International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Privacy My Decision Control of Photo Sharing on Online Social Networks

Mrs N Pushpalatha & Shivaji Bugga
[1]Assoc professor Dept of CSE MLR Institute of Technology, Hyderabad, Telangana
[2] M.Tech CSE (PG Scholar), CSE MLR Institute of Technology, Hyderabad, Telangana

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[1]. 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 privacy using encryption algorithm and opensource. Our mechanism is implemented as a proof of concept Android application on Face book's platform.*

Keywords— **online social networks, FR system, open social, privacy, homomorphic encryption**

I. INTRODUCTION

The Internet has become an evitable part of the lives of people today. Gone are the days when people would browse the net only to retain and even enhance their social lives through Social Networking Sites. By being aware of your cyber-surroundings and who you are talking to, you should be able to safely enjoy social networking online. Our intension is directed at the issue of privacy risk and user behaviour in order to suggest viable solutions for users to both improve their privacy protection, and be able to deploy the social functions expected from these types of network.

A survey was conducted to study the effectiveness of the existing counter measure of un-tagging and shows that this counter measure 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 [2]. This happens when the appearance of user 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 [3][4]. 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 Facebook'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. 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. During the first loop, there is no privacy concern 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.

II. HOMOMORPHIC ALGORITHM

There are two steps to build classifiers for each neighborhood: firstly find classifiers of fself, friendg for each node, and then find classifiers of ffriend, friendg. 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.

A. Homomorphic Encryption Algorithm:

Homomorphic encryption is a form of encryption that allows computations to be carried out on cipher text, 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.

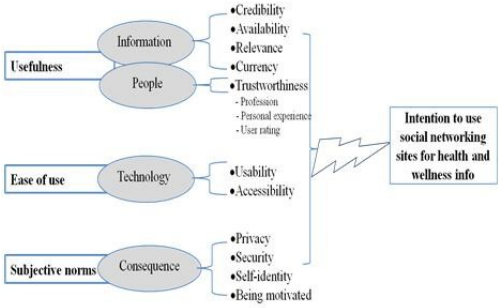

Figure1: Intention to use social networking sites

B. Photo privacy

Users' cares 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 [5]. 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.

C.Risks in Online Social Networks

The personal information shared in online social networks can harm the user in often unexpected ways Photos uploaded to online social networks can also be harmful for someone when they fall into the wrong hands. Uploading photos of a wild party might be harmless when shared with friends who were also at that party but it might not benefit the applicant if those photos fall into the hands of his spotter[8]. There's a lot of confusion about what is handled as public, semi-public or private information in online social networks. While several social networking sites offer data sharing controls, there's no standard way of checking and controlling which personal information is shared with whom.

III.OPENSOCIAL

OpenSocial is a set of APIs which is not being developed by a single online social network. Unfortunately OpenSocial was not designed with privacy in mind. It provides no way to access privacy settings. It does not provide any information about who can access which resource and also does not allow specifying with whom a resource is shared. When creating a new resource it also does not allow to differ from the default privacy setting, which is in general not known and not specified in OpenSocial[1]. The API specification was developed by a community which treats it like an open source software project. The four basic principles are:

1. Participation is open to anyone
2. Decisions are made on the spec list (not behind closed doors)
3. All proceedings are captured in a public archive
4. Individuals represent themselves, not companies

Privacy Metrics

Measuring privacy in social networks is a difficult task. It's not inherently clear which information can lead to considerable damage such as identity theft. Other risks are even harder to assess: comments and pictures which are harmless for some people can be harmful for others.

One common approach to define risk is by the following formula:

$$risk = negative\ consequence \times likelihood$$

They define the privacy risk score based on the following two premises:

1. The more sensitive data a user reveals, the higher his privacy risk is
2. The more people know some piece of information about the user, the higher his privacy risk is

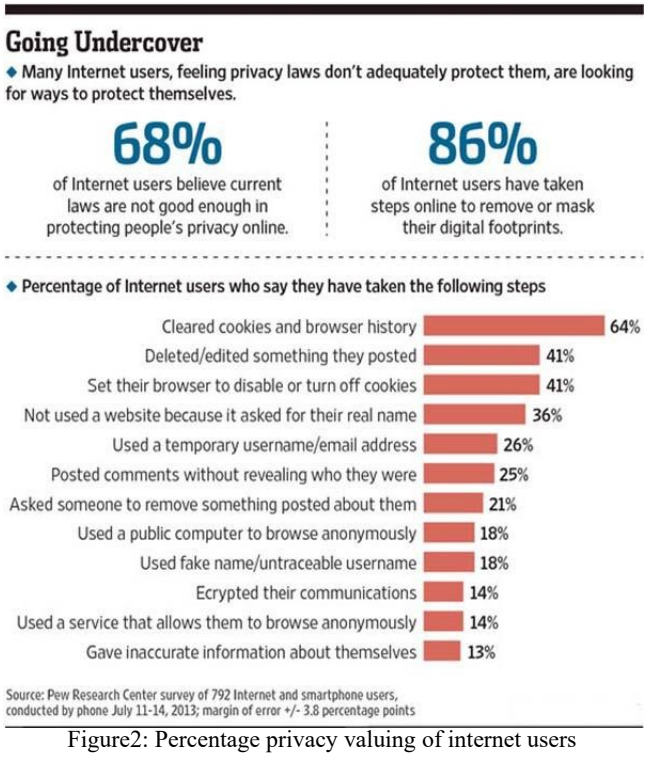

Figure2: Percentage privacy valuing of internet users

IV.CONCLUSION

Online social networks help people to socialize with the world. But users should be aware of threats that can be faced due to lack of proper privacy settings. In this paper a novel method for collaborative sharing of data in OSNs is discussed as well as a method to resolve privacy conflicts that can occur while multiple persons share a data. Evaluation results show that privacy risk and data sharing loss are minimized in this approach. Various websites offer services such as uploading, hosting, and managing for photo-sharing (publicly or privately). These functions are provided by websites and applications that facilitate the upload and display of images. The term may even be useful for online photo galleries that are positioned up and managed by individual users, including photo blogs. The system used a toy system with two users to demonstrate the principle of the design. It is very efficient than existing system. The system can reduce the privacy leakage by using opensource and Homomorphic Encryption Algorithm. The proposed system features a low computation cost and confidentiality of the training set. Future enhancement can be done by using extended futures of opensource APIs in more efficient privacy training set.

REFERENCES

[1] Open Social. specs. http://www.opensocial.org/specs, 2010.
[2] Open Social. website.http://www.opensocial.org, 2010.
[3] Face book help centre.http://www.facebook.com/help/.
[4] http://www.facebook.com/press/info.php?Statistics, 2010.
[5] World Wide Web Consortium (W3C). Platformfor privacy preferences (p3p) project.http://www.w3.org/P3P/
[6] Kaihe Xu, Yuanxiong Guo, Linke Guo, YuguangFang, Xiaolin Li, "Privacy control in photo Sharing", IEEE Transaction on Dependable and Secure Computing, Volume: PP , Issue: 99, pp-1-1, 2015
[7] Anna Cinzia Squicciarini, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge And Data Engineering, Vol. 27, no. 1, January 2015.
[8] Nithya Sara Joseph" Collaborative data sharing in online social network resolving privacy risk and sharing loss" *(IOSR-JCE) e-ISSN: 2278- 0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VI (Sep-Oct. 2014), PP 55-61*
[9] J. Lydia Jeba, R. Nandhini " A Novel Approach Of MPAC Model For Online Social Network" (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-3, February 2014
[10] A. k. Rachel Praveena, B. Dr. S. Durga Bhavani,C.k.Suresh Babu,International journal of computer science & Network Solutions December.2013-Volume 1. No4 ISSN 2345- 3397.
[11] Raynes-Goldie. (2011). Annotated Bibliography: Digitally mediated surveillance, Privacy and social network sites. (misc)
[12] A. A. Sattikar, Dr. R. V. Kulkarni"A Review of Security and Privacy Issues in Social Networking" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2784-2787.