International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 3 (March'2016)

FACE RECOGNITION SYSTEM FOR ENHANCING PRIVACY OF PHOTO SHARING IN ONLINE SOCIAL NETWORK

E.Silambarasan,
Department of Information Technology
Saranathan College of Engineering,
Tiruchirapalli,Tamilnadu,India.

V.Amrudha Devi,
Department of Information Technology
Saranathan College of Engineering,
Tiruchirapalli,Tamilnadu,India.

A.Abirekha,
Department of Information Technology
Saranathan College of Engineering,
Tiruchirapalli,Tamilnadu,India.

P.Bhavani Devi,
Department of Information Technology
Saranathan College of Engineering,
Tiruchirapalli,Tamilnadu,India.

Abstract: Photo sharing is an attractive feature which popularizes Online Social Networks. Unfortunately, it may leak user's privacy if they are allowed to post, comment, and tag a photo freely. 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. By combining digital signature along with the shared image we can provide the data security for the image. The User can share the image combined with the steganography digital signature. If any other user who wants to share that particular image the permission request is automatically redirect to the user if the owner is giving privilege to share the data then it will be posted.

Keywords: Social network, photo privacy, secures multi-party computation, Face Recognition, support vector machine, steganography.

I.INTRODUCTION

Social-networking users unknowingly reveal certain kinds of personal information that malicious attackers could profit from to perpetrate significant privacy breaches. The first decade of the 21st century saw the popularization of the Internet and the growth of web services that facilitate participatory information sharing and collaboration. Specifically, Social Network Sites (SNS), allow users to interact with others in an unprecedented way. Recently, SNSs, more than just web applications, have become part of human culture and how society interacts. News agencies, big and small companies, governments, famous personalities and the general population all use SNSs to interact with each other.

In existing system, Conditional random field (CRF) model is used. 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 dramatically improve automatic photo annotation. The system have applied our technique to a portion of the world's largest database of hand-labeled faces, the tagged faces in personal photographs posted on the popular social network Facebook.

The main disadvantages is Currently there is no restriction with sharing of co-photos, on the contrary, social network service providers like Facebook are encouraging users to post co-photos and tag their friends in order to get more people involved. Its computation cost is very high. When posting a photo, a user is not required to ask for permissions of other users appearing in the photo. So, In this paper we proposed, the owners of shared photos can be automatically identified with or without user-generated tag First user post the image the image has contains digital signature along itself. After sharing that image if any user who will need to access that particular image it will ask the permission to the owner. The owner information's are appended with the digital signature it will automatically redirected to the user. The Advantages of our paper are to use private photos in a privacy-preserving manner and social contexts to derive a personal FR engine for any particular user. Orthogonal to the traditional cryptographic solution, we propose a consensus-based method to achieve privacy and efficiency.

II. RELATED WORK

In [2], João Paulo Pesce. Study the act of tagging pictures on the social-networking site of Facebook. It is possible to generalize them to any sensitive attribute. It cannot be treated as the actual CC of the ego-network.

In[1], Stephen Boyd, Neal Parikh, Eric Chu, Borja Pele and Jonathan Eckstein. Focus on General distributed optimization methodology. It can be used as well as lasso for obtaining a good cardinality-fit trade-off. disk throughput was shared among processes on the same machine but not across machine.

In[3], Barbara carminati Elena Ferrari Andrea Perego. An access control model for WBSNs, where policies are expressed as constraints on the type, depth, and trust level of existing relationships. It possible to enforce information interchange across multiple WBSNs. It may grant access to non-authorized users, and it is not flexible enough in denoting authorized users.

IJCRCST © 2016 | All Rights Reserved

In[5], JaeYoung Choi', Wesley De Nevel, Yong Man Ro l, and Konstantinos N Plataniotis. Use a new collaborative face recognition (FR) method that aims to improve face annotation accuracy. This is especially a critical advantage for web-based face annotation applications, which frequently have to deal with large-scale databases. It is not more efficient.

In[4], Barbara Carminati a, Elena Ferrari a, Raymond Heatherly b,*, Murat Kantarcioglu b, Bhavani Thuraisingham . Improving social network access control systems. relationships among many different social network concepts can be naturally represented using OWL. It cannot be enforced by simply supporting negative access control policies.

III. PRIVACY FOR PHOTO SHARING

The main aim of this area is to provide privacy for photo sharing in Online Social Network. This is done using face recognition system by comparing pixel of posted image with owner's image

A .*User login and Register:*
In this framework, if user is already register to our network then using email id and password as a input he/she login to him/her profile page. For new user it is necessary to register their details in sign up page.

B. *Friend Request:*
In this subsection, friend request is seeking permission for the user who wants to be a friend. They can send the request for the user than it will be redirect to the particular user. After accepting the friend request he/she will be add to the friend lists. This will be helpful to the contracts management.

C. Picking Friend:
In this section, A user needs to manually specify the set of "close friends" among their social website friends with the button "Pick friends" as their neighborhood. In this application each user picks up "close friends". All the selected friends are required to install our application to carry out.

D. *Sharing Photo:*
In this section, User can share the photo to the friends. If user who wants to protect the photo against the unauthenticated sharing user piggyback the digital signature behind the image using steganography. If any user has share the image to the another person, it automatically verify the digital signature and redirect permission to the owner. Data parsing is the technique to extract the information's from piggybacked data. In the Data parsing module digital signature and the client information is extracted from the data.

E. *Steganography:*
Image steganography is the method of hiding secure information, behind the digital media like images. In the field of information secrecy it was the high authentic method. It is better than cryptography technique.

F. *Auth*entication:
For avoiding the misuse in image sharing in online image processing the authentication of data sharing is important. If any user has share the image to others it automatically verify the digital signature and redirect permission to the owner. After owner acknowledgement it will be shared without user acknowledgement the photo would not be shared.

IV.SYSTEM OVERVIEW

A. *Implementation*
Our prototype application is implemented on windows 7 with Net Beans and Facebook interface. We use OpenCV Library 2.4.6 to carry out the face detection and Eigen face method to carry out the FR. Fig.3 shows the graphical user interface (GUI). A sign in/out button could be used for log in/out with Facebook. After logging in, a greeting message and the profile picture will be shown.

B. *Friend List Manager:*
The owner logs on to the profile and in search tab enters the friend name and click the search button to search for new friends. Then click the add friend button the friend request is sent to your friend. If he/she accepts the friend request sent by owner then his/her name is added to the friend list.These activities are managed by the friend list manager and the information is stored in friend list information database.

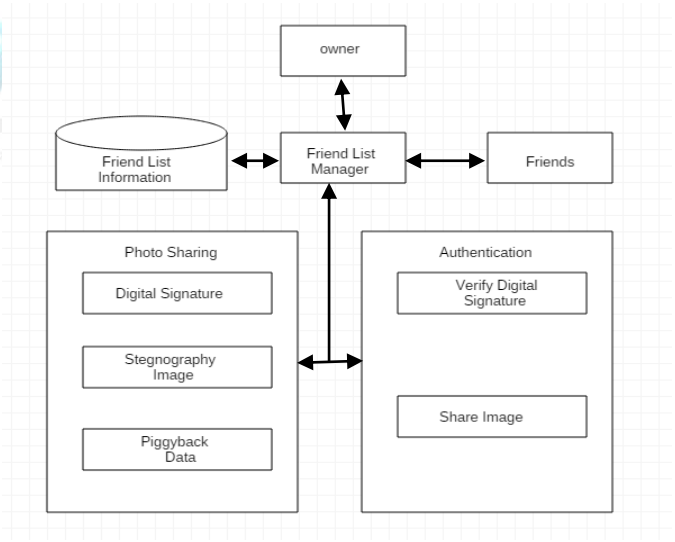

Figure 1: System architecture of our application

C. *Photo* Shar*ing:*
When user posting the photo the digital signature is generated and it is hidden behind the image which is posted using stenography method. The stenography is the technique of hiding secure information inside the text or images/video or audio. The digital signature behind the image is piggy bagged. These process are monitored by friend list manager and information are exchanged.

D. Authentication:
If any other user wants to share a photo of owner,then the digitial signature behind the photo is verified and the permission is automatically redirected to the owner.After the owner acknowledgement the photo will be shared in the

social network without the owner permission it cannot be shared

V. CONCLUSION

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 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. Moreover, 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.

VI. REFERENCES

[1] Stephen Boyd, Neal Parikh, Eric Chu, Borja Peleato and Jonathan Eckstein, "Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers",, 2010.

[2] João Paulo Pesce, "Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook", 2012.

[3] Barbara Carminati, Elena Ferrari, and Andrea Perego , "Rule-Based Access Control for Social Networks", 2006.

[4] Barbara Carminati a, Elena Ferrari a, Raymond Heatherly b,*, Murat Kantarcioglu b, Bhavani Thuraisingham, "Semantic web-based social network access control", 2011.

[5] 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", Jae Young, 2009.

[6] Hao Zhu, Alfonso Cano, and Georgios B. Giannakis, "In-Network Channel Decoding Using Consensus on Log-Likelihood Ratio Averages2008.

[7]Pedro A. Forero Alfonso Cano, Georgios B. Giannakis, "Consensus-Based Distributed Support Vector Machines", 2010.

[8] "On Private Scalar Pro duct Computation for Privacy-Pre serving Data Mining", Bart Go ethals1, Sven Laur2, Helger Lipmaa2, and Taneli Mielik¨ainen, 2005.