Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 10, October -2016

My Security My Right: Control of photograph sharing in Online Social Media: overview

Shradha Neharkar[1], Manisha Bhor[2], Nilam Shirsat[3]

[1,2,3] *Department Of Computer Engineering, Jaihind College of Engineering, Pune*

Abstract — *Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. In this paper, we attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). 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. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system[1]. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of privacy using encryption algorithm and opensource. Our mechanism is implemented as a proof of concept Android application on Face book's platform.*

Keywords- ***O****nline social networks, FR system, open social, privacy, homomorphic encryption*

I. INTRODUCTION

The Internet has become associate avertible a part of the lives of individuals these days. Gone ar the times once individuals would browse net solely to retain and even enhance their social lives through Social Networking Sites. By being attentive to your cyber-surroundings and UN agency you're reprimand, you must be ready to safely fancy social networking on-line. Our import is directed at the problem of privacy risk and user behavior so as to counsel viable solutions for users to each improve their privacy protection, and be ready to deploy the social functions expected from these styles of network. A survey was conducted to review the effectiveness of the present counter live of un-tagging and shows that this counter live is much from satisfactory users are worrying concerning violative their friends once un-tagging. As a result, they supply a tool to alter users to limit others from seeing their photos once denote as a complementary strategy to safeguard privacy. However, this technique can introduce an oversized variety of manual tasks for finish users. In, Squicciarini et al. propose a game-theoretic theme during which the privacy policies are collaboratively implemented over the shared knowledge. This happens once the looks of user has modified, or the photos within the coaching set are changed adding new pictures or deleting existing pictures. The friendly relationship graph might amendment over time. sadly, on most current OSNs, users don't have any management over the knowledge showing outside their profile page. In Thomas, Grier and Nicol examine however the dearth of joint privacy management will unknowingly reveal sensitive info a couple of user. To mitigate this threat, they counsel Facebook's privacy model to be tailored to attain multi-party privacy. In these works, versatile access management schemes supported social contexts are investigated. However, in current OSNs, once posting a photograph, a user isn't needed to provoke permissions of alternative users showing within the ikon. Basically, in our planned one-against-one strategy a user has to establish classifiers between self, friend and friend, friend conjointly referred to as the 2 loops in algorithmic rule. throughout the primary loop, there's no privacy concern of Alice's friend list as a result of friendly relationship graph is aimless. However, within the second loop, Alice have to be compelled to coordinate all her friends to create classifiers between them.

II. LITERATURE REVIEW

1. Imagined communities: Awareness, information sharing, and privacy on the Facebook
AUTHORS: A. Acquisti and R. Gross
Online social networks like Friendster, MySpace, or the Facebook have knowledgeable exponential growth in membership in recent years. These networks provide engaging suggests that for interaction and communication, however additionally raise privacy and security issues. during this study we tend to survey a stratified sample of the members of the Facebook (a social network for schools and high schools) at a USA tutorial establishment, and compare the survey

knowledge to data retrieved from the network itself. we glance for underlying demographic or behavioural variations between the communities of the network's members and non-members; we tend to analyze the impact of privacy issues on members' behavior; we tend to compare members' explicit attitudes with actual behavior; and that we document the changes in behavior after privacy-related data exposure. we discover that associate individual's privacy issues ar solely a weak predictor of his membership to the network. additionally privacy involved people be part of the network and reveal nice amounts of private data. Some manage their privacy issues by trusting their ability to manage the data they supply and also the external access to that. However, we tend to additionally realize proof of members' misconceptions regarding the net community's actual size and composition, and regarding the visibility of members' profiles.

2. Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing.
AUTHORS: S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair,
As sharing personal media on-line becomes easier and wide unfold, new privacy issues emerge - particularly once the persistent nature of the media and associated context reveals details concerning the physical and social context during which the media things were created. in a very first-of-its-kind study, we tend to use context-aware camerephone devices to look at privacy choices in mobile and on-line pic sharing. Through information analysis on a corpus of privacy choices and associated context information from a real-world system, we tend to determine relationships between location of pic capture and pic privacy settings. Our information analysis ends up in more queries that we tend to investigate through a collection of interviews with fifteen users. The interviews reveal common themes in privacy considerations: security, social speech act, identity and convenience. Finally, we tend to highlight many implications and opportunities for style of media sharing applications, together with mistreatment past privacy patterns to stop oversights and errors.

3. Why we tag: Motivations for annotation in mobile and online media
AUTHORS: M. Ames and M. Naaman,

Why do people tag? Users have mostly avoided annotating media such as photos -- both in desktop and mobile environments -- despite the many potential uses for annotations, including recall and retrieval. We investigate the incentives for annotation in Flickr, a popular web-based photo-sharing system, and ZoneTag, a cameraphone photo capture and annotation tool that uploads images to Flickr. In Flickr, annotation (as textual tags) serves both personal and social purposes, increasing incentives for tagging and resulting in a relatively high number of annotations. ZoneTag, in turn, makes it easier to tag cameraphone photos that are uploaded to Flickr by allowing annotation and suggesting relevant tags immediately after capture. A qualitative study of ZoneTag/Flickr users exposed various tagging patterns and emerging motivations for photo annotation. We offer a taxonomy of motivations for annotation in this system along two dimensions (sociality and function), and explore the various factors that people consider when tagging their photos. Our findings suggest implications for the design of digital photo organization and sharing applications, as well as other applications that incorporate user-based annotation.

4. Tagged photos: Concerns, perceptions, and protections
AUTHORS: A. Besmer and H. Lipford.
Photo sharing has become a preferred feature of the many on-line social networking sites. several of the exposure sharing applications on these sites, enable users to annotate photos with people who ar in them. variety of researchers have examined the social uses and privacy problems with on-line exposure sharing sites, however few have explored the privacy problems with exposure sharing in social networks. during this paper, we start by examining a number of our findings from a series of focus teams on exposure privacy within the social networking domain. we tend to then devise a replacement mechanism to boost exposure privacy supported these findings.

5. Prying data out of a social network
AUTHORS: J. Bonneau, J. Anderson, and G. Danezis.
Preventing adversaries from compiling significant amounts of user data is a major challenge for social network operators. We examine the difficulty of collecting profile and graph information from the popular social networking Website Facebook and report two major findings. First, we describe several novel ways in which data can be extracted by third parties. Second, we demonstrate the efficiency of these methods on crawled data. Our findings highlight how the current protection of personal data is inconsistent with user's expectations of privacy.

III. PROPOSED SYSTEM

In this paper, we tend to planned to empower folks conceivably in an exceedingly photograph to allow the consents before posting a co-photograph. we tend to printed a security protective francium framework to tell apart folks in an exceedingly co-photograph. The planned framework is highlighted with low calculation expense and classification of the preparation set. hypothetic investigation and analyses were directed to indicate adequacy and proficiency of the planned arrange. we tend to expect that our planned arrange be very useful in making certain clients' security in

photograph/picture sharing over on-line informal communities. Then again, there reliably exist exchange off within the middle of protection and utility. for example, in our gift automaton application, the co-photograph should be post with consent of all the co-proprietors. Dormancy conferred during this procedure can unbelievably have an effect on shopper expertise of OSNs. More over, near francium making ready can drop battery chop-chop.

IV. ALGORITHMS USED

Existing system
A generic face recognition system The input of a face recognition system is always an image stream. The output is an identification or verification of the subject or subjects that appear in the image.

Step1: Face detection
Face detection is defined as the process of extracting faces from scenes. So, the system positively identifies a certain image region as a face. This procedure has many applications like face tracking, pose estimation or compression.
Step2: Feature Extraction
Feature Extraction- involves obtaining relevant facial features from the data. These features could be certain face regions, variations, angles or measures, which can be human relevant (e.g. eyes spacing) or not.
Step 3: Face Recognize
In an identification task, the system would report an identity from a database. This phase involves a comparison method, a classification algorithm and an accuracy measure.

Propose System:

The ideal scenario for face detection would be one in which only frontal images were involved.

Feature occlusion:
The presence of elements like beards, glasses or hats introduces high variability. Faces can also be partially covered by objects or other faces.

Facial expression:
Facial features also vary greatly because of different facial gestures.

Imaging conditions: Different cameras and ambient conditions can affect the quality of an image, affecting the appearance of a face.

A3P
Step1: User enters the Query(Image).

Step2: A3P-Core(Classification and Adaptive policy prediction)

Step3: Content Based Classification.

Step4: Metadata Based Classification.

Step5: Policy mining

Step6: Policy prediction

Step7: Social Context modelling.

Step8: Pivotal user selection.

A3P-CORE
There are two major components in A3P-core:
(i) Image classification and (ii) Adaptive policy prediction.
For each user, his/her images are first classified based on content and metadata. Then, privacy policies of each category of images are analyzed for the policy prediction.
Content-Based Classification
Our approach to content-based classification is based on an efficient and yet accurate image similarity approach. Specifically, our classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation.

Metadata-Based Classification

The metadata-based classification groups images into subcategories under aforementioned baseline categories. The process consists of three main steps.

The first step is to extract keywords from the metadata associated with an image.

The second step is to derive a representative hypernym (denoted as h) from each metadata vector.

The third step is to find a subcategory that an image belongs to. This is an incremental procedure. At the beginning, the first image forms a subcategory as itself and the representative hypernyms of the image becomes the subcategory's representative hypernyms.

V. MATHEMATICAL MODEL

Let S is the Whole System Consists:

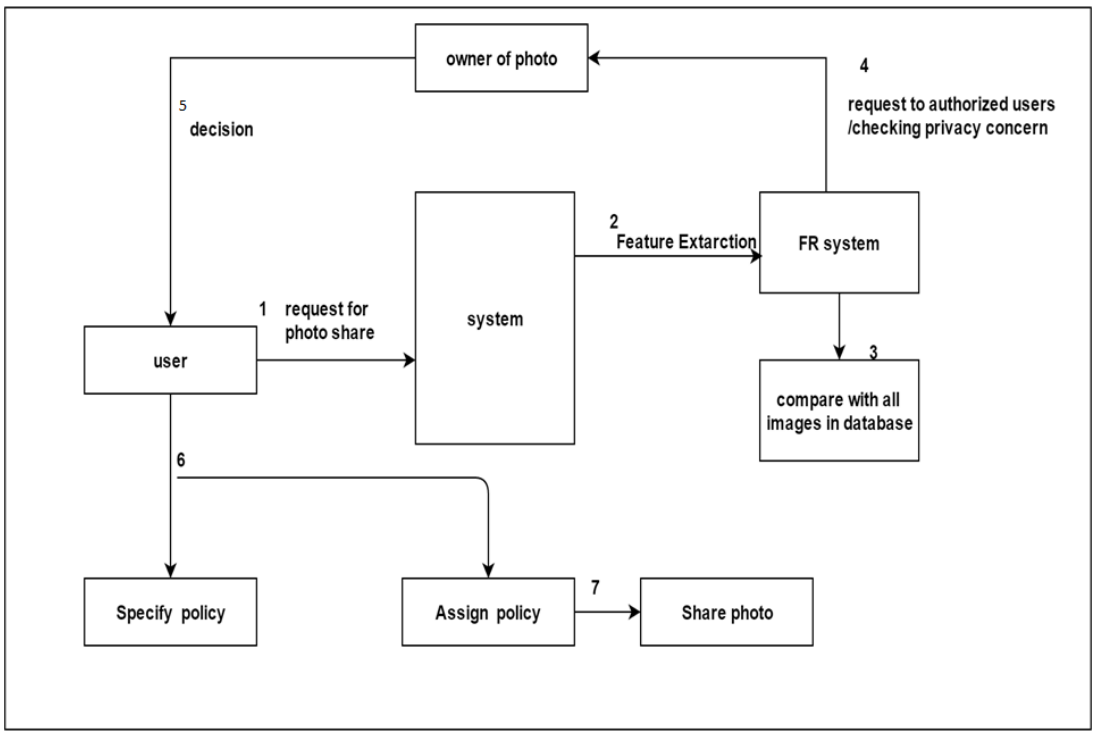
S = {U,SP,TS,PP,PF }.

1. U is the set of number users.
   U={U1,U2…Un}.
2. SP is the set of special policy.
   SP={SP1,SP2……SPn}.
3. TS is set of number tanning set.
   TS={TS1,TS2…..TSn}.
4. PF is set of numbers of post photo.
   PF={PF1,PF2…..PFn}

Step 1: user interface with GUI.
Step 2: user specify policy for security and privacy.
SP={SP1,SP2……SPn}
Step 3:user use training set for posting a photo.
TS={TS1,TS2…..TSn}.
Step 4:After getting permission post a photo.
PF={PF1,PF2…..PFn}

Output: we get a secure photo posting mechanism.

VI. SYSTEM ARCHITECTURE



VII. CONCLUSION

In this paper, we tend to planned to empower folks conceivably in an exceedingly photograph to allow the consents before posting a co-photograph. we tend to printed a security protective francium framework to tell apart folks in an exceedingly co-photograph. The planned framework is highlighted with low calculation expense and classification of the preparation set. hypothetic investigation and analyses were directed to indicate adequacy and proficiency of the planned arrange. we tend to expect that our planned arrange be very useful in making certain clients' security in photograph/picture sharing over on-line informal communities. Then again, there reliably exist exchange off within the middle of protection and utility. for example, in our gift automaton application, the co-photograph should be post with consent of all the co-proprietors. Dormancy conferred during this procedure can unbelievably have an effect on shopper expertise of OSNs.

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.

