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

Ulhas Shelke[1], Zuber Shaikh[2], Nikhil Deshpande[3], Puja Shinde [4]
[1, 2, 3, 4] Zeal College Of Engineering And Research

Abstract-*Photo sharing is a 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. Attempt to detect this issue and study this scenario when a user shares a photo containing individuals other than himself(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, there is need of 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. 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.The power-law distribution is caused by the preferential attach process, in which the probability of a user A connecting to a user B is proportional to the number of B's existing connections. show the snapshots of the contact network and fan network in YA, respectively. We see some nodes do not have either fans or contacts, while a few nodes have a very large degree.

Keywords-Photo privacy, Social network, Friend list, Collaborative Learning

I. INTRODUCTION

Nowadays we will be giving some security password which can be hacked and can be used by the others and 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. 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 consensus based 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.

II. EXISTING SYSTEM

A survey was conducted in to study the effectiveness of the existing countermeasure of un tagging and shows that this countermeasure is far from satisfactory users are worrying about offending their friends when un tagging. 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 , Squicciarini et al. propose a game-theoretic scheme in which the privacy policies are collaboratively enforced over the shared data. This happens when the appearance of user i has changed, or the photos in the training set are modified adding new images or deleting existing images. The friendship graph may change over time.

III. PROPOSED SYSTEM

During the process of privacy regulation, we strive to match the achieved privacy level to the desired one.

Unfortunately, on most current OSNs, users have no control over the information appearing outside their profile page. In , 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 Face book's privacy model to be adapted to achieve multi-party privacy. 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 , Besmer and Lipford study the privacy concerns on photo sharing and tagging features on Facebook. A survey was conducted in 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 un tagging. 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 Squicciarini et al. propose a game-theoretic scheme in which the privacy policies are collaboratively enforced over the shared data. 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.

IV. PROPOSED SYSTEM ALGORITHMS

there are two steps to build classifiers for each neighborhood: firstly find classifiers of self, friends for each node, then find classifiers of friend, friends. Notice that the second step is tricky, because the friend list of the neighborhood owner could be revealed to all his/her friends. On the other hand, friends may not know how to communicate with each other.

Homomorphic Encryption Algorithm:

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services.

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 between Bob and Tom, which has already been computed by Bob. Alice will first query user k to see if you 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' 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".

V. SYSTEM ARCHITECTURE

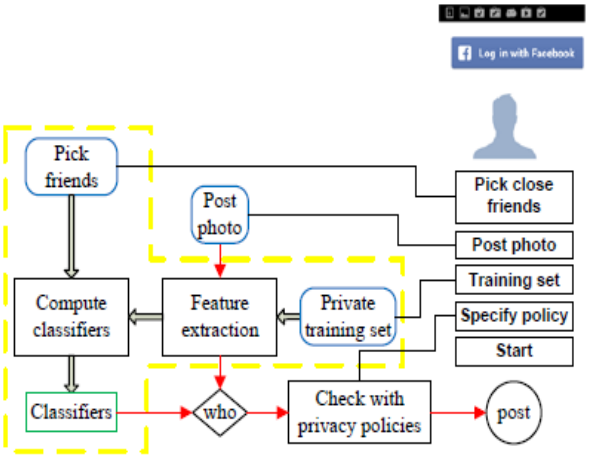

Fig. 4: System structure of our application

VI. CONCLUSION

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 potentiallyin 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.

REFERENCES

[1] Ya-qiong, P. 2007. A study on evaluation of consumer credit's risks of commer-cialbanks. In Proceeding of International Conference on Wireless Communications (WiCom 2007). pp. 4531-4534.

[2] Yu, L., Wang, S. A. and Lai, K. K. 2008. Credit risk assessment with a multistage neural network ensemble learning approach. Expert systems with applications. vol. 34. pp. 1434-1444.

[3] u, L., Wang, S. and Lai, K. K. 2009. An intelligent-agentbased fuzzy group decision making model for nancial multicriteria decision support: the case of credit scoring. Europeanjournal of operational research. vol. 195. pp. 942-959.

[4] Tsai, C.-f. and Wu, J.-w. 2008. Using neural network ensembles for bankruptcy prediction and credit scoring. Expert systems with applications. vol. 34. pp. 2639-2649.

[5] Altman, I. E. 1968. Financial ratios, discriminant analysis and the prediction of corporate banlruptcy. The journal of nance. vol. 23. pp. 589-611.

[6] Lee, T. S., and Chen, I. F. 2005. A two-stage hybrid credit scoring model using arti-cial neural networks and multivariate adaptive regression splines. Expert systems with application. vol. 28. pp. 743-752.

[7] West, D. 2000. Neural network credit scoring models. Computers and operations research. vol. 27. pp. 1131-1152.

[8] Wang, Y.-q. 2008. Building credit scoring systens based on support-based support vector machine. In proceeding of the Fourth international conference on natural computation. (ICNC 2008). pp. 323-327.

[9] Min, J. H. and Lee, Y.-C. 2005. Bankruptcy prediction using support vector machine with optimal choice of kernel function parameters. Expert systems with applications. vol. 28. pp. 603-614.

[10] Baesens, B., Van Gestel, T., Viaene, S., Stepanova, M., Suykens, J. and Vanthienen, J. 2003. Benchmarking stateof- art classi cation algorithm for credit scoring. Journal of operational research society. vol. 54. pp.