ACCESS CONTROL THROUGH USER DECISION IN ONLINE SOCIAL NETWORK USING MODEL ACCESS CONTROL

Simikutty Antony[1] | R.Sujitha[2]

[1](UG Student, Christ the King Engineering College, simiantony955@gmail.com)
[2](Assistant Professor, Christ the King Engineering College, srisuji14@gmail.com)

Abstract— *Online Social Networks (OSNs) such as Facebook, Google, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family, and even with strangers. A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and WebPages, such as wall in Facebook, where users and friends can post content and leave messages. In addition, users can not only upload content into their own or others' spaces but also tag other users who appear in the content. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. To overcome the problem based on Online Social Networks, a systematic solution to facilitate multiparty access control (MPAC) of shared data in OSNs is introduced. The user can share their data or images to their friends. When the user is tried to share other user's data, the request will be send to the owner of the data. After receiving the request, the owner of the data has rights to accept or reject the request. The User can only share others data after getting the approval from the data owner, otherwise the user cannot share that data to others.*

Keywords— Social Network, Photo Privacy, Secure Multiparty Communication,Support Vector Machine, Collaborative Learning

1. INTRODUCTION

Online Social Networks have become integral part of our daily life and has profoundly changed the way we interact with each other, fulfilling our social needs–the needs for social interactions, information sharing, appreciation and respect. It is also this very nature of social media that makes people put more content, including photos, over OSNs without too much thought on the content. However, once something, such as a photo, is posted online, it becomes a permanent record, which may be used for purposes we never expect. For example, a posted photo in a party may reveal a connection of a celebrity to a mafia world. Because OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue. When more functions such as photo sharing and tagging are added, the situation becomes more complicated. For instance, nowadays we can share any photo as we like on OSNs, regardless of whether this photo contains other people (is a co- photo) or not. Currently there is no 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. However, what if the co-owners of a photo are not willing to share this photo? Is it a privacy violation to share this co photo without permission of the co-owners? Should the co-owners have some control over the co-photos? To answer these questions, we need to elaborate on the privacy issues over OSNs. Traditionally, privacy is regarded as a state of social withdrawal. According to Altman's privacy regulation theory , privacy is a dialectic and dynamic boundary regulation process where privacy is not static but "a selective control of access to the self or to ones group". In this theory,

"dialectic" refers to the openness and closeness of self to others and "dynamic" means the desired privacy level changes with time according to environment. During the process of privacy regulation, we strive to match the achieved privacy level to the desired one. At the optimum privacy level, we can experience the desired confidence when we want to hide or enjoy the desired attention when we want to show. In this paper, we propose a novel consensus based approach to achieve efficiency and privacy at the same time.

2.RELATED WORKS

Traditionally, privacy is regarded as a state of social withdrawal. According to Altman's privacy regulation theory , privacy is a dialectic and dynamic boundary regulation process where privacy is not static but "a selective control of access to the self or to ones group". In this theory, "dialectic" refers to the openness and closeness of self to others and "dynamic" means the desired privacy level changes with time according to environment. During the process of privacy regulation, we strive to match the achieved privacy level to the desired one. At the optimum privacy level, we can experience the desired confidence when we want to hide or enjoy the desired attention when we want to show. However, if the actual level of privacy is greater than the desired one, we will feel lonely or isolated; on the other hand, if the actual level of privacy is smaller than the desired one, we will feel over-exposed and vulnerable. 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. Specifically, there should be a mutually acceptable privacy policy shared. To achieve this, OSN users are asked to specify a privacy policy and a exposure policy. Privacy policy is used to define group of users that are able to access a photo when being the owner, while exposure policy is used to define group of users that are able to access when being a co- owner. For this a systematic solution to facilitate conflict detection of shared data in OSNs is introduced. The user can share their data or images to their friends. When the user is tried to share other user's data, the request will be send to the owner of the data. After receiving the request, the owner of the data has rights to accept or reject the request. The User can only share others data after getting the approval from the data owner, otherwise the user cannot share that data to others. To pursue a systematic solution to facilitate collaborative management of shared data in OSNs.We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data.

2.1Multiparty access control (MPAC)

To pursue a systematic solution to facilitate collaborative management of shared data in OSNs.We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data. Some typical data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, an MPAC model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs.

This system analyze three scenarios—profile sharing, relationship sharing, and con tent sharing—to understand the risks posted by the lack of collaborative control in OSNs. We leverage Face book as the running example in our discussion because it is currently the most popular and representative social network provider. In the meantime, we reiterate that our discussion could be easily extended to other existing social network platforms, such as Google++.

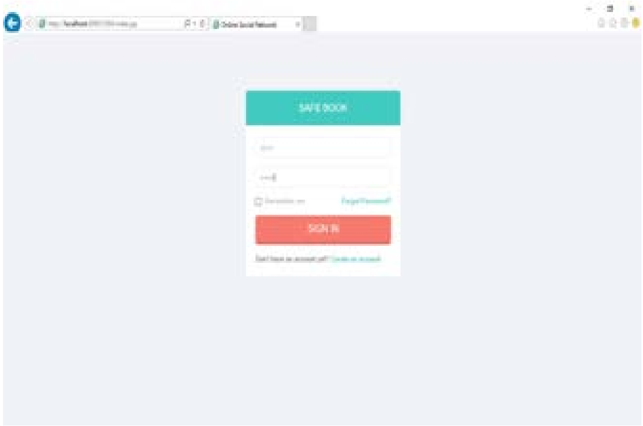
2.2 CONFLICT DETECTION

We need a way to compare the individual privacy preferences of each negotiating user in order to detect conflicts among them. However, each user is likely to have defined different groups of users, so privacy policies from different users may not be directly comparable. To compare privacy policies from different negotiating users for the same item, we consider the effects that each particular privacy policy has on the set of target users T . Privacy policies dictate a particular action to be performed when a user in T tries to access the item. In particular, we assume that the available actions are either 0 (denying access) or 1 (granting access).

3. USER INTERFACE DESIGN

3.1 User Registration and login

This module can be also used to register users for custom modules that support personalization and user specific handling. If the users wish to create their own user accounts, i.e. register, then registration checks for the username availability and assign unique Digit provides functionality to register viewers of the learning site in order to get access to personalized content that the site using this module provides to its users. After registration and login, there is option to form the friends list. The friend suggestions will be there to add a new friend. Accept/ Reject option will be there for accept or reject the friend request. Through this process, friend circle are formed for each users.



3.2 Policy Evaluation

This module evaluates the policy the each users which are currently in communication. Policy means identifies which users are owner, access or and disseminator. The user who makes the profile updating, sharing, are considered as owners. The access or users who have rights to access the owner shared data. Disseminator is users who not have rights for viewing the owner images. This module evaluates the policy of the users based on the above contents. In this paper we assume that each user I has a privacy policy pi(x) and a exposure policy vi(x) for a specific photo x.the privacy policy indicates the set of users who can access the image,and exposure policy indicates the set of users who can access x when user I is involved. it can be calculated as

$$S = Pi(x)k2I/Vk(x)$$

We assume that our users have defined their privacy policy and exposure policy and these policies are modifiable. The exposure policy is treated as a private data that shall not be revealed, and a secure set intersection protocol is used to find the access policy s in 1.

After the access policy s is established, the co-photo x will be shared with users s. privacy is a generic process that occurs in all cultures but that also differs among cultures in terms of the behavioral mechanisms used to regulate desired levels of privacy. Ethnographic data are examined from a variety of cultures, particularly from societies with apparently maximum and minimum privacy, and from analyses of various social relationships, such as parents and children, in-laws, husbands and wives. It is concluded that privacy is a universal process that involves culturally unique regulatory mechanisms. This article addresses the question posed in the title, namely, is privacy regulation a culturally universal process or is it a culturally specific phenomenon? Like the rabbi of Jewish folklore faced with petitioners holding irreconcilable opinions, my answer is “yes, both positions are correct!” This seemingly paradoxical response is based on an analysis of privacy as (a) a culturally universal process involving dynamic, dialectic, and optimization features, and @) a culturally specific process in terms of mechanisms used to regulate social interaction. Thus, I view privacy to be culturally pervasive at one level of analysis and culturally unique at another level of analysis. The first section of the article summarizes a theoretical model and rationale for conceiving privacy as a cultural universal. Dilemmas, issues, and a strategy for dealing with the question of cultural universals are then discussed, followed by a review of ethnographic data related to privacy. This article has presented a heuristic analysis of privacy in relationship to culture. I propose a framework emphasizing dialectic and boundary control features of privacy, whereby people can make themselves accessible or inaccessible to others. Furthermore, I suggest that privacy regulation involves more than use of the physical environment alone, but includes a variety of verbal, nonverbal, environmental, and cultural mechanisms.

Thus, I conceptualize privacy as a complex and molar phenomenon that requires a broader perspective than it has received in the past. In pursuing this line of reasoning, I have also speculated about the cultural pervasiveness of privacy regulation. It seems that the ability to regulate interaction is necessary for individual and cultural survival, and unless people have figured out ways to control interaction, their status as intact human beings can well be in jeopardy. However, to simply posit that privacy is a cultural universal does not say very much, so I have suggested that (a) people in all cultures engage in the regulation of social interaction-sometimes being accessible to others and sometimes being inaccessible to others, and (b) the behavioral mechanisms by which accessibility is controlled are probably unique to the particular physical, psychological, and social circumstances of a culture. I then explored these points through an analysis of cultures with apparently maximum and minimum privacy and through an analysis of various relationships, for example, acquaintances, in-laws, and family members.

We need a way to compare the individual privacy preferences of each negotiating user in order to detect conflicts among them. However, each user is likely to have defined different groups of users, so privacy policies from different users may not be directly comparable. To compare privacy policies from different negotiating users for the same item, we consider the effects that each particular privacy policy has on the set of target users T . Privacy policies dictate a particular action to be performed when a user in T tries to access the item. In particular, we assume that the available actions are either 0 (denying access) or 1 (granting access). The action to perform according to a given privacy policy is determined as follows,

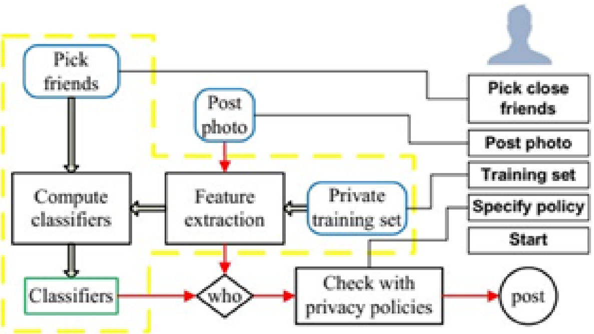
Algorithm 1 Conflict Detection

```
Input: N, Pn1; : : : ; PnjNj , T Output: C
1: for all n 2 N do 2: for all t 2 T do 3: vn[t] 0
4: for all G 2 Pn:A do 5: if 9u 2 G; u = t then 6: vn[t] 1
7: end if
8: end for
9: end for
10: for all e 2 Pn:E do 11: vn[e] :vn[e]
12: end for
13: end for
14: C ;
15: for all t 2 T do 16: Take a 2 N

17: for all b 2 N n fag do 18: if va[t] 6= vb[t] then 19: C C[
ftg
20: end if
21: end for
22: end for
```

4.IMAGE CLASSIFICATION

User will first make a list for desired classifiers use private set operations in to request against friends neighbors’ classifiers lists one by one. We propose an image classification which classifies images first based on their friend list and then refine each category into sub categories based on their classifier. 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 are no privacy concerns of user1 friend list because friendship graph is undirected. However, in the second loop, user1 need to coordinate all user1 friends to build classifiers between them. According to our protocol, user1 friends only communicate with user1 and they have no idea of what they are computing for.



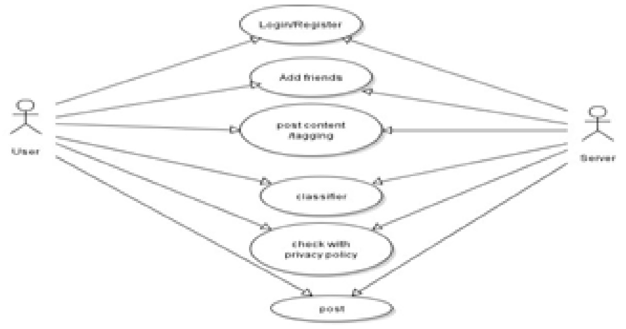
Our prototype works in three modes: a setup mode, a sleeping mode and a working mode. Running in the setup mode, the program is working towards the establishment of the decision tree. For this purpose, the private training set Xi and neighbourhood Bi need to be specified. Xi could be specified by the user with the button “Private training set”. When it is pressed, photos in the smart phone galleries could be selected and added to Xi. To setup the

neighbourhood Bi, at this stage, a user needs to manually specify the set of" close friends" among their Face book friends with the button "Pick friends" as their neighbourhood. According
to the Face book statistics, on average a user has 130friends, we assume only a small portion of them are" close friends". In our application, each user picks up to 30 "close friends".

Notice that all the selected friends are required to install our application to carry out the collaborative training. With Xi and Bi specified, the setup mode could be activated by pressing the button" Start". Key operations and the data flow in this mode are enclosed by a yellow dashed box on the system architecture Fig.4During the training process, a socket is established exchange local training results. After the classifiers are obtained, decision tree is constructed and the program switches from the setup mode to the sleeping mode. Face book allows us to create a list of friends such "close friends" or "Acquaintances". We can share a photo only to friends on list. According to the proposed scheme, this friend list should be intersection of owner's privacy policy and co-owners' exposure policies. However, in Face book API, friend lists are read-only items, they cannot be created or updated through the current API. That means we cannot customize a friend list to share a co-photo. Currently, when the button "Post Photo" is pressed, co-owners of x are identified, then notifications along with x are send to the co-owners to request permissions. If they all agree to post x, x will be shared on the owner's page like a normal photo. In this sense, users could specify their privacy policy but their exposure policies are either everybody on earth or nobody depending on their attitude toward
x. The data flow for a photo posting activity is illustrated by the solid red arrows. After the requests are sent out, the program will go back to the sleeping mode. If Xi or Bi is modified, the program will be invoked to the setup mode. In this case, the operations in the yellow dashed box will be performed again and decision tree will be updated.

5.SECURE SHARING AND BLOCK IMAGE ACCESS RIGHTS

This module is for sharing of resources, it gets the policy of the users and the contents what want to share. As per the policy of each data sharing, the data will shared for only the users who all have the access rights. This module is to block the download rights and saving rights for the images. The images can be viewed or sharing only by the authorized users.



6.RECOMMENDED LIST

In this module to share the images to particular friend list, create domain groups for each friends in particular categories (for ex college, family, native. etc.,) with his friend request. After connect with different group of We now introduce the policy recommendation process based on the social groups obtained from the previous step. Suppose that a user uploaded a new images then proposed method will invoked the images for user policy decision.

In many important applications, a collection of mutually distrustful parties must perform private computation over multisite. Each party's input to the function is his private input multisite. In order to protect these private sets, the players perform privacy-preserving computation; that is, no party learns more information about other parties' private input sets than what can be deduced from the result. In this paper, we propose efficient techniques for privacy-preserving operations on multisets. By employing the mathematical properties of polynomials, we build a framework of efficient, secure, and composable multiset operations: the union, intersection, and element reduction operations. We apply these techniques to a wide range of practical problems, achieving more efficient results than those of previous work. Private computation over sets and multisets is required in many important applications. In the real world, parties often resort to use of a trusted third party, who computes a fixed function on all parties' private input multisite, or forgo the application altogether. This unconditional trust is fraught with security risks; the trusted party may be dishonest or compromised, as it is an attractive target. We design efficient privacy-preserving techniques and protocols for computation over multisite by mutually distrustful parties: no party learns more information about other parties' private input sets than what can be deduced from the result of the computation. For example, to determine which airline passengers appear on a 'do-not-fly' list, the airline must perform a set-intersection operation between its private passenger list and the government's list.

This is an example of the Set-Intersection problem. If a social services organization needs to determine the list of people on welfare who have cancer, the union of each hospital's lists of cancer patients must be calculated (but not revealed), then an intersection operation between the unrevealed list of cancer patients and the welfare rolls must be performed. This problem may be efficiently solved by composition of our private union and set-intersection techniques. Another example is privacy- preserving distributed network monitoring.

In this scenario, each node monitors anomalous local traffic, and a distributed group of nodes collectively identify popular anomalous behaviors: behaviors that are identified by at least a threshold t number of monitors. This is an example of the Over- Threshold Set-Union problem. Our protocols are provably secure in the PPT-bounded adversary model. We consider both standard adversary models: honest-but-curious adversaries (HBC) and malicious adversaries. For protocols secure in the HBC model, we prove that the information learned by any coalition of honest- but-curious players is indistinguishable from the information learned in the ideal model, where a trusted third party (TTP) calculates the function. For protocols secure in the malicious model, we provide simulation proofs showing that for any strategy followed by a malicious coalition Γ in the real protocol, there is a translated strategy they could follow in the ideal model, such that, to Γ, the real execution is computationally indistinguishable from ideal execution. Our protocols are more efficient than the results obtained from previous work. General multiparty computation is the best previous result for most of the problems that we address in this paper. Only the private Set- Intersection problem and two-party Cardinality Set-Intersection problem have been previously studied However, previous work only provides protocols for 3-or-more-party Set-Intersection secure only against honest-but-curious players; it is not obvious how to extend this work to achieve security against malicious players. Also, previous work focuses on achieving results for the Set-Intersection problem in isolation – these techniques cannot be used to compose set operations.

7.CONCLUSION AND DISCUSSION

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 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. 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. We expect

that our proposed scheme be very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-off between privacy and utility. For example, in our current Android application, the co- photo could only be post with permission of all the co-owners. Latency introduced in this process will greatly impact user experience of OSNs. Moreover, local FR training will drain battery quickly. Our future work could be how to move the proposed training schemes clouds like Drop box and/or cloud.

REFERENCES

[1] Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3):66–84, 1977.
[2] Besmer and H. Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In Proceedings of the SIGCH IConference on Human Factors in Computing Systems, CHI '10, pages1563–1572, New York, NY, USA, 2010. ACM
[3] S. Boyd, N. Parikh, E. Chu, B. Plato, and J. Eckstein. Distributed optimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn., 3(1):1–122, Jan.2011.
[4] B. Carminati, E. Ferrari, and A. Perego. Rule-based access controlfor social networks. In R. Meersman, Z. Tari, and P. Herrero,editors, On the Move to Meaningful Internet Systems 2006: OTM2006 Workshops, volume 4278 of Lecture Notes in Computer Science,pages 1734–1744. Springer Berlin Heidelberg, 2006.
[5] J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborativeface recognition for improved face annotation in personal photocollections shared on online social networks. Multimedia, IEEETransactions on, 13(1):14–28, 2011.
[6] K. Choi, H. Byun, and K.-A. Toh. A collaborative face recognitionframework on a social network platform. In Automatic Face GestureRecognition, 2008. FG '08. 8th IEEE International Conference on,pages 1–6, 2008.
[7] 7.K.-B. Duan and S. S. Keerthi. Which is the best multiclass svmmethod? an empirical study. In Proceedings of the 6th internationalconference on Multiple Classifier Systems, MCS'05, pages 278–285,Berlin, Heidelberg, 2005. Springer-Verlag.
[8] P. A. Forero, A. Cano, and G. B. Giannakis. Consensus-baseddistributed support vector machines. J. Mach. Learn. Res., 99:1663–1707, August 2010.
[9] B. Goethals, S. Laur, H. Lipmaa, and T. Mielik?inen. On privatescalar product computation for privacy-preserving data mining.In In Proceedings of the 7th Annual International Conference in Information Security and Cryptology, pages 104–120. Springer-Verlag,2004.
[10] L. Kissner and D. Song. Privacy-preserving set operations. InIN ADVANCES IN CRYPTOLOGY - CRYPTO 2005, LNCS, pages241–257. Springer, 2005.
[11] L. Kissner and D. X. Song. Privacy-preserving set operations.In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes inComputer Science, pages 241–257. Springer, 2005.
[12] N. Mavridis, W. Kazmi, and P. Toulis. Friends with faces: Howsocial networks can enhance face recognition and vice versa. InComputational Social Network Analysis, Computer Communicationsand Networks, pages 453–482. Springer London, 2010
[13] R. J. Michael Hart and A. Stent. More content - less control: Access control in the web 2.0. In Proceedings of the Workshop on Web 2.0Security and Privacy at the IEEE Symposium on Security and Privacy, 2007.
[14] E. Newman. The structure and function of complex networks. SIAM review, 45(2):167–256, 2003.
[15] L. Plane. Unpacking privacy for a networked world. Pages 129–136. Press, 2003.