Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multiparty Frame work Access Control in Online Social Network

B. Durga Sri[1], R. V. Sudhakar[2], Sirisha N[3], P. Suman Kumar[4]
[1, 3] Dept of Computer Science & Engineering in **MLR Institute of Technology**, R.R Dist, Telengana, India
[2] Dept of Computer Science & Engineering in **St.Martin's Engineering College**, R.R Dist, Telengana, India
[4] Dept of Computer Science & Engineering in **MTIET**, Palamaner, Chittoor, AP, India

Abstract: In this paper Online Social Networks offers attractive interactions and information sharing, and also will raise a number of security and privacy issues. In recent years we have been watching a tremendous increase in the growth of online social networks (OSNs). OSNs enable people to share personal and public information and make social connections with friends, family members and other peoples. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to totally enforce privacy issue solver associated with multiple users. The proposed method implements a solution you facilitate collaborative management of common data item in OSNs. Each controller of the data item can set his privacy settings to the shared data item. A logical representation of access control model which allows us to leverage the features of existing logic solvers to perform various analysis tasks on this model. A proof-of-concept prototype has also been implemented as part of an application in Face book and provide usability study and system evaluation of this project. We begin by investigate how the lack of multiparty access control for data sharing in OSNs can undermine the protection of user data.

Key Terms: multiparty access control, security model, policy specification and management, multiparty policy specification scheme, a policy enforcement mechanism, Multiparty Access Control (MPAC).

I. INTRODUCTION

In recent years we have been watching a tremendous increase in the growth of online social networks (OSNs).OSNs enable people to share personal and public information and make social connections with friends, family members and other peoples. In addition to the rapid increase in the use of social network, it raises a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to totally enforce privacy issue solver associated with multiple users. The proposed method implements a solution to facilitate collaborative management of common data item in OSNs. Each controller of the data item can set his privacy settings to the shared data item. The proposed method also identifies privacy conflicting segments and helps in resolving the privacy conflicts and a final decision is made whether or not to provide access to the shared data item. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of 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 associate with multiple users. To this end, we propose an approach to enable the protection of shared data associated with multiple users in OSNs. We formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model which allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof-of-concept prototype of our approach as part of an application in Facebook and provide usability study and system evaluation of our method.

Online social networks (OSNs) such as Facebook, Twitter, and Google+ are inherently designed to enable people to share personal and public information and make social connections with co-workers, family, friends, colleagues, and even with strangers. In Facebook users can allow groups, friends, and friends of friends or public to right to use their data, depending on their personal authorization and privacy requirements. Although Online social networks presently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no power over data residing outside their spaces. Such as, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment.

II. RELEATED WORK

MPAC model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs. In this model multiparty policy specification scheme is used.

Existing System:

OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no power over data residing outside their spaces. Such as, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment. In another case, while a user uploads tags and the photograph friends who appear in the photograph, the tagged friends cannot restrict who can see this photograph, even though the tagged friends may have different privacy concerns about the photo. To address such a serious issue, beginning protection mechanisms have been offered by existing online social networks (OSNs).

1. Access to a resource is granted while the requestor is able to demonstrate of being authorized.
2. Every user in the group can access the shared content.
3. Not give any mechanism to enforce privacy concerns over data associated with multiple users
4. if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment
5. While a user uploads a photo and tags friends who appear in the photograph, the tagged friends cannot restrict who can see this photograph.

Proposed System:

Our solution is to support the analysis of multiparty access control model and mechanism systems. The correctness of execution of an access control model is based on the premise that the access control model is suitable. Moreover, while the use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in Online social networks (OSNs), it may potentially reduce the certainty of system authorization consequences due to the reason that authorization and privacy conflicts need to be resolved elegantly. We specially analyze the scenario like content sharing to understand the risks posted by the lack of collaborative control in online social networks (OSNs).

Proposed System Advantages

1. It checks the access request against the policy specified for every user and yields a decision for the access.
2. The use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in online social networks.
3. Present any mechanism to enforce privacy concerns over data associated with many users
4. If a user posts a comment in a friend's space, he/she can specify which users can view the comment.

In this paper, a formal model is used for addressing the multiparty access control issue in OSNs, along with policy specification scheme and flexible conflict resolution mechanism for collaborative management of shared data in OSNs. Proposed work can also conduct various analysis tasks on access control mechanisms used in OSNs, which is not addressed by prior work. Users upload the photo in their own space and tags to their friends, and the owner of the photo will be the uploaded person, and stakeholders of the photo will be the tagged members. All users can specify access control policies to control over the photo and can see the photo. OSNs also enable users to share others' contents. To view a photo in friend's space and decide to share that photo with our friends, the photo will be in turn posted in their space and can specify access control policy to authorized friends to see that photo. In such cases, the person is a disseminator who shared their friend's photo.

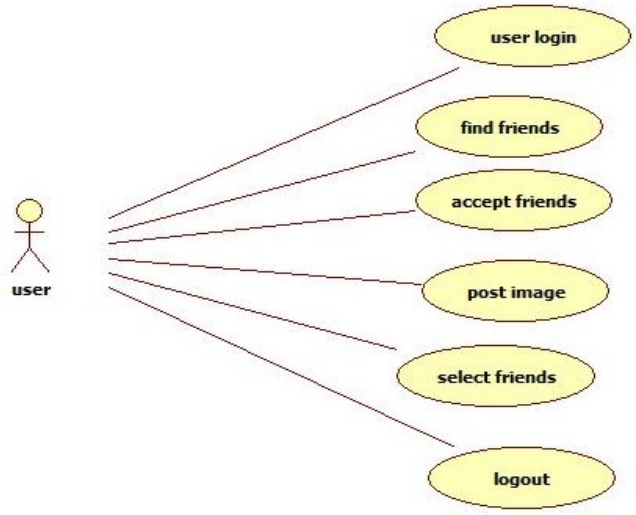

Fig: Use case diagram for User

A use case diagram is a graph of actors, a set of use cases enclosed by a system boundary, communication (participation) association between the actors and the use cases, and generalization among the use cases. A use case diagram is a type of behavioural diagram created from a Use-case analysis. The purpose of use case is to present overview of the functionality provided by the system in terms of actors, their goals and any dependencies between those use cases.

User has to sign up his account, if he has no account before. After signing up user can login to the account. A separate profile will be displayed for him. User can add friends. User can search friends after that he can add friends into his account. User can view friends profile and user can send friend request to his friend. In case if user wants to upload his image on his wall, he can upload the image by browsing it and he can upload the image. After uploading it, the image will be displayed on the wall.

III. WEB ACCESS CONTROL POLICIES

Representing and Reasoning:

We propose a systematic method to represent XACML policies in answer set programming (ASP), a declarative programming paradigm oriented towards combinatorial search problems and knowledge intensive applications. Compared to a few existing approaches to formalizing XACML policies. Our formal representation is more straightforward and can cover more XACML features. Furthermore, translating XACML to ASP allows us to leverage off-the-shelf ASP solvers for a variety of analysis services such as policy verification, comparison and querying. In addition, in order to support reasoning about role-based authorization constraints, we introduce a general specification scheme for RBAC constraints along with a policy analysis framework, which facilitates the analysis of constraint violations in XACML-based RBAC policies. The expressivity of ASP, such as ability to handle default reasoning and represent transitive closure, helps manage XACML and RBAC constraints that cannot be handled in other logic-based approaches . We also overview our tool XACML2ASP and conduct experiments with real-world XACML policies to evaluate the effectiveness and efficient of our solution.

Requirements for Web 2.0 Security and Privacy:

The increased social networking capabilities provided by Web 2.0 technologies requires a examination of what we consider "private" and what we consider "personal" information, and will consequently drive a new way of limiting and monitoring the information that we make public online. Web 2.0 applications are creating large, composite conglomerations of personal data and so we need new approaches to describe and execute access organize on that data.
"Private" information at present tends to be insecurely defined by legislation, rather than by what individuals consider to be personal. Generic information such as a person's home address and phone number are normally considered personally identical information (PII) and are to be protected when collected and stored by an organization in addition, the use and release of exact data, such as medical or financial information, is restricted legislatively. However, It also exists information that an individual may consider to be personal, and want to let loose only to people meeting particular criteria (such as people attending the same school) or particular people (such as close friends). Thus someone might want to control portions of their digital life in the same manner that they control what information is released in their analog life. In the world, a person can choose to tell someone or some group some piece of information about themselves. On the other hand, it is often the case that in the online world these controls do not exist, most important to de facto public disclosure.
Protection model and policy language:

Social Network Systems pioneer a paradigm of access control that is distinct from traditional approaches to access control. The Gates coined the term Relationship-Based Access Control (ReBAC) to refer to this paradigm. Relationship-Based Access Control is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships. This work explores what it takes to widen the applicability of Relationship-Based Access Control to application domains other than social computing. We prepare an archetypical Relationship-Based Access Control model to capture the essence of the standard, that is, authorization decisions are based on the relationship between the resource owner and the resource access or in a social network maintained by the security system. A novelty of the model is that it captures the contextual nature of associations. We work out a policy language, based on modal logic, for composing access control policies that support delegation of trust. We use a case study in the domain of Electronic Health Records to demonstrate the utility of our model and its policy language. This provides initial evidence to the feasibility and utility of Relationship-Based Access Control as a general-purpose paradigm of access control.

Multiparty Authorization Framework for Data Sharing and An Active Detection of Identity Clone Attacks:

We propose a multiparty authorization framework (MAF) to model and realize multiparty access control in online social networks. We begin by examining how the lack of multiparty access control for data sharing in online social networks can undermine the security of user data. A multiparty authorization model is then formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems and models for online social networks. In Meanwhile, as conflicts are inevitable in multiparty authorization specification and enforcement, systematic conflict resolution mechanism is also addressed to cope with authorization and privacy conflicts in our framework. We first examine and characterize the behaviours of ICAs. Then we propose a detection framework that is focused on discovering suspicious identities and then validating them. Towards detecting suspicious identities, we propose two approaches based on attribute similarity and similarity of friend networks. The first approach addresses a simpler scenario where mutual friends in friend networks are considered; and the second one captures the scenario where similar friend identities are concerned. We also current experimental results to demonstrate flexibility and effectiveness of the proposed approaches. Finally, some feasible solutions to validate suspicious identities.

IV. SCREENSHOTS

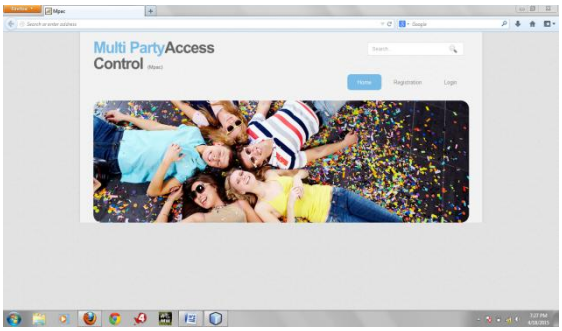

Fig: Home page

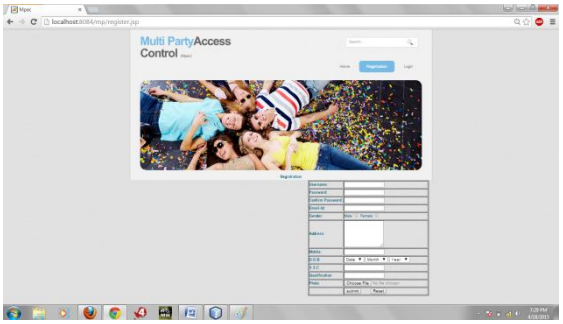

Fig: Registration

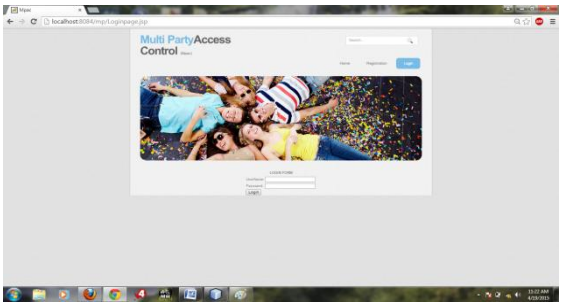

Fig: Login

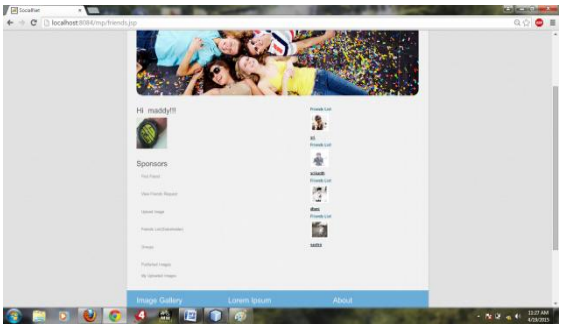

Fig: Finding friends

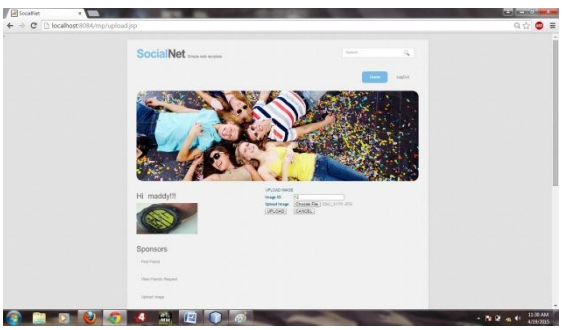

Fig: Uploading images

V. CONCLUSION & FUTURE ENHANCEMENT

We have proposed a technique of secured sharing of any data object .In this project we used images as a main data object. We hope that our work will increase the privacy settings of a website. This allows access control and prevents unauthorized sharing. In our multiparty access control system for model and mechanism, a group of users could collude with one another so as to manipulate the final access control decision. An attack scenario, anywhere a set of malicious users may want to make a shared photo available to a wider audience. Suppose they can access the photo, and then they all tag themselves or fake their identities to the photo. In addition, they collude with each other to assign a very low sensitivity level for the photo and specify policies to grant a wider audience to access the photo with a large number of colluding users, the photo may be disclosed to those users who are not expected to gain the access. To prevent such an attack scenario from occurring, three conditions need to be satisfied:

(1) There is no fake identity in OSNs;
(2) All tagged users are real users appeared in the photo;
(3) All controllers of the photo are honest to specify their privacy preferences.

Future Enhancement:

Many applications can be developed using this concept. OSNs enable people to share personal and public information and make social connections with friends, family members and other peoples. Online social networks can be developed based on this theory. We define security to the application where the data which is being shared by the owner in the wall of the friends profile is restricted to share in his wall based on the sharing policy defined by the owner.

REFERENCES

[1] G. Ahn, H. Hu, J. Lee, and Y. Meng. Representing and reasoning about web access control policies. In Computer Software and Applications Conference (COMPSAC), 2010 IEEE 34th Annual, pages 137–146. IEEE, 2010.

[2] E. Carrie. Access Control Requirements for Web 2.0 Security and Privacy. In Proc. Of Workshop on Web 2.0 Security & Privacy (W2SP). Citeseer, 2007.

[3] J. Choi, W. De Neve, K. Plataniotis, and Y. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011.

[4] P. Fong. Relationship-based access control: Protection model and policy language. In Proceedings of the first ACM conference on Data and application security and privacy, pages 191–202. ACM, 2011.

[5] J. Golbeck. Computing and applying trust in web-based social networks. Ph.D. thesis, University of Maryland at College Park College Park, MD, USA. 2005.

[6] H. Hu and G. Ahn. Multiparty authorization framework for data sharing in online social networks. In Proceedings of the 25th annual IFIP WG 11.3 conference on Data and applications security and privacy, pages 29–43. Springer-Verlag, 2011.

[7] H. Hu, G. Ahn, and K. Kulkarni. Anomaly discovery and resolution in web access control policies. In Proceedings of the 16th ACM symposium on Access control models and technologies, pages 165– 174. ACM, 2011.

[8] B. Viswanath, A. Post, K. Gummadi, and A. Mislove. An analysis of social network- based sybil defenses. In ACM SIGCOMM Computer Communication Review, volume 40, pages 363–374. ACM, 2010.

[9] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. A practical attack to de-anonymize social network users. In 2010 IEEE Symposium on Security and Privacy, pages 223–238. IEEE, 2010.

[10] E. Zheleva and L. Getoor. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In Proceedings of the 18th international conference on World wide web, pages 531–540. ACM, 2009.

[11] P. Fong, "Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems," Proc. IEEE Symp. Security and Privacy (SP), pp. 263-278, 2011.

[12] P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 191-202, 2011.

[13] 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.

[14] J. Golbeck, "Computing and Applying Trust in Web-Based Social Networks," PhD thesis, Univ. of Maryland at College Park, College Park, MD, USA, 2005.

[15] M. Harrison, W. Ruzzo, and J. Ullman, "Protection in Operating Systems," Comm. ACM, vol. 19, no. 8, pp. 461-471, 1976.

[16] H. Hu and G. Ahn, "Enabling Verification and Conformance Testing for Access Control Model," Proc. 13th ACM Symp.Access Control Models and Technologies, pp. 195-204, 2008.

AUTHOR'S PROFILE

Mrs. B. Durga Sri Post Graduated in Computer Science & Technology (M. Tech), Andhra University, Vishakapatnam in 2010 and Graduated in Information Technology (B. Tech) from JNTU Hyderabad in 2008. She is working as an Assistant Professor in Department of Computer Science & Engineering in **MLR Institute of Technology**, R.R Dist, Telangana, and India. She has 5+ years of Teaching Experience. Her Research Interests Include Computer Networks, Network Security, Data Warehousing and Data Mining.

Mr Rayapati Venkata Sudhakar register Ph.D in JNTUH in 2012 on cloud computing, Post Graduated in Computer Science & Engineering (M.Tech), JNTUH , 2008, and graduated in Information Technology (B.Tech) From JNTU Hyderabad, 2005. He is working presently as Associate Professor in Department of Computer Science & Engineering in **St. Martin's Engineering College**, RR Dist, and Telangana , INDIA. He has 6+ years Experience. His Research Interests Include Software Engineering & Cloud Computing.

Mrs. Sirisha N, Post Graduated in Software Engineering (M. Tech), JNTU Hyderabad, in 2012 and Graduated in Computer Science & Engineering (B.Tech) from JNTU Hyderabad in 2009. She is working as an Assistant Professor in Department of Computer Science & Engineering in **MLR Institute of Technology**, R.R Dist, Telangana, and India. She has 3+ years of Teaching Experience. Her Research Interests Include Computer Networks and Network Security.

Mr. P. Suman Kumar , Post Graduated in Computer Science & Engineering (M.Tech) from JNTUA, Anantapuramu in 2009 and M.Sc in Mathematics in 2007 and B.Sc in MECs in 2005 in SVU, Tirupathi. He is working as an Associate Professor of Computer Science & Engineering in Mother Theresa Institute Of Engineering & Technology, Palamaner. He has 8+ years of Teaching Experience. His Research Interests Include Network Security, Cloud Computing & Data Warehousing and Data Mining.

