International Journal for Modern Trends in Science and Technology, 8(09): 196-199, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809041
Available online at: http://www.ijmtst.com/vol8issue09.html

Photo Sharing in Online Social Networks that Respects Privacy Based in Trust

T Padam Santhoshi [1] | K Lakshamana Reddy[2]

[1]Master of Computer Applications (MCA), SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
T Padam Santhoshi and K Lakshamana Reddy. Photo Sharing in Online Social Networks that Respects Privacy Based in Trust. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 196-199. https://doi.org/10.46501/IJMTST0809041

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

With the development of social media technologies, sharing photos in onlinesocial networks has now become a popular way for users to maintain social connections with others. However, the rich information contained in a photo makes it easier for a malicious viewer to infer sensitive information about those who appear in the photo. How to deal with the privacy disclosure problem incurred by photo sharing has attracted much attention in recent years. When sharing a photo that involves multiple users, the publisher of the photo should take into all related users' privacy into account. In this paper, we propose a trust-based privacy preserving mechanism for sharing such co-owned photos. The basic idea is to anonymize the original photo so that users who may suffer a high privacy loss from the sharing of the photo cannot be identified from the anonymized photo. The privacy loss to a user depends on how much he trusts the receiver of the photo. And the user's trust in the publisher is affected by the privacy loss. Simulation results demonstrate that the trust-based photo sharing mechanism is helpful to reduce the privacy loss, and the proposed threshold tuning method can bring a good payoff to the user.

1. INTRODUCTION

Social media , which enable people to interact with each other by creating and sharing information, has now become an imporatant part of our daily life. Users of social media services create a huge amount of information in forms of text posts, digital photos or videos. Such user-generated content is the lifeblood of social media . However, user-generated content usually involves the creator's sensitive information, which means the sharing of such content may compromise the creator's privacy. How to deal with the privacy issues caused by information sharing is a long active topic in the study of social media . A major form of the content sharing activities in social media websites is the sharing of digital photos. Some popular online social networking services, such as Instagram1 , Flicker2 , and Pinterest3 , are mainly designed for photo sharing. Compared to textual textual data, photos can deliver more detailed information to the viewer, which is detrimental to individual's privacy. Moreover, the background information contains in a photo may be utilized by a malicious viewer to infer one's sensitive information. On the good side, it is more convenient for a user to hide his sensitive information, without too much damage to insensitive information, by image processing (e.g. blurring) than by text editing. In this paper we study the privacy issue raised by photo sharing in online social networks (OSNs). Privacy policies in current OSNs are

mainly about how a user's information will be explored by the service provider, and through which methods a user can control the scope of information sharing. Most OSNs offer a privacy setting function to their users . A user can specify, usually based on his relationships with others, which users are allowed to access the photo he shares. It should be noted that the photo shared by a user may relate to other users. If the sharing of such photos is fully controlled by one user, then the privacy of other related users may be compromised.

2. LITERATURE SURVEY

As sharing personal media online becomes easier and widely spread, new privacy concerns emerge – especially when the persistent nature of the media and associated context reveals details about the physical and social context in which the media items were created. In a first-of-its-kind study, we use context-aware camerephone devices to examine privacy decisions in mobile and online photo sharing. Through data analysis on a corpus of privacy decisions and associated context data from a real-world system, we identify relationships between location of photo capture and photo privacy settings. Our data analysis leads to further questions which we investigate through a set of interviews with 15 users. The interviews reveal common themes in privacy considerations: *security*, *socialdisclosure*, *identity* and *convenience*. Finally, we highlight several implications and opportunities for design of media sharing applications, including using past privacy patterns to prevent oversights and errors.

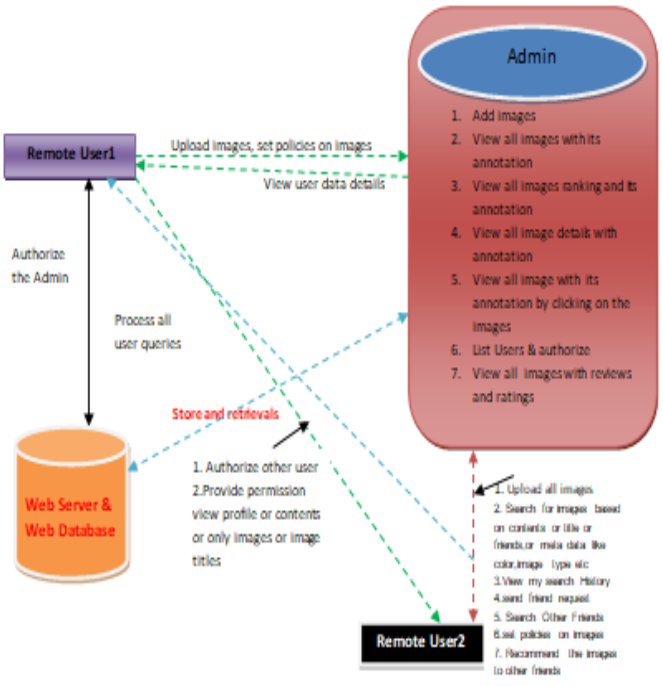
#2.Privacy Suites: Shared Privacy for Social Networks

Creating privacy controls for social networks that are both expressive and usable is a major challenge. Lack of user un- derstanding of privacy settings can lead to unwanted disclosure of private information and, in some cases, to material harm. We propose a new paradigm which allows users to easily choose \suites" of privacy settings which have been speci_ed by friends or trusted experts, only modifying them if they wish. Given that most users currently stick with their default, operator-chosen settings, such a system could dramatically increase the privacy protection that most users experience with minimal time investment.

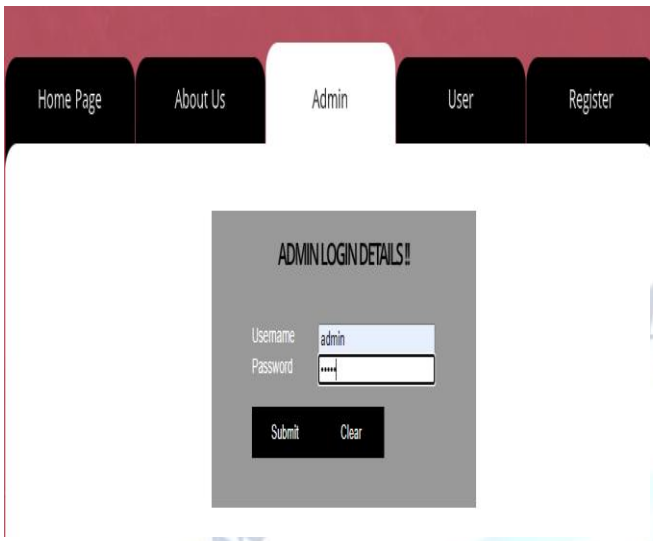
3. PROBLEM STATEMENT

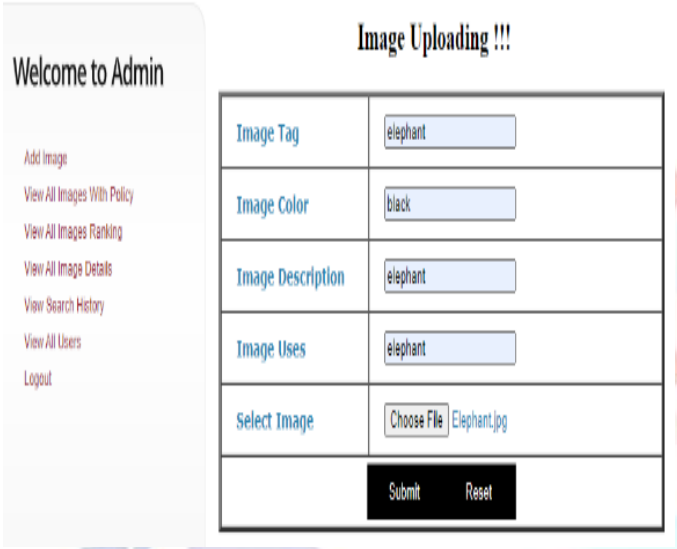
In our previous work [10], a trust-based mechanism is proposed for collaborative privacy management in OSNs. The proposed mechanism requires a user to solicit related users' opinions before sharing a data item with others. The trust values between users are utilized to generate an aggregated option. By comparing the aggregated option with a threshold, the user decides whether to share the data item. Previous studies usually consider the data item to be shared as a whole. That is to say, a user can either obtain all the information contained in the data item or get nothing. However, the aggregated access control policy cannot always make every related user satisfied. In the above example, suppose there is another user David in the photo taken by Alice. If both Alice and David want Charlie to have this photo and Bob does not, then the aggregated policy generated by a majority voting scheme will authorize Charlie to view this photo. As a result, Bob's privacy is still compromised. While in fact, in the case of photo sharing, it is possible to completely resolve the conflicts among users' privacy requirements, though it is hard to realize in the case of textual data sharing. The rationale is that a photo can be divided into multiple disjoint areas. Each area can be correlated to a specific user. If we delete this area or make the area blurred,
then the corresponding user's privacy can be preserved when the photo is accessible to an undesired user.

4. ARCHITECTURE



5. RESULTS





6. CONCLUSION

Sharing one co-owned photo in an OSN may compromise multiple users' privacy. To deal with such a privacy issue, in this paper we propose a privacy-preserving photo sharing mechanism which utilizes trust values to decide how a photo should be anonymized. The photo that a user wants to share is temporarily holden by the service provider. Based on the trust relationship between users, the service provider estimates how much privacy loss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from the photo. After the photo is shared, each stakeholder evaluates the privacy loss he has really suffered, and his trust in the publisher changes accordingly. This trust-based mechanism motivates the publisher to protect the stakeholders' privacy. However, the anonymization operation leads a loss in the shared information. Considering that the threshold specified by the publisher controls the trade-off between privacy preserving and information sharing, we propose a service providerassisted method to help the publisher to tune the threshold. By using synthetic network data and real-world network data, we conduct a series of simulations to verify the proposed photo sharing mechanism and the threshold tuning method. Simulation results demonstrate that incorporating trust values into the photo anonymization process can help to reduce user's privacy loss, and adaptively setting the threshold is necessary for the publisher to balance between privacy preserving and photo sharing. In current study, we mainly focus on the sharing between one publisher and one receiver. Considering that in practice, a user generally shares a photo with multiple users simultaneously, we'd like to investigate such a one-to-many case in future work. The proposed threshold tuning method can be seen as a greedy method, in the sense that the publisher prefers to choose the threshold that brings him the maximal instant payoff. Due to the correlation between privacy loss and trust values, current choice of the threshold will affect the publisher's future payoffs. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] W. G. Mangold and D. J. Faulds, "Social media: The new hybrid element of the promotion mix," Business horizons, vol. 52, no. 4, pp. 357–365, 2009.

[2] A. M. Kaplan and M. Haenlein, "Users of the world, unite! the challenges and opportunities of social media," Business horizons, vol. 53, no. 1, pp. 59–68, 2010.

[3] J. A. Obar and S. S. Wildman, "Social media definition and the governance challenge-an introduction to the special issue," 2015.

[4] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, 2014.

[5] S. K. N, S. K, and D. K, "On privacy and security in social media a comprehensive study," Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st International Conference on Information Security and Privacy 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211

[6] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.
[7] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.
[8] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.
[9] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 7, pp. 1851–1863, July 2016. [10] L. Xu, C. Jiang, Y. Qian, Y. Zhao, J. Li, and Y. Ren, "Dynamic privacy pricing: A multi-armed bandit approach with time-variant rewards," IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 271–285, February 2017.
[11] M. Duggan and J. Brenner, "The demographics of social media users 2012," 2013.
[12] L. Yuan, P. Korshunov, and T. Ebrahimi, "Privacy-preserving photo sharing based on a secure jpeg," in Computer Communications Workshops, 2015, pp. 185–190.
[13] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 2, pp. 199–210, March 2017.

Authors Biography

T Padma Santhoshi currently pursuing MCA in SVKP & Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannaya University, Rajamahendravaram. Her research include Web technologies,java script ,java.

K.Lakshamana Reddy is working as Associate Professor in SVKP & Dr K S Raju Arts & Science College,Penugonda,West Godavari District, A.P. He received MCA from Andhra University, 'C' level from DOEACC, New Delhi and M.Tech from Acharya Nagarjuna University, A.P. He attended and presented papers in conferences and seminars. He has done online certifications in several courses from NPTEL. His areas of interests include Computer Networks, Network Security and Cryptography, Formal Languages and Automata Theory and Object Oriented programming languages.