



CONTROL OF PHOTO SHARING USING FACE RECOGNITION ON OSN

Sunil Wilson Pereira¹, Sumithradevi.C²

1. P.G. Student, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India
2. Asst.Professor, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

ABSTRACT : Photo sharing is an alluring component which enhances Online Social Networks. Sadly, it may release clients' security on the off chance that they are permitted to post, remark, and label a photograph openly. We study the situation when a client shares a photograph containing people other than her (termed co-photograph for short). We need to minimize the security breaches that happen because posting the photos of people without the awareness of people involved in photo. For this reason, we require a proficient facial acknowledgment (FR) framework that can perceive everybody in the photograph. Notwithstanding, all the more requesting security setting may restrain the photographs' quantity freely accessible to prepare the FR framework. To manage this issue, our instrument endeavors to use clients' private photographs to plan a customized FR framework particularly prepared to separate conceivable photograph co-proprietors without releasing their protection. We additionally add to a disseminated accords based system to diminish the computational many-sided quality and ensure the private preparing set. We demonstrate that our framework is better than other conceivable methodologies as far as acknowledgment proportion and effectiveness. Our instrument is executed as a proof of idea Android application on Facebook's stage. OSNs will not contaminate to true users and polluted by unauthorized users and their posting the photos in insecure way. Hence OSNs will be secure and safest.

Keywords: Photo Privacy, Social networks, secure multi-party computation, collaborative learning.

I. INTRODUCTION

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.

Whenever a photograph is shared it includes everybody's security, which can be put on risk if the proper permissions are not sought. We need to enforce maximum level of privacy and security of the content being uploaded on social sites. So while using the online social networks one can feel desired level of confidence and security. He/she can confidently make use of social sites without worrying or photos being shared in insecure and unauthorized way. Desired level of privacy and security is a first important thing for a user using online social sites. With respect to current architecture and implementations of social sites, either user will alone because highly imposed security constraints else will be impacted by several security threats because of low security mechanisms. Few authors studied about the security challenges because of lack of joint or collaborative control over the images being shared across the online 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.

Efficiency and privacy can be achieved by simultaneously comparing the current and previous experiments.

1. The users in a shared photo are automatically detected without being tagged by somebody.
2. We propose a secure sharing of private photos



by making use of social context to have personal FR Engines.

3. We can achieve privacy, security and efficiency.

II. BACKGROUND AND RELATEDWORK

1) A Paper on “On the Move to Meaningful Internet Systems” AUTHORS: M B. Carminati, E. Ferrari, and A. Perego. The degree of edibility of workflow management systems heavily influences the way business processes are executed. Constraint-based representations are deliberated to be more flexible than traditional models because of their semantics: everything that does not violate constraints is permissible. Though constraint-based representations are elastic, changes to process descriptions might be desired to comply with evolving business domains and exceptional situations. Elasticity can be enlarged by run-time support for dynamic changes. Transferring instances to a new model and ad-hoc changes. Changing the process definition for one instance. Proposed a general framework for a constraintbased process modeling language and its implementation. Approach supports both ad-hoc as well as dynamic changes.

2) 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.

3) A Paper on “The FERET database and evaluation procedure for face-recognition algorithms”. AUTHORS: K. Choi, H. Byun, and K.-A. Toh. This database is a large database of facial images, divided into expansion and repossessed parts. The development part is made available to researchers, and the repossessed portion is for testing face recognition algorithms. The FERET assessment process was designed to: (1) allow a comparison between different algorithms, (2) identify the most important procedures, (3) examine the state of the art in recognition, (4) identify future guidelines of research, and (5) improvement of state of the art in FR.

4) A Paper on “Proceedings of the 6th international conference on Multiple Classifier Systems” AUTHORS: K.-B. Duan and S. S. Keerthi. Cooperative multi agent systems MAS are ones in which several agents attempt through their



interaction to jointly solve tasks. Because of communications among the agents, multi-agent problem complexity can rise with increase agents or their behavioral superiority. Provided a broad survey of the cooperative multi-agent learning literature. Past surveys of this area have largely concentrated on issues to particular subareas e.g. robotics. In this survey, they attempt to draw from multi-agent learning work in a spectrum of areas including RL, evolving computation, game theory, agent modeling, and robotics. They found it leads to a division of the work into two categories. Applying a single learner to discover joint solutions to multi-agent problems which is called as team learning or using multiple parallel learners one per agent concurrent learning. They conclude with a presentation of multi-agent learning problem domains and resources.

5) 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. RESEARCH ELABORATION

3.1. EXISTING SYSTEM

Adaptive Privacy Policy Prediction (A3P) A3P system 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.

3.1.1 Disadvantages of Existing System

1. Lots of manual work
2. Affected by noise

3.2. PROPOSED SYSTEM

To enable sharing of pictures or images in secure manner so that privacy is maintained and there will be less possibility of loss of information. We will propose to empower people conceivably in a photograph to give notifications before any photo is posted online. It will distinguish or detect the faces to people getting affected by other person who is posting the photo online. The proposed framework is highlighted with low calculation expense and classification of the preparation set. Hypothetical investigation and analyses were directed to show adequacy and proficiency. This method of photo sharing is more trustworthy and effective in maintaining the security and privacy over online social networks.

3.2.2 Advantages of Proposed System

1. Sharing of photo efficient
2. Security of sharing photo is increased
3. Less possibility of loss of information

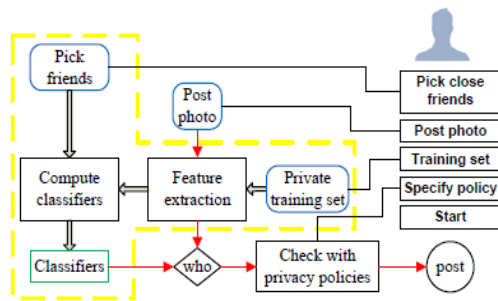


Fig. 1 System Architecture

We will propose to empower people conceivably in a photograph to give notifications before any photo is posted online. It will distinguish or detect the faces to people getting affected by other person who is posting the photo online. The proposed framework is highlighted with low calculation expense and classification of the preparation set. Hypothetical investigation and analyses were directed to show adequacy and proficiency. This method of photo sharing is more trustworthy and effective in maintaining the security and privacy over online social networks. Once user logs in greetings along with profile picture will be displayed. In the Set up the system will generate decision tree. For this purpose private training set of user is used means his photo gallery. Whenever this process of detecting the faces is going on user needs to select the close friends. From the FB survey it is identified every users has average of 150 friends and among 35 are close friends. Each of user needs to have this Application installed. In the set up mode classifiers are selected and process for creation of group where we can share the photo starts, based on privacy and exposure policy. Currently in online social applications we can't customize friends list. But here we can implement that. When a photo is posted as clicking on "Post" a notification and image will be sent to all the users who are co-owners of that photo. Coowners have

the right to accept or reject that invitation. Once that is done owner of photo can share photo, if he get the rejection he can't post the photo.

We will be using ASP.Net technologies for designing a social site like framework. And would be using SQLServer to store images and other profile information. Image processing algorithms will be used to identify/detect the faces. We will be using the profile images as reference.

3.3 PROPOSED SYSTEM ALGORITHM

3.3.1 Featurebased Approach

In featurebased approaches, local features on face such as nose, and then eyes are segmented and then used as input data for structural classifier. Pure geometry, dynamic link architecture, and hidden Markov model methods belong to this category.

Geometric featurebased approach: This technique can detect facial features such as eyes, nose, mouth, and chin. Properties of and relations (areas, distances, angles) between the features are used as descriptors for face recognition.

3.3.2 Modules Implementation

A. User Interface Design

User interface is the computers design, with the main focus on the interaction and experience of the user. The aim of user interface is to make user's interaction as simple as possible. The end user can execute the project easily with the help of GUI.

B. User Profile Creation

A user profile (user profile, or simply profile when used in-context) is a collection of personal data associated to a specific user. A profile refers therefore to the explicit digital representation of a person's identity. A user profile can also be considered as the computer representation of a user model. A user profile is a visual display of personal data associated with a specific user, or a customized desktop environment. A profile refers



therefore to the explicit digital representation of a person's identity. A user profile can also be considered as the computer representation of a user model. A profile can be used to store the description of the characteristics of person. This information can be exploited by systems taking into account the persons' characteristics and preferences. The user personal data store in ONLINE social networks (OSNs) database that details contain informs like first name, last name, username, password, email Id, gender etc.

C. Post Wall Creation

The Website wallpost in most social network is enabled with photo sharing activities. Protected albums allow users to set their albums with access protection. This is one of the beneficial features from wallpost that who fear with photo scams on photo sharing websites. Photo tagging the option makes the photo search easier after a long period of time. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces.

D.FR Engine

To enable sharing of pictures or images in secure manner so that privacy is maintained and there will less possibility of loss of information. We will propose to empower people conceivably in a photograph to give notifications before any photo is posted online. It will distinguish or detect the faces to people getting affected by other person who is posting the photo online. The proposed framework is highlighted with low calculation expense and classification of the preparation set Hypothetical investigation and analyses were directed to show adequacy and proficiency. This method of photo sharing is more trustworthy and effective in

maintaining the security and privacy over online social networks

IV.CONCLUSION

Photograph sharing is a standout amongst the most prevalent elements in online informal organizations for example Facebook Lamentably imprudent photograph posting may uncover security of people. To control the security spillage we proposed to authorize people possibly in a photograph to provide alerts before anybody is posting a photo where user is involved. We planned a security safeguarding FR framework to identify people in a co photograph. The proposed framework is highlighted with low calculation expense. We designed a plan be exceptionally helpful in ensuring clients' protection in photograph/picture over online sites. Moreover neighborhood Facebook Recognition preparing will deplete battery rapidly. Proposed Future work is Automatic Tagging- Whenever we are posting a photo we will get a notification of automatically tagging friends, we can opt to tag the photo or reject it. 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 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 I, 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.