International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 8 –NOVEMBER 2016.

A NOVEL APPROACH FOR PRIVACY PRESERVING PHOTO SHARING ON SNSS

SHAIK.NOORUDDIN[#1], I. TABHITA[*2]and SAYEED YASIN[*3]

[#] *M.Tech (CSE) Student, Nimra College of Engineering & Technology, A.P., India.*

[*2]*Assistant Professor, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

[*3]*Associate professor & Head, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

***Abstract*— The massive use of social networking sites and with the vogue of photo sharing on social networking sites users naively tends to share personal information. Social networking users may or may not be aware of getting their personal information to be leaked or will benefit the malevolent hackers or may commit any kind of privacy breaches. 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. 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 mechanism. Post may have different format such as text, image, video etc. There should be some mechanism that enables the user to participate in decision making activity of his/her photo and video sharing on any users wall.**

Index Terms*— *Social network, photo privacy Photo Sharing, Collaborative Learning.

I. INTRODUCTION

Nowadays if we like any photo/videos on social sites, we immediately share that photo without thinking that shared photo may contain other people (is a cophoto) or not. There is no restriction with sharing of co-photos. But problem is that, if co-partner involved in that photo/video may not will to share their photo/video on OSN, also OSN suffered from problems like, inaccuracy, subjectivity etc. Currently, many OSN users do not have control over the information which is appearing outside of their profile page of OSN. Social sites have become important part of our daily life.Online social networks (OSNs) such as face book, Google and sound of birds are inherently designed to make able people to part personal and public information and make social connections with friends, coworkers, persons having like-position, family, and even with strangers. To keep safe (out of danger) user facts, way in control has become a chief thing point of OSNs. However it becomes everlasting record once some photo/image is posted/uploaded. Late consequences can be dangerous, people may use it for different unexpected purposes. For example a posted may reveal the mafia relationship of any celebrity. A user profile usually includes information with respect to the users work history birthday, sex, residence, interests, education, and, travel information and be in touch information. Moreover, users upload the picture and tag other people even though they are willing or not willing to be part of uploaded image/content. When other people are tagged the situation becomes more complicated. The user uploading the image is totally unaware of the consequences that arise for the person which is involved in tagging or image. Currently nobody can stop such unavoidable situation. We need to have a control over such actions to minimize the risks of photos being tagged or uploaded. Instead of imposing restrictions over such incidents or increasing security, sites like FB and Instagram are encouraging people to get into such things more. Most of the times user is unwilling to get tagged or being exposed without his permission. Is it violation if we share picture without taking a permission from all the people involved in picture? To answer this we need to explain the privacy and security issues over the social sites. To minimize this or to completely avoid this they have suggested social sites like Facebook, Instagram to make use of multi-party privacy model to

increase privacy. There should be mutual acceptable policy to grant access for a photo when multiple user are involved. For security user might need to create a group where they can grant access for their uploaded images. Exposure policy can be defined as the group of users where an image can be accessed when particular user is involved and the privacy policy can be stated as the group of users/friends who can have a direct access of the uploaded images. These two policies are used to define the overall audience or group of users/friends who can be given access to uploaded image. But before establishing this there should be a proper process of defining these groups. For this the facial recognitions are used. Most of the times the people found in the co-photo are close friends. So face recognitions engines are trained for identifying the friends in social circle. FR engines with more accuracy rates require large number of test data/samples specific to a person but most of the times it is not possible. Users who care about the privacy and security mostly restrict themselves from uploading the photos but if these people are provided with proper privacy preserving techniques then they can post photos without any reluctance. We are designing a privacy enhancing system of photo sharing which makes use of collaborative training system. We are enabling the users of social site to have own personal FR engine based on social relations which will make use of images stored in their personal system. It will help to build a social relationship tree, which can be used for policies for sharing of data. We make use of cryptographic techniques are well to build such training data. We need to propose a secure approach to gain efficiency and privacy both. The user is trained first from his local training set, means set of photos in her gallery. Exposure policies are defined to have access on photo. And then by global knowledge of relationships the photo sharing can be initiated. Finally data will be distributed to the right people who have access.

II. LITERATURE REVIEW

A. A Paper on "Face recognition for improved face annotation in personal photo collections shared on online social networks".

AUTHORS: M. Bellare, C. Namprempre, and G. Neven

Using face annotation for effective management of personal photos online, Proposed a novel collaborative face recognition framework enlightening the correctness of face annotation by effectively making use of many Recognition engines available in an OSN. In particular collaborative FR framework consists of two major parts, select FR engines and merge multiple FR results. The selection of FR engines aims at determining a set of customized FR engine which are suitable for knowing query for facial images belonging to a particular user. For this purpose they exploit both social network group context in social sites and social context in phone galleries. Additionally to take advantage of the availability of multiple FR results retrieved from the selected FR engines they devise two effective solutions for integration Face Recognition results adopting old fashioned techniques for merging many classifier results Experiments were conducted using around 547 thousand personal photos collected from an existing social site networks. Results prove this method gives more accuracy matched to conventional Face Recognition approaches that only make use of a single FR engine. Further demonstrated that their collaborative FR framework has a low computational cost and comes with a decentralized design.

B. Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks.

This paper represents key idea of an OSN that are strongly correlated real-world activities i.e. By computing the correlation between the personal context models of the OSN members, the accuracy of event-based image annotation can be significantly improved. In this paper authors mainly did the personalize image search, a tag-based query only for retrieving images.

C. Rule-Based Access Control for social networks.

This paper introduced WBSN i.e. an access control model. In that policies are specified in terms of type of data and belief of relationship. Social Network Management Systems (SNMSs) allow users to state whether specific information e.g., personal data and resource should be public or private. In this paper simple strategy has straightforward approach but, they are not flexible enough in denoting authorized users because they may grant access to non-authorized users.

D. A Paper on "Moving Beyond Untagging: Photo Privacy in Tagged World"

AUTHORS: Andrew Besmer& Heather Richter Lipford.

Department of Software and Information Systems. Photo tagging is a popular feature of many social networks. Examined privacy concerns and mechanisms for tagged images. Using a focus group, explored the needs and concerns of users, resulting in a design considerations collections for tagged photo privacy and security. Designed a privacy enhancing mechanism based on their findings, and tested it using a mixed methods approach. Results identify the social tensions that tagging generates, and the needs of privacy tools to address photo privacy management issues.

III. PROPOSED SYSTEM

During the process of privacy regulation, we strive to match the achieved privacy level to the desired one. Unfortunately, on most current OSNs, users have no control over the information appearing outside their profile page. In , Thomas, Grier and Nicol examine how the lack of joint privacy control can inadvertently reveal sensitive information about a user. To mitigate this threat, they suggest Facebook's privacy model to be adapted to achieve multi-party privacy. In these works, flexible access control schemes based on social contexts are investigated. However, in current OSNs, when posting a photo, a user is not required to ask for permissions

of other users appearing in the photo. In , Besmer and Lipford study the privacy concerns on photo sharing and tagging features on Facebook. A survey was conducted in 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 un tagging. As a result, they provide a tool to enable users to restrict others from seeing their photos when posted as a complementary strategy to protect privacy. However, this method will introduce a large number of manual tasks for end users. In Squicciarini et al. propose a game-theoretic scheme in which the privacy policies are collaboratively enforced over the shared data. Basically, in our proposed one-against-one strategy a user needs to establish classifiers between self, friend and friend, friend also known as the two loops in Algorithm. 2. During the first loop, there is no privacy concerns of Alice's friend list because friendship graph is undirected. However, in the second loop, Alice need to coordinate all her friends to build classifiers between them. According to our protocol, her friends only communicate with her and they have no idea of what they are computing for

A. Advantages

Secret Sharing Photo Unknown Person cannot Access The Photos And Any Data Its Access Permission only .

B. Proposed System Algorithms

According to algorithms**:** there are two steps to build classifiers for each neighborhood: firstly find classifiers of fself, friendg for each node, then find classifiers of ffriend, friendg. Notice that the second step is tricky, because the friend list of the neighborhood owner could be revealed to all his/her friends. On the other hand, friends may not know how to communicate with each other.

C. Homomorphic Encryption Algorithm:

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services.

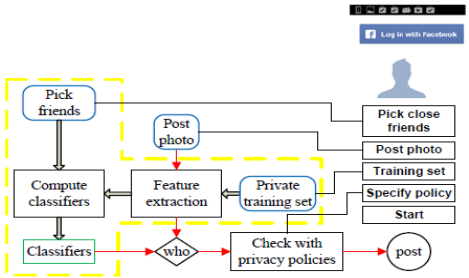

Figure: System Architecture

IV. RELATED WORK

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. 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.

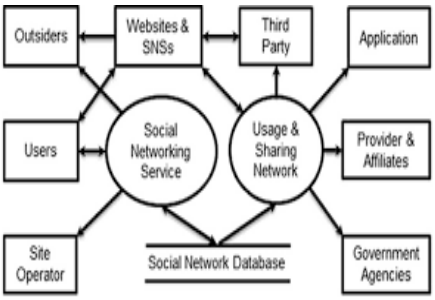

Figure: Model

V. CONCLUSION & FUTURE WORK

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. 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. More over, 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] I. Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3):66–84, 1977.
[2] 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, CHI '10, pages 1563–1572, New York, NY, USA, 2010. ACM.
[3] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein. Distributed optimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn., 3(1):1–122, Jan. 2011.
[4] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In R. Meersman, Z. Tari, and P. Herrero, editors, On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, volume 4278 of Lecture Notes in Computer Science, pages 1734–1744. Springer Berlin Heidelberg, 2006.
[5] 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, 13(1):14–28, 2011.
[6] K. Choi, H. Byun, and K.-A. Toh. A collaborative face recognition framework on a social network platform. In Automatic Face Gesture Recognition, 2008. FG '08. 8th IEEE International Conference on, pages 1–6, 2008.
[7] K.-B. Duan and S. S. Keerthi. Which is the best multiclass svm method? an empirical study. In Proceedings of the 6th international conference on Multiple Classifier Systems, MCS'05, pages 278–285, Berlin, Heidelberg, 2005. Springer-Verlag.
[8] P. A. Forero, A. Cano, and G. B. Giannakis. Consensus-based distributed support vector machines. J. Mach. Learn. Res., 99:1663–1707, August 2010.
[9] B. Goethals, S. Laur, H. Lipmaa, and T. Mielik?inen. On private scalar product computation for privacy-preserving data mining. In In Proceedings of the 7th Annual International Conference in Information Security and Cryptology, pages 104–120. Springer-Verlag, 2004.
[10] L. Kissner and D. Song. Privacy-preserving set operations. In IN ADVANCES IN CRYPTOLOGY - CRYPTO 2005, LNCS, pages 241–257. Springer, 2005.
[11] L. Kissner and D. X. Song. Privacy-preserving set operations. In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes in Computer Science, pages 241–257. Springer, 2005.
[12] N. Mavridis, W. Kazmi, and P. Toulis. Friends with faces: How social networks can enhance face recognition and vice versa. In Computational Social Network Analysis, Computer Communications and Networks, pages 453–482. Springer London, 2010.

SHAIK.NOORUDDIN is a student of Nimra college of engineering and Technology, Jupudi, NimraNagar, VIJAYAWADA. he is presently pursuing her M.Tech degree from JNTU, Kakinada.

I. TABHITA is presently working as Assistant professor in CSE department in Nimra college of Engineering and Technology, Jupudi, Nimra Nagar, VIJAYAWADA.

SAYEED YASIN received his M.TECH in Computer Science & Engg from JNTU Hyderabad. He is pursuing Ph.D., in Rayalaseema University, Kurnool. He is currently working as an Associate Professor & Head in Nimra College of Science & Technology the Department of Computers Science and Engineering & Technology, Jupudi, Ibrahimpatnam,Vijayawada-521456. He has more than Eight years of experience in teaching field. His area of interests are wireless networks & programming, & Mobile Computing.