Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 12, December-2016

Privacy Decision for controlling photo sharing on Online Social Network

Kapil Pardeshi[1], Dhiraj Patil[2], Ninad Chhatre[3], Raju Naikare[4], Prof. Deepak Gupta[5]
[1]*Computer Engineering, Siddhant College of Engineering*
[2]*Computer Engineering, Siddhant College of Engineering*
[3]*Computer Engineering, Siddhant College of Engineering*
[4]*Computer Engineering, Siddhant College of Engineering*
[5]*Computer Engineering, Siddhant College of Engineering*

Abstract —*Photo sharing is a charming component which progresses Online Social Networks (OSNs). Unfortunately, it might release users' security if they are allowed to post, comment, and mark a photo openly. In this paper, we try to address this issue and study the situations when a user shares a photo containing individuals other than him/her. To anticipate possible security spillage of a photo, we designed a system to enable each individual in a photo aware of the posting activity and share in the decision making on the photo posting. Consequently, we require a capable facial acknowledgement (FR) structure that can see everyone in the photo. In any case, all the additionally asking for security setting may control the photos' quantity freely available to design the FR system. To deal with this issue, our system attempts to utilize users' private photos to arrange an altered FR system especially arranged to isolate possible photo co-proprietors without releasing their privacy. We also add to a disseminated accords based framework to reduce the computational versatile quality and guarantee the private get ready set. We exhibit that our system is superior to anything other possible procedures to the extent acknowledgment extent and adequacy i.e. effectiveness.*

Keywords: *Social network, photo privacy, secure multi-party computation, LRR.*

I. INTRODUCTION

Photo sharing is a charming component which progresses Online Social Networks (OSNs). Unfortunately, it might release users' security if they are allowed to post, comment, and mark a photo openly. In this paper, we try to address this issue and study the sitiations when a user shares a photo containing individuals other than himself/herself. To anticipate possible security spillage of a photo, we designed a system to enable each individual in a photo aware of the posting activity and share in the decision making on the photo posting. Consequently, we require a capable facial acknowledgement(FR) structure that can see everyone in the photo. In any case, all the additionally asking for security setting may control the photos' quantity freely available to design the FR system. To deal with this issue, our system attempts to utilize users' private photos to arrange an altered FR system especially arranged to isolate possible photo co-proprietors without releasing their privacy. We also add to a disseminated accords based framework to reduce the computational versatile quality and guarantee the private get ready set. We exhibit that our system is superior to anything other possible procedures to the extent acknowledgment extent and adequacy i.e. effectiveness. In Mavridis et al. study the insights of photograph sharing on informal communities and propose a three domains show: "a social domain, in which characters are elements, what's more, kinship a connection; second, a visual tangible domain, of which faces are elements, and co-event in pictures a connection; and third, a physical domain, in which bodies have a place, with physical closeness being a connection." hey demonstrate that any two domains are very corresponded. Given data in one domain, we can give a decent estimation of the relationship of the other domain. In Stone et al., interestingly, propose to utilize the logical data in the social domain and co photo relationship to do programmed FR. They characterize a pair wise restrictive arbitrary field (CRF) model to locate the ideal joint maximizing so as to mark the contingent thickness. In particular, they utilize the current marked photographs as the preparation tests and join the photograph co event measurements and standard FR score to move forward the exactness of face annotation.

II. LITERATURE SURVEY

Paper 1: Andrew Besmer and Heather Richter Lipford.
AUTHORS: Department of Software and Information Systems

Description: The Photo tagging and sharing is a popular feature of most of the all social network sites that allows users to annotate uploaded photos with those who are in them i.e. photo, explicitly linking the photo to every person's profile. In this paper, it is examined that privacy concerns and approaches surrounding these tagged images. Utilizing a focus group, we explored the require and concerns of users, resulting in a number of design considerations for sharing and

tagged photo privacy. Furthermore, designed a privacy enhancing methodology based on our findings, and validated it by mixed method. Our results identify the social tensions that sharing and tagging generates, and the needs of privacy tools to resolve the social implications of photo privacy management.

Paper 2: On the Move to Meaningful Internet Systems
AUTHORS: M B. Carminati, E. Ferrari, and A. Perego.

Description: The degree of edibility of work management systems heavily influences the way business processes are executed. Constraint-based models are considered to be more flexible than traditional models because of their semantics: the entire thing that does not violate constraints is allowed. Although constraint-based models are flexible, changes to process dentitions might be needed to comply with evolving business domains and exceptional situations. The flexibility can be increased by run-time support for dynamic changes .transferring instances to a new model and the ad-hoc changes. Changing the process dentition for one instance. In this paper we propose a general framework for a constraint-based process modeling language and its implementation. Our approach supports both the dynamic and ad-hoc change, and the transfer of instances can be done easier than in traditional approaches.

Paper 3: Face recognition for improved face annotation in personal photo collections shared on online social networks.
AUTHORS: M. Bellare, C. Namprempre, and G. Neven

Description: Utilizing face annotation for better management of personal photos in online social networks (OSNs) is currently of considerable practical interest. In this paper, we propose a novel collaborative the face recognition (FR) approach, improving the correctness of face annotation by effectively making use of multiple FR engines available in an OSN. In particular, our collaborative FR framework consists of two parts: selection of FR engines and combing (or fusion) of multiple FR results. The selection of FR engines aims at determining a set of personalized FR engines that are related for detecting the query face images belonging to a particular user of the OSN. For this purpose, we exploit both social network context in an OSN and social context in personal image collections. Additionally, to take benefit of the availability of the multiple FR results retrieved from the selected FR engines, we devise two effective solutions for merging FR results, adopting traditional schemes for merging multiple classifier results. Experiments were conducted using 547,991 personal photos collected from an existing OSN. Our results demonstrate that the introduced collaborative FR scheme is able to significantly improve the accuracy of face annotation, compared to conventional FR approaches that only make use of a single FR engine. Further, we showed that our collaborative FR system has a low computational cost and comes with a design that is suited for deployment in a decentralized OSN.

Paper 4: The FERET database and evaluation procedure for face-recognition algorithms
AUTHORS: K. Choi, H. Byun, and K.-A. Toh.

Description: The FERET (Face Recognition Technology) program database is a huge database of facial images, divided into development and sequestered portions. The development portion is made available to researchers, and the sequestered part is reserved for testing face recognition (FR) methodologies. The FERET evaluation procedure is an independently administered test of face-recognition algorithms. The test was designed to: (1) allow a direct comparison between various algorithms, (2) identify the most promising approaches, (3) assess the state of the art in face recognition, (4) identify future directions of research, and (5) advance the state of the art in face recognition.

Paper 5: Proceedings of the 6th international conference on Multiple Classifier Systems
AUTHORS: K.-B. Duan and S. S. Keerthi.

Description: Cooperative multi-agent systems (MAS) are ones in which several agents attempt, through their interaction, to jointly solve tasks or to maximize utility. Due to the interactions among the agents, multi-agent problem complexity can rise rapidly with the number of agents or their behavioral sophistication. The challenge this presents to the task of programming solutions to MAS problems has spawned increasing interest in machine learning techniques to automate the search and optimization process. We provide a broad survey of the cooperative multi-agent learning literature. Previous surveys of this area have largely focused on issues common to specific subareas (for example, reinforcement learning, RL or robotics). In this survey we attempt to draw from multi-agent learning work in a spectrum of areas, including RL, evolutionary computation, game theory, complex systems, agent modeling, and robotics. We find that this broad view leads to a division of the work into two categories, each with its own special issues: applying a single learner to discover joint solutions to multi-agent problems (team learning), or using multiple simultaneous learners, often one per agent (concurrent learning). Additionally, we discuss direct and indirect communication in connection with learning, plus open issues in task decomposition, scalability, and adaptive dynamics. We conclude with a presentation of multi-agent learning problem domains, and a list of multi-agent learning resources.

III. EXISTING SYSTEM:

It is also this very nature of social media that makes people put more content, including images, over OSNs without more thought on the content. However, once something, such as a photo, is posted online, it becomes a permanent record, which may be used for purposes never expected. Such as, a uploaded photo in a party may reveal a connection of a celebrity to a mafia world. Because OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue. For instance, nowadays we can share any photo as we like on OSNs, regardless of whether this photo contains other people (is a co-photo) or not. At present there is no restriction with tagging and 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. The statistics of photo sharing on social networks and propose a three realms model: "a social realm, in which identities are entities, and friendship a relation; second, a visual sensory realm, of which faces are parts, and co-occurrence in images a relation; and third, a physical realm, in which bodies belong, with physical proximity being a relation." he show that any two realms are highly correlated. Given information in one realm, we can give a good estimation of the relationship of the other realm. In Stone et al., for the first time, propose to use the contextual information in the social realm and co photo relationship to do automatic FR. They define a pairwise CRF (conditional random field) model to locate the optimal joint labeling by maximizing the conditional density. Specifically, they use the existing labeled photos as the training samples and combine the photo co-occurrence the statistics and the baseline FR score to improve the accuracy of face annotation.

A. Disadvantages Of Existing System:

- Security and privacy issues
- Lack of access control to co-owned user.
- Lots of manual work .
- Affected by noise.

IV. GOALS AND OBJECTIVES

A. Goals:

1. In this project, the potential owners of shared items (photos) can be automatically identified with/without user-generated tags.
2. We propose to use private photos in a privacy-preserving manner.
3. Propose the social contexts to derive a personal FR engine for any particular user.
4. Orthogonal to the traditional cryptographic solution, we propose a consensus based method to achieve privacy and efficiency.

B. Objectives:

1. To elaborate on the privacy issues over OSNs.
2. To implement FR system.
3. To achieve the privacy for profile images in OSNs.
4. To provide a mutually acceptable privacy policy determining which content should be posted and shared

V. PROPOSED SYSTEM:

Here, 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. Privacy policy is used to define group of users that are able to access a photo only when owner permits it. Different policies are used to define group of users that are able to access when a co-owner gives access permission. In our project, we proposed to enable individuals potentially in a image to give the permissions before posting a photo. We designed a privacy-preserving FR (Face Recognition) system to identify individuals in a co-photo.

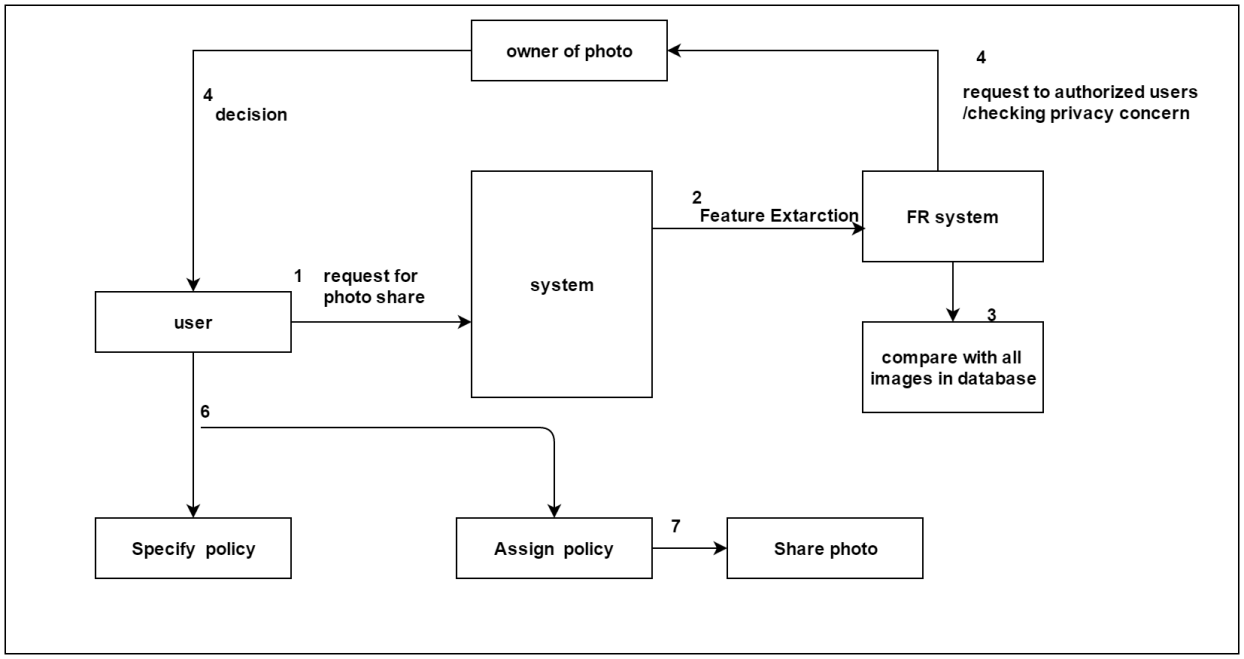

Fig. System Architecture

A. Advantages Of Proposed System:

- The proposed system is featured with low computation cost and confidentiality.
- Provides Security of sharing photo is increased.
- Less possibility of loss of information.

B. Algorithm used

1. Face Detection

Face detection is a computer technology being used in a variety of applications that identifies human faces in digital images. Face detection also refers to the psychological process by which individuals locate and attend to faces in a visual manner. Face-detection algorithms focus on the detection of frontal human faces. It is analogous to image detection in which the image of a person is matched point by point or bit by bit. Image matches with the image available in database. Any facial feature changes in the database will invalidate the matching process.

2. Low Rank Representation LRR

New method LRR which calculate the first affinity matrix using the resultant reconstruction coefficient matrix. LRR utilizes the weak supervision from image captions and also considers the image-level constraints.

VI. 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 tranning 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.

VII. CONCLUSION

We have proposed a Privacy Policy framework that assists clients with computerizing the security arrangement settings for their transferred images. The system gives a comprehensive structure to infer privacy protection inclinations considering the data accessible for a given client. We additionally viably handled the issue of utilizing social setting data. Our exploratory study demonstrates that our Privacy Policy is a tool that offers significant improvements over current approaches to privacy.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFERENCES

[1] K. Thomas, C. Grier, and D. M. Nicol. unfriendly: Multi-party privacy risks in social networks. In M. J. Atallah and N. J. Hopper, editors, Privacy Enhancing Technologies, volume 6205 of Lecture Notes in Computer Science, pages 236252.
Springer, 2010.

[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 inComputing Systems, CHI 10, pages 15631572, 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):1122, Jan. 2011.

[4] L. Kissner and D. X. Song. Privacy-preserving set operations. In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes in Computer Science, pages 241257. Springer, 2005.

[5] 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 453482. Springer London, 2010.