JOURNAL FOR INNOVATIVE DEVELOPMENT IN PHARMACEUTICAL AND TECHNICAL SCIENCE

Volume-2,Issue-3 (Mar-2019)
ISSN (O) :- 2581-6934

MULTIPARTY ACCESS CONTROL FOR PHOTO SHARING USING TRUST BASED MANAGEMENT

Ms.R.A.MABEL ROSE[1] , M.M. AARTHI [2]
[1] Assistant Professor ,M.E ,[2] M.E
[1 2] Computer Science and Engineering, Rajas International Institute of technology for women

Abstract:- ***Online social networks have now become the most popular platforms for people to share information with others. Along with this, there is a serious threat to individuals' privacy. In the proposed system, a trust-based mechanism to realize collaborative privacy management. Basically, a user decides whether or not to post a data item based on the aggregated opinion of all involved users. The trust values between users are used to weight users' opinions, and the values are updated according to users' privacy loss. Moreover, the user can make a trade-of between data sharing and privacy preserving by tuning the parameter of the proposed mechanism. If any of the hacker hack the database of the user, the information or photos that are shared between the users are get hacked. To provide the better security for the database, Secured Hash Algorithm is introduced and it avoids the hacking of password in the database. The proposed system mainly focuses on the privacy management on photo sharing and password protection. It plays the two-level protection on the social networks***

Index Terms—social trust, voting scheme, multi-armed bandit, collaborative privacy management, online social network

Introduction

It's obvious that people are more likely to use online social networks such as Google+, Twitter and Facebook for their needs to connect with the society. It has become common for people to upload and post information about the daily events in text, photos and video format in this types of social network sites. Such posts may involve sensational information of the user who posted the data or of other persons. In case, the data is exposed to some unofficial persons, security of the user's data will be on risk. Privacy problem is one of the major point of study concerning the usage of social network sites.

It's a great responsibility of the service providers of these sites to form methods for protecting the uses data from being hacked. meanwhile the users also can decide their own data access by making use of the privacy setting facilities provided by the social network sites. The level of privacy of the person using a social network site will be clearly explained by the particular site including the information of whom can access the data and this information's are collectively named as privacy policy. The information of the relationship between users have been made used by the online social networks to find the difference between official and unofficial users.

The power of a Facebook user to determine the exposure of his or her data to friend for particular groups or everyone is a great example of improved authority over the accessibility of the data.

These privacy measures taken by recent online social networks apply restriction only on the users who need to access other user's data. Despite, there is no governance over the users who upload the particular data. This may lead to the users posting data and breaking the privacy policy rules without any motive. For example, consider a person A uploading a photo of himself dancing with person B. Here, person A has posted the photo consciously. But, it is not sure that person be has full will on posting the particular photo. So, the privacy of person B is in risk as the post is out of B's consciousness. Here the person A unintentionally violates the privacy policy of the online social network and person B suffers privacy issue. Complication is that the picture which is posted is co-owned by both A and B. In online social networks it is common for two or more persons owning same photo. Maintaining privacy

policy needs a good cooperation between multiple users of same post.

Managing the cooperation between the users has become a challenge for online social networks. First the problems arising in the privacy of the users must be studied well and then corrected policies should be generated by the OSN. Privacy policy basically interconnects the user who uses the data and all other users to whom the owner wants the data to share with. A middle person involves in gathering all the user's policy and making a collective determination through an aggregation scheme. These developed privacy schemes do not always assure cent percent privacy to the users, hence the conflict will still exist. The method that can be used for eliminating the conflict between data sharing and privacy protection is being the most important questions among online social networks.

In traditional methods a mediator lies between the user who posts data and the users who are involved in the post to make an effective collaboration between the users. But in this approach the posting user itself is directly in collaboration with the users who are involved in the post tense should assure that the privacy is met. The past system consists of facilities where the user can upload a photo in which all the users involved are tagged in or they can be easily found out by some other recognizing techniques. Here as the mediator is in between he also comes to know the uses involved in the particular post. Practically it is impossible or hard to identify or recognize the users involved in the post automatically. Hence we propose a system in which the user who post the data is supposed to get permission from all the users that are involved in the post. This may be considered as such trust-weighted voting scheme.

Particularly whenever a data or information is to be posted by a user he or she gets a vote from all the involved users which is an approval for whether the data is to be posted and the post is inclusive of all involved user's privacy policy. The trust value lying between the user who post the data and the user who is involved in the post determines the importance of the voting system. The time the data gets fulfilled of all permission through the voting system the particular data gets approved to be posted. Here, the trust value can be altered and it is not fixed. A user's trust on other one gets lost if the other user post data that affects the privacy of the first person. Likewise, user wants more trust if he or she follows and prospects the opinions of others. Now, it gets total responsibility for the user to lose or gain their trust value, thus he or she becomes alert while posting data thereby securing the privacy of the user involved.

RELATED WORK

Collective Privacy Management

Although current OSNs do not execute limitations on the sharing of co-owned data, the delinquent of cooperative privacy management has been reviewed for a period in academia. In [6], Squicciarini et al. first examined this drawback by using game theory. To accumulate dissimilar individuals' privacy policies, they anticipated a Clark-Tax mechanism which can inspire personalities to report their true favorites on privacy policies. In [7], Hu et al. proposed a space segmentation method to recognize the conflicts among individuals' confidentiality policies. And they anticipated a conflict resolution mechanism that considers both the privacy risk and the data sharing loss. In their trail up work [10], they expressed the multiparty access control problem as a game played by multiple users. And an iterative update algorithm was intended to compute the equilibrium of the game. Based on the multiparty access control model proposed in [11], Vishwamitra et al. [12] proposed a model that can enable concerted control of the personally identifiable evidence in a data item.

Comprehending that users are willing to consult and make indulgences to achieve an agreement on the privacy policy, some academics studied negotiation-based methods. In [13], Mehregan and Fong proposed a denial process in which a privacy policy is repeatedly modified until it gratifies certain availability criteria. In [8], the concessions that users may be disposed to make in diverse situations are demonstrated as a set of concession rules, and a computational mechanism is planned to solve the privacy conflicts. Studies introduced above usually accept that there is anupright mediator (e.g. the service provider of the OSN) who distinguishes users' privacy policies detailed for a specific data item. The final privacy policy is managed by the mediator. While in the mechanism proposed in this paper, such a mediator is surplus to requirements. The user, who wants to post data, is responsible to gather feedbacks from

ISSN:- 2581-6934 |www.jidps.com

other involved users and make the final decision. Such mechanism is more concrete, pondering the privacy management in current OSNs.

Trust-based Incentive Mechanisms

As pointed out in [14], trust plays a vital role in network-based applications, such as peer-to-peer (P2P) systems, resourceful mobile networks [15], [16], and online social networks. In the analysis of OSNs, the trust relationship between users has been investigated to protect complex data of users [17], or to verify the user's identity [18]. In [19], Sherchan et al. given a complete review of trust in the framework of social networks. They considered studies on social trust based on three criteria, namely trust data compilation, trust assessment, and trust distribution. The procedure proposed in this paper encompasses estimating the trust values between two consumers centered on their communications.

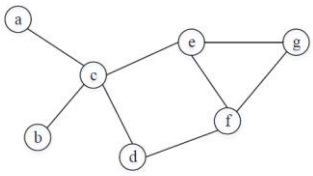

Fig. 1. A simple graph representation of the online social network.

Trust-based incentive mechanisms have been widely deliberate in peer to peer systems to distribute with the free-riding problem. Tang et al. obtained a brief review of such methods in [20]. So far we have only understood few literatures applying trust to the cooperative privacy management problem. In [21], Rathore and Tripathy offered a trust-based access control method which exploits the trust values to describe access conditions. That is, a user can stipulate the minimum trust level that is needed for alternative user to gain access to his/her information. In [22], Sun et al.proposed a trust-weighted voting stratagem to combine different users' privacy policies. In this paper, we also use trust values to designate how much impact a user's opinion will have on the combined decision. While, dissimilar from Sun et al.'s work where the trust values are secure, the trust values in the proposed mechanism are associated to users' privacy damage, and hence they change over time.

SYSTEM MODEL

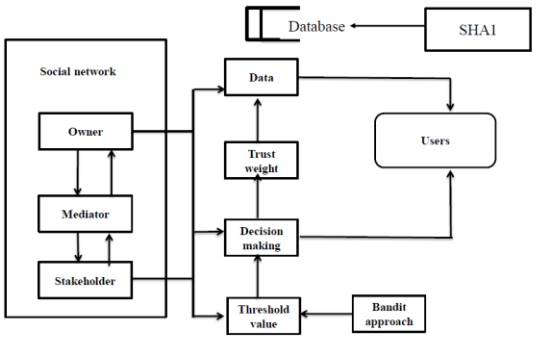

Fig: Architecture of the proposed System

Online Social Network

An OSN can be characterized by an edge-labeled directed graph G = (V, E), where V is the set of vertices and E is the set of edges. Every single vertex signifies a user. In subsequent descriptions, unless otherwise specified, we promote the two terms "vertex" and "user" manageable. Every single edge in the graph denotes a correlation between two users. Let RT stand for the set of relationship types hold up by the OSN. The edge from user's v_i to v_j can be shown by a 3-tuple (v_i, v_j, r_{ij}), where r_{ij} 2 RT is the label associated with the edge. By swapping all the directed edges in G with undirected edges, we can manage the distance between any two users. Specifically, given a pair of users (v_i, v_j), if there is a route between the two users, then the distance d_{ij} is definite as the length of the shortest path between user's v_i and v_j. If there is no path between user's vi and v_j then we define d_{ij} = 1. For example, in the graph showed in Fig. 1, the distance between two users a and c is 1, and the distance between a and g is 3.

Trust Evaluation

Trust plays a crucial role in the privacy managing mechanism anticipated in this paper. For any two user's v_i and v_j, no matter they are directly coupled by an edge or not, we use t_{ij} to signify the trust of user v_i in user v_j. We define t_{ij} 2 [0; 1]. The more user vi trusts user v_j, the higher t_{ij} is.The trust of user v_j in user vi is denoted as v_{ji}. Generally, thereis v_{ij} 6= v_{ji}. Various models have been proposed to evaluatetrust in social networks [19], including network structurebasedmodels [23] and interaction-based models [24]. In thispaper, we mainly focus on how the trust between users canbe leveraged to realize

ISSN:- 2581-6934 |www.jidps.com

collective privacy management. Herewe first use a simple distance-based method to determinethe initial trust values. And in the following section, we willdiscuss how to update the trust values based on the interactionsbetween users.Given a pair of users vi and v_j , we define t_{ij} = 0 if d_{ij} =1. If the two users are directly connected, namely d_{ij} = 1,t_{ij} is set to a positive constant which is determined by therelationship type r_{ij} . For example, if user v_j is user v_i's familymember, we can set t_{ij} = 0:8; while if user vj is user vi'scolleague, we can set t_{ij} to a lower value, say 0:6. When1 < d_{ij}< 1, we utilize the transitivity property of trust [25],[26] to compute the trust value. Specifically, t_{ij} is computedbyt_{ij}.

Given a pair of user's v_i and v_j, we define t_{ij} = 0 if d_{ij} =1. If the two users are directly connected, namely dij = 1,t_{ij} is set to a positive constant which is determined by the relationship type r_{ij} . For example, if user v_j is user v_i's family member, we can set t_{ij} = 0:8; while if user v_j is user vi's colleague, we can set t_{ij} to a lower value, say 0:6. When 1 < dij < 1, we utilize the transitivity property of trust [25],[26] to compute the trust value. Specifically, t_{ij} is computedby

$$t_{ij} = \pi_{k=1,\ldots,dij}\, t_{pk\,pk+1},$$
$$(v_{pk}, v_{pk+1}) \epsilon P_{ath\ ij}$$

Multiparty Access Control

An eminent characteristic of OSNs is that they afford expedient ways for users to share data with others. Usually, a user can: post a data item, such as a photo, a video clip or a text message, in his/her own space or additional user's space; distribute a data item, which was formerly posted by alternative user, by sending it in his/her own space.In either one of the overhead two cases, we denote to the user as the owner of the data item. Properly, given a data item d, we signify the owner of d as od. If d encompasses multiple users, then d is co-owned by the users. All the users related with d, except od, are indicated to as consumers. The set of consumers is designated by S_d. It would be noted that each one consumer S_2 S_d may retain a data item d_0 which has the similar contented with d (i.e. d_0 is a duplicate of d). And if the owner od and the shareholder s want to post data items at the same time, we contemplate the two data items d and d_0 independently, meaning that for the data item d_0 we treat the consumer s as the owner and the owner od as the consumer. When posting the data item d, the owner o_d needs to specify a privacy policy to control which users are allowed to access.

Let U_o a represent the set of consumers who get the approval from the owner. In system, Uo a is frequently governed by the relationship type. For instance, when redistribution a photo taken at a home party, the owner can specify that only his/her family members and relatives can view this photo. If any unauthorized user accesses the data, the owner will suffer a loss in privacy. Let Uo u denote the set of unauthorized users that can retrieve the data item d. Then the privacy loss to the owner, denoted as l_o, can be defined as

$$\mathbf{L_0 = |U_u^0| \square_0}$$

TRUST-BASED COLLABORATIVE PRIVACY MANAGEMENT

As stated in Section I, in progress OSNs do not influence the user to ask other users for authorization of posting co-owned data items. To terminate the privacy issue instigated by the conflicts amid the owner's privacy policy and the consumers' policies, in this segment we recommend a trust-based method that can inspire the owner to solicit the shareholders'thoughts and make anaggregate decision.

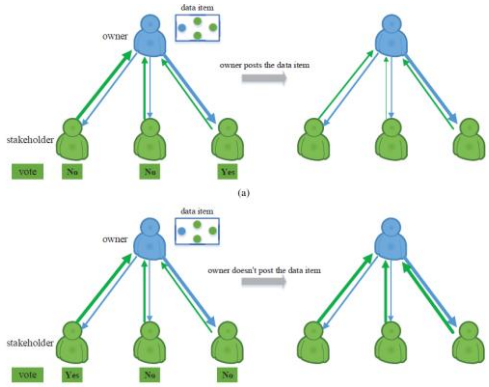

Fig: Simple illustration of the trust-based privacy management mechanism

Trust-Weighted Voting Scheme

Given a data item d, the subsequent owner o_d and the set of participants S_d, we in view of the following two cases:1) The owner openly posts the information without asking the

ISSN:- 2581-6934 |www.jidps.com

shareholders for consent: In such a case, it is very likelythat the shareholders 'privacy will be revealed. Take into account that all the consumers can take in the solitude disclosure (if exists) after d is posted. According to (3), the consumer'ss ϵS_d needs to know U_o a to evaluate the privacy loss l_s. However, generally the set Uo a cannot be fully observed by

$t' = t_{so} g(l_s)$

Trust as Incentive

Above we have termed how the owner chooses whether to post a co-owned data item. A simple design of the proposed trust-based mechanism. The trust values are not only used to weigh the consumers' votes but also reorganized with the privacy loss of the consumers. Corresponding to the update rule of the trust value, if the owner $o_d$posts a data item and obtains a privacy loss of a consumer s, the consumer's trust in the owner will reduce. Consider that at some point in the future, consumer s wants to post a data item linking owner o_d. Even if s plead with o_d's opinion, due to the low trust of consumer s in owner od, the opinion of owner od will be less valued by consumer s. As an outcome, it is more likely that the concluding pronouncement of consumer s is opposite to the view of owner o_d. In other words, the possibility that owner o_d suffers a privacy loss becomes higher. On the other hand, if the owner o_d solicits the consumers' opinions before posting the data, then the owner may gain more trust from some of the consumers. In the future, when these consumers ask owner od for authorization to post data, owner o_d's opinions will be more valued, and the potential privacy loss of owner o_d will be less. Above argument suggests that even though the owner is not indebted to seeking the consumers' opinions before posting data, from the viewpoint of privacy preserving, it is better for the owner to do so. In [27], an evolutionary game model is planned to analyze how users' outcomes on privacy protection influence each other. The game model undertakes that communications of users only happen among those who are in the same community. In our delinquent setting, the owner and the consumers form a special community, where the owner's decision has direct impact on the consumers' privacy and indirect influence on his/her own privacy.

TRADE-OFF BETWEEN PRIVACY PRESERVING AND DATA SHARING

Require: $\alpha \in \mathbb{R}^+$
for t=1 to K **do**
choose arm $I_t = t$
Observe and record the reward $r_{I_t,t}$
$r_t \leftarrow r_{I_t,t}$
$n_{I_t} \leftarrow 1$
end for
for t=K+1 to T **do**
for i=1 to K **do**
$\bar{r}_i \leftarrow \frac{1}{n_i}\sum_{r=1}^{t-1} r_r 1(I_r = i)$
end for
Choose arm $I_t = \underset{i=1,\ldots\ldots K}{argmax}(\bar{r}_i + \alpha\sqrt{\frac{\ln t}{n_i}})$ with ties broken arbitrarily.
Observe and record the reward $r_{I_t,t}$
$r_t \leftarrow r_{I_t,t}$
$n_{I_t} \leftarrow n_{I_t}+1$
end for

Fig: Algorithm for Upper Confidence Bound

Based on the trust-based mechanism suggested in the above section, we can draw the following simple conclusion: if the user never posts data that will disclose other users' privacy, then the user can preserve a high standing. And the user's privacy can be well conserved by other users, since his/her opinions are highly valued by others. However, seeing that the core purpose of OSNs is data sharing, it is irrational to overwhelm the sharing of co-owned data. How to accomplish a balance between data sharing and privacy preserving is a significant issue in the study of data privacy [28], [29]. In this section, we discuss how to exploit the threshold b_{th} familiarized in the trust-based mechanism to make a trade-off between privacy preserving and data sharing. Precisely, we model the selecting of the threshold as a multi-armed thug problem and apply the upper confidence bound policy to find the optimal threshold. we evaluate whether the UCB policy can help the user find a proper threshold.

CONCLUSION

In this paper we study the privacy issue caused by the distribution of co-owned information in OSNs. To help the owner of data cooperate with the consumers on the control of data sharing, we recommend a trust-based mechanism. When a consumer is about to post a data item, the user first implores the consumers' views on data sharing, and then makes the final decision by associating the aggregated outlook with a pre-quantified threshold. The more the user trusts a consumer, the

ISSN:- 2581-6934 |www.jidps.com

more the user values the consumer's opinion. If a user agonizes a privacy loss because of the data sharing performance of another user, then the user's trust in another user diminishes. On the otherhand, since that the user needs to balance between data sharing and privacy preserving, we apply a bandit tactic to tune the threshold in the proposed trust-based mechanism, so that the user can get a high long-turn payoff which is well-defined as the difference between the advantage from posting data and the privacy loss caused by other users. We have led imitations on synthetic data and real-world data to verify the probability of the planned methods. And by harnessing the proposed UCB policy to reveal the threshold, the user can get elevated payoffs than setting the threshold to a fixed or random value.

REFERENCES

[1] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for onlinesocial networks: challenges and opportunities," IEEE Network, vol. 24,no. 4, pp. 13–18, July 2010.

[2] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security inbig data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176,2014.

[3] L. Xu, C. Jiang, Y. Chen, J. Wang, and Y. Ren, "A framework forcategorizing and applying privacy-preservation techniques in big data mining," Computer, vol. 49, no. 2, pp. 54–62, Feb 2016.

[4] M. Qiu, K. Gai, and Z. Xiong, "Privacy-preserving wirelesscommunications using bipartite matching in social big data,"Future Generation Computer Systems, 2017.
[Online].
Available:http://www.sciencedirect.com/science/article/pii/S0167739X17301449

[5] 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?: Privacysettings and social media content sharing," in Proceedings of the 2017ACM Conference on Computer Supported Cooperative Work and Social
Computing, March 2017, pp. 567–580.

[6] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy managementin social networks," in Proceedings of the 18th ACM InternationalConference on World Wide Web, April 2009, pp. 521–530.

[7] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacyconflicts for collaborative data sharing in online social networks," inProceedings of the 27th ACM Annual Computer Security ApplicationsConference, December 2011, pp. 103–112.

[8] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts insocial media," IEEE Transactions on Knowledge and Data Engineering,vol. 28, no. 7, pp. 1851–1863, July 2016.

[9] P. Auer, N. Cesa-Bianchi, and P. Fischer, "Finite-time analysis of themultiarmed bandit problem," Machine learning, vol. 47, no. 2-3, pp.235–256, 2002.

[10] H. Hu, G.-J. Ahn, Z. Zhao, and D. Yang, "Game theoretic analysis ofmultiparty access control in online social networks," in Proceedings ofthe 19th ACM Symposium on Access Control Models and Technologies,New York, NY, June 2014, pp. 93–102.

[11] H. Hu, G. J. Ahn, and J. Jorgensen, "Multiparty access control foronline social networks: Model and mechanisms," IEEE Transactions onKnowledge and Data Engineering, vol. 25, no. 7, pp. 1614–1627, July
2013.

[12] N. Vishwamitra, Y. Li, K. Wang, H. Hu, K. Caine, and G.-J. Ahn,"Towards pii-based multiparty access control for photo sharing in onlinesocial networks," in Proceedings of the 22Nd ACM on Symposium onAccess Control Models and Technologies, June 2017, pp. 155–166.

[13] P. Mehregan and P. W. Fong, "Policy negotiation for co-owned resourcesin relationship-based access control," in Proceedings of the 21st ACMon Symposium on Access Control Models and Technologies, June 2016,pp. 125–136.

[14] J. Golbeck, "Trust on the world wide web: A survey," Foundations andTrends in Web Science, vol. 1, no. 2, pp. 131–197, 2008.

[15] S. Zakhary, M. Radenkovic, and A. Benslimane, "Efficient locationprivacy-aware forwarding in opportunistic mobile networks," IEEETransactions on Vehicular Technology, vol. 63, no. 2, pp. 893–906,

February 2014.

[16] S. Zakhary and A. Benslimane, "On location-privacy inopportunistic mobile networks, a survey," Journal of Networkand Computer Applications, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517303557

[17] S. Xu, X. Li, T. P. Parker, and X. Wang, "Exploiting trust-based socialnetworks for distributed protection of sensitive data," IEEE Transactions
on Information Forensics and Security, vol. 6, no. 1, pp. 39–52, March2011.

[18] N. Z. Gong and D. Wang, "On the security of trustee-based socialauthentications," IEEE Transactions on Information Forensics and Security,
vol. 9, no. 8, pp. 1251–1263, Aug 2014.

[19] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in socialnetworks," ACM Computing Surveys, vol. 45, no. 4, pp. 47:1–47:33,August 2013.

[20] Y. Tang, H. Wang, and W. Dou, "Trust based incentive in p2p network,"in IEEE International Conference on E-Commerce Technology forDynamic E-Business, September 2004, pp. 302–305.

[21] N. C. Rathore and S. Tripathy, "A trust-based collaborative accesscontrol model with policy aggregation for online social networks," SocialNetwork Analysis and Mining, vol. 7, no. 1, p. 7, February 2017.

[22] Y. Sun, C. Zhang, J. Pang, B. Alcalde, and S. Mauw, "A trust-augmentedvoting scheme for collaborative privacy management," J. Comput. Secur.,vol. 20, no. 4, pp. 437–459, July 2012.

[23] V. Buskens, "The social structure of trust," Social Networks, vol. 20,no. 3, pp. 265–289, 1998.

[24] S. Nepal, W. Sherchan, and C. Paris, "Strust: A trust model forsocial networks," in 2011 IEEE 10th International Conference on Trust,Security and Privacy in Computing and Communications, November2011, pp. 841–846.

[25] O. Richters and T. P. Peixoto, "Trust transitivity in social networks,"PLOS ONE, vol. 6, no. 4, pp. 1–14, 04 2011. [Online]. Available:
https://doi.org/10.1371/journal.pone.0018384

[26] G. Liu, Y. Wang, M. A. Orgun et al., "Trust transitivity in complexsocial networks." in AAAI, vol. 11, no. 2011, 2011, pp. 1222–1229.

[27] J. Du, C. Jiang, K. C. Chen, Y. Ren, and H. V. Poor, "Communitystructuredevolutionary game for privacy protection in social networks,"IEEE Transactions on Information Forensics and Security, vol. PP,no. 99, pp. 1–1, 2017.

[28] L. Xu, C. Jiang, Y. Chen, Y. Ren, and K. J. R. Liu, "Privacy or utility indata collection? a contract theoretic approach," IEEE Journal of SelectedTopics in Signal Processing, vol. 9, no. 7, pp. 1256–1269, 2015.

[29]"User participation in collaborative filtering-based recommendationsystems: A game theoretic approach," IEEE Transactions onCybernetics, vol. PP, no. 99, pp. 1–14, 2018.

[30] S. Bubeck and N. Cesa-Bianchi, "Regret analysis of stochastic andnonstochastic multi-armed bandit problems," Foundations and TrendsRin Machine Learning, vol. 5, no. 1, pp. 1–122, 2012.

[31] L. Xu, C. Jiang, Y. Qian, Y. Zhao, J. Li, and Y. Ren, "Dynamic privacypricing: 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.