International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 4374–4379

Review of Privacy Violation Identification Methods For Social Networking Sites

Mr. Vishwas Kalunge -- *PHD Student, University of Technology, Jaipur.*
Dr. S. Deepika -- *PHD Guide, University of Technology, Jaipur.*

ABSTRACT

(OSNs) is an online social network which allows user in order to produce and spread content and information about each other. It shows more information about the users when many people or users start to share their content, that content can easily reach unrelated users or individuals instead. Applications that exist already does not take precautions about user privacy violation beforehand. This issue will focus on agent-based representation of social network, where users' privacy requirements are managed by agents as well as created and managed by agents as well. Some privacy content, such as the relationship of users or among them, different information present in the system argues that in solving some privacy examples reported in the literature commonsense reasoning the literature is useful. It will be reviewed in order to find out the Privacy violations.

KEYWORDS: *Social Networks, Privacy Violations, Risk of social network and Detection of violation.*

1. INTRODUCTION

An individual or group can seclude themselves by the ability of privacy , or information about themselves or related to them, and thereby express themselves selectively. The boundaries and content that is considered private differ among cultures and individuals, but share common themes or platform. When something is private or exclusive to a person, it commonly means that something is personal or inherently special and sensitive to them. The domain of privacy partially overlaps security (confidentiality), and it includes concepts of appropriate use, and protection of information as well [1].

Violation of Privacy or intrusion in private data by misusing someone's private information, like their passwords or passkeys, their security numbers or codes, can steal privacy for a user, which is illegal as invasion of privacy [2].

Violation of privacy transpires when:

1. Private user information enters the program.
2. The data is written to the external locations, for instance the console, file system, network, etc.

Private data can enter a program in the various ways:

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

There are 2 important axis to understand the privacy violations:

1. One is the main contributor of the situation
2. The other axis tells about how information or data is disclosed or revealed

ISSN: 2233-7857 IJFGCN

1.1. Threats of Online Social Networks

Social networking sites are the platform at which any user is allowed to share data that access other users to read, saw and interact with[3]. This can be the user themselves sharing an information that may lead to or can reveal private data or it can be some other user that are sharing content that reveals the data about some other user that they are not comfortable to show. A much better approach for managing users'privacy is for detecting privacy violations and make the user aware of it so that they can secure the content as per their need.

It's crucial that if privacy of an user is violated, then the system takes an appropriate and immediate action to avoid this or if that cannot be done then letting the user be aware of the circumstance so that they can fix it. In today's world, users are expected to take note of their privacy and take care of it by looking out itself in order to save it from getting violated.

1.2. Social Network Site Review

Detecting privacy violations are done in a very centralized manner [4]. First implementation are needed for privacy agreements between agents. Second, to develop model further to identify privacy violations itself before they can arise in this system. It helps agents to reach problems automatically improving the system further. Agents may have privacy issues and these conflicts should be secured as their privacy is utmost. The next step is that researchers uses technologies to shield privacy; example, making of an offer or a counter-offer to negotiate; making of an argument and an attack in argumentation. The analytical structure of an SNS is shown in Figure 1.

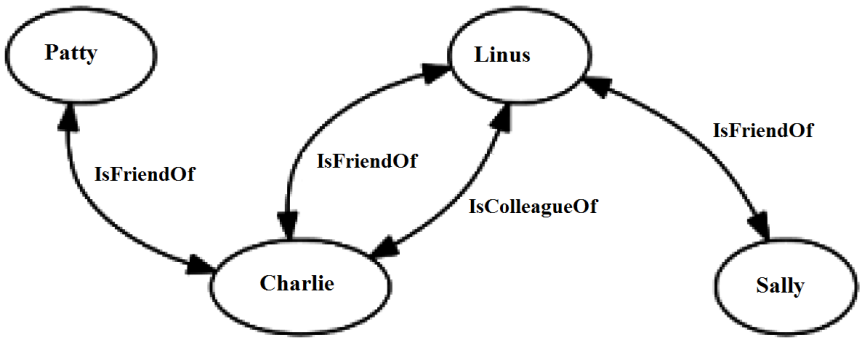

Figure 1: Analytical Structure of an SNS

It has found that solving some of this conflicting situations are very useful. This information is enough to be processed further by agent, then the agent will make the decision whether a post is private or not. Therefore, user can take action themselves, and it has never been used before in the context of privacy and since users itself sometimes don't have faith in a central to protect their privacy. Maybe it may need asking for proofs from other sources and agents as well and new ways are found for agents so they can gather such proofs to detect violation of privacy.

2. REVIEWED TECHNIQUES

To review these techniques there are three ways.
1.-To abstract the commitment among individuals when carrying out agreements.
2. -Checking and verifying that characteristic properties hold in the system or not.
3.–Using the help of ontologies to define semantics of concepts related to OSNs and privacy and reason about their relationships.

2.1. Commitments

A commitment (if a specified condition is achieved) is a deal between two people about to bring

ISSN: 2233-7857 IJFGCN

about a specific attribute [5]. A commitment is not simply a static representation of an agreement, it is an active entity that reflects the current state of the underlying agreement. To achieve this, a commitment is associated with a state of the system that develops over time in coordination with the state of the representation agreement. In the conditional state, a commitment is made, in which neither the response nor the commitment results successfully. When the commitment response is received, the commitment status changes to Active. If the result of the commitment is satisfied, the commitment condition changes to the state of completion.

3. RELATED WORKS

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 aloof or not. Golbeck and Hanson [7] showed the way of seeing how we can spot political choices of different users on a social networking, truly based on what these users allows us to see. 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 . All these efforts helps one to find and know about user's personal info with their own consent.

3.1. Ontology

Ontology is an understanding for a specific domain. It aids in stating concepts of domain and their relations semantically. We can describe these concepts by using their attributes. The connections permit concepts to hold together. A usual connection between concepts is the relation, which tells that one concept. From the perspective of privacy, that content linked to privacy can be seen as a domain system and shown as an ontology technique.That the information given or represented was not given by the user.

The second set helps to recognize risky user's who are highly likely to violate privacy of anyone. While it is a very informative that when initial information is not therein the system, would not be an approachable way to work.

Table 1: Comparison chart of various research works on privacy violations and social networking sites

Author Name	Paper Title	Algorithm/Methods	Objective
M. X. Zhou, J. Nichols, T. Dignan, S. Lohr, J. Golbeck, and J. W. Pennebaker [6]	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 [7]	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 [8]	Preventing private information inference attacks on social networks	Naïve Bayes Clssification and Collective Interference Methods.	In this paper, use of inference attacks usingsocial networking data to predict private information and propose sanitization

ISSN: 2233-7857 IJFGCN

			techniques to prevent inference attacks.
C. G. Akcora, B. Carminati, and E. Ferrari [9]	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 [10]	A framework for computing the privacy scores of users in online social networks	In this IRT based computation of the PrivacyScoreandalsouse method to handled polytomous response matrices.	The paper proposes a modelto 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 [11]	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 et. al. [12]	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 Kafal, Akin Günay, Pınar Yolum [13]	Detecting and predicting privacy violations in online social networks	PROTOSS for detecting and predicting violations.	In this paper, we have developed protos, a runtime tool for detecting and predicting Privacy violations 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 [14]	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

ISSN: 2233-7857 IJFGCN

			captures the principals who learn a piece of information rather than who can directly access a piece of info.
Philip W. L. Fong [15]	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

4. EXISTING ALGORITHMS

Current system for privacy violation available on social networking sites is similar to the violations of access control. In access control scenarios, there is only one authority can permit access to users when they requires. Though , in social networking sites, there are numerous sources to control, i. e. Every user can give their contribution in sharing of the content by putting up posts and pictures of them or others. Furthermore, viewers of a post can re-share the content, makes it accessible to watch or interact for others. Though these interactions can sometimes leads to privacy violation, which is hard for the user to detect. Hence, taking away the important right from user's of knowing who are having access to their posts.

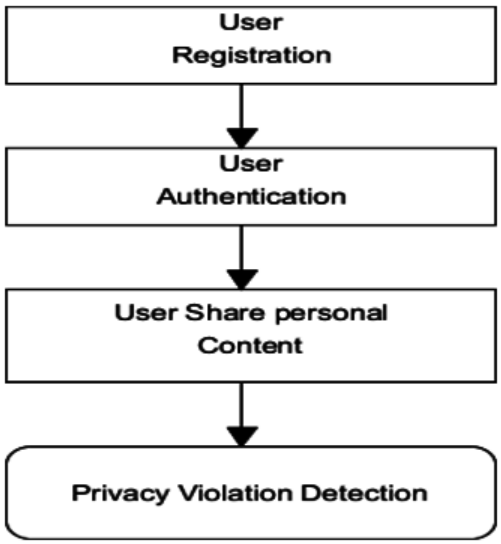

Figure 2: Existing Systems Architecture

5. REVIEW OUTCOME

After performing many surveys, it has become very clear that all around the world users are facing privacy violations and related concerns in their everyday life. Each and every work is done and handled easily by the first violation type as it is endogenous and direct. This is, this privacy constraint can be enforced if a user can tell that a privacy constraint is not related to any other or someone else's user's perspective.

6. CONCLUSION

In this paper we discussed about many different privacy related queries and issues and saw the approach to solve them. It includes privacy content, relationship between a user and the other content types, is collected with the help of using description logic to explain the social network

ISSN: 2233-7857 IJFGCN

domain and commitments that helps a user or helps the system to clear the privacy requirement of the user's itself.

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 incomputing systems. ACM, 2014, p. p. 1081 - 1086.

[7] J. Golbeck and D. Hansen, " A method for computing political preference among twitter followers, " Social Networks, vol. 36, p. p. 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, p. p. 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, p. p. 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, p. p. 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 "

ISSN: 2233-7857 IJFGCN