International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

PHOTO SHARING IN ONLINE SOCIAL NETWORKS SHARING SITES IN TRUST BASED PRIVACY

I V N LALITHA[1], SK.SUBHANI [2]

[1] PG SCHOLAR, DEPT OF CSE, ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.

[2]ASST. PROFESSOR[M.TECH], DEPARTMENT OF CSE, ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.

ABSTRACT: With the development of social media technologies, sharing photos in online social 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. The anonymiation result of a photo is controlled by a threshold specified by the publisher. We propose a greedy method for the publisher to tune the threshold, in the purpose of balancing between the privacy preserved by anonymization and the information shared with others. 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 [1], which enable people to interact with each other by creating and sharing information, has now become an imporation 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 [2], [3]. 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 [4], [5].

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 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

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

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 [6] 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. This privacy issue can be further explained via the following example. Suppose that Alice takes a photo of herself and her friend Bob, and then shares the photo to her colleague Charlie without telling Bob. If Bob does not know Charlie well, then the sharing of the photo will becomes a privacy invasion to Bob.

2.LITERATUREREVIEW

Social media: The new hybrid element of the promotion mix by W. G. Mangold and D. J. Faulds

The emergence of Internet-based social media has made it possible for one person to communicate with hundreds or even thousands of other people about products and the companies that provide them. Thus, the impact of consumer-to-consumer communications has been greatly magnified in the marketplace. This article argues that social media is a hybrid element of the promotion mix because in a traditional sense it enables companies to talk to their customers, while in a nontraditional sense it enables customers to talk directly to one another. The content, timing, and frequency of the social media-based conversations occurring between consumers are outside managers' direct control. This stands in contrast to the traditional integrated marketing communications paradigm whereby a high degree of control is present. Therefore, managers must learn to shape consumer discussions in a manner that is consistent with the organization's mission and performance goals. Methods by which this can be accomplished are delineated herein. They include providing consumers with networking platforms, and using blogs, social media tools, and promotional tools to engage customers.

Users of the world, unite! The challenges and opportunities of social media by A. M. Kaplan and M. Haenlein

The concept of Social Media is top of the agenda for many business executives today. Decision makers, as well as consultants, try to identify ways in which firms can make profitable use of applications such as Wikipedia, YouTube, Facebook, Second Life, and Twitter. Yet despite this interest, there seems to be very limited understanding of what the term "Social Media" exactly means; this article intends to provide some clarification. We begin by describing the concept of Social Media, and discuss how it differs from related concepts such as Web 2.0 and User Generated Content. Based on this definition, we then provide a classification of Social Media which groups applications currently subsumed under the generalized term into more specific categories by characteristic: collaborative projects, blogs, content communities, social networking sites, virtual game worlds, and virtual social worlds. Finally, we present 10 pieces of advice for companies which decide to utilize Social Media.

3.EXISTING SYSTEM

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

In [12], Yuan et al. proposed a privacy-preserving photo sharing framework which uses visual obfuscation technique to protect users' privacy. When processing a photo, the proposed framework considers both the content and the context of a photo. In [13], Xu et al. designed a mechanism that enables all the related users of a photo participate in the decision making process of photo sharing. With the help of a facial recognition technique, they developed a distributed consensus based method to generate the final decision. Based on the encryption algorithm proposed in [14], Ma et al. proposed a key management scheme to authorize and repeal a user's privilege of accessing multimedia data [15].

With the help of image processing techniques, we can realize a fine-grained privacy management of photo sharing. In [16], Ilia et al. proposed an access control model for photo sharing, where a photo is transformed into a set of layers each of which contains a single blurred face. Based on each user's privacy policy, the final photo presented to a viewer is generated by superimposing certain layers.

In [17], Lee et al. proposed a multiparty access model for photo sharing in OSNs, where the granularity of access control can be gradually tuned from photo level to face level. In [18], Vishwamitra et al. proposed a collaborative privacy management approach for photo sharing in OSNs. The proposed approach considers the personally identifiable information (PII) items in a photo, and designs a conflict resolution method for PII-level access control policies. The photo sharing mechanism proposed in this paper also aims at a fine-grained privacy protection for users. Different from previous studies, the mechanism proposed in this paper does not utilize the access control policies of related users to make the decision on photo sharing. Instead, the service provider estimates the privacy loss to each related user, and then decides which users' privacy should be preserved.

In the decentralized online social network proposed by Datta et al. [20], a user can tell another user with whom he trusts most to store his profile. Based on the access control policies provide by other users, a user can decide with whom to share the sensitive information. In [21], Rathore et al. proposed a trust-based access control model for resource sharing. The model considers the authorization requirements of all related users. And the trust between users is utilized to resolve the conflict among different users' access control policies.

In [22], Gay et al. proposed a relationship-based access control mechanism with which users can control how their data are reshared. And they built a trust model to quantify user relationships. In [23], Yu et al. applied deep learning algorithm to determine the privacy settings for photo sharing.

There is no threshold based access control on Photo Sharing in online social network.

Less security due to no fine-grained privacy management of photo sharing.

4. PROPOSED SYSTEM

In the proposed, the system considers a photo-sharing scenario where the user who publishes the photo, referred to as publisher, decides how to process the photo so as to protect privacy of related users. A trust-based mechanism is proposed to help the publisher make a proper decision. Different from our previous work [10], the publisher does not communicate with other related users before he posts the photo. Instead, the publisher predicts the privacy loss to each

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

related user in case that the photo is shared with a certain user.

The system explores the trust between users to measure the privacy loss. The basic idea is that whether a user allows another user to learn his sensitive information depends on how much the former trusts the latter. Also, whether a user is willing to protect another user's privacy depends on how much the former trusts the latter. Basically, if the publisher predicts a high privacy loss to a related user who is also highly trusted by the publisher, then the publisher will "delete" the user from the photo by processing the corresponding area of the photo.

Those related users are not directly involved in the decision making process of the publisher. After the photo is processed and sent to the user designated by the publisher, each related user can evaluate whether his privacy is disclosed. If the user suffers a privacy loss, he will lose trust in the publisher. And if the user finds that his privacy is protected by the publisher, he may have more trust in the publisher. Due to the correlation between privacy and trust, the publisher will not ignore other users' privacy when sharing photos.

Intuitively, if the publisher deletes all users from the photo, then no one will suffer a privacy loss, and the publisher will gain more trust from others. As a result, the publisher's privacy will be more valued by other users. However, with all user related information being deleted, the sharing of the photo becomes meaningless. In the proposed mechanism, a threshold is introduced to control the number of users deleted from a photo. To find a balance between privacy preserving and photo sharing, we propose a method to make the threshold adaptive to the trust relationship between users. The main contributions of this paper are summarized as follows:

A trust-based mechanism is proposed for photo sharing in OSNs. The trust values between users are utilized to determine whether a user's privacy will be protected. The trust values are updated according to the privacy loss, and the proposed mechanism can prevent the user from ignoring other users' privacy.

To balance between photo sharing and privacy preserving, we propose a method to tune the threshold that determines the number of users deleted from a photo.

The system has conducted a series of simulations to demonstrate the effectiveness of the proposed methods.

More Security due to Trust-based Photo Anonymization and Trust-based Privacy-Preserving Approaches.

A threshold is introduced to control the number of users deleted from a photo. To find a balance between privacy preserving and photo sharing, the system proposes a method to make the threshold adaptive to the trust relationship between users.

5.SYSTEM ARCHITECTURE

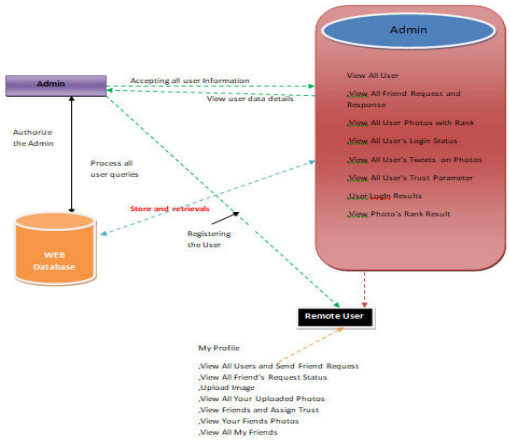

Fig 1 Architecture Diagram

6.IMPLEMENTATION

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Photo privacy:
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.

Social network:
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. 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 pair wise 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 co occurrence statistics and baseline FR score to improve the accuracy of face annotation. 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. social networks such as Face book. 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.

Friend list:
Basically, in our proposed one-against-one strategy a user needs to establish classifiers between self, friend and friend, friend also known as the two loops in Algorithm. 2. During the first loop, there is no privacy concerns of Alice's friend list because friendship graph is undirected. However, in the second loop, Alice need to coordinate all her friends to build classifiers between them. According to our protocol, her friends only communicate with her and they have no idea of what they are computing for. Friend list could also be revealed during the classifier reuse stage. For example, suppose Alice want to find ubt between Bob and Tom, which has already been computed by Bob. Alice will first query user k to see if ukj has already been computed. If this query is made in plaintext, Bob immediately knows Alice and Bob are friends. To address this problem, Alice will first make a list for desired classifiers use private set operations in [10] to query against her neighbors'

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

classifiers lists one by one. Classifiers in the intersection part will be reused. Notice that even with this protection, mutual friends between Alice and Bob are still revealed to Bob, this is the trade-off we made for classifiers reuse. Actually, OSNs like Face book shows mutual friends anyway and there is no such privacy setting as "hide mutual friends"

Collaborative Learning:

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. 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 This data isolation property is the essence of our secure collaborative learning model and the detailed security analysis. With KKT conditions and Wolfe dual, detailed iterative updates are listed in Eq

7.SCREEN SHOTS

8.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 provider assisted 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.

BIBILOGRAPHY

[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.
[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
[15] C. Ma, Z. Yan, and C. W. Chen, "Scalable access control for privacy aware media sharing," IEEE Transactions on Multimedia, pp. 1–1, 2018.
[16] P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '15, 2015, pp. 781–792.
[17] L. Chao,W.Wang, and Y. Guo, "A fine-grained multiparty access control model for photo sharing in osns," in IEEE First International Conference on Data Science in Cyberspace, 2016, pp. 440–445.
[18] N. Vishwamitra, Y. Li, K. Wang, H. Hu, K. Caine, and G.-J. Ahn, "Towards pii-based multiparty access control for photo sharing in online social networks," in Proceedings of the 22Nd ACM on Symposium on Access Control Models and Technologies, June 2017, pp. 155–166.
[19] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," ACM Computing Surveys, vol. 45, no. 4, pp. 47:1–47:33, August 2013.
[20] A. Datta, S. Buchegger, L. H. Vu, T. Strufe, and K. Rzadca, Decentralized Online Social Networks, 2010.
[21] N. C. Rathore and S. Tripathy, "A trust-based collaborative access control model with policy aggregation for online social networks," Social Network Analysis and Mining, vol. 7, no. 1, p. 7, 2017.
[22] R. Gay, J. Hu, H. Mantel, and S. Mazaheri, "Relationship-based access control for resharing in decentralized online social networks," in International Symposium on Foundations and Practice of Security, 2017, pp. 18–34.