International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

My Privacy My decision: Control of Photo Sharing on Online Social Networks

Prashant Abhang[1], S. B. Rathod[2]

[1]Student,Dept. of computer engineering, Sinhgad Academy of Engineering, pune.
[2]Professor, Dept. of computer engineering, Sinhgad Academy of Engineering, pune.

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.*

Key Words: **Online Social Network, privacy preserving, photo sharing, FR system, face detection, feature extraction**

1. 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 pro t 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 pro le 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. Even if the individuals in a photo are not explicitly identified by photo tags, the combination of publicly available information and face recognition software can be used to infer someones identity. These kinds of problems are defined as collateral damage: users unintentionally put their own privacy or their friends privacy at risk when performing events on SNSs such as Facebook.

2. LITERATURE SURVEY

In 2006, Barbara Carminati, Elena Ferrari, and Andrea Perego [3], presents a sys-tem that consists of policies in the form of constraints on the type, depth and trust level of the relationship that are existing on the access control model for Web-based social networks (WBSNs). The authenticity to the relationships are presented in the form of certificates and rule based approach is used on the client side enforcement to provide access control where the user requesting for access has the entire rights to it. The system doesn't use the relationship among users to provide access as the relationship might not be a strong point of consideration. Instead the trust factor and the depth of relationship among users are very important and based on that the access is provided. A rule-based access control model is proposed for WBSNs, which allows the requirement of access rules for

online resources where the relationship be-tween authorized users in the network is denoted in terms of the relationship type, depth, and trust level. In this system, the certificates which are specified by the users are stored and managed by the central node of the network, whereas storing of access control and performing access control is done by a set of peripheral nodes.

In 2009, Jonathan Anderson proposed a paradigm called Privacy Suites [7] 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 2011, Barbara Carminati, Elena Ferrari , Raymond Heatherly, Murat Kantar-cioglub, Bhavani Thuraisingham [11], address that security and privacy concerns need to be addressed for creating applications of online social networks that include person specific information. So a prime concern is given towards improving social network access control systems. But the current OSNs provide very basic access control system to the users such as marking a particular item as public, private or accessible by their direct contacts but they lack exibility as they do not specify the access control requirements. So a ne-grained OSN access control model based on semantic web technologies is proposed in [11] which encode social network-related information by means of ontology. Semantic Web Rule Language (SWRL) can be used to set the security policies in the form of rules which are expressed in ontology and this can be enforced by simply querying the authorizations. In 2013, Kambiz Ghazinour proposed a recommender system known as Your Privacy Protector [17] that assists by understanding the behavior of privacy setting and recommends reasonable privacy options. The personal pro le of the user is constructed based on the parameters such as users interests, users privacy settings and users personal pro le on photo albums and based on this pro le of users it assigns the privacy options. The user is granted permission to see their current privacy settings which will be monitored by the system and if any risk is detected it adopts the necessary privacy settings.

In 2015, Anna Cinzia Squicciarini developed an Adaptive Privacy Policy Pre-diction (A3P) [18] system, that automatically generates personalized policies as it is a free privacy settings system. Based on the images content, persons 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.

3. SYSTEM ARCHITECTURE

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 de ne 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.

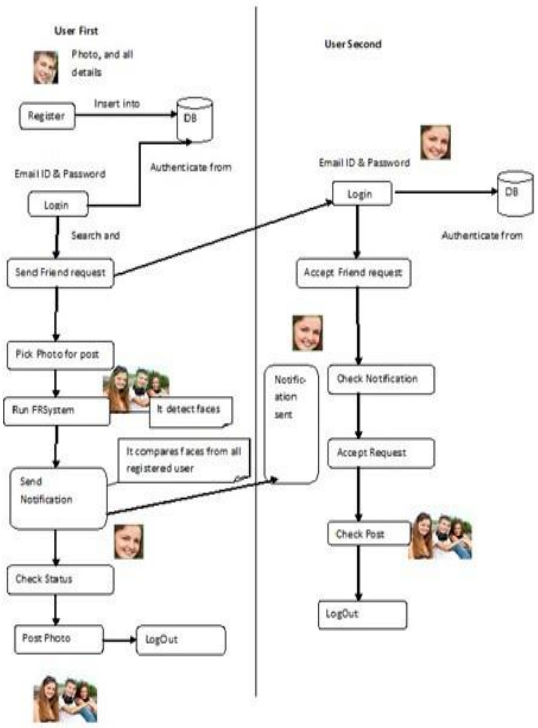

Fig -1: System Architecture

A. Steps in project:

1. User needs to register his account.
2. Login to the home page of the application.
3. Enter OTP which will be sent to an authorized user.
4. Upload train images where the faces will be detected and cropped.
5. Search for friends if any or else send friend request to other users.
6. Request can be accepted if any user has sent any request.
7. Upload or add photo on the home page.
8. OTP will be sent to the registered mail id of an authorized user.
9. Face recognition algorithm is used to recognize the faces present in the uploaded photo
10. If faces are recognized then notification is sent to the co-owner about posting activity.
11. Finally, if permission is given by the co-owner then photo will be uploaded.

4. RESULT

The proposed scheme is very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-o 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 satis es. To make the system more secured the noti cation 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 hisaccount 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 re ects the di erence 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.

5. CONCLUSION

Photo sharing is the process of publishing or transfer of a user's digital photos on-line. 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 o er 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.

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] 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, "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.

[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 Im-ages on Content Sharing Sites, IEEE Transactions On Knowledge And Data Engineering, vol. 27, no. 1, January 2015.