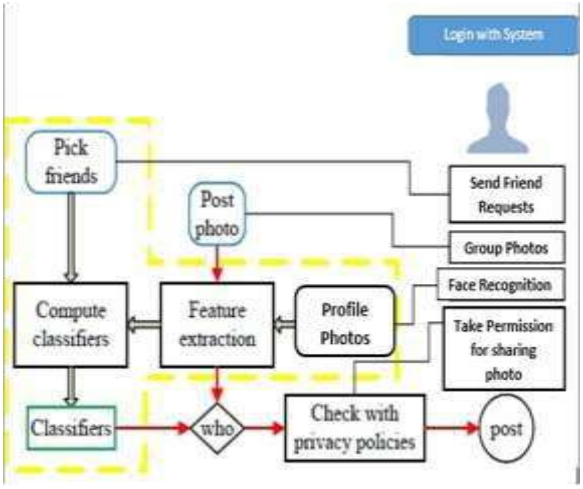

Figure1. Proposed System

A. Module Description

1. Set Up: This module will setup basic framework to accept user profiles and their face pictures. It has different tabs on home screen about project description, New user registration, Login and Contact Us page.

2. Face Recognition: According to the Facebook statistics, on average a user has many friends but only few of them are trustworthy. We assume only a small portion of them are close friends. In our application, each user picks up to 30 friends. Notice that all the selected friends are required to use our application and register their profile by uploading their profile photos to carry out the collaborative training. After the classifiers are obtained, feature extraction is done, decision is taken to classify whether picture is a face or non-face. Viola Jones algorithm is used for the checking if the uploaded image is face or not.

3. Privacy Policy and Face Matching : After taking the registrations from user, user can send the friend request to anybody to become friends and other requested person can accept friend request if he wish to become friend. Whenever user wants to upload a group photo then he can upload a group picture using ”Update Status” option given in system.

Once photo uploading is done, face recognitions are done and checked if anybody in the system has the similar face. Nearest neighbor algorithm is used for finding best match. If the face matching is successful then a request sent to them for seeking a permission for uploading the photo.

4. Control decisions for privacy : Once somebody uploads users X’s photo, he will get the request from the person who is uploading the photo, he can wish to allow or deny him from uploading the photo. Before proceeding to vote for permission he needs to answer the security question provided by him during the profile creation. This is just to add the more security for the system. Secure key can be shared between two people which can be used while taking permission for uploading the photo. Once user allows to upload the photo by clicking on ”Allow” photo will be shared and if he clicks on ”Deny” photo will not be posted.

5. Other Security policies : When a photo is shared online, another users will not be able to manipulate it. Users are not allowed to save it , which adds more security to the system and the privacy of posted photos is preserved.

5. CONCLUSION

Photo sharing is the process of publishing or transfer of a user’s digital photos online. Individuals in a co-photo are identified by the proposed FR system. The system reveals the detailed description of our system. Generally speaking, the consensus result could be achieved by iteratively refining the local training result. Various websites offer services such as uploading, hosting, and managing for photo-sharing (publicly or privately). 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.

6.REFERENCES

1. Kaihe Xu, Yuanxiong Guo, Linke Guo, Yuguang Fang, 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, “Autotagging facebook: Social network context improves photo annotation”, IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 1-8, 2008.

3. A. 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. JaeYoung Choi’, Wesley De Nevel, Yong Man Ro l, and Konstantinos N Plataniotis, ”Face Annotation for Personal Photos Using Collaborative Face Recognition in Online Social Networks”, 16th International Conference on Digital Signal processing, pp.1-8, 2009.

6. C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, “Providing access control to online photo albums based on tags and linked data”,9–14, 2009.

7. 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.

8. Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu, Bhavani Thuraisingham, ”Semantic web-based social network access control”, pp. 108-115, 2011.

9. Alessandra Mazzia Kristen LeFevre and Eytan Adar, “The PViz Comprehension Tool for Social Network Privacy Settings”, Tech. rep., University of Michigan, 2011.

10. Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , “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.

11. Kambiz Ghazinour, Stan Matwin and Marina Sokolova, “Yourprivacyprotector: A Recommender System For Privacy Settings In Social Networks”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.

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.