International Conference on Engineering & Technology (ICET-2020)

Available at: *International Journal of Scientific Research and Engineering Development*

RESEARCH ARTICLE OPEN ACCESS

Encryption of Image for Security in Social Networks Using Support Vector Machine

Mr.T.Sathish[1], Assistant Professor,
Department Of CSE,
Selvam College of Technology, Namakkal.
Sathish.cse@selvamtech.edu.in

N.Gowshika[3], UG Student,
Department Of CSE,
Selvam College of Technology, Namakkal.
gowshikananthil@gmail.com

R.Anitha[2], UG Student,
Department Of CSE,
Selvam College of Technology, Namakkal.
anithar020799@gmail.com

S.Jayasurya[4], UG Student,
Department Of CSE,
Selvam College of Technology, Namakkal.
charlesjaisu21@gmail.com

----------**********----------

Abstract:

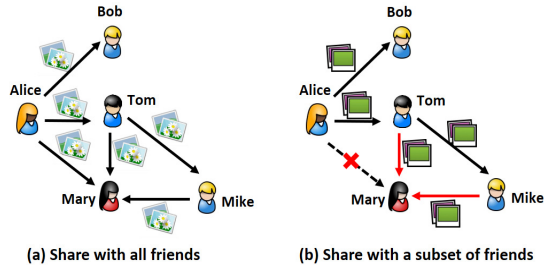
People constantly share their photos with others through various social media sites. With the aid of the privacy settings provided by social media sites, image owners can designate scope of sharing, e.g., close friends and acquaintances. However, even if the owner of a photo carefully sets the privacy setting to exclude a given individual who is not supposed to see the photo, the photo may still eventually reach a wider audience including those clearly undesired through unanticipated channels of disclosure, causing a privacy breach. Moreover, it is often the case that a given image involves multiple stakeholders who are also depicted in the photo. Due to various personalities, it is even more challenging to reach agreement on privacy settings for these multi-owner photos. In this work, we propose a privacy risk reminder system called REMIND, which estimates the probability that a shared photo may be seen by unwanted people - through the social graph - who are not included in the original sharing list. We tackle this problem from a novel angle by digging into the big data regarding image sharing history. Specifically, the social media providers possess a huge amount of image sharing information of their users. If the computed disclosure probability indicates high risks of privacy breach, a reminder is issued to the image owner to help revise the privacy settings. The proposed REMIND system also has a nice feature of policy harmonization that helps resolve privacy differences in multi-owner photos. We have carried out a user study to validate the rationale of our proposed solutions and also conducted experimental studies to evaluate the efficiency of the proposed REMIND system.

Key words: REMIND (Risk Estimation Mechanism for Images in Network Distribution)

----------**********----------

I. INTRODUCTION

With social media affecting the way millions of people live their lives each day, we have assisted to an explosion of user contributed content online, especially images and media files. Some of the user-contributed photos may be harmless and effective for users' self-recognition and gratification. However, for many of these photos, the portrayed content affects individuals' social circles, as it either explicitly includes multiple users or it relates to users other than the original poster (e.g. a child or a house/location). To further complicate this issue, photos may be leaked or disclosed with an audience larger than expected, for both the image owner and its stakeholders. To alleviate privacy concerns, many social websites provide basic privacy configurations that allow the users to specify whom they would like to share the photos with. Some social websites like Facebook offer more sophisticated privacy configuration options including the control of how the photos being re-shared among friends of friends. Another critical factor that could cause a privacy



(a) Share with all friends (b) Share with a subset of friends

breach is the difference among privacy preferences of people depicted in the same photo. Due to the variety of personalities, users may drastically disagree on the scope of sharing for a given co-owned image causing some significant conflicts. In some instances, it can be courtesy that these users may personally discuss which photos can be posted and by whom so that there are no conflicts of interest, but that takes time and is not often the route pursued. An increasing number of recent works have analyzed how to address the policy conflict, by considering every user's prior privacy preferences of sharing or through semi-automated resolution mechanisms. These existing works are usually based on fuzzy logics while we aim to provide clear evidence of chances of privacy breach.

2. RELATED WORK

Our work shares similar goals of privacy protection with existing works on privacy policy recommendation systems, privacy risk estimation and privacy violation detection in social networks. However, our proposed probability-based approach is unique that has not been explored in the past. More details are elaborated in the following. There have been many privacy policy recommendation systems. They typically utilize certain types of machine-learning algorithms to analyze users' profiles, historical privacy preferences, image content and meta data, and/or social circles, in order to predict privacy policies. Instead of relying on social circles and clustering social contexts, another thread of work looks into the image content and metadata directly In order to even better capture the users' privacy preferences, there is a new trend of hybrid approaches which combine knowledge learned from both social contexts and the image content. For example, Squicciarini et al. propose to utilize community practices for the cold start problem in new users and image classification based approaches for users with long privacy configuration history. Yu et al. consider both content sensitiveness of the images being shared and trustworthiness of the users being granted to see the images during the fine-grained privacy settings for social image sharing.

3. PROPOSED SYSTEM

Environment A is the one without the REMIND system which is similar to the existing social networks where people share images as usual. Specifically, a user is presented with an image and corresponding background story of the image so that the user can feel more personal about the image. There are total 10 scenarios and each scenario contains two images targeting female and male participants, respectively. The 10 scenarios aim to cover common cases where people may have privacy concerns, such as funny costumes, crazy parties, family vacations, selfie of bad mood, surprising gift, casual time at home, sickness, dangerous sports, and risky adventure. Then, the user is asked to select one or more groups of users that they would like to share the image. We provide six common groups for the users to choose, which are close family members, relatives, close friends, friends, co-workers, and boss. This mimic the common practice in the real social networks.

Algorithm:

A. Support Vector Machine(SVM)

A Support Vector Machine (SVM) is discriminative classifier formally defined by a separating hyper plane. In other words, given labeled training data (supervised learning), the algorithm outputs an optimal hyperplane. In this project we use svm algorithm for classifying and fetch the data.

B.3DES

In cryptography, Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block .The Data Encryption Standard's (DES) 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. However, an adapted version of DES, Triple DES (3DES), uses the same algorithm to produce a more secure encryption.

4.ADVANTAGE

Initialization: Starting from the photo owner node uo's initial sharing list, we look for the children nodes of the users in the sharing list and add them into the priority queue. Checking current node in the priority queue: Then, we examine the node in the priority queue one by one.

5. METHODOLOGY

A. Effect of the Number of Propagation Hops

In the first round of experiments, we evaluate the effect of the number of image propagation hops ranging from 1 to 5. When there is only one hop, the photo owners share the photos with their direct friends and their friends will not forward the photos to anyone else. When there are five hops, the photos will be forwarded by the photo owners' friends to the friends' friends until 5 hops.

B. The Number of Friends in the Initial Sharing

This is because the more people in the initial sharing list, the wider audience the photos may reach, which leads to a complicated sharing graph. As a result, there may be more ancestor nodes to be computed before finalizing a user's disclosure probability. Note that the wider audience also means the corresponding increase in the average disclosure probabilities

C. The Sharing Of Convergence Speed

Observe that the calculation time decreases when the sharing convergence speed increases. This is because the number of people in the sharing list at each hop decreases, and hence the overall size of the sharing graph decreases too. In other words, the smaller the scope of the sharing, the faster the calculation. **Large-Scale Testing** The number of hops for the image propagation is set to the default value 3, and each user forwards the images to 15 randomly selected friends. From the figure, we can observe that the calculation time only increases slightly with the total number of nodes in the social network. This again indicates the advantage of our proposed personal sharing graph which does not increase due to the increase of the social network size.

6. CONCLUSION

social network users a quantitative view of their image sharing risks due to friend-to-friend re-sharing. Our proposed REMIND system is based on a sophisticated probability model that models the large-scale image sharing statistic information and captures the complicated sharing propagation chains and loops. Our system also addresses the policy harmonization challenges in multi-owner photos

7. FUTURE WORKS

We have carried out both user studies and performance studies to validate the effectiveness and efficiency of our approach.

8. BIBLIOGRAPHY

[1] C. G. Akcora, B. Carminati, and E. Ferrari, “Risks of friendships on social networks,” in Data Mining (ICDM), 2012 IEEE 12th International Conference on, 2012, pp. 810–815.

[2] N. Laleh, B. Carminati, and E. Ferrari, “Graph based local risk estimation in large scale online social networks,” in IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), 2015, pp. 528–535.

[3] O¨ . Kafalı, A. Gu¨nay, and P. Yolum, “Detecting and predicting privacy violations in online social networks,” Distributed and Parallel Databases, vol. 32, no. 1, pp. 161–190, Mar 2014. Z

[4] N. Kokciyan and P. Yolum, “Priguard: A semantic approach to detect privacy violations in online social networks,” IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 10, pp. 2724– 2737, 2016.

[5] J. Bonneau, J. Anderson, and G. Danezis, “Prying data out of a social network,” in Social Network Analysis and Mining, 2009. ASONAM’09. International Conference on Advances in. IEEE, 2009, pp. 249–254.

[6] L. Fang and K. LeFevre, “Privacy wizards for social networking sites,” in Proceedings of the 19th international conference on World wide web. ACM, 2010, pp. 351–360.

[7] A. Mazzia, K. LeFevre, and E. Adar, “The pviz comprehension tool for social network privacy settings,” in Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, 2012, p. 13.

[8] R. G. Pensa and G. Di Blasi, “A semi-supervised approach to measuring user privacy in online social networks,” in Discovery Science, T. Calders, M. Ceci, and D. Malerba, Eds., Cham, 2016, pp. 392–407.

[9] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, “A3p: Adaptive policy prediction for shared images over popular content sharing sites,” in Proceedings of the 22Nd ACM Conference on Hypertext and Hypermedia, 2011, pp. 261–270.

