EFFECTIVE AND PROFICIENT TRUST BASED COMMUNICATIVE MANAGEMENT SYSTEM FOR SOCIAL NETWORKS

U. Mohan Srinivas,

Assoc. Prof., Department of CSE & MCA, QIS College of Engineering and Technology, Ongole,

M. Anusha,

Final Year Student of Master of Computer Applications, QIS College of Engineering and Technology, Ongole

Abstract: *Online interpersonal organizations have now turned into the most well known stages for individuals to impart data to other people. Alongside this, there is a genuine risk to people's protection. One security hazard originates from the sharing of co-claimed information, i.e., when a client shares an information thing that includes numerous clients, a few clients' protection might be undermined, since various clients for the most part have distinctive conclusions on who can get to the information. The most effective method to plan a community the executives system to manage such a security issue has as of late pulled in much consideration. In this paper, we propose a trust-based system to acknowledge collective security the board. Fundamentally, a client chooses whether or not to post an information thing dependent on the collected feeling of every included client. The trust esteems between clients are utilized to weight clients' feelings, and the qualities are refreshed by clients' security misfortune. Additionally, the client can make an exchange off between information sharing and security protecting by tuning the parameter of the proposed system. We plan the choosing of the parameter as a multi-outfitted crook issue and apply the upper certainty bound approach to take care of the issue. Recreation results show that the trust-based instrument can urge the client to be circumspect of others' protection, and the proposed outlaw methodology can bring the client a high result.*

I. INTRODUCTION

Online social networks (OSNs), such as Facebook, Google+, and Twitter, have become the most important platforms for people to make social connections with others. Thousands of millions of users post data about their daily lives in terms of text messages, photos, or videos on OSNs. Such data often contain sensitive information of users. If the data can be accessed by unauthorized entities, users' privacy will be compromised. The privacy issue has always been a major concern in studies related to OSNs [1], [2], [3], [4]. To protect users' privacy, on one hand, the service providers of OSNs need to take measures to prevent data breach. On the other hand, users themselves can control the access to their data by using the privacy setting function implemented in OSNs [5]. An access control policy, also referred to as the privacy policy, defines which users are allowed to access a user's data. Current OSNs often utilize user relationship to distinguish [9], [10], [11], [12], [13], between authorized users and unauthorized users.For example, Facebook users can specify if their data can be accessed by friends, specific groups or everyone. The privacy control mechanisms implemented in current OSNs only impose restrictions on users who want to access others' data. While there is no strict restriction on users who post data. A consequence of this one-side restriction is that the user who posts data may unintentionally violate other users' privacy. Consider the following example. Suppose [14], [15], [16], [17], [18], that a user A posts a photo of him/her playing with a friend B, and user A specifies that the photo can be accessed by his/her colleagues. If user B considers this photo to be sensitive and user B is not familiar with user A's colleagues, then user B's privacy will be violated. In the above case, the photo is actually coowned by the two users. Hence, the privacy policy specified by user A should be compatible with user B's privacy policy, otherwise, user B will suffer a loss in privacy. Data which are co-owned by multiple users are quite common in OSNs. Privacy management of such data requires a collaboration of all involved users. The problem of collaborative privacy management in OSNs has attracted much attention in recent years [6], [7], [8]. Most studies deal with this problem by first detecting the conflicts among different users' privacy policies, and then generating an aggregated policy that can resolve the conflicts to the largest extent. Given a data item (e.g. a photo), a user's privacy policy is generally represented by a set of users with whom the user wants to share the data. Usually there is a mediator who collects users' policies and makes a group decision via some aggregation scheme. In most cases, the conflicts among users' privacy policies can not be completely eliminated, which means the aggregated policy may still cause a privacy loss to

some of the users. How to make a trade-off between data sharing and privacy preserving is an important [19], question for the design of the conflict resolution method. Different from previous studies which rely on a mediator to coordinate among multiple users, in this paper we assume that it is the user who wants to post data makes a collective decision based on other users' privacy requirements. Previous [20], studies usually assume that the user who posts the data will tag all the users involved, or the involved users can be identifiedvia some technique (e.g. face reorganization). In such a case, the mediator [21], is able to notify the involved users about the posting of the data. However, in practice, it is likely that the user posts the data with out tagging other users and the in volved users are hard to be identified automatically. Considering this, we propose a mechanism which requires the user to solicit other users' opinions before posting data. And a trust-weighted voting scheme is applied to aggregate different users'opinions. Specifically, given the data item that a user wants to post and the privacy [22], policy specified by the user, every involved user makes a "vote" to state whether he/she approves of the privacy policy. The importance of the vote depends on the trust [23], value between the two users. Only when the aggregation of the votes satisfies a certain condition, the data can be posted. Moreover, the trust values between users are not fixed. A user will lose the trust of others if he/she posts a data item that incurs [24], privacy loss of others. Also, a user can gain more trust from others if he/she adopts others' opinions. The interaction between the trust value and the privacy loss implies that if the user wants to reduce his/her privacy loss, then when posting a co-owned [25], data item, the user should always consider others' privacy requirements rather than taking a unilateral decision. In the proposed trust-based privacy management mechanism, we introduce a threshold based on which the user makes the final decision [26], on data posting. Simply speaking, a high threshold indicates that the user has a relatively low tendency to share the data with others, and only when the majority of the involved users or users that are highly trusted agree to post the data, the data can finally be posted. By tuning the threshold, the user can make a trade-off between data sharing and privacy preserving.Considering that a user continually posts data items in an OSN, we model the threshold selecting problem as a sequential decision-making problem. More specifically, we form u late the problemasa multi- armedbandit problem [9]and apply the upper confidence bound (UCB) policy to solve the problem. Simulation results show that dynamically adjusting the threshold according to the UCB policy can lead to a higher payoff than using a fixed threshold. The main contributions of this paper are as follows: • A trust-based mechanism is proposed for collaborative privacy management in OSNs. The trust values between users are associated with users' privacy loss, and the proposed mechanism can encourage users to be more considerate of other users' privacy. • A bandit approach is proposed to adjust the parameter of the trust-based mechanism. By applying the UCB policy, the user can make a rational trade-off between data sharing and privacy preserving.

II RELATED WORK

Collective Privacy Management

Though current OSNs do not yet impose restrictions on the sharing of co-owned data, the problem of collective privacy management has been studied for a while in academia. In [6], Squicciarini et al. first investigated this problem by using game theory. To aggregate different individuals' privacy policies, they proposed a Clark-Tax mechanism which can encourage individuals to report their true preferences on privacy policies. In [7], Hu et al. proposed a space segmentation approach to identify the conflicts among individuals' privacy policies. And they proposed a conflict resolution mechanism that considers both the privacy risk and the data sharing loss. In their follow-up work [10], they formulated the multiparty access control problem as a game played by multiple users. And an iterative update algorithm was proposed 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 facilitate collaborative control of the personally iden-tifiable information in a data item.

Realizing that users are willing to negotiate and make concessions to achieve an agreement on the privacy policy, some researchers studied negotiation-based methods. In [13], Mehregan and Fong proposed a negation process in which a privacy policy is repeatedly modified until it satisfies certain availability criteria. In [8], the concessions that users may be willing to make in different situations are modeled as a set of concession rules, and a computational mechanism is proposed to solve the privacy conflicts.

Studies introduced above usually assume that there is a trustworthy mediator (e.g. the service provider of the OSN) who knows users' privacy policies specified for a certain data item. The final privacy policy is determined by the mediator. While in the mechanism proposed in this paper, such a mediator is dispensable. The user, who wants to post data, is responsible to gather feedbacks from other involved users and make the final decision. We think such a mechanism is more practical, considering the privacy management in current OSNs.

B. Trust-based Incentive Mechanisms

As pointed out in [27], trust plays a quite important role in network-based applications, such as peer-to-peer (P2P) systems, opportunistic mobile networks [28], [29], and online social networks. In the study of OSNs, the trust relationship between users has been explored to protect sensitive data of users [17], or to verify the user's identity [30]. In [19], Sherchan et al. presented a comprehensive review of trust in the context of social networks. They categorized studies on social trust based on three criteria, namely trust informa-tion collection, trust evaluation, and trust dissemination. The mechanism proposed in this paper involves evaluating the trust values between two users based on their interactions.

However, different from the studies reviewed in [19], we mainly focus on how to utilize trust to encourage the users to be more considerate of others' privacy.

Trust-based incentive mechanisms have been widely studied in P2P systems to deal with the free-riding problem. Tang et al. presented a brief survey of such mechanisms in [20]. So far we have only seen few literatures applying trust to the collective privacy management problem. In [21], Rathore and Tripathy proposed a trust-based access control method which utilizes the trust values to define access conditions. That is, a user can specify the minimum trust level that is required for another user to access his/her data. In [22], Sun et al. proposed a trust-weighted voting scheme to aggregate different users' privacy policies. In this paper, we also use trust values to indicate how much influence a user's opinion will have on the aggregated decision. While, different from Sun et al.'s work where the trust values are fixed, the trust values in the proposed mechanism are related to users' privacy loss, and hence they change over time.

Disadvantages

1. There is no Access Control Based Policy Settings.
2. There is no collaborative privacy management.

III PROPOSED SYSTEM

In the proposed trust-based privacy management mechanism, we introduce a threshold based on which the user makes the final decision on data posting. Simply speaking, a high threshold indicates that the user has a relatively low tendency to share the data with others, and only when the majority of the involved users or users that are highly trusted agree to post the data; the data can finally be posted. By tuning the threshold, the user can make a trade-off between data sharing and privacy preserving. Considering that a user continually posts data items in an OSN, we model the threshold selecting problem as a sequential decision-making problem. More specifically, the system formulates the problem as a multi-armed bandit problem [9] and apply the upper confidence bound (UCB) policy to solve the problem. Simulation results show that dynamically adjusting the threshold according to the UCB policy can lead to a higher payoff than using a fixed threshold.

Advantages

- A trust-based mechanism is proposed for collaborative privacy management in OSNs. The trust values between users are associated with users' privacy loss, and the proposed mechanism can encourage users to be more considerate of other users' privacy.
- A bandit approach is proposed to adjust the parameter of the trust-based mechanism. By applying the UCB policy, the user can make a rational trade-off between data sharing and privacy preserving.
- The performance of the proposed methods is evaluated via a series of simulations. By conducting comparison among different methods, we demonstrate the advantage of the proposed methods.

IV METHODOLOGY

Trust-Based Collaborative Privacy Management

A. Online Social Network An OSN can be represented by an edge-labeled directed graph G = (V,E), where V is the set of vertices and E is the set of edges. Each vertex represents a user. In subsequent descriptions, unless otherwise specified, we use the two terms "vertex" and "user" exchangeable. Each edge in the graph represents a relationship between two users. Let RT denote the set of relationship types supported by the OSN. The edge from users v_i to v_j can be described by a 3-tuple (v_i, v_j , r_{ij}), where r_{ij} €R_T is the label associated with the edge.

By replacing all the directed edges in G with undirected edges, we can compute the distance between any two users. Specifically, given a pair of users (v_i, v_j), if there is a path between the two users, then the distance d_{ij} is defined as the length of the shortest path between users vi and vj . If there is no path between users vi and vj , then we define d_{ij} = 1. For example, in the graph depicted in Fig. 1, the distance between two users a and c is 1, and the distance between a and g is 3.

B. Trust Evaluation Trust plays a key role in the privacy management mechanism proposed in this paper. For any two users v_i and v_j, no matter they are directly connected by an edge or not, we use t_{ij} to represent the trust of user v_i in user v_j . We define t_{ij} [0, 1]. The more user vi trusts user vj , the higher t_{ij} is. The trust of user vj in user vi is denoted as v_{ji}. Generally there is v_{ij} 6= v_{ji}. Various models have been proposed to evaluate trust in social networks [19], including network structure based models [23] and interaction-based models [24]. In this paper, we mainly focus on how the trust between users can be leveraged to realize collective privacy management. Here we first use a simple distance-based method to determine the initial trust values. And in the following section, we will discuss how to update the trust values based on the interactions between users. Given a pair of users v_i 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 the relationship type r_{ij}. For example, if user vj is user vi's family member, we can set t_{ij}= 0:8, while if user v_j is user v_i's colleague, we can set t_{ij} to a lower value, say 0:6. When 1 < d_{ij} < 1, we utilize the transitivity property of trust [25], [26] to compute the trust value. Specifically, t_{ij} is computed by tij = Yk=1;___ ;dij (vpk ;vpk+1)2Pathij tpkpk+1; (1) (1)

where $Path_{ij}$ denotes the shortest path from users v_i to v_j,(v_{pk} , v_{pk+1}) are two adjacent users in the path, p1 = i, pdij+1 = j. Since the trust value ranges from 0 to 1, above equation implies that as the distance between the two users increases, the trust of one user in another decreases.

C. Multiparty Access Control

An important feature of OSNs is that they provides convenient ways for users to share information with others. Generally, a user can: post a data item, such as a photo, a video clip or a text message, in his/her own space or another user's space, disseminate a data item, which was originally posted by another user, by posting it in his/her own space. In either of the above two cases, we refer to the user as the owner of the data item. Formally, given a data item d, we denote the owner of d as od. If d involves multiple users, then d is co-owned by the users. All the users associated with d, except od, are referred to as stakeholders. The set of stakeholders is denoted by Sd. It should be noted that each stakeholder s 2 Sd may possess a data item d 0 which has the same content with d (i.e. d 0 is a duplicate of d). And if the owner od and the stakeholder s want to post data items at the same time, we consider the two data items d and d 0 separately, meaning that for the data item d 0 we treat the stakeholder s as the owner and the owner od as the stakeholder. When posting the data item d, the owner od needs to specify a privacy policy to control which users are allowed to access.

The Proposed system architecture:

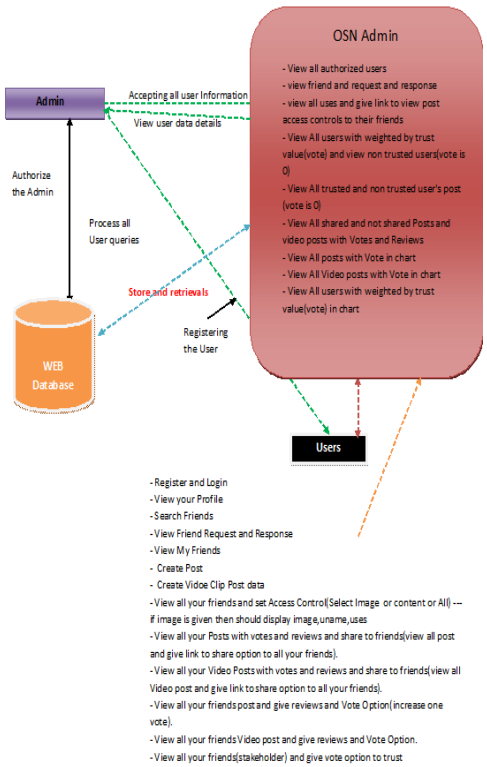

Fig: The Proposed system architecture

OSN Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can perform some operations such as View all authorized users, view friend and request and response, view all users and give link to view post access controls to their friends, View All users with weighted by trust value(vote) and view non trusted users(vote is 0) , View All trusted and non trusted user's post (vote is 0), View All shared and not shared Posts and video posts with Votes and Reviews, View All posts with Vote in chart, View All Video posts with Vote in chart, View All users with weighted by trust value(vote) in chart

Friend Request & Response

In this module, the admin can view all the friend requests and responses. Here all the requests and responses will be displayed with their tags such as Id, requested user photo, requested user name, user name request to, status and time & date. If the user accepts the request then the status will be changed to accepted or else the status will remains as waiting.

Users

In this module, there are n numbers of users are present. User should register before performing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Verify finger print and Login Once Login is successful user can perform some operations like View your Profile, Search Friends, View Friend Request and Response, View My Friends, Create Post, Create Vidoe Clip Post data, View all your friends and set Access Control, View all your Posts with votes and reviews and share to friends(view all post and give link to share option to all your friends), View all your Video Posts with votes and reviews and share to friends, View all your friends post and give reviews and Vote Option, View all your friends Video post and give reviews and Vote Option,View all your friends(stakeholder) and give vote option to trust

Searching Users to make friends

In this module, the user searches for users in Same Network and in the Networks and sends friend requests to them. The user can search for users in other Networks to make friends only if they have permission.

V CONCLUSION

In this paper we study the privacy issue caused by the sharing of co-owned data in OSNs. To help the owner of data collaborate with the stakeholders on the control of data sharing, we propose a trust-based mechanism. When a user is about to post a data item, the user first solicits the stakeholders' opinions on data sharing, and then makes the

final decision by comparing the aggregated opinion with a pre-specified threshold. The more the user trusts a stakeholder, the more the user values the stakeholder's opinion. If a user suffers a privacy loss because of the data sharing behavior of another user, then the user's trust in another user decreases. On the other hand, considering that the user needs to balance between data sharing and privacy preserving, we apply a bandit approach to tune the threshold in the proposed trust-based mechanism, so that the user can get a high long-turn payoff which is defined as the difference between the benefit from posting data and the privacy loss caused by other users. We have conducted simulations on synthetic data and real-world data to verify the feasibility of the proposed methods. Simulation results show that compared to directly posting data without asking others for permission, a user will suffer less privacy loss if he/she always considers other users' privacy. And by applying the proposed UCB policy to determine the threshold, the user can get higher payoffs than setting the threshold to a fixed or random value.

VI REFERENCES

[1] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social 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 in big 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 for categorizing 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 wireless communications 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?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM 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 manage-ment in social networks," in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.

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

[8] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social 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 the multiarmed 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 of multiparty access control in online social networks," in Proceedings of the 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 for online social networks: Model and mechanisms," IEEE Transactions on Knowledge 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 online social networks," in Proceedings of the 22Nd ACM on Symposium on Access Control Models and Technologies, June 2017, pp. 155–166.

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

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

[15] S. Zakhary, M. Radenkovic, and A. Benslimane, "Efficient location privacy-aware forwarding in opportunistic mobile networks," IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 893–906, February 2014.

[16] S. Zakhary and A. Benslimane, "On location-privacy in opportunistic mobile networks, a survey," Journal of Net-work and omputer 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 social networks for distributed protection of sensitive data," IEEE Transactions on Information

Forensics and Security, vol. 6, no. 1, pp. 39–52, March 2011.

[18] N. Z. Gong and D. Wang, "On the security of trustee-based social authentications," 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 social networks," 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 for Dynamic E-Business, September 2004, pp. 302–305.

[21] N. C. Rathore and S. Tripathy, "A trust-based collaborative access control model with policy aggregation for online social networks," Social Network 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-augmented voting 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 for social networks," in 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, November 2011, 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 complex social 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, "Communitystructured evolutionary 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 in data collection? a contract theoretic approach," IEEE Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp. 1256–1269, 2015.

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

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