Review on Semantic Approach to Detect Privacy Violations in Online Social Networks

Karuna Sonone[1] V. M. Barkade[2]
[1,2]Department of Computer Engineering
[1,2]Rajashri Shahu College of Engineering

Abstract— Social network users expect the social networks that they use to preserve their privacy. However, in online social networks, privacy breaches are not necessarily .In this proposed, first categorizes to protect the consumer that take place in online social networks. Our proposed approach is based on agent-based representation of a social network, where the agents manage users' privacy requirements by creating commitments with the system. The proposed detection algorithm performs reasoning using the description logic and commitments on a varying depths of social networks. The proposed detection algorithm performs reasoning using the description logic and commitments on a varying depths of social networks.

Key words: Social Networks, Facebook, Privacy, Filtering

I. INTRODUCTION

Typical examples of privacy violations on social networks resemble violations of access control. In typical access control scenarios, there is a single authority (i.e., administrator) that can grant accesses as required. However, in social networks, there are multiple sources of control. That is, each user can contribute to the sharing of content by putting up posts about her-self as well as others. Further, audience of a post can re-share the content, making it accessible for others. These interactions lead to privacy violations, some of which are difficult to detect by users. Our review of privacy violation reveals two important axis for understanding privacy violations. The first axis is the main contributor to the situation. This could be the user her-self putting up a content that reveals unwanted information or it could be other people sharing content that reveals information about the user. The second axis is how the information is revealed; if the information was itself unwanted or the information led to new information being revealed. (i.e., through inferences) [1].

According to these two axis, we recognize four types of privacy violations. In type (i), a user shares some content with some privacy settings, the system acts against these settings and shares the content with people that it was not supposed to. In type (ii), information about a user is shared by another person. In online social networks, information about a user can easily propagate in the system, without users consent. In type (iii), a user puts up a content on the social network without realizing that more information can be inferred from her post; e.g., giving away location information through a landmark. In type (iv), a friends action leads to a privacy leakage but the leakage can only be understood with some inferences in place; e.g., a friends tag revealing friendship status. Moreover, content may lead to [2]. Privacy violations occur due to its semantics. A post may annoy or insult the user, or it may include private information; e.g., sharing a post that reveals the users politic affiliation. In that research paper, we innovated the an approach for managing users privacy constraints in online social networks for detecting privacy violations and guide the user to protect her privacy.

The Privacy has long been accepted as an important concept in developing and running software. Typically, the software publishes its privacy agreement and the user accepts the agreement to use it. A similar pattern applies in online social networks, with additional handles to customize various parts of the policy. For example, a user can choose to share content with her friends but not anyone else, whereas a second user may choose to share content with everyone in the system. However, many times users' privacy requirements or expectations do not agree with each other. Contrary to typical software, in social networks, users can manipulate the content by tagging users, re-sharing content, and so on. Thus, content could become available to various audiences without the consent of some of the users involved. Consider a user who wants to post a picture of herself with one of her friends. For the user, the posting could be harmless but her friend may be unhappy about it because the picture violates her privacy. One common way of dealing with this in current social networks, such as Facebook, is to report the picture as inappropriate and let the user know that the person is unhappy about the content and would prefer it to be removed. [3].

Thus, the user is free to decide what to do about it. This requires a lot of human interaction online. More importantly, by this time, the picture has already been up and might well been viewed by many social network users. This simple example is significant because it suggests various interesting properties for privacy protection. These properties are, Automation, Fairness, Concealment of privacy concerns, and Protection before exposure [4].

In Automation properties, Privacy protection calls for automated methods. Considering the volume of social media transactions that are done every hour, it is not plausible for humans to discuss content that is related to them in person. Hence, an agent that represents a user is needed to keep track of its user's preferences and policies and act on behalf of them, accordingly. Fairness properties for, If a post is deemed private for a user, one approach is to take it down from the system completely. This all-or-nothing approach is simple but leaves the party who wants to keep the post up in a disadvantaged position. Instead, it is best if the users identify what is wrong with the post (in terms of privacy) and improve those aspects only. For example, if the text of a picture post is causing a privacy violation, the text can be removed while managing in picture.

Concealment of privacy concerns properties that, Privacy preferences may reveal personal information that should be kept private from others. That is, a user might say that she does not like the text of a post, but she does not need to identify why that is the case. Ideally, a proposed

approach to privacy protection should keep users privacy concerns private, without revealing users privacy concerns. In Protection before exposure that, Contrary to existing systems, such as Facebook, where a privacy violation is caught after it happens, and the fact that content is private should be identified before the content is put up online. Otherwise, there is a risk that the content reaches unintended audience. Hence, a proposed approach should be in place before the content is put up rather than after.

Accordingly, this proposes an agreement platform for privacy protection that addresses the above properties. One recent study has shown that many times invading a friend's privacy on a social network is accidental and the user invading the privacy is not aware of it. When the user is notified for the situation, many of them choose to put down a content rather than breaching their friends privacy. This naturally suggests that if the users could have agreed on the content before it went up, then many privacy leakages could have been avoided to begin with. We exploit this idea by developing a platform where the agents interact to reach a consensus on a post to be published. We assume that each user is helped by a software agent to manage her privacy. The agent is aware of the user's privacy concerns and expectations but also knows about the user's social network, such as her friends. When a user is about to post a new content, she delegates the task to her agent. The agent reasons on behalf of the user to decide which other users would be affected by the post and contacts those users agents. The negotiation protocol we develop enables agents to discuss their user's constraints and agree on a suitable way to post the content such that none of the user's privacy is violated. Additionally, we present the recent works on conducted on different types of privacy violation detection in online social network. In section II, we are presenting the related study of OSN (online social network).

II. RELATED WORKS

A. Nadim kokciyan, Pinar Yolum et.al (2016):

In [1], Social network users expect the social networks that they use to preserve their privacy. Traditionally, privacy breaches have been understood as malfunctioning of a given system. However, in online social networks, privacy breaches are not necessarily a malfunctioning of a system but a by product of its workings. The users are allowed to create and share content about themselves and others. When multiple entities start distributing content without a control, information can reach unintended individuals and inference can reveal more information about the user. Accordingly, this paper first categorizes the privacy violations that take place in online social networks. Our categorization yields that the privacy violations in online social networks stem from intricate interactions and detecting these violations requires semantic understanding of events. Our proposed approach is based on agent-based representation of a social network, where the agents manage users' privacy requirements by creating commitments with the system. The privacy context, including the relations among users or content types is captured using description logic. The proposed detection algorithm performs reasoning using the description logic and commitments on a varying depths of social networks. Author implements the proposed model and evaluate approach using real-life social networks.

B. Zhou et.al (2014):

In [2], author show that by processing public information about social network users, one can identify various personal traits such as whether the person is introvert or not.

C. J. Golbeck and D. Hansen (2014):

In [3], author represent that, anecdotal evidence and a variety of methods, claims are constantly being made about the bias of media outlets. As many of those outlets create online personas, we seek to measure the political preferences of their audience, rather than of the outlet itself. In this paper, we present a method for computing political preferences of an organization's Twitter followers using congressional liberal/conservative ADA scores as a seed. Authors apply this technique to characterize the political preferences of major news media Twitter audiences. Also authors show that, how this technique can be extended or used to create personalized recommendations and insights for news seekers and social media analysts and marketers.

D. R. Heatherly, M. Kantarcioglu, and B. Thuraisingham et.al (2013):

In [4], authors represent that, use inference attacks using social networking data to predict private information and propose sanitization techniques to prevent inference attacks. This direction of work aims to discover personal information about users when that information was not explicitly declared by the user herself.

E. Akcora, Carminati et.al (2012):

In [5], author Akcora, Carminati and Ferrari 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 violate privacy constraints. While this is useful information, when previous information is not available, this would not be an applicable direction to pursue.

F. Liu and Terzi (2010):

In [6], author Liu and Terzi propose a model to compute a privacy score of a user. The privacy score increases based on how sensitive 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 of users as we have done in this work. Hence, they are not targeted to detecting individual privacy violations but to form a general opinion of the network.

G. L. Fang and K. LeFevre et.al (2010):

In [7], author Fang and LeFevre propose a privacy wizard that automatically configures the user's privacy settings based on an active learning paradigm. The third set of approaches learns the privacy concerns of the user so that the system can (semi-) automatically suggest policies. The user provides privacy labels for some of her friends and the proposed privacy wizard automatically assigns privacy labels to the remaining set of friends

H. Squicciarini (2015):

In [8], author Squicciarini propose that, an Adaptive Privacy Policy Prediction (A3P) system that guides users to

compose privacy settings for their images. They use content features and social features of the users in the system. They first classify an image into a category based on content and metadata. Then, they find privacy policies that are related to this category and recommend the most promising one according to their policy prediction algorithm. These approaches are complementary to our approach. In developing our detection approach, we assume that the users have their policies in place. However, it would be useful to have a method that can recommend users privacy policies.

I. Kafali et.al (2012):

In [9], author Kafali develop that PROTOSS, where the users' privacy agreements are checked against an OSN using model checking. The number of states that are generated even in a small network is huge and may not be applicable in large networks. In PRIGUARD, privacy violations in OSNs of a significantly larger size can be detected much more quickly.

J. P. W. Fong, (2011):

In [10], author presented another approach that uses model checking is Fong's Relationship-based Access Control (ReBAC) model, where access control policies are specified in terms of the relationships between the resource owner and the resource accessory in the social network.

K. Mainack Mondal, Peter Druschel, Krishna P. Gummadi (2014):

In [11] author invented that, access control, the dominant model for modeling and managing privacy in today's online world, is fundamentally inadequate. First, with access control, users must a priori specify precisely who can or cannot access information by enumerating users, groups, or roles—a task that is difficult to get right. Second, access control fails to separate who can access information from who actually does, because it ignores the difficulty of finding information. Third, access control does not capture if and how a person who has access to some information redistributes that information. Fourth, access control fails to account for information that can be inferred from other, public information. The author present exposure as an alternate model for information privacy; exposure captures the set of people expected to learn an item of information eventually. We believe the model takes an important step towards enabling users to model and control their privacy effectively.

L. R. Fogues, J. M. Such, A. Espinosa (2013):

In [12] authors innovated that, Social networking services (SNSs) such as Facebook or Twitter have experienced an explosive growth during the few past years. Millions of users have created their profiles on these services because they experience great benefits in terms of friendship. SNSs can help people to maintain their friendships, organize their social lives, start new friendships, or meet others that share their hobbies and interests. However, all these benefits can be eclipsed by the privacy hazards that affect people in SNSs. People expose intimate information of their lives on SNSs, and this information affects the way others think about them. It is crucial that users be able to control how their information is distributed through the SNSs and decide who can access it. This paper presents a list of privacy threats that can affect SNS users, and what requirements privacy mechanisms should fulfil to prevent this threat. Then, we review current approaches and analyze to what extent they cover the requirements.

III. COMPARATIVE ANALYSIS

The methods are studied above and compared in terms of advantages, disadvantages, techniques. Table 1 is showing the comparative study among these methods.

Paper Title	Key Techniques and Methods	Advantages	Disadvantages
PRIGUARD: A Semantic Approach to Detect Privacy Violations in Online Social Networks	The user OSN, Agent-based representation of social network, Privacy context	Improve the privacy detection, and this approach is scalable.	Users cannot trust a central entity.
A method for computing political preference among twitter followers	Twitter, Politics, Liberal, Conservative, News, Journalism. Congressional l liberal/conservative ADA	An analysis of this method applied to major media outlets, a wide range of government agencies, and think tanks. to characterize the political preferences of major News media Twitter audiences.	Minimum space are the disadvantage of this technique.
Preventing private information inference attacks on social networks	OSNS, Facebook, machine learning algorithm, naïve-bayes, sanitization technique	To predict private information. Explore the effectiveness of these techniques and attempt to use methods of collective inference to discover sensitive attributes of the data set.	Limited access network, repeated Distributions of sanitized data over time.
Risks of friendships on social networks	Social network, risk analysis risk dynamics and friendship	To compute risk labels of friends. found that the Number of mutual friends is not very important to change the risk perception of a user towards a friend	privacy settings can be automatically applied to different social network users

		of friend.	
A framework for computing the privacy scores of users in online social networks	Privacy and social network, QDOS, NAIVE PRIVACY-SCORE	To enhance public awareness of privacy to reduce the complexity of managing information sharing in social Networks.	The issue of privacy in online social networking from a new use r-centred perspective and can prove useful in growing users' awareness
Privacy wizards for social networking sites	Social Network Privacy, Usability, Active Learning, security, integration and protection	the removes much of the burden from individual users, to automatically Configure the user's detailed privacy settings. reducing the amount of user effort, while still producing high-accuracy Settings.	other sources of information may be Taken into account.
Privacy policy inference of user-uploaded images on content sharing sites	Online information services, web-based services, Adaptive Privacy Policy Prediction	To helps users automate the privacy policy Settings for their uploaded images. To improve the privacy of user data.	the issue of cold-start, leveraging Social context information.
Detecting and predicting privacy violations in online social networks.	Privacy-preserving social networking techniques Model checking Ontological reasoning Commitments	Enable users to share, discuss, and create content together with various others. to manage and maintain their agreements through well-founded methods.	it is difficult to keep private information contained.
Relationship-based access control: Protection model and policy language	Contexts, electronic health records, modal logic, policy language, relationship-based access control, social networks	To facilitate the specification and composition of ReBAC policies. An provided initial evidence on the feasibility and utility of ReBAC as a general-purpose protection Approach for application security and privacy.	the problem is that model checking could become intractable and representational completeness

Table 1: Comparative Study of Image Forgery Detection Methods

IV. CONCLUSION

This paper acquainted a meta-display with characterizing online informal communities as operator based interpersonal organizations to formalize protection necessities for clients and their infringement. Keeping in mind the end goal to comprehend security infringement that occurs in genuine online interpersonal organizations, we have directed an overview with Facebook clients and sorted the infringement regarding their causation. We additionally propose PRIGUARD, an approach that sticks to the proposed meta model and uses portrayal rationale to depict the informal community space and responsibilities regarding indicating the security necessities of the clients. Our proposed calculation in PRIGUARD to identify security infringement is both sound and finish. The calculation can be utilized before making a move to check on the off chance that it will prompt an infringement, in this manner forestalling it forthrightly. On the other hand, it can be utilized to do sporadic keeps an eye on the framework to check whether any infringement has happened. In the two cases, the framework, together with the client, can work to fix the infringement. In the actualized PRIGUARD in an apparatus called PRIGUARDTOOL and exhibited that it can deal with case situations from different infringement classes effectively. Its execution comes about on genuine systems are promising.

V. REFERENCES

[1] Nadin K¨okciyan and Pınar Yolum, "PRIGUARD: A Semantic Approach to Detect Privacy Violations in Online Social Networks", IEEE Transactions on Knowledge and Data Engineering, 2016.
[2] 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. of the extended abstracts of ACM conference on Human factors in computing systems. ACM, 2014, pp. 1081–1086.
[3] J. Golbeck and D. Hansen, "A method for computing political preference among twitter followers," Social Networks, vol. 36, pp. 177–184, 2014.
[4] 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, 2013.

[5] C. G. Akcora, B. Carminati, and E. Ferrari, "Risks of friendships on social networks," in IEEE International Conference on Data Mining (ICDM), 2012, pp. 810–815.
[6] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 5, no. 1, pp. 6:1–6:30, 2010.
[7] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in Proceedings of the 19th international conference on World wide web. ACM, 2010, pp. 351–360.
[8] 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, 2015.
[9] O. Kafalı, A. G¨unay, and P. Yolum, "Detecting and predicting privacy violations in online social networks," Distributed and Parallel Databases, vol. 32, no. 1, pp. 161–190, 2014.
[10] P. W. Fong, "Relationship-based access control: Protection model and policy language," in Proceedings of the First ACM Conference on Data and Application Security and Privacy (CODASPY), 2011, pp. 191–202.
[11] Mainack Mondal, Peter Druschel, Krishna P. Gummad," Beyond Access Control: Managing Online Privacy via Exposure"*Proc.Workshop Usable Security*, pp. 1-6, Feb. 2014.
[12] R. Fogues, J. M. Such, A. Espinosa, 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.

