ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Control of Photograph Sharing On the Web Social Interpersonal Organisation

Dharani.R[#1], Vidhya lakshmi.T[#2], Deebika.S[#3], Supriya .R[#4],

Assistant Professor, Department of IT, Panimalar Institute of Technology, Chennai, India [#1]

Student, Department of IT, Panimalar Institute of Technology, Chennai, India[#2, #3, #4]

ABSTRACT: Photograph sharing is an appealing component which advances Online Social Network [OSN]. Sadly, it might release users security in the event that they are permitted to post, comment, and tag a photograph unreservedly. In this system, we endeavor to address this issue and concentrate the situation when a user shares a photograph containing people other than him/her (named co-photograph for short).To overcome the existing drawback, we require a proficient Face Recognition (FR) framework that can perceive everybody in the photograph. Implementing the more requesting protection setting may constrain the quantity of the photographs openly accessible to prepare the FR framework. To manage this problem, our instrument endeavors to use users' private photographs to outline a customized FR framework particularly prepared to separate conceivable photograph co-proprietors without releasing their security. We additionally build up a dispersed agreement based technique to decrease the computational multifaceted nature and ensure the private preparing set. We demonstrate that our framework is better than other conceivable methodologies as far as acknowledgment proportion and proficiency. Our technique is actualized as a proof of idea Android application on Facebook's stage.

KEYWORDS: Online Social Network(OSN), Privacy Preserving, Photo Sharing, Face Recognition(FR).

I. INTRODUCTION

In online social networks, the photo sharing is most attracting features.In our project, we attempt to address this vissue and study the scenario when a user shares a photo containing individuals other than himself.To prevent possible privacy leakage of a photo, we implement a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decisionmaking on the photo posting. The project also has an added advantage of creating account in a secured manner.

II. RELATED WORK

In the year of 2013 the authors **Z. Stone, T. Zickler, and T. Darrell** proposed a paper titled "**Auto tagging Facebook: Social Network Context Improves Photo Annotation".**They explained the techniques and algorithms to train support vector machines. Using the alternating direction method of multipliers, fully distributed training algorithms are obtained without exchanging training data among nodes.

In the year of 2014 authors. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Proposed a paper titled "**Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia**".Experiments were conducted using personal photos collected from an existing OSN. Our results demonstrate that the proposed collaborative FR method is able to significantly improve the accuracy of face annotation

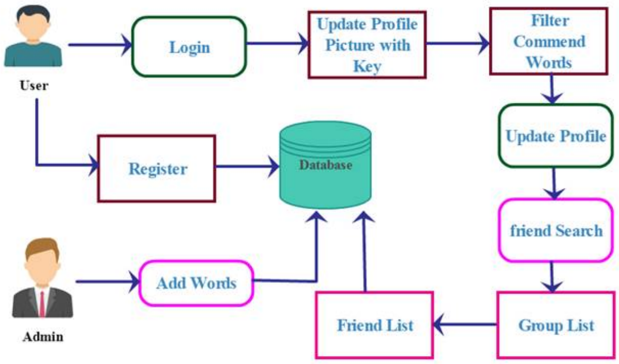


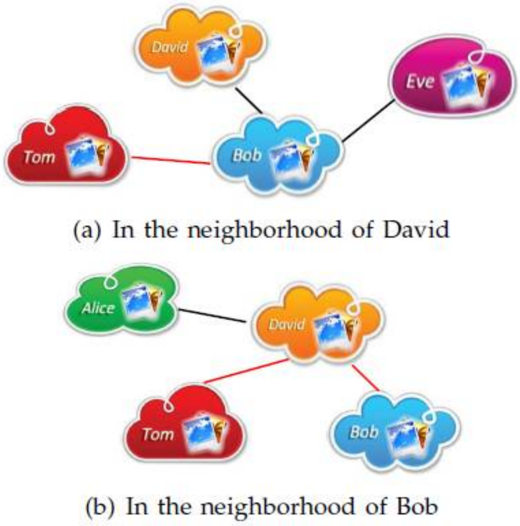
Fig.1 Proposed System Architecture

III. SYSTEM IMPLEMENTATIONS

The proposed system is composed based on several sections. All are listed and summarized below in detail.

A. Authorization and Authentication

In this section normal users create an account on this site by executing registration process providing basic details like user name, password, address, e-mail id and also phone number. After registration if the user want to access account they have to enter correct user name / e-mail id and password. If credentials are correct then server allows going to inside the websites or else user name or password alert is generated by server.



(a) In the neighborhood of David

(b) In the neighborhood of Bob

Fig.2 A. One-hop neighbor B. Two-hop neighbor

B. Details Updation and TimeLine Management

After the login, user must update him / her own profile, because this is the key process for all of the other activities in this system. In that page user enter additional information`s like Interests, schooling information, college name and other details and also select profile picture then click update profile then it will be reflected on server with automatically generated profile key. Sometimes user want to change her / him profile picture, then go to profileUpdation page,In this page select new profile picture then click update profile, then again server generate new profile key then update those details into the server. In this modules User post some image contents for share him / her feelings to other peoples means share within friends lists. This post will be displayed on the timeline of him / her friends list.

C. Friend Request and Profile Matching

In this section user enter some of the string into the search bar and then send this string as request to the server.When receive this requests then server automatically checks the possibility of results and then respond to the requested user,This response has only name of the persons, does not contain any information. If user wants to friend with any member from these lists then select parameters and then send friend request. Whenever an user make a friend requests then this module will be executed by server itself. Server Initially get the another user name and profile information from database and also collect profile details of requested users. After that server matches both the profiles with specified five parameters by using profile matching algorithm, this process is known as profile matching. Finally generate a single value based on five parameter matching.Request Received user view friends requests information's with this profile value. Based on this user may accept or reject the request.

D. Secure Profile View and Group Actions

In this module users have some lists of peoples known as friend's lists. But these peoples cannot view the profile details of another. If any user wants to view the profile then get the profile key from the profile owner and then view the profile information. In Group Actions module users are able to create group for sharing information with in specified users, so want to create group then server automatically create group key. Based on this key only group actions are performed.

IV. ISSUES IN PAST SYSTEM AND ITS RESOLUTION

In past systems, nature of social media that makes people put more content, including photos, over OSNs without too much thought on the content.The existing approaches contain lots of disadvantages, some of them are listed below:

(a) currently there is no restriction with sharing of co-photos.

(b) On the contrary, social network service providers like Facebook are encouraging users to post co-photos and tag there.

(c) Friends in order to get more people involved.

(d) Is it a privacy violation to share this co-photo without permissionss of the co-owners?

(e) Should the co-owners have some control over the co photos?

The proposed approaches contains lots of advantages, some of them are listed below:

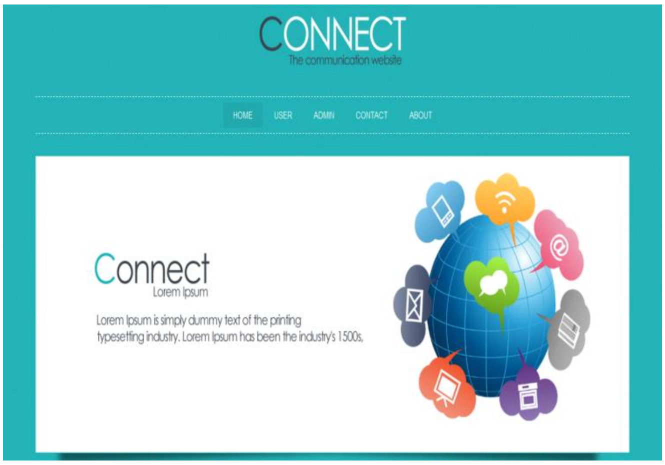
(a)The potential owners of shared items (photos) can be automatically identified with/without user-generated tags.

(b) We propose to use private photos in a privacy-preserving manner.

(c) Orthogonal to the traditional cryptographic solution, we propose a consensus-based method to achieve privacy and efficiency.

V. EXPERIMENTAL RESULTS

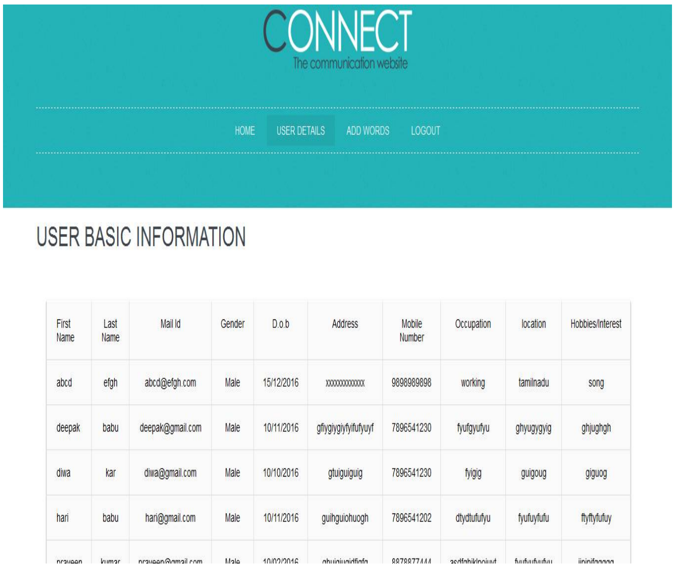
The following figure illustrates the Home page of the proposed system design.



Lorem Ipsum is simply dummy text of the printing typesetting industry. Lorem Ipsum has been the industry's 1500s,

Fig.3 Home Page Design

The following figure illustrates the User details Page design.



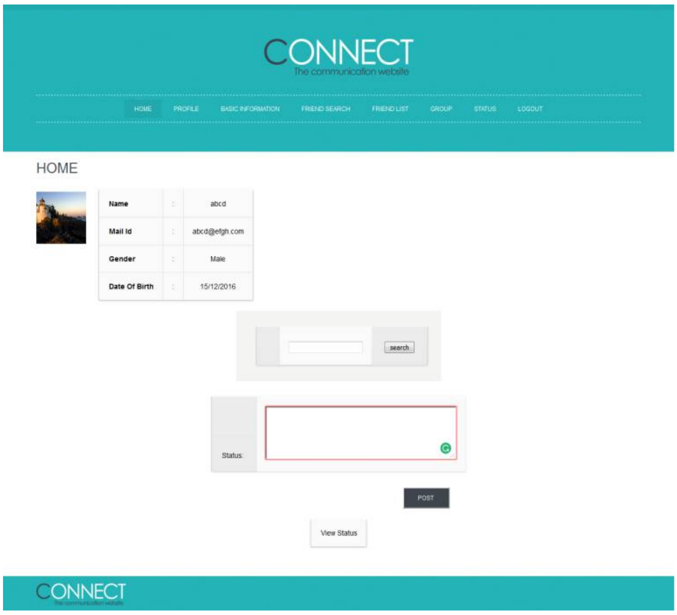
USER BASIC INFORMATION

First Name	Last Name	Mail Id	Gender	D.o.b	Address	Mobile Number	Occupation	location	Hobbies/Interest
abcd	efgh	abcd@efgh.com	Male	15/12/2016	xxxxxxxxxxxxx	9898989898	working	tamilnadu	song
deepak	babu	deepak@gmail.com	Male	10/11/2016	gfiygiygiyfyifufyuyf	7896541230	fyufgyufyu	ghyugygyig	ghjughgh
diwa	kar	diwa@gmail.com	Male	10/10/2016	gtuiguiguig	7896541230	fyigig	guigoug	giguog
hari	babu	hari@gmail.com	Male	10/11/2016	guihguiohuogh	7896541202	dtydtufufyu	fyufuyfufu	ftyftyfufuy
praveen	kumar	praveen@gmail.com	Male	10/02/2016	ghuigiugidfigfg	8878877444	asdfghjklpoiuyt	fyufyufyufyu	jipipifggggg

Fig.4 User Details Page

DOI: 10.15680/IJIRCCE.2018.0602044

The following figure illustrates the User Home Page of the proposed system design.



HOME

Name	:	abcd
Mail Id	:	abcd@efgh.com
Gender	:	Male
Date Of Birth	:	15/12/2016

Status:

Fig.5 User Home Page

VI. STEP BY STEP ALGORITHM FOR RSA ALGORITHM

Step-1:
First choose two large prime numbers p and q and find their product, n.n is also called modules in RSA jargon.

Step-2:
Compute z=(p-1)(q-1)

Step-3:
Next Choose a number e, relatively prime to z=(p-1)(q-1)- this is the encryption keysss
E<n,gcd(e,(n))=1

Step-4:
Finally compute d such that the product of e and d is congruent to 1 mod((p-1)(q-1)). This is the decryption key
e.d=1mod(n), 0<d<n.

VII. CONCLUSION

Photograph sharing is a standout amongst the most prominent highlights in online interpersonal organization.we proposed to empower people conceivably in a photograph to give the consents previously posting a co-photograph. We outlined a protection saving FR framework to recognize people in a co-photograph. The proposed framework is highlighted with low calculation cost and privacy of the preparation set. Hypothetical examination and tests were led to indicate viability and proficiency of the proposed plot. We expect that our proposed plot be extremely helpful in ensuring clients' protection in photograph/picture sharing over online informal communities. For instance, in our present Android application, the co-photograph must be post with consent of all the co-proprietors.More finished, nearby FR preparing will deplete battery rapidly. Our future work could be the means by which to move the proposed preparing plans to individual mists like Dropbox as well as icloud.

VIII. ACKNOWLEDGMENT

We would like to thank our Head Of Department Dr.A.Joshi for encouraging us and sharing her pearls of wisdom with us.We thank Mrs.R.Dharani Asst.professor for her assistance and for the comments that greatly improved the manuscript.

REFERENCES

1. H.Yu, X. Jiang, and J. Vaidya.”Privacy-preserving svm using nonlinear kernels on horizontally partitioned data”. In Proceedings of the 2006 ,ACM symposium on Applied computing 2006.
2. 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 2010
3. Z. Stone, T. Zickler, and T. Darrell.”Toward large-scale face recognition using social network context”. Proceedings of the IEEE, 98(8):2014.
4. Z. Stone, T. Zickler, and T. Darrell. “Autotagging facebook: Social network context improves photo annotation”. In Computer Vision and Pattern Recognition Workshops, 2013.
5. I. Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3):66–84, 1977.
6. 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.
7. 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.
8. 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.
9. P. A. Forero, A. Cano, and G. B. Giannakis. Consensus-based distributed support vector machines. J. Mach. Learn. Res., 99:1663–1707, August 2010.
10. 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.
11. L. Kissner and D. Song. Privacy-preserving set operations. In IN ADVANCES IN CRYPTOLOGY - CRYPTO 2005, LNCS, pages 241–257. Springer, 2005.
12. 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.
13. 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.
14. R. J. Michael Hart and A. Stent. More content - less control: Access control in the web 2.0. In Proceedings of the Workshop on Web 2.0 Security and Privacy at the IEEE Symposium on Security and Privacy, 2007.
15. M. E. Newman. The structure and function of complex networks. SIAM review, 45(2):167–256, 2003.
16. L. Palen. Unpacking privacy for a networked world. pages 129–136. Press, 2003.