A Critical Review of Detection of Privacy Violation in Online Social Network.

Grishma R. Pardeshi.[1], Prof. Rajesh H. Kulkarni[2]

[1]*ME Student, Dept of Computer, JSPM NTC,PUNE,India*
[2]*Professor, Dept of computer Engineering, JSPM NTC,Pune,India*

---***---

Abstract - In online social networks (OSNs), users are allowed to create and share content and information about themselves and others. When many entities start distributing content, information can reach unrelated individuals and inference can show more Information about the user. Existing applications do not focus on detecting privacy violations before they occur in the system. This paper aim agent-based representation of a social network, where the agents manage users' privacy requirements and create privacy agreements with agents. The privacy content, such as the relationship among users, various information in the system. Here argue that commonsense reasoning could be useful to solve some of privacy examples reported in the literature. It is first reviewed to find out the Privacy violation .

Key Words :Social Network, Privacy Violation, Agent-based representation, Violation Detection.

I. INTRODUCTION

Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share common themes. When something is private to a *person*, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information.

Violation of Privacy Mishandling private information, such as customer passwords or social security numbers, can compromise user privacy, and is often illegal.

Privacy violations occur when:

1. Private user information enters the program.
2. The data is written to an external location, such as the console, file system, or network.

Private data can enter a program in a variety of ways:

- Directly from the user in the form of a password or personal information
- Accessed from a database or other data store by the application
- Indirectly from a partner or other third party

Privacy violations reveals two important axis for understanding privacy violations.

The first axis is the main contributor to the situation.

The second axis is how the information is revealed

Risk at Online Social Network :

Social networking sites allow any user to post information that thousands of other users can read. But that is not at all. In this Q&A, information security threats expert reveals how sites like Myspace and Youtube let the bad guys post something more dangerous: malware.

This could be the user herself putting up a information that reveals unwanted information or it could be other people sharing content that reveals information about the user that doesn't want to show. A approach for managing users'

privacy constraints in online social networks for detecting privacy violations and guides the user to protect her privacy as well.
It is important that if a user's privacy will be broken, then either the system takes an appropriate action to avoid this or if it is unavoidable at least let the user know so that they can address the violation. In current online social networks, users are expected to monitor how their content circulates in the system and manually find out if their privacy has been breached.

The review and its outcome are further organized as follows. Section II reveals the review of various techniques in online social network. Section III reveals the many papers survey and calculate the optimal technique. Section IV reveals the algorithmically reviewed by existing system. Section V reveals the review of outcome and finally Section VI concluded the review.

A) SOCIAL NETWORK SITE REVIEW

Privacy agreements (between an agent and the OSN) through commitments and the corresponding violations statements, and detect privacy violations in a centralized way are represented. Firstly extend this implementation to cover privacy agreements between agents. Second, to improve our initial model to detect privacy violations automatically before they would occur in the current system. For this, it improve model by enabling agents to reach agreements automatically. Agents may have conflicting privacy constraints and we want them to be able to resolve such conflicts. In the next step, researches further how to use agreement technologies in privacy context; e.g., formulation of an offer or a counter-offer in negotiation; formulation of an argument and an attack in argumentation.

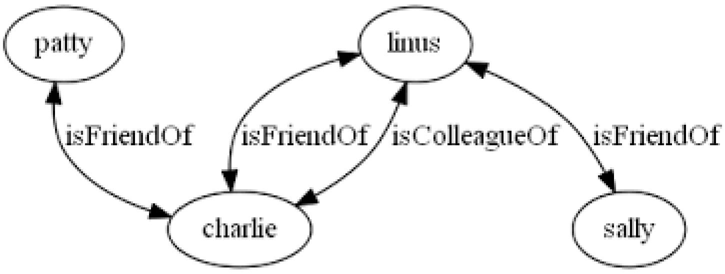

Fig.1 Analytical Structure of Social site

it could be useful to solve some of them. For this, some information can be extracted from a post; e.g., the context of a post, entities in a post text or a picture and so on. Such information can be processed by an agent to decide whether a post is private or not. For example, if an agent knows that a diamond ring is ink picture, and the context is an engagement; then, it can actively notify the current user that the picture might be private and suggest him to not show the picture to his friend. Hence, the user can take an action Study of logic-based and language-based (e.g., Concept Net) commonsense reasoning tools, which have never been applied to privacy context
Since users cannot trust a central to protect their privacy. Sometimes requires collecting proof from other agents in the social network. New methods for agents to collect such evidence and process it for detecting privacy violations.

II. Reviewed Technique

There are three techniques underlying this approach. The first one is the abstraction of commitment among individuals when carrying out agreements. The second one is checking models of systems to verify whether certain properties hold in the system. The third one is the use of ontologies to define the semantics of concepts related to OSNs and privacy and reason about their relationships.

Commitments

A *commitment* is an agreement from one person to another to bring about a certain property, if a specified condition is achieved. A commitment is not just a static representation of an agreement, it is an active entity that reflects the current state of the underlying agreement. In order to achieve this, a commitment is associated with a stateof system that evolves over time in coordination with the status of the represented agreement. A commitment is created in *conditional* state, in which neither the antecedent nor the consequent of the commitment is achieved successfully. When the antecedent of the commitment is achieved, the state of the commitment changes to *active*. If the consequent of the commitment is satisfied, then the state of the commitment changes to *fulfilled status*. On the other hand, if the consequent of the commitment fails due to any reason while the commitment is active, then the state of the commitment changes to *violated*.

Model checking

Model checking is a computational method to automatically verify whether a certain property holds in a given system. The system under consideration is modeled as a state transition graph in some simple formal language and the property that is aimed to be verified is represented as a logic formula in a suitable language, such as linear temporal logic (LTL) or computation tree logic (CTL).

Ontologies

An ontology is a conceptualization of a particular domain. An ontology enables specification of domain concepts and their relations semantically. The concepts are defined using their defined properties. The relations enable concepts to be bind together. A common relation between concepts is the *isA* relation, which denotes that one concept. From a privacy perspective, content related to privacy can be thought of as a domain system and represented as an ontology technique.

III. RELATED WORK

Zhou et al. [6] 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.

Golbeck and Hanson [7] show how one can detect political preferences of users on a social network users, again based on what they have exposed so far.

Heatherly et al. [10] use inference attacks using social networking data is to predict private information and propose sanitization techniques to prevent inference attacks made by attacker . This direction of work aims to discover personal information about users when that information was not explicitly declared by the user herself/himself.

The second set of approaches aim to identify potentially risky users who are likely to breach privacy. Akcora, Carminati and Ferrari [9] 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 of user data . While this is useful information, when previous information is not available in system , this would not be an applicable direction to work.

Liu and Terzi [12] propose a model to compute a privacy score of a user.

Author Name	Paper Title	Algorithm/Methods	Objective
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.	It Focused on technology Online reputation management(ORM)and CHI technique.	The paper show that by processing public information about social n/w users, one can identify various personal traits such as whether the person is introvert or not.
J. Golbeck and D. Hansenn	A method for computing political preference among twitter followers.	In this uses scoring users and organizations technique for this quantitative validation and qualitative validation used .	In this show how one can detect political preferences of users on a social network user, again based on what they have exposed so far.

R. Heatherly, M. Kantarcioglu, and B. Thuraisingham	Preventing private information inference attacks on social networks	Naïve Bayes Clssificationand Collective Interference Methods.	In this paper, use of inference attacks using social networking data to predict private information and propose sanitization techniques to prevent inference attacks.
C. G. Akcora, B. Carminati, and E. Ferrari	Risks of friendships on social networks	In this Uses Friends Risk Labels and Friend Impact Method to calculation.	In this paper 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
K. Liu and E. Terzi	A framework for computing the privacy scores of users in online social networks	In this IRT based computation of the Privacy Score and also use method to handled polytomous response matrices.	The paper proposes 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.
Lujun Fang and Kristen LeFevre	Privacy Wizards for Social Networking Sites	Privacy Preference Model as classifier. visualization of decision tree model.	We propose a template for the design of a social networking *privacy wizard*. The intuition for the design comes from the observation that real users conceive their privacy preferences based on an implicit set of rules
Hongxin Hu,	Multiparty Access Control for Online Social Networks: Model and Mechanisms	Multiparty access control (MPAC) for data sharing in OSN's.	These OSNs offer attractive means for digital social interactions and information sharing, but also raise several security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users.
Özgür Kafalı · Akın Günay · Pınar Yolum	Detecting and predicting privacy violations in online	PROTOSS for detecting and predicting violations.	In this paper, we have developed protos, a run time tool for detecting and predicting Privacy violate ions

	social networks		in Online Social networks. protos captures relations among users, their privacy agreements with an online social network operator, as well as domain-based semantic information and rules.
Mainack Mondal, Peter Druschel	Beyond Access Control: Managing Online Privacy via Exposure	Privacy Model of exposure and access control.	we propose an alternative model for information privacy based on exposure. A key difference compared to access control is that exposure captures the principals who learn a piece of information rather than who *can directly access* a piece of info.
Philip W. L. Fong	Relationship-Based Access Control:Protection Model and Policy Language	REBAC(Relationship based Access control) Model	Multiple inheritance corresponds to a more flexible means of constraining when relationships can be "activated" simultaneously

IV. REVIEW OF EXISTING ALGORITHM

In the existing system privacy violation on social networks look like a violations of access control. In typical access control scenarios, there is a single authority (i.e., administrator) that can grant accesses as required per user. 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 and pictures about herself as well as others. Further, audience of a post can reshare the content, making it accessible for others. These interactions lead to privacy violations, some of which are difficult to detect by users.

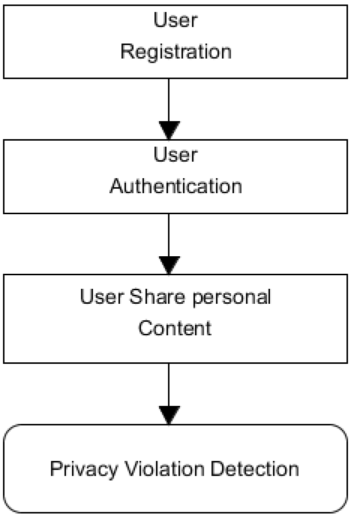

Fig System Architecture of Existing System:

V. REVIEW OUTCOME

Based on a survey performed, it is clear that huge percentage of users are facing these privacy violations Problem in day today life.

All works are handle the first violation type easily in which the violation is endogenous and direct. This is, if a user specifies a privacy constraint that is independent of any other user's perspective then this privacy constraint can be enforced.

VI. CONCLUSION

In this paper various privacy requirement and related issues has been discussed and interpreted. The privacy context, including the relations among users or content types, is captured using description logic to describe the social network domain and commitments to specify the privacy requirements of the users.

REFERENCES

1 N. K¨okciyan and P. Yolum. Commitment-based privacy management in online social networks. In First International Workshop on Multiagent Foundations of Social Computing at AAMAS, 2014.

2 J. McCarthy. Artificial intelligence, logic and formalizing common sense. In Philosophical Logic and Artificial Intelligence, pages 161–190. Springer, 1989.

3 M. P. Singh. An ontology for commitments in multiagent systems. Artificial Intelligence and Law, 7(1):97–113

4 M. Bennicke and P. Langendorfer. Towards automatic negotiation of privacy contracts for internet services. In Networks, 2003. ICON2003. The 11th IEEE International Conference on, pages 319–324. IEEE, 2003.

5 M. Horridge and S. Bechhofer. The OWL API: A Java API for OWL ontologies. Semantic Web, 2(1):11–21, 2011.

6 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.

7 J. Golbeck and D. Hansen, "A method for computing political preference among twitter followers," Social Networks, vol. 36, pp. 177–184, 2014.

8 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.

9 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.

10 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.

11 Lu jun Fang and Kristen LeFevre 2010, Privacy Wizards for Social Networking Sites.

12 Hongxin Hu, Multiparty Access Control for Online Social Networks: Model and Mechanisms.

13 Özgür Kafalı · Akın Günay · Pınar Yolum 2013 Detecting and predicting privacy violations in online social networks.

14 Mainack Mondal, Peter Druschel 2014, Beyond Access Control: Managing Online Privacy via Exposure.

15 Philip W. L. Fong 2011 Relationship-Based Access Control:Protection Model and Policy Language.

16 K. M. Heussner, "Celebrities' photos, videos may reveal location," ABC News, Available at: http://goo.gl/sJIFg4.

17 J. Leskovec and J. J. Mcauley, "Learning to discover social circles in ego networks," in Advances in Neural Information Processing Systems

18 F. Pereira, C. Burges, L. Bottou, and K. Weinberger, Eds. Curran Associates, Inc., 2012, pp. 539–547

19 B. Krishnamurthy, "Privacy and online social networks: can colorless green ideas sleep furiously?".

20 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.