ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 5, MAY 2015, PP 293-295

New Access Control Methodology for Online Social Network

Sandip Sharad Shirgave, Prof. S. V. Pingale, Prof. A. A. Rajguru, Prof. N. M. Sawant

Abstract— A social networking sites are a platform to build social networks or social relations within people who share interests, activities, backgrounds or real-life connections with each other. A social network service mostly consists of a representation of each user like a profile, his or her social links, and a variety of additional services. Social network sites are web-based services that allow individuals to create a public profile, to create a list of users with whom to share connections, and view and cross the connections within the system.Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging.But present social networking sites can not provide mechanism for restricting the information associated with multiple users. This paper shows different methods used by different authors.

Index Terms— Social network, security, privacy, methodology.

1 INTRODUCTION

The Online social networks are the most popular web services during several years and have attracted a large amount of online users all over the world.For example, Facebook, the leading social network service, has more than one billion active users. With the large amount of data maintained in social network websites, privacy concerning user's personal information becomes an important but technically challenging problem. Access control schemes are naturally introduced to protect online user's privacy in social networks. They can be used to guarantee that information are accessible by multiple users, but not by other users. The availability of this information obviously raises privacy and confidentiality issues. Users typically do not want to share all of their information with everyone.

Consequently, Online Social Networks must provide the right mechanisms in order to give users more control on distribution of their information, which may be accessed by a multiple users far wider than they expected. Todays social networking sites provide only the most basic access control policies, e.g. a user can specify whether a particular of information shall be publicly available, private (no one can see it) or accessible only by direct user. This simple access control mechanism has the advantage of being simple, intuitive and easy to implement. However, it is not flexible enough to fit with the requirements of all users. It is either too loose because it grants access to all users (public), or it is too restrictive by limiting too much information sharing (private). Thus, social networking applications need mechanisms that support high-

Level complicated access control policies.

If a online user posts a comment in a friend's space, she/he cannot specify which online users can view the comment or photo or video or weblink. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo. Since multiple associated users may have different privacy concerns over the shared data, privacy conflicts occur and the lack of collaborative privacy control increases the potential risk in leaking sensitive information by friends to the public.

2. PRIVACY CONFLICTS IN ONLINE SOCIAL NETWORKS

Users in OSNs can post statuses and notes, upload photos and Videos in their own spaces, tag others to their content, and share the content with their friends. On the other hand, users can also post content in their friends' spaces. The shared content may be connected with multiple users.

A privacy policy conflict occurs when more than two users co-own an identical piece of information or data, and both of them are capable of configuring their own publication settings in-dividually. Multiple associated users may have different privacy concerns over the shared content, privacy conflicts can occur among the multiple users.

3 PROBLEM STATEMENT

To enable the protection of shared data associated with multiple users in OSNs with the help of access control mechanism.

- *Sandip Sharad Shirgave is currently pursuing master's degree program in computer science & engineering in SKN Sinhgad College Of Engineering, Korti, Solapur University, India, PH-09850004107. E-mail: sandipshirgave@gmail.com*
- *Prof.S. V. Pingale is currently working as a professor in SKN Sinhgad College Of Engineering,Korti,Solapur University, India, E-mail: sub.pingale83@gmail.com*
- *Prof. A. A. Rajguru is currently working as a Head Of Computer Deaprtment in SKN Sinhgad College Of Engineering,Korti,Solapur University, India, E-mail: abhijitcse08@gmail.com*
- *Prof. N. M. Sawant is currently working as a professor in SKN Sinhgad College Of Engineering,Korti,Solapur University, India*

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 5, MAY 2015, PP 293-295

4 LITERATURE REVIEW

Author Name	B.Carminati,E.Ferrari,A.Perego
Paper Name	Rule-Based Access Control for Social Networks
Method Used	Rule Based
Advantage	Certificates for granting Relationships and Authenticity
Disadvantage	1) The support for topical trust. 2) The usage of access rules also for certificate protection.
Application	Facebook

Author Name	Yuan Cheng, Jaehong Park and Ravi Sandhu
Paper Name	Relationship based Access Control for Online Social Networks: Beyond User-to-User Relationships
Method Used	Relationship Based
Advantage	1)On the basis of user and users resource Relationship.
Disadvantage	1)We cant use Attribute
Application	Facebook

Author Name	Anna Squicciarini, Susha Karumanchi, Dan Lin, Nicole De-Sisto
Paper Name	Identifying hidden social circles for advanced privacy configuration
Method Used	Circle Grouping
Advantage	1)Easy to implement on the basis of friends , College us, coworkers.
Disadvantage	1)For the multiple users it is not possible
Application	Facebook,Google+

Author Name	Talel Abdessalem, Imen Ben Dhia
Paper Name	A Reachability Based Access Control Model for Online Social Networks
Method Used	Trust and depth level
Advantage	1) Reachability based approach, where a subject requesting to access an object must satisfy policies determined by the object owner.
Disadvantage	1) There are no automatic access policies.
Application	Facebook

Author Name	P. Fong,M. Anwar, and Z. Zhao
Paper Name	A privacy preservation model for facebookstyle social network systems.
Method Used	Privacy setting in the history
Advantage	1) Easy to implement on the basis of history.
Disadvantage	1) For the multiple users it is not possible.
Application	Facebook.

Author Name	F. Paci
Paper Name	Collective privacy management in social networks
Method Used	Access control policies of a content that is coowned by multiple users.
Advantage	1) Useful for multi-users at the same time.
Disadvantage	1)It is hard to implement when coowned Users having different privacy preference.
Application	Google plus, Google Circle

5 MULTIPARTY ACCESS CONTROL MECHANISM FOR ONLINE SOCIAL NETWORKS TERMS

5.1 Profile Sharing:

In the profile sharing term social networking site shares the user's information like birthday, activities, Interests and so on.With the help of this term social networking sites shares the user's information with other users or with other applications.

5.2 Relationship Sharing:

In this term social networking site shares the user's relationship status with another user or with another application.

5.3 Content Sharing:

In this term online social network mechanism provides mechanisms enabling users to communicate and share contents with other members. users can post statuses and notes,upload photos and videos in their own spaces, tag others to their contents, and share the contents with their friends. On the other hand, users can also post contents in their friends' spaces. The shared contents may be connected with multiple users.

6 MULTIPARTY POLICY EVALUATION

In the multiparty policy evaluation policy is checked for each users.Sometimes contents may be associated with single users and sometimes with multiple users.In this policy evaluation each user specify his/her own privacy regarding the data or content, sometimes he/she permit the data to show with public and sometimes he/she deny to show the data with public.He/she post or shares the data/contents with public or in private.

In the multiparty policy evaluation process decisions are also made with the help of permit and deny.

7 USER AUTHORISATIONS IN DISTRIBUTED ENVIRONMENT

Require: userName ≠ null and password ≠ null
Ensure: authresult € {true, false}

AuthD «= perform local authentication
If authD ≠ true then
If userServer ≠ null then
AuthD «=authenticate directly on user's server
End if
If authD ≠ true then
ResultT able «=perform query in network
For elem € resultT able do
If elem [result] = true then
AuthD = true
End if
End for
End if
End if
Return authD

8. OSN REQUIREMENTS

Confidentiality

Any kind of content created by any aaplication should be accessible only to those authorized to have access fully-customizable confidentiality is the most effective patch to stop information leakage.

Ownership privacy

The owner of content should be enabled to not disclose the ownership information to other users.

Social interactions privacy

Social tiesandthe dataflowingon themcan tell much information on the behavior of individuals and onthe dynamics of groups in a networked environment.

9 .CONCLUSION

In this paper, we first identified a new type of access control policies that are meaningful but have never been addressed in the literature. Namely, users in social networks can express access control requirements not only based on their social relations, but also on their connections through public information. Then we defined a social network model containing users and public information.

ACKNOWLEDGMENT

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.Second, I would like to thank Prof. A. A. Rajguru and Prof. N. M. Sawant to read my review paper and to provide valuable advices. 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] S. Kruk, S. Grzonkowski, A. Gzella, T.Woroniecki, and H. Choi.D-FOAF: Dis- tributed identity management with access rights delegation". The Se- mantic WebASWC 2006, pages 140154, 2006

[2] "Multiparty Access Control for Online Social Networks: Model and Mecha- nisms" Hongxin Hu, Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Jan Jorgensen.IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 7, JULY 2013

[3] Fong, P.W.L., Siahaan, I.: Relationship-based access control policies and their policy languages. In: Proc. 16th ACM Symposium on Access Control Models and Technologies (SACMAT), ACM (2011) 51-60

[4] Cheng, Y., Park, J., Sandhu, R.S.: Relationship-based access control for online social networks: beyond user-to-user relationships. In: Proc. 4th IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT), IEEE CS (2012) 646-655.

[5] Carminati, B., Ferrari, E.: Enforcing relationships privacy through collaborative access control in web-based social networks. In: Proc. 5th International Conference on Collaborative Computing (CollaborateCom), IEEE CS (2009) 1-8

[6] S. Kruk, S. Grzonkowski, A. Gzella, T.Woroniecki, and H. Choi.D-FOAF: Distributed identity management with access rights delegation". The Se- mantic WebASWC 2006, pages 140154, 2006

[7] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 17341744. Springer, 2006

[8] P. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for facebookstyle social network systems. In Proceedings of the 14th Euro- pean conference on Research in computer security, pages 303320. Springer- Verlag, 2009.

[9] E. Carrie. Access Control Requirements forWeb 2.0 Security and Privacy. In Proc. of Workshop on Web 2.0 Security and Privacy (W2SP). Citeseer, 2007.

[10] F. Paci. Collective privacy management in social networks. In Proceedings of the 18th international conference on World wide web, pages 521530. ACM,2009.