ISSN: 2455 - 9172

EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR)

Einstein International Journal Organization (EIJO)

Available Online at: www.eijo.in

Volume – 2, Issue – 3, May - June 2017, Page No. : 44 - 47

Privacy Violation in Online Social Network Using Agent Based Architecture

Grishma R. Pardeshi

Department of Computer Engineering JSPM Narhe Technical Campus, Narhe.

Rajarshi Shahu School of Engineering and Research Pune, Maharashtra, India.

E-Mail: Grp.pardeshi92@gmail.com

Rajesh H. Kulkarni

Department of Computer Engineering JSPM Narhe Technical Campus, Narhe.

Rajarshi Shahu School of Engineering and Research Pune, Maharashtra, India.

E-Mail: Rkpv2002@gmail.com

Abstract

In online social networks (OSNs), users are permit to create and Post content and information about themselves and others. When many entities start distributing content, information can get 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 state that agent-based representation of a social network in this agents manage users privacy related requirements and create privacy agreements with agents at time of entering. The privacy content, such as the relationship between users, many related 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. However, in online social networks, privacy violates are not necessarily a malfunctioning of a user's system but a byproduct of its workings. The users are allowed to create and share content or pictures about themselves and others. When multiple entities start interpreting content without a control, information can reach unrelated individuals and inference can reveal more information about the user private data. Accordingly, this paper first look to the privacy violations that take place in online social networks.

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

Introduction

Privacy is the right of an individual to express herself selectively. An individual may prefer to expose some information about herself to a other group of others, but may choose to hide another set of information. This right is difficult to maintain on the Web since information can propagate easily. It is even worse on online social networks since different users can share content about an individual, without expecting an explicit confirmation from the individual. This results in tremendous privacy violations to take place. Violation of Privacy: Misuses private information, such as passwords or social security numbers, can affect user privacy. Privacy violations occur when: Privacy violations occur when:

1. Private user information enters the program.

2. The data is written to an external location, such as the console Prompt, file system, or network. Private data can enter a program in a variety of ways

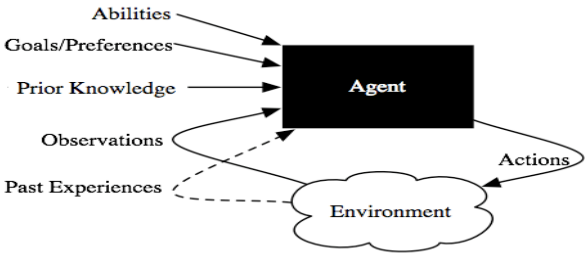

Figure 1: Agent Architecture

Violation of Privacy

Misuses private information, such as passwords or social security numbers, can affect user privacy. 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.

Problem Statement

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 information so that they can address the violation. In current online social networks, users are expected to observe how their shared content circulates in the system and manually find out if their privacy has been collapsed.

System Architecture

System aim to identify when the privacy of an individual will be broken based on a content that is shared in the online social network. The content or post that is shared by the user herself or by others, the content may change, including a images, a text message, a check-in information or even a declaration of users personal information. An agent based representation of social networks, where each user is represented by a software agent in system. And that agent keeps track of its user's privacy requirements that are mention, either by acquiring them explicitly from the user or learning them over time. The agent is then responsible for checking if these privacy requirements are being met by the online social network.

A. Architecture

This approach offers three distinct advantages. First, that scheme offers the embedding capacity that is corresponding to the size of the stego texture image. Second, a steganalytic algorithm is the not likely to the defeat our steganography approach. Third, the reversible capability inherited from our scheme to provide the functionality which allows to the recovery of the source texture.

B. Module Description

OSN Template: An ABSN model should conform to an OSN template. Here, we present an ABSN model that conforms to the following OSN template: teF B is an OSN template that represents a subset of Facebook. In this template, teF B.Rtype is the set of subroles of is Connected To and te F B. C type is the set of sub concepts of Content is an ABSN model that conforms to teF B template. Agents (A) are individuals of Agent concept.

Relationships (R): In a social network, agents are connected to one other via various relationships. Each agent labels his social network using a set of relationships. We use is Connected To method to describe relations between agents. This property only states that an agent is connected to another one. Posts (P): A social network consists of agents who interact with each other by sharing posts (sharesPost) and seeing posts (canSeePost).

C. Mathematical model

Module 1: conducts this idea by first checking for violation close to the user. The algorithm takes two inputs: a commitment C to be taken for check against violations and m the maximum number of iterations to run the algorithm for this m is set to maximum depth of the social network (MAX) as the default. The output is a set of privacy that are violated V. The agent should be knowledge of the domain and the norms that form the initial knowledge base KB.

Expected Result

An agent-based representation of social networks, where each user is represented by a software agent. Each agent keeps track of its users privacy requirements, either by acquiring them explicitly from the user or learning them over time. The agent is then responsible for checking if these privacy requirements are being met by the online social network. The goal is to detect when the privacy of a user will be violated based on a content that is shared in the online social network. The content that might be shared by the user herself or by others; the content may vary, including a picture, a text message, a check-in information or even a declaration of personal information. Whenever such a content is shared, it is meant to be seen by certain individuals; sometimes, a set of friends or sometimes, the entire social network.

Conclusion

With the proposed system presented a meta-model to describe online social networks as agent-based social networks to validate privacy requirements of users and their violations. To recognize privacy violations that occurs in realtime online social networks, conducted a survey with Facebook users and categorized the violations in terms of their causation.

Acknowledgment

I express true sense of gratitude towards my project guide Prof. R.H.Kulkarni, of computer department for his in valuable co-operation and guidance that he gave me throughout my research, for inspiring me and providing me all the lab facilities, which made this research work very convenient and easy. I would also like to express my appreciation and thanks to our HOD Prof. R.H.Kulkarni and Director Dr. A.B. Auti and all my friends who knowingly or unknowingly have assisted me throughout my hard work.

References

[1]. N. Kokciyan 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. Mc Carthy. Artificial intelligence, logic and formalizing common sense. InPhilosophicalLogicandArtificialIntelligence,pages161190.Springer, 1989.

[3]. M. P. Singh. An ontology for commitments in multiagent systems. Artificial Intelligence and Law, 7(1):97113

[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 319324. IEEE, 2003.

[5]. M. Horridge and S. Bechhofer. The OWL API: A Java API for OWL ontologies. Semantic Web, 2(1):1121, 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. 10811086

[7]. J. Golbeck and D. Hansen, A method for computing political preference among twitter followers, Social Networks, vol. 36, pp. 177184, 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. 18491862, 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. 810815.

[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. 6:16:30, 2010