ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Survey on Selective Control of Access of Photo Sharing on Online Social Network

Anusha Rao, Sonal Fatangare, Jyoti Raghatwan

ME Student, Dept. of Computer Engineering, RMD SSOE, Warje, Pune, India

Assistant Professor, Dept. of Computer Engineering, RMD SSOE, Warje, Pune, India

Assistant Professor, Dept. of Computer Engineering, RMD SSOE, Warje, Pune, India

ABSTRACT: Photo sharing refers to the transfer or publishing of a user's digital photos online and the website which provides such acquaintances offer 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 copyright options for their photos. Unfortunately, it may reveal user's privacy if they are permitted to post, comment, and tag a photo liberally. To address this problem, various systems have been explained that can be used to 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 user's current concerns and behaviors.

KEYWORDS: Online Social Network, Photo privacy, Photo Sharing, Collaborative Learning, Support Vector Machine

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 profit the malicious attackers and may perpetrate significant privacy breaches. The first 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 lead 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 company's privacy policy or because of user's unawareness 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.

DOI: 10.15680/IJIRCCE.2015. 0311120

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 someone's 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. With the ease and need of fulfilling our social needs social interactions, information sharing, appreciation and respect Social Networking sites have became the integral part of daily life. With this ease and nature of social media people put more content, including photos, over OSNs without too much thought on the content. Once a photo is posted online it becomes a permanent record which may further be used for malicious purposes. For example, a posted photo in a party may reveal a connection of a celebrity to a mafia world. As OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue.

Another features of the Social networking Sites like photo tagging etc may create more complications when user privacy come in concerns. So far there is no restriction with sharing of co-photos, on the converse, social network service providers like Facebook are encouraging users to post co-photos and tag their friends in order to get more people involved. Users may even post information about others without their consent. A lack of experience and awareness in users, as well as proper tools and design of the OSNs, perpetuate the situation.

This paper proposes a system based on novel consensus, approach to achieve efficiency and privacy at the same time. The main focus is to let each user only deal with his/her private photo set as the local train data which can be used by the users to learn out the local training result. Once the local training results are achieved then it can be exchanged among various users to form a global knowledge. In the next round, each user learns over his/hers local data again and takes the global knowledge as a reference. Finally the information is spread over users and consensus can be reached.

II. RELATED WORK

There are several systems proposed for privacy preserving on online social network.

Rule Based Access Control

It presents a system 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 between authorized users in the network is denoted in terms of the relationship type, depth, and trust level. In this system [2], 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.

Face Annotation using Collaborative Face Recognition

Face annotation (or tagging) method aimed towards improving the accuracy of face annotation by making use of multiple and distributed databases and FR engine which are distributed on online social network. The FR recognition method was done using the standard MPEG-7VCE-3 data set and a set of real-world personal photos from the web. The system devise a collaborative FR method [7] aiming to improve the face annotation accuracy by combining 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.

Semantic Web based

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 flexibility as they do not specify the access control requirements. So a fine-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.

Photo Tagging

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 [4], 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.

PViz Comprehension Tool

It is a tool that explains how users model groups and privacy policies applied to their networks. PViz [13] is an interface and system that allows the user to understand its profile based on various factors such as natural sub-groupings of friends that is constructed at different levels of granularity. The group labels are provided so that the user can identify and distinguish automatically constructed groups. This tool is better than other tools like Facebook's Audience View and Custom Settings page.

Privacy Suites

Privacy Suites [6] 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.

Social Circles

Privacy settings based on the concept of social circles [5] which protects personal information through a web based solution was developed. 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.

Privacy-Aware Image Classification and Search

In 2012, Sergej Zerr developed a technique [15] 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 the 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.

Decentralized authentication protocol

An access control system based on a [9], descriptive tags and linked data of social networks in the Semantic Web. It allows users to create expressive policies for their photos stored in one or more photo sharing sites, and users can specify access control rules based on open linked data provided by other parties.

Adaptive Privacy Policy Prediction (A3P)

A3P system [17] 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.

Conditional Random Field (CRF)

The conditional random field is a pair wise model which based on the conditional density finds the optimal joint labeling. In CRF, the accuracy of the face annotation is improved by considering the existing labeled photos as the training sample along with the FR score. The system combine face recognition scores with social context in a conditional random field (CRF) model and apply this model to label faces in photos from the popular online social network Facebook, which is now the top photo-sharing site on the Web with billions of photos in total. Existing metadata from online social networks can improve automatic photo annotation.

But it will be impossible for the system to label some individuals in newly posted photos.

Facial recognition (FR) System

A privacy-preserving FR system is used to identify individuals in a co-photo. The owners of shared photos can be automatically 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 define 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.

III. Research elaboration

The study was done on the social context and based on study three realms models were proposed which are a social realm, a visual sensory realm and a physical realm. A social realm is the one in which identities are entities, and friendship a relation; a visual sensory realm in which faces are entities and co-occurrence in images a relation; and a physical realm in which bodies belong with physical proximity being a relation. These realms are highly correlated.

Research conveys that the recent system designed for OSNs is better than traditional FR system in terms that a customized FR system for each user is much more accurate in his/her own photo collections. Choi et al in [3], has done related work in which he suggest to use multiple personal FR engines which can be used to mutually to get better recognition ratio. Social context is use to select the appropriate FR engines and this engines contain identity of queried face image with high prospect.

The security and privacy issues in OSNs appear as significant and vital research topics although thorough research interests stretch towards FR engines refined by social connections. The investigation of flexible access control schemes based on social contexts are done while doing this work. While posting a photo user does not ask for permission of other users in present OSNs which are used. We can find study on privacy concerns related to photo sharing and tagging on Facebook which is been done by Besmer and Lipford in [9]. In these works, flexible access control schemes based on social contexts are investigated. However, in current OSNs, when posting a photo, permissions for using other features on Facebook are not required by the user. In [9], Besmer and Lipford study the privacy concerns on photo sharing and tagging features on Facebook. A survey was conducted in [9] to study the effectiveness of the existing countermeasure of untagging and shows that this countermeasure is far from satisfactory: users are worrying about offending their friends when untagging. We can find a tool which can help users to avoid other users to see their photos when posted as a complementary strategy so that the privacy of user will be maintained. But by implementing this method there will be several manual tasks to be carried by end users.

We can find a scheme of game-theoretic suggested by Squicciarini et al in [8]. In this scheme privacy policies are mutually enforced over the shared data. It is possible for every user to define his/her privacy policy and exposure policy. When a photo is processed with owner's privacy policy and co-owners exposure policy only then it could be posted. But it is difficult to find co-owner of co-photo automatically. Tagging feature on present OSNs must be used to find potential co-owner in this case.

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 a 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:

- 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.
- 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.
- Orthogonal to the conventional cryptographic solution, we propose a consensus-based method to achieve privacy and efficiency.

The figure below shows the system structure of the FR system.

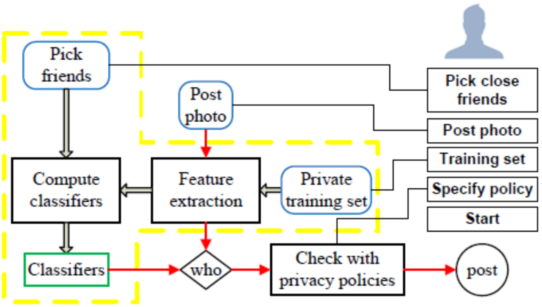

Fig.1. System Structure of FR System

IV. Discussion

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. A privacy-preserving FR system is developed 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 useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-off 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.

V. Conclusion

Photo sharing is the process of publishing or transfer of a user's digital photos online. This system proposes a privacy-preserving FR system to identify individuals in a co-photo. 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 are provided by websites and applications that 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

DOI: 10.15680/IJIRCCE.2015. 0311120

has proven that shows how to build a general personal FR with more than two users. It is very efficient than existing system. The system can reduce the privacy leakage by using this design. The proposed system features a low computation cost and confidentiality of the training set.

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. B. Carminati, E. Ferrari, and A. Perego, “Rule-based access control for social networks”, Springer Berlin Heidelberg, Vol.278, pp.1734-1744, 2006.
3. K. Choi, H. Byun, and K.-A. Toh, “A collaborative face recognition framework on a social network platform”, 8th IEEE International Conference on Automatic Face and Gesture Recognition, pp. 1-6, 2008.
4. 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.
5. 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.
6. J. Bonneau, J. Anderson, and L. Church, “Privacy suites: Shared privacy for social networks”, in Proc. Symp. Usable Privacy Security, 2009.
7. 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.
8. A. C. Squicciarini, M. Shehab, and F. Paci., “Collective privacy management in social networks”, In Proceedings of the 18th International Conference on World Wide Web, pp. 521–530, 2009.
9. 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.
10. 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.
11. Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu, Bhavani Thuraisingham, ”Semantic web-based social network access control”, pp. 108-115, 2011.
12. 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”, IEEE Transactions on Multimedia, Vol.13 (1), pp.14-28, 2011.
13. Alessandra Mazzia Kristen LeFevre and Eytan Adar, “The PViz Comprehension Tool for Social Network Privacy Settings”, Tech. rep., University of Michigan, 2011.
14. Joao Paulo Pesce, ”Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook”, 2012.
15. 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.
16. 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.
17. 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.

BIOGRAPHY

Anusha P. Rao is a Master of Engineering student in the Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule Pune University. She received Bachelor of Engineering degree in 2012 from DPCOE, Wagholi, Pune. Her research interests are Image Processing, Data Mining, Network security etc.

Sonal Fatangare is an Assistant Professor in the Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule Pune University. She received Master of Engineering degree in 2014 from JSPM, BSIOTR, Wagholi, Pune. Her research interests are Data Mining and Network security.

Jyoti Raghatwan is an Assistant Professor in the Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule Pune University. She received Master of Engineering degree in 2012 from Sinhgad College of Engineering, Pune. Her research interests are Information Security.