International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

My Privacy My Decision: Control of Photo Sharing on Online Social Networks

Mr. Nallavelli Mahender
Mtech 2nd year
Department of CSE
Anurag Group of Institutions

Ms.K.Shailaja
Assistant Professor
Department of CSE
Anurag Group of Institutions

Dr.G.Vishnu Murthy
Professor ,HOD
Department of CSE
Anurag Group of Institutions

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. 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 consensusbased 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 recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Facebook's platform.*

Index Terms—Social network, photo privacy, secure multi-party computation, support vector machine, collaborative learning

INTRODUCTION O SNS have become integral part of our daily life and has profoundly changed the way we interact with each other, fulfilling our social needs– the needs for social interactions, information sharing, appreciation and respect. It is also this very nature of social media that makes

people put more content, including photos, over OSNs without too much 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 we never expect. For example, a posted 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. When more functions such as photo sharing and tagging are added, the situation becomes more complicated. 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. 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. However, what if the co-owners of a photo are not willing to share this photo? Is it a privacy violation to share this cophoto without permission of the co-owners? Should the co-owners have some control over the co-photos? To answer these questions, we need to elaborate on the privacy issues over OSNs. Traditionally, privacy is regarded as a state of social withdrawal. According to Altman's privacy regulation theory [1][15], privacy is a dialectic and dynamic boundary regulation process where privacy is not static but "a selective control of access to the self or to ones group". In this theory, "dialectic" refers to the openness and closeness of self to others and "dynamic" means the desired privacy level changes with time according to environment. During the process of privacy regulation, we strive to match the achieved privacy level to the desired one. At the optimum privacy level, we can experience the desired confidence when we want to hide or enjoy the desired attention when we want to show. However, if the actual level of privacy is greater than the desired one, we will feel lonely or isolated; on the other hand, if the actual level of privacy is smaller than the desired one, we will feel over-exposed and vulnerable. Unfortunately, on most current OSNs, users have no control over the information appearing outside their profile page. In [21], Thomas, Grier and Nicol examine how the lack of joint privacy control can inadvertently reveal sensitive information about a user. To mitigate this threat, they suggest Facebook's privacy

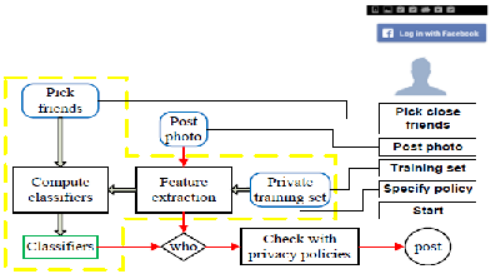
model to be adapted to achieve multi-party privacy. Specifically, there should be a mutually acceptable privacy policy determining which information should be posted and shared. To achieve this, OSN users are asked to specify a privacy policy and a exposure policy. Privacy policy is used to define group of users that are able to access a photo when being the owner, while exposure policy is used to define group of users that are able to access when being a co-owner. These two policies will together mutually specify how a co-photo could be accessed. However, before examining these policies, finding identities in cophotos is the first and probably the most import step. In the rest of this paper we will focus on a RF engine to find identities on a co-photo. FR problems over OSNs are easier than a regular FR problem because the contextual information of OSN could be utilized for FR[20]. For example, people showing up together on a co-photo are very likely to be friends on OSNs, and thus, the FR engine could be trained to recognize social friends (people in social circle) specifically. Training techniques could be adapted from the off-the-shelf FR training algorithms, but how to get enough training samples is tricky. FR engine with higher recognition ratio demands more training samples (photos of each specific person), but online photo resources are often insufficient. Users care about privacy are unlikely to put photos online. Perhaps it is exactly those people who really want to have a photo privacy protection scheme. To break this dilemma, we propose a privacy-preserving distributed collaborative training system as our FR engine. In our system, we ask each of our users to establish a private photo set of their own. We use these private photos to build personal FR engines based on the specific social context and promise that during FR training, only the discriminating rules are revealed but nothing else. With the training data (private photo sets) distributed among users, this problem could be formulated as a typical secure multi-party computation problem. Intuitively, we may apply cryptographic technique to protect the private photos, but the computational and communication cost may pose a serious problem for a large OSN. In this paper, we propose a novel consensusbased approach to achieve efficiency and privacy at the same time. The idea is to let each user only deal with his/her private photo set as the local train data and use it to learn out the local training result. After this, local training

results are exchanged among users to form a global knowledge. In the next round, each user learns over his/hers local data again by taking the global knowledge as a reference. Finally the information will be spread over users and consensus could be reached. We show later that by performing local learning in parallel, efficiency and privacy could be achieved at the same time. Comparing with previous works, our contributions are as follows. 1) In our paper, 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 and social contexts to derive a personal FR engine for any particular user. 3) Orthogonal to the traditional cryptographic solution, we propose a consensus-based method to achieve privacy and efficiency

RELATED WORK In [12], Mavridis et al. study 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 entities, and co-occurrence in images a relation; and third, a physical realm, in which bodies belong, with physical proximity being a relation." They 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 [19], [20], Stone et al., for the first time, propose to use the contextual information in the social realm and cophoto relationship to do automatic FR. They define a pairwise conditional random field (CRF) model to find the optimal joint labeling by maximizing the conditional density. Specifically, they use the existing labeled photos as the training samples and combine the photo cooccurrence statistics and baseline FR score to improve the accuracy of face annotation. In [6], Choi et al. discuss the difference between the traditional FR system and the FR system that is designed specifically for OSNs. They point out that a customized FR system for each user is expected to be much more accurate in his/her own photo collections. A similar work is done in [5], in which Choi et al. propose to use multiple personal FR engines to work collaboratively to improve the recognition ratio. Specifically, they use the social context to select the suitable FR engines that contain the identity of the queried face image with high probability While intensive research interests lie in FR

engines refined by social connections, the security and privacy issues in OSNs also emerge as important and crucial research topics. In [17], the privacy leakage caused by the poor access control of shared data in Web 2.0 is well studied. To deal with this issue, access control schemes are proposed in [13] and [4]. In these works, flexible access control schemes based on social contexts are investigated. However, in current OSNs, when posting a photo, a user is not required to ask for permissions of other users appearing in the photo. In [2], Besmer and Lipford study the privacy concerns on photo sharing and tagging features on Facebook. A survey was conducted in [2] to study the effectiveness of the existing countermeasure of untagging and shows that this countermeasure is far from satisfactory: users are worrying about offending their friends when untagging. As a result, they provide a tool to enable users to restrict others from seeing their photos when posted as a complementary strategy to protect privacy. However, this method will introduce a large number of manual tasks for end users. In [18], Squicciarini et al. propose a game-theoretic scheme in which the privacy policies are collaboratively enforced over the shared data. Each user is able to define his/her privacy policy and exposure policy. Only when a photo is processed with owner's privacy policy and co-owner's exposure policy could it be posted. However, the co-owners of a co-photo cannot be determined automatically, instead, potential co-owners could only be identified by using the tagging features on the current OSNs.

SYSTEM ARCHITECTURE:



CONCLUSION AND DISCUSSION

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 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. Our future work could be how to move the proposed training schemes to personal clouds like Dropbox and/or icloud.

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.

[11] 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.

[12] 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.

[13] 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. [14] M. E. Newman. The structure and function of complex networks. SIAM review, 45(2):167–256, 2003.

[15] L. Palen. Unpacking privacy for a networked world. pages 129– 136. Press, 2003. [16] J. C. Platt, N. Cristianini, and J. Shawe-taylor. Large margin dags for multiclass classification. In Advances in Neural Information Processing Systems 12, pages 547–553, 2000.

[17] D. Rosenblum. What anyone can know: The privacy risks of social networking sites. Security Privacy, IEEE, 5(3):40–49, 2007.

[18] 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, WWW '09, pages 521–530, New York, NY, USA, 2009. ACM.

[19] Z. Stone, T. Zickler, and T. Darrell. Toward large-scale face recognition using social network context. Proceedings of the IEEE, 98(8):1408–1415.

[20] Z. Stone, T. Zickler, and T. Darrell. Autotagging facebook: Social network context improves photo annotation. In Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on, pages 1–8. IEEE, 2008.

[21] 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 236–252. Springer, 2010.

[22] M. Turk and A. Pentland. Eigenfaces for recognition. Journal of cognitive neuroscience, 3(1):71–86, 1991.

Author Details

Mr.Nallavelli Mahender

Mtech 2nd year

Department of CSE

Anurag Group of Institutions

Ms.K.Shailaja

Assistant Professor

Department of CSE

Anurag Group of Institutions

Dr.G.Vishnu Murthy

Professor ,HOD

Department of CSE

Anurag Group of Institutions