International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Multiparty Protection Mechanism for Online Social Networks

T. Adlin Brainy,
Department of Computer Science,
Ponjesly College of engineering,
Nagercoil, 629004,India.

V. Angel Gnana Shiny,
Department of Computer Science,
Bharath University,
Selaiyur, Chennai 600073, India.

***Abstract*- Online Social Network has to designed an enable person to share their personal and public information and make a social connection with friends, co-workers, even families etc. So increase the number of security level and privacy issues. Currently do not provide any access control mechanism to users to access information. But a simple access control mechanisms are used to access information it only support single controller. Unfortunately there have no control over data residing outside their space. In proposed using a flexible access control mechanism for online social networks to support multiple controller in multiuser environment. The use of MPAC mechanism is to support a user for sharing data in online social networks. It makes a protection of shared data associated with multiple users in online social networks.**

Keywords: Online social Networks, Access control mechanism, Social network, Multiparty access control, Policy specification.

I. INTRODUCTION

A Network of social interactions and personal relationships with other. A dedicated website or other application which enable user to communicate with each other by posting information, messages, political orientation etc. Online social networks are a representation of each user and a variety of additional services. OSN allow a user to share their ideas, activities, events and interests with their individual networks. In Online social network contain several access control mechanism used. Hardware or software features, operating procedures, management procedures and various combinations of these designed to detect and prevent unauthorized access and permit authorized access in an automated system. Online social network variety of sensitive data should be shared. So increase a number of security and privacy issues. Currently several access control mechanism used to support single controller [1], [2]. In a social network the access control mechanisms are

Discretionary access control: If an individual user can set an access control mechanism to allow or deny access to an object, that mechanism is as discretionary access control or identity based access control. Discretionary access control is a type of access control defined by the Trusted Computer System Evaluation Criteria as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense of passing that permission on to any other subject.

Mandatory access control: When a system controls access to an object and an individual user cannot alter that access control, that mechanism called Mandatory access control or Rule-based access control [2]. The term mandatory in MAC has acquired a special meaning derived from its use with military systems. MAC means access controls that are mandated by order of a government and so enforcement is supposed to be more imperative than for commercial applications. This precludes enforcement by best-effort mechanisms, only mechanisms that can provide absolute, or near-absolute enforcement of the mandate are acceptable for MAC.

In some systems, users have the authority to decide whether to grant access to any other user. It is allowed that all users have clearances for all data. This is not necessarily true of a MAC system. If individuals or processes exist that may be denied access to any of the data in the system environment, then the system must be trusted to enforce MAC. Since there can be various levels of data classification and user clearances, this implies a quantified scale for robustness.

Originator controlled access control: It is a bases access on creator of an object or the information it contains. ORCON is a decentralized system of access control in which each originator determines who needs access to the data. No centralized set of rules controls access to data; access is at the complete discretion of the originator. A solution is to combine features of the MAC and DAC models. The rules are

- The owner of an object cannot change the access controls of the object.
- When an object is copied, the access control restrictions of that source are copied and bound to the target of the copy.
- The creator (originator) can alter the access control restrictions on a per-subject and per-object basis.

Although currently OSNs provide simple access control mechanism allowing user to access information in their own spaces, unfortunately there is no control over outside residing data. Access to a resource is granted while the requester is able to demonstrate of being authorized. Every user in a group can access a shared content. Not any mechanism to provide privacy associated with multiple

users. For illustration when a user uploads a photo he cannot specify which user can view a photo. In a OSNs like facebook allow user to tagged a photo may have different privacy concerns. However, these simple access control mechanism have several limitations occur. Hence, used a multiparty protection mechanism for online social networks, it support multiple controller in multiuser environment. It checks the access request against the policy specified for every user and yields a decision for the access. Use of MPAC mechanism, it is flexible for regulating data sharing in OSN. Prevent any mechanism to enforce privacy concerns over data associated with many users. For instance, when a user uploads a photo he can specify which user can view the photo.

II. MPAC FOR OSNs

Profile sharing: It support a feature for social applications written by an external party developer to build some functionality for user profiles. Profile sharing is to share profile information to others. You can choose what you share on your network profile using your profile settings. You can pick who sees your information, as well as what information people can see [11].

Relationship sharing: A set of users to share their relationship to another. User can share their relationship like friends, colleges, group etc.

Content sharing: Provide mechanism a user can communicate and share their content to other users. If you have content on your website you should strongly encourage people to share it. This means providing social sharing plugging that stand out on the page. It also means doing some sharing yourself immediately when you have a new piece of content. Your visitors like social proof so when they see content is shared already they are more likely to share.
A group of users could collide with one another so as to manipulate a final access control decision. There is no fake identity of online social networks.

III. MPAC MODEL

MPAC for online social network is a relationship network, a set of user group, collection of user data. A relationship network is represented by directed labeled graph, each node in a graph denoted by users and each edge denoted by relationship. A label associated with each edge represented by type of relationship. In a directed labeled graph initial node establish an access request and terminal node access the request. In OSNs users are organized in to groups, each group have unique name. Users in OSNs can easily identify the other users for sharing demographic groups, political orientation, relationship etc. OSNs can provide each user web space for store and manage their profile information, relationship and content. Recently many access control mechanisms used for fine grained data sharing in OSN, but it only support a single controller. Currently a flexible access control mechanisms are used to support multiple controller in multi user environment. The multiple controllers are owner, contributor, stakeholder, and disseminator.

Owner: Let a data item in the space of a user u in social network. The user u is called owner of the data item.

Contributor: Let a data item can be published by a user u in someone else space in the social network. The user u is called contributor of data item. The memory space for the user be allotted according to user request for content sharing.

Stakeholder: Let a data item in the space of a user u in social network. Let T be a set of tagged users who can tag their data item. The user u is called stakeholder of data item.

Disseminator: Let a data item can be shared by a user u from someone else space to his/her space in social network. The user u is called disseminator of data item. Effective access control mechanisms should be applied in each procedure to regulate sharing behaviors.

IV. ONLINE SOCIAL NETWORK POLICY EVALUATION

Two steps for checking access request in online social network policy specification. The first step to check the access request against the policy specified by the controller and makes a decision for the controller. If the policy is applicable, the evaluation process returns a decision to make permit to access an object. If the policy is not applicable, the evaluation process returns a decision to deny access an object. The second step to make a decision from all the controllers and aggregated to make a final access control decision. The data controller can make a conflicts occur. To resolve the conflict using conflicts resolution mechanism.

Privacy conflicts: The multiple controllers in shared data item that data item have different privacy preferences. Privacy conflicts may occur in multiparty control over shared data item.

Naive solution: The naive solution is used for resolving multiparty privacy conflicts for sharing data item. It can share a data in common users in accessor set defining multiple controllers to access data item. Unfortunately it is too restrictive in many cases and does not produce a desirable result.

Strong conflict resolution: Strong conflicts resolution make a better privacy protection for shared data item. Also it can reduce social vale for data sharing.

V. PRIVACY CONFLICT IDENTIFICATION AND RESOLUTION

In these mechanism used for privacy conflict identification and resolution, in privacy conflict identification first introduce a space segmentation approach to partition the accessor space. Then identify the conflicting segments then

get all the controllers associated with a segment s. Accessor space can be in two categories: non conflicting segment and conflicting segment. Non-conflicting segment covers all controllers' accessor space and indicating no privacy conflict occurs. A conflicting segment does not contain all controllers' access spaces within the segment are untreated by some controllers. The resolution of privacy conflict makes a decision for allow or deny the accessors within the conflicting segment to access an object. To access the data item may cause privacy risks, but denying a set of accessors in this segment to access data item may result in sharing loss. This privacy conflict resolution approach attempts to find optimal trade-off between privacy protection and data sharing. Using strong conflict resolution mechanism may provide better privacy protection for sharing data. In this mechanism based on voting scheme for resolving multiparty privacy conflicts in OSNs.

VI. DECISION MAKING BASED ON VOTING SCHEME

In a voting scheme mechanism contains two voting mechanisms: decision voting and sensitivity voting.

A. Decision Voting

A decision voting value (DV) derived from policy evaluation is defined as follows; the evaluation of policy is deny means the decision voting value is zero. Otherwise the evaluation of policy is permit means the decision voting value is one. Then find the aggregated decision voting value, the sum of decision voting value for owner, contributor and stakeholder is divided by the number of controllers.

B. Sensitivity Voting

Each controller assigns a sensitivity level (SL) for sharing data then calculates the sensitivity score for based on sensitivity level. The sensitivity score can be calculated as, the sum of sensitivity level for owner, contributor and stakeholder divided by the number of controller.

VII. CONFLICT RESOLUTION FOR THRESHOLD APPROACH

After finding the sensitivity score the calculate threshold for decision making, if the sensitivity score is higher, the decision to make a privacy protection of high sensitive data. Also if the sensitivity score is lower, the utility of the OSNs is not affected. The aggregated decision voting value and sensitivity score will recompute the final decision may be changed.

VIII. CONFLICT RESOLUTION BASED ON STRATEGY

The strategy based conflict resolution approach is used for introducing the multiparty privacy conflicts.

A. Owner Overrides

The owner's decisions have the highest priority. If the aggregated decision voting value is one means to permit the access request. Otherwise if the aggregated decision voting value is zero means to deny the access request.

B. Full Consensus Permit

The controllers decision have a highest priority, if the aggregated decision voting value is one means to permit the access request otherwise deny the request.

C. Majority Permit

This strategy permits an access request if the number of controllers to permit the request is greater than number of controller to deny the access request. This majority voting strategy can be easily supported in strong majority permit and super majority permit.

IX. CONCLUSION

Online social networks help people to share personal and public information. In multiparty protection mechanism for online social network has a new model for collaborative management of shared data in OSNs. A multiparty access control model provides a policy specification and policy evaluation mechanism. In these OSNs a group of users could collide with one another so as to manipulate the final access control decision. There is no fake identity in OSNs. My recent work has evaluated the effectiveness of MPAC conflict resolution approach based on the tradeoff of privacy risk and sharing loss. Users may be involved in the control of a larger number of shared photos and the configurations of the privacy preferences may become time-consuming and tedious tasks. As part of future work using inference-based techniques for automatically configure privacy preferences in MPAC.

REFERENCES

[1]. Hongxin Hu H., Gail-Joon Ahn G. and Jan Jorgensen J. (2013) 'Multiparty Access Control for Online Social Networks: Model and Mechanisms' IEEE Trans. Knowledge, vol. 25, no. 1, pp. 1614-1627.

[2]. Carminati B., Ferrari E. and Perego A. (2006) 'Rule-Based Access Control for Social Networks', Proc. Int'l Conf. On the Move to Meaningful Internet Systems.

[3]. Fong P., Anwar M. and Zhao Z. (2009) 'A Privacy Preservation Model for Facebook-Style Social Network Systems', Proc. 14th European Conf. Research in Computer Security.

[4]. Squicciarini A., Shehab M. and Paci F. (2009) 'Collective Privacy Management in Social Networks', Proc. 18th Int'l Conf. World Wide Web.

[5]. Bilge L., Strufe T., Balzarotti D. and Kirda E.(2009) 'All Your Contacts Are Belong to Us: Automated Identity theft Attacks on Social Networks', Proc. 18th Int'l Conf. World Wide Web.

[6]. Ahn G. and Hu H. (2007) 'Towards Realizing a Formal RBAC Model in Real Systems', Proc. 12th ACM Symp. Access Control Models and Technologies.

[7]. Jin L., Takabi H. and Joshi J. (2011) 'Towards Active Detection of Identity Clone Attacks on Online Social Networks', Proc. First ACM Conf. Data and Application Security and Privacy.

[8]. Choi J., De Neve W., Plataniotis K. and Ro Y.(2011) 'Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks', IEEE Trans. Multimedia, vol. 13, no. 1, pp. 14-28.

[9]. Douceur J. (2002) 'The Sybil Attack', Proc. Int'l Workshop Peer-to-Peer Systems, pp. 251-260.
[10]. Ahn G., Hu H., Lee J. and Y. Meng (2010) 'Representing and Reasoning about Web Access Control Policies', Proc. IEEE 34th Ann. Computer Software and Applications Conf. (COMPSAC), pp. 137-146.
[11].Hu H., Ahn G. and Jorgensen J.(2011) 'Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks', Proc. 27th Ann. Computer Security Applications Conf., pp. 103-112.
[12]. Carrie E. (2007) 'Access Control Requirements for Web 2.0 Security and Privacy', Proc. Workshop Web 2.0 Security & Privacy (W2SP).
[13]. Golbeck J. (2005) 'Computing and Applying Trust in Web-Based Social Networks', PhD thesis, Univ. of Maryland at College Park, College Park, MD, USA.
[14]. Harrison M., Ruzzo W. and Ullman J. (1976) 'Protection in Operating Systems', Comm. ACM, vol. 19, no. 8, pp. 461-471.
[15]. Hu H. and Ahn G. (2008) 'Enabling Verification and Conformance Testing for Access Control Model', Proc. 13th ACM Symp. Access Control Models and Technologies, pp. 195-204.
[16]. Zheleva E. and Getoor L. (2009) 'To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles', Proc. 18th Int'l Conf. World Wide Web, pp. 531-540.
[17]. Hu H. Ahn G. and Kulkarni K. (2011) 'Anomaly Discovery and Resolution in Web Access Control Policies', Proc. 16th ACM Symp. Access Control Models and Technologies, pp. 165-174.
[18]. Lam L. and Suen C. Y. (1997) 'Application of Majority Voting to Pattern Recognition: An Analysis of Its Behavior and Performance' IEEE Trans. Systems, Man and Cybernetics, Part A: Systems and Humans, vol. 27, no. 5, pp. 553-568.
[19]. Li N., Mitchell J. and Winsborough W. (2005) 'Beyond Proof-of-Compliance: Security Analysis in Trust Management', J. ACM, vol. 52, no. 3, pp. 474-514.
[20]. Staab E. and Engel T. (2009) 'Collusion Detection for Grid Computing', Proc. Ninth IEEE/ACM Int'l Symp. Cluster Computing and the Grid, pp. 412-419.

AUTHORS PROFILE

Adlin Brainy T received the M.Sc degree in Software Engineering from Sun College Of Engineering, Anna University, and Chennai in 2013. And pursuing her M.E. degree in computer science from Anna University, Chennai. Her research interests include access control models and mechanisms, security and privacy in social networks.

Angel Gnana Shiny V received her B.Tech Information Technology degree from Ponjesly college of Engineering, Anna University, Chennai in 2010 . And pursuing her M.Tech. degree in computer science from Bharath University, Chennai. Her research interests include access control models and mechanisms, security and privacy in social networks.