International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

PRIVACY PROTECTION USING FORMAL LOGICS IN ONLINE SOCIAL NETWORKS

Chrsitina Rini.R[1], Jathursana.L[2], Dhivya Keerthana.S[3], Ms.V.Sathiya[4]

[123]*Student, Department of CSE, Panimalar Engineering College, Chennai, India.*
[4]*Associate Professor, Department of CSE,Panimalar Engineering College,Chennai, India*

Abstract- Privacy breaches have been understood as the malfunctioning of a given system. However, a byproduct of its workings. The users are allowed to create and share content about themselves can reach unintended individuals and inference can reveal more information about the user. Social networks our categorization yields that the privacy violations in online social networks of events. Our proposed approach is based on agent-based representation of a social network, The privacy context, including the relations among users or content types, are captured using and our approach using real-life social networks.

Index Terms— Privacy, social networks, ontology, formal model

I. INTRODUCTION

Were used to share personal content with friends (e.g., Facebook.com), more and more a large number of users; however each user shares content with only a small subset of these of the user. For example, a user might share contact information with all of her acquaintances, the user might not even want all her friends to see it. That is, privacy constraints vary based with their users. However, when that happens, it is difficult to enforce users' privacy requirements. That is, each user can contribute to the sharing of content by putting up posts. It accessible for others. These interactions privacy violations, some of which are to deal with privacy violations [2].

That is shared in the online social network (OSN). The content that might be shared by the user herself or by others; the content may vary, entire social network. Whenever this content reveals information to an unintended audience, the user's privacy is breached.

It is important that if a user's privacy will be breached, then either the system takes an appropriate action to avoid this or if it is unavoidable at least let the user know so that she can address circulates in the system and manually find out if their privacy has been breached. This is of social networks, where each user is represented by a software agent. Each agent keeps track them over time. The agent is then responsible for checking if these privacy requirements are expectations from the system. Since privacy requirements differ per person, the agent is responsible for creating on-demand privacy agreements with the system. Formalization of users' privacy requirements is important since privacy violations result because of the variance in expectation violation for a second user. By individually representing these for each user, one can check for the violations per situation. Once the agent forms the agreements then it can query the system for privacy violations at particular states of the system. Since privacy violations require semantic understanding of situations.

Checking for privacy violation can be useful in two ways. First is to find out whether the current system currently violates a privacy constraint of a user. That is, to decide if the actions of others or the user have already created a violation. Second is to find out whether taking a particular action will lead to a violation (e.g., becoming friends with a new person). That is, to decide if a future state will cause a violation. If so, the system can act to prevent the violation, for example by disallowing a certain friendship or removing some contextual there are .

Using the meta-model,we formally define agent-based social networks, privacy requirements, PRIGUARD for representing a model that conforms to the meta-model.This semantic approach uses description logic (DL) [3] to represent information about the social network core of the approach is an algorithm that checks if commitments are violated, leading to a an open-source software tool, PRIGUARDTOOL that implements the approach using ontologies of our approach through this tool shows that different types of privacy violations can be detected are available in the literature..

Section 5 uses the meta-model to model a real-life social network and constructs with pointers for future work.

II.RELATED WORK

Privacy in social networks has been studied in various stances. The first set of approaches study to find out the private personal information that can be discovered for a user. Zhou based on what they have exposed so far. Heatherly et al. [10] use using social inference attacks. here is on capturing privacy requirements and detecting their violations automatically. While these approaches do not attempt that, they successfully show the power of capturing inferences. Our work currently
is based on defined inference rules but could very well benefit from data-driven inferences done in these works.

Privacy Akcora, Carminati, and Ferrari [11] develop a graph-based approach and a risk model to learn risk labels of strangers with the intuition that risky strangers are more likely to and visible a profile item is and can be used to adjust the privacy settings of friends. These approaches identify risky users in general, rather than considering individual privacy requirements privacy violations but to form a general opinion of the network.

(Semi-) automatically suggest policies. Fang and LeFevre propose a privacy wizard that automatically configures the user's privacy settings based on an active learning paradigm [13]. The user provides privacy labels for some of her friends and the proposed privacy wizard automatically Privacy Policy Prediction (A3P) system that guides users to compose privacy settings for their first classify an image into a category based on content and metadata. Then, they find privacy to their policy prediction algorithm. These approaches are complementary to our approach. In developing would be useful to have a method that can recommend users privacy policies.

The last set of approaches detect privacy violations in a given system. Privacy IQ is a Facebook extension where users can see the privacy reach of their posts and the effect of their past privacy settings [15]. PRIGUARD shares a similar intuition by comparing the user's privacy expectations with the actual state of the system. Our contribution is on detecting privacy breaches that take place because of interactions among users and inferences on content.

Is huge and may not be applicable in large networks. In PRIGUARD, privacy violations in OSNs policies are specified in terms of the relationships between the resource owner and the resource her privacy concerns in terms of relationships with other users (e.g., friends of the user)(such as the violation types iii and iv) and does not provide results on the performance of [18]. In this work, they introduce a social network model, a multiparty policy specification scheme and a mechanism to enforce policies to resolve multiparty privacy conflicts. They adopt Answer Set Programming (ASP) to represent their proposed model. Our model shares similar intuitions. Our proposed semantic architecture uses SPARQL queries to detect privacy violations, rather than an ASP solver. In their work, each user manually specifies a policy per resource, which is time-consuming for a user. Moreover, privacy concerns of the users are not formally defined and the In PRIGUARD, we advocate policies to represent privacy concerns of the users and the detection framework tmanage access control in OSNs by generating semantic policies [19]. The social network. [19] and improves it in various ways. First,we provide a rich ontology hence we are able to represent privacy policies in a fine-grained way. Second, the ontological reasoning task in our work is decidable since we use Description Logics rules in our implementation in contrast to Semantic Web Rule Language (SWRL) rules. Third, it is known that access control policies are subject to change often. If a SWRL rule is modified to reflect this change then the ontology privacy concerns of the users as commitments, which are widely-used constructs for modeling interactions between agents [20]. Hence, our model can deal with changes in privacy concerns of the users.

III. EXISTING METHODOLOGY

The existing system is that the user has the activity in their social networking account such as changing the profile picture, posting the recent activity , sending friend request ,accept or reject friend request, chatting with friends , sharing the post that posted by some other user etc ..The user privacy get affected in the existing system by, imagine that if the user post the microblog with the view privilege of "FRIENDS". It means that the user who is friend of the posted user can able to view, like, comment, share the post. Here the users privacy get affected when the viewing user share the post with the privilege of "PUBLIC"or "FRIENDS"or"FRIEND OF FRIENDS" then the post can be viewed by all the account holders.

IV.PROBLEMS IN THE EXISTING SYSTEM

The major problem that we face while you are having an account holder in the social networking are the privacy of the respective micro blog (post) holder may get affected with some privacy issues, if the privileged view user for respective post share the post in the non permitted environment by the micro blog posted person.

V. PROPOSED WORK

In order to reduce the privacy problem that we face in social networking, they introduce an intermediate third person called trusted-third party. And now, if the user post the micro blog with the privilege "FRIEND" The third party take the micro blog to the account and verify the privacy policy that provided by the user. If the privileged user shares the respective user micro blog, the share request will be submitted to the third party. The third party validate the share request and allow the share if the privacy policy provided by the posted user don't get violated or deny if violated.

VI.CONCLUSION

The user privacy of the user post (micro blog) has been preserved by preventing the unprivileged share and full filled sharing for unprivileged post by submitting the share request and share if the posted user permutes.

REFERENCES

[1] M. Mondal, P. Druschel, K. P. Gummadi, and A. Mislove,"Beyond Access Control: Managing Online Privacy via Exposure," in Proc. Workshop Usable Security, Feb. 2014, pp. 1–6.

[2] R. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "Open challenges in relationship-based privacy mechanisms for social network services," Int. J. Hum.-Comput. Interact., vol. 31, no. 5,pp. 350–370, 2015.

[3] M. S. Bernstein, E. Bakshy, M. Burke, and B. Karrer, "Quantifying
the invisible audience in social networks," in Proc. SIGCHI Conf.Hum. Factors Comput. Syst., 2013, pp. 21–30.

[4] L. Andrews, I Know Who You Are and I Saw What You Did: Social
Networks and the Death of Privacy. New York, NY, USA: The Free Press, 2013.

[5] M. X. Zhou, J. Nichols, T. Dignan, S. Lohr, J. Golbeck, and J. W. Pennebaker, "Opportunities and risks of discovering personality
traits from social media," in Proc. Extended Abstracts Hum.Factors Comput. Syst., 2014, pp. 1081–1086.

[6] J. Golbeck and D. Hansen, "A method for computing political
preference among Twitter followers," Soc. Netw., vol. 36, pp. 177–184, 2014.

[7] R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Preventing private information inference attacks on social networks," IEEE Trans. Knowl. Data Eng., vol. 25, no. 8, pp. 1849–
1862, Aug. 2013.

[8] C. G. Akcora, B. Carminati, and E. Ferrari, "Risks of friendships on social networks," in Proc. IEEE Int. Conf. Data Min., 2012,pp. 810–815.

[9] K. Liu and E. Terzi, "A framework for computing the privacy
scores of users in online social networks," ACM Trans. Knowl. Discovery Data, vol. 5, no. 1, pp. 6:1–6:30, 2010.

[10] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in Proc. 19th Int. Conf. World Wide Web, 2010, pp. 351–360.

[11] A. C. Squicciarini, D. Lin, S. Sundareswaran, and J. Wede,"Privacy policy inference of user-uploaded images on content sharing sites," IEEE Trans. Knowl. Data Eng., vol. 27, no. 1,pp. 193–206, Jan. 2015.

[12] B. Krishnamurthy, "Privacy and online social networks: Can colorless green ideas sleep furiously?" IEEE Secur. Priv., vol. 11,no. 3, pp. 14–20, May2013.