JES Journal of Engineering Sciences

Vol 10, Issue 11, Nov /2019
ISSN NO:0377-9254

Trust Based Collaborative Privacy Management in Online Social Networks

[1]P.SWETHA, [2]A.D.SIVARAMA KUMAR

[1]M.Tech Student, [2]Assistant Professor
DEPT OF CSE
SVR Engineering College, Nandyal

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. One privacy risk comes from the sharing of co-owned data, i.e., when a user shares a data item that involves multiple users, some users' privacy may be compromised, since different users generally have different opinions on who can access the data. How to design a collaborative management mechanism to deal with such a privacy issue has recently attracted much attention. In this paper, we propose 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 tradeoff between data sharing and privacy preserving by tuning the parameter of the proposed mechanism. We formulate the selecting of the parameter as a multi-armed bandit problem and apply the upper confidence bound policy to solve the problem. Simulation results demonstrate that the trust-based mechanism can encourage the user to be considerate of others' privacy, and the proposed bandit approach can bring the user a high payoff.

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. 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. 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 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 another users' privacy.

Consider the following example. Suppose 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 co-owned 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. 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 cannot 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 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 project we assume that it is the user who wants to post data makes a collective decision based on other users' privacy requirements. Previous studies usually assume that the user who posts the data will tag all the users involved, or the involved users can be identified via some technique (e.g. face reorganization). In such a case, the mediator 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 without tagging other users and the users are hard to be identified automatically.

Considering this, I 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 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 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 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 data item, the user should always consider others' privacy requirements rather than taking a unilateral decision. In the proposed trust-based privacy management mechanism, I 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, I model the threshold selecting problem as a sequential decision-making problem. More specifically, I formulate the problem's multi-armed bandit problem and apply the upper confidence bound (UCB) policy to solve the problem.

II. EXISTING SYSTEM

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 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.

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 , 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 an existing system, Vishwamitra et al. proposed a model that can facilitate collaborative control of the personally identifiable 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. Mehregan and Fong proposed a

Journal of Engineering Sciences

negation process in which a privacy policy is repeatedly modified until it satisfies certain availability criteria. In, 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 project, 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. I think such a mechanism is more practical, considering the privacy management in current OSNs.

Trust-based Incentive Mechanisms

As pointed out, trust plays a quite important role in network-based applications, such as peer-to-peer (P2P) systems, opportunistic mobile network and online social networks. In the study of OSNs, the trust relationship between users has been explored to protect sensitive data of users, or to verify the user's identity. 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 information collection, trust evaluation, and trust dissemination. The mechanism proposed in this project involves evaluating the trust values between two users based on their interactions. However, different from the studies reviewed in, I 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 here. So far I have only seen few literatures applying trust to the collective privacy management problem. The 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.

Sun et al. proposed a trust-weighted voting scheme to aggregate different users' privacy policies. In this project, I 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

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

III.PROPOSED SYSTEM

In the proposed trust-based privacy management mechanism, I 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, I model the threshold selecting problem as a sequential decision-making problem. More specifically, the system formulates the problem as a multi-armed bandit problem 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, I am going to demonstrate the advantage of the proposed methods.

Journal of Engineering Sciences

Journal of Engineering Sciences
Vol 10, Issue 11, Nov /2019
ISSN NO:0377-9254

IV. SYSTEM DESIGN

4.1 System Architecture:

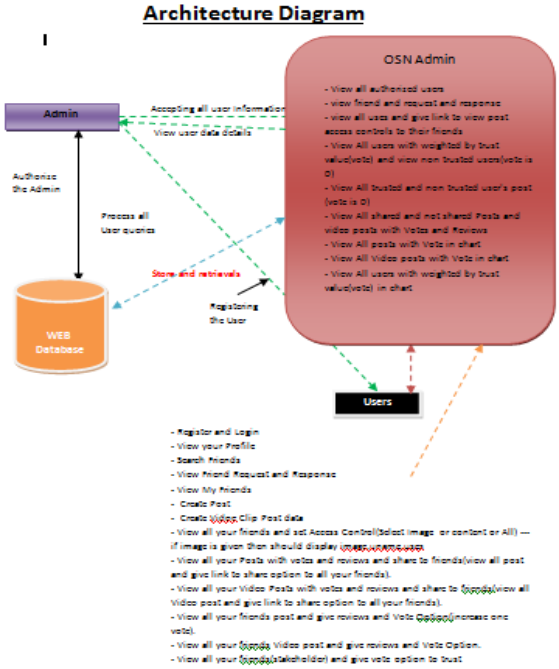

Fig 4.1 System Architecture:

V.MODULES

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 and 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 remain 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 Video 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 User 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.

VI. CONCLUSION

In this project, the privacy issue caused by the sharing of co-owned data in OSNs is studied. To help the owner of data collaborate with the stakeholders on the control of data sharing, I 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 stake holder'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, I apply a bandit approach (UCB Policy) to tune the threshold in the proposed trust-based mechanism, so that the user can get a benefit from posting data and privacy loss caused by the users.

Journal of Engineering Sciences

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 management 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.

Journal of Engineering Sciences