International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

Detecting and Resolving Privacy Conflicts in Online Social Networks

Prof. Subhash V. Pingale[1], Sandip S. Shirgave[2]

[1] Professor in Department Of Computer Engineering, SKN Sinhgad College of Engineering, Korti, Pandharpur, India-413 304

[2] ME Student in Department Of Computer Engineering, SKN Sinhgad College of Engineering, Korti, Pandharpur, India-413 304

Abstract - ***We have seen lot of growth in online social networks (OSNs) in last few years. These online social networks are not only offer attractive means for virtual social interactions and information and resource sharing but also raise a number of security and privacy issue regarding particular to that shared data. Although online social networks allow a single user to govern access to his or her data, currently they do not provide any system or mechanism to provide privacy over data associated with multiple users. In this paper, we propose an approach to enable collaborative privacy management of shared data and resources in online social networks (OSNs).***

Key Words: *Social network, privacy, collaborative access, security.*

1. INTRODUCTION

Social networks are the sites where people can connect with each other, these people are each other's school friends, college friends co-workers in office and sometimes may be stranger's too. Social networking is used my many reasons some of them is given below.

Because of social networking sites many users are attracted to these social networking sites. With the help of these social networking sites peoples can connect with each other, sometimes they can share information and sometimes they can share private and public information with each other. With the help of social network peoples are connected with each from all over the world. There are many social networking sites are available on internet for example facebook, linked-in, twitter etc.

Online social networks (OSNs) are web based and they work as a client server architecture which is very common in web based services. Some of the online social networking sites are having premium account means where user need to pay money for surfing and checking the events on social networks.

The tremendous growth in the use of online social networks, (developed on web 2.0) such as linked-In, twitter, facebook, myspace and YouTube etc. If we see the internet usage report then it will shows the huge use of activities in social networking sites. These online social networking sites are developed on Web 2.0 technologies. Facebook claims that it having 1.44 billion monthly active users and 936 million daily active users. This means about 70 percent of Facebook's users use the service daily, and 65 percent of its mobile members use it daily on mobile phones. Twitter has 400 million monthly active users and around 500 million Tweets are sent per day, the study shown that 80% of Twitter active users are on mobile phones. Twitter supports 33 main languages; because of this it is easy to use for particular regions peoples. Twitter gives everyone the power to create and share ideas and information instantly, without barriers.

The main goal of online social network is communication between peoples, and makes available information which is published and shared by online users. The information may be anything (e.g. photos, videos, web-contents, and opinions about particular topic or event, contacts) and another purpose to meet other peoples for different kinds of reasons; it may be entertainment, business, and dating and religion occasion etc.

This type of available information creates privacy and confidentiality issues. Typically users do not want to share every information or contents with everyone. Today's online social network provide mechanism to protect the information shared in online space, it gives access control to the user for the distributed of their information or resources. Recent social networking sites provides user can control only own information or resources. It means currently online social networking sites (OSN) provide simple and easy access control technique permitting users to access to information obtained in their own profile.

Most of the recent online social networking sites only provide the basic access control policies for example user only can specify the policy that whether the information shall be publicly available, private or that information is only accessible by directly connected users.

We have seen tremendous growth in online social networks (OSNs) in recent years. These OSNs not only offer attractive means for virtual social interactions and

information sharing, but also raise a number of security and privacy issues.

2. RELATED WORK

a. Rule-Based Access Control for Social Networks (Barbara Carminati, Elena Ferrari, and Andrea Perego)

In this paper, author represented an access control model for web based online social networks, where policies are is in the terms of type, depth and trust level of relationship which is present between the online social network users.

The feature of this model is the use of certificate granting based on authenticity and client based access control which is rule based ,where subject is requesting to access an object must demonstrate that it has the rights of doing that.

b. A Reachability Based Access Control Model for Online Social Networks(Talel Abdessalem, Imen Ben Dhia)

In this paper, author developed an access control model for online social networks that enables a fine-grained description of privacy policies. These policies are specified in terms of constraints on the type, direction, depth of relationships and trust levels between users, as well as on the user's properties.

In this model author developed a model which relies on a reachability-based approach, where a subject requesting to access an object must satisfy policies determined by the object owner.

For developing the model author used the following algorithm for access control protocol.

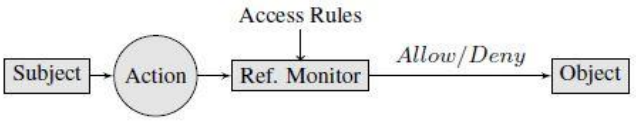
Algorithm 1: Access Control Protocol

Precondition: A requester R wants to get access to an object res of O.
Input : A requester R and an object identifier rid.
Output : $Allow$ or $Deny$ access.

Begin

```
1  ARS ← getRules(rid);
2  if ARS= ∅ then
3  |  ARS ← default access rule;
   else
4  foreach AR ∈ ARS do
5  |  foreach AC ∈ AR do                    // AC=(O, p, T)
6  |  |  if (p = *) then
7  |  |  |  if (T=*) then
8  |  |  |  |  return Allow;
   |  |  |  else
9  |  |  |  |  if (traverse(O, R, T) ≥ T.t_min) then
10 |  |  |  |  |  Allow;
   |  |  |  |  else
11 |  |  |  |  |  Deny;
   |  |  else
12 |  |  |  if (checkPath(O, R, p)) then
13 |  |  |  |  Allow;
   |  |  |  else
14 |  |  |  |  Skip to next AR;
15 return Deny;
   End
```

Author also used the Access control architecture which is shown below.



c. The Walls Have Ears: Optimize Sharing for Visibility and Privacy in Online Social Networks (Thang N. Dinh*, Yilin Shen*, and My T. Thai)

Author formulated the optimization problem, namely maximizing a circle of trust (MCT), of which author construct a circle of trust to maximize the expected visible friends such that the probability of information leakage is reduced to some degree. We have proven the inapproximability and provided a randomized algorithm with theoretical guarantees for the 2-MCT problem.

d. Identifying hidden social circles for advanced privacy configuration (Anna Squicciarini , Sushama Karumanchi , Dan Lin , Nicole DeSisto)

In this paper, author proposed an approach which helps online social users in managing their social network friend circle (contacts) into relevant groups automatically, and also helps online social users set up their privacy policies automatically for their uploaded content on the online users own wall or others wall. Organizing friend circle (contacts) into groups helps users set privacy settings for newly added content or new contacts joining their social circles.

3. CONCLUSION

In this paper we have seen different author's related work and their methodology; we have also seen the protection in the online social network.

ACKNOWLEDGEMENT

First and foremost, I would like to thank Prof. S. V. Pingale for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper. Finally, I sincerely thank to my parents, family, and friends, who provide the advice and financial support. The product of this review paper would not be possible without all of them.

REFERENCES

[1] P. Fong, M. Anwar, and Z. Zhao, "A Privacy Preservation Model for Facebook-Style Social Network Systems", Proc. 14th European Conf. Research in Computer Security, pp. 303-320, 2009.

[2] Jun Pang and Yang Zhang "A New Access Control Scheme for Facebook-style Social Networks", , arXiv:1304.2504v2 [cs.CR] 16 Dec 2013

[3] Thang N. Dinh, Yilin Shen, and My T. Thai. "The Walls Have Ears: Optimize Sharing for Visibility and Privacy in Online Social Networks" CIKM'12, October 29–November 2, 2012, Maui, HI, USA. Copyright 2012 ACM 978-1-4503-1156-4/12/10

[4] Karr-Wisniewski, Pamela; Wilson, D; and Richter-Lipford, "A New Social Order: Mechanisms for Social Network Site Boundary Regulation" (2011). AMCIS 2011 Proceedings - All Submissions. Paper 101.

[5] Victoria Kisekka , Sharmistha Bagchi-Sen , H. Raghav Rao. "Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users" 0747-5632/$ - see front matter _ 2013 Elsevier Ltd. http://dx.doi.org/10.1016/j.chb.2013.07.023

[6] Y. Cheng, J. Park, and R. Sandhu. " A user-to-user relationship-based access control model for online social networks ". In Proceedings of the 26th IFIP Annual WG 11.3 Conference on Data and Application Security and Privacy (DBSec '12), 2012.

[7] Mehmet Sahinoglua, Aysen Dener Akkayab, David Angc "Can We Assess and Monitor Privacy and Security Risk for Social Networks?", 2012. International Conference on Asia Pacific Business Innovation and Technology Management.

[8] Imen Ben Dhia "Access Control in Social Networks : A reachability-Based Approach", EDBT/ICDT Workshops March 26-30, 2012, Berlin, Germany. Copyright 2012 ACM 978-1-4503-1143-4/12/03.

[9] S.M.A. Abbas, J.A. Pouwelse, D.H.J. Epema, and H.J. Sips. A gossip-based distributed social networking system. In Enabling Technologies: Infrastructures for Collaborative Enterprises, 2009.WETICE '09. 18th IEEE International Workshops on, pages 93 {98, 29 2009-july 1 2009.

[10] Alessandro Acquisti and Ralph Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In Privacy Enhancing Technologies, pages 36{58, 2006.

[11] Alessandro Acquisti and Ralph Gross. Predicting social security numbers from public data. Proceedings of the National Academy of Sciences, 106 (27):10975{10980, 2009.

[12] Jonathan Anderson, Claudia Diaz, Joseph Bonneau, and Frank Stajano. Privacy-enabling social networking over untrusted networks. In Proceedings of the 2nd ACM workshop on Online social networks, WOSN '09, pages 1{6, New York, NY, USA, 2009. ACM.

[13] L. Backstrom, P. Boldi, M. Rosa, J. Ugander, and S. Vigna. Four degrees of separation. CoRR, abs/1111.4570, 2011.

[14] S. Benferhat, R. El Baida, and F. Cuppens. A stratification-based approach for handling conflicts in access control. In Proceedings of the eighth ACM symposium on Access control models and technologies, SACMAT '03, pages 189–195, New York, NY, USA, 2003. ACM.

[15] E. Bertino, S. Jajodia, and P. Samarati. Supporting multiple access control policies in database systems. ACM Transactions on Database Systems, 26:2001, 1996.

[16] E. Bertino, S. Jajodia, and P. Samarati. A flexible authorization mechanism for relational data management systems. ACM Trans. Inf. Syst., 17(2):101–140, Apr. 1999.

[17] E. Bertino, P. Samarati, and S. Jajodia. Authorizations in relational database management systems. In Proceedings of the 1st ACM confer-ence on Computer and communications security, CCS '93, pages 130– 139, New York, NY, USA, 1993. ACM.

[18] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thu-raisingham. A semantic web based framework for social network access control. In Proceedings of the 14th ACM symposium on Access control models and technologies, SACMAT '09, pages 177–186, New York, NY, USA, 2009. ACM.

Prof. Subhash V. Pingale is the professor of the department of Computer science and engineering in SKN Sinhgad College of Engineering, Korti, and Pandharpur, India. His main areas of interest are Social Networks and web mining and their applications.

Mr. Sandip Shirgave born in India, in 1988. He received the B.E. degree in Computer Science & Engineering from D.K.T.E College from Shivaji University, Ichalkaranji, India, in 2012, and pursuing the Master of Engineering degrees in Computer Science & Engineering from the SKN Sinhgad College of Engineering, Korti, and Pandharpur India. His main areas of interest are Social Networks and web mining and their Applications.