International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 6 4075 - 4080

Online Social Networks with Message Filtered Policy Administration by Multiparty Access Control

Bhushan Nanche
D Y Patil COE, Akurdi
Savitribai Phule Pune University
e-mail: bnanche@gmail.com

Shanthi K.Guru
D Y Patil COE, Akurdi
Savitribai Phule Pune University
e-mail: gurushaanguru@gmail.com

***Abstract*—** Recently we have studied the Multiparty Access management for Online Social Networks Model and Mechanisms. Online social networks have experienced massive growth in recent years and become a de facto portal for millions of Internet users. These OSNs offer fetching means for digital social interactions and information sharing, but also occurs a number of security and privacy issues. While OSNs allow users to limit access to shared data, they at present do not provide any mechanism to enforce privacy concerns over data related with multiple users. To this end, we propose an approach to enable the security of shared data related with multiple users in OSNs. They make an access control model to capture the spirit of multiparty authorization requirements, along with a multiparty policy requirement scheme and a policy application mechanism. In addition, we access control model that we have various tasks on our model to analyze the features of existing logic solvers allows to take advantage of a logical representation exists. We have more comprehensive privacy approach to conflict resolution and analysis services for collaborative management of shared data in OSNs are proposed.

Keywords*—Social network, multiparty access control, security model, policy detail and management.*

*****

I. INTRODUCTION

Naturally, such as Facebook, Google+ and Twitter are designed as online social network of private and public information sharing and, with friends, colleagues, associates, family, and even with strangers, able to make social connections. In recent years, we have seen an unprecedented increase in the application of OSNs. For example, one representative from Face book, social network sites, boasts that it has more than 800 million active users and content sharing over 30 billion pieces each month. To protect user data, access control has get a central characteristic of OSNs.

A typical user profile information for each user, the UN, and Facebook, where users can post messages, content and Web pages with friends and friends offer a virtual space containing a list of wall. A user profile is usually the user's birthday, gender, interests, education, and work history information, and includes contact information. In addition, users can not only upload their own content or spaces, but also to other users, others the content that will appear in the tag. Each tag is a clear reference is a link to the user's location. To protect user data, current OSNs are indirectly system and policy administrators to regulate their data where users trusted users to a specific set of shared data can restrict users require.

Although OSNs currently provide simple access control mechanisms permitting users to direct access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces.

II. LITERATURE SURVEY

Several researchers have done the Multiparty Access Control for Online Social Networks Model and Mechanisms. By means of different performance and using different techniques for this purpose, as well as many new techniques introduced below in literature we are discussing some of them,

G. Ahn and H. Hu, [1] in this paper identified components and characteristics in their framework can be utilized for arranging the NIST/ANSI RBAC standard model using UML and OCL, and declaring authorization policies using RCL2000 and OCL. In addition, paper implemented a systematic tool called RAE. They believe that this is the first attempt to implement such an intuitive tool including critical features such as the validation and code generation for role-based systems.

G. Ahn, H. Hu, J. Lee, and Y. Meng, [2] in this paper provided a formal foundation of XACML in terms of ASP. Also, paper further introduced a policy analysis framework for identifying constraint violations in XACML-based RBAC policies, explicitly demonstrating existing XACML standard does not support the constrained RBAC. In addition, they have described a tool called XACML2ASP, which can seamlessly work with existing ASP solvers for XACML policy analysis. Their experiments showed that the performance of analysis approach could efficiently support larger access control policies.

A. Besmer and H.R. Lipford, [3] in this paper Photo tagging is a popular feature of many social network sites that allows users to interpret uploaded images with those who are in them, externally linking the photo to each person's profile. In this paper, theyidentify privacy concerns and mechanisms surrounding these tagged images. Using a focus group, they explored the needs and concerns of users, resulting in a set of design considerations for tagged photo privacy. They later designed a privacy enhancing mechanism based on our findings, and validated it using a mixed methods approach. Our results identify the social tensions that tagging create, and

 ISSN: 2321-8169
4075 - 4080

the needs of security tools to address the social implications of photo privacy management.

L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, [4] in this paper gate how easy it would be for a potential attacker to launch automated crawling and identity theft (i.e., cloning) attacks against 5 popular social networking sites. They present and experimentally evaluate two identity theft attacks. When the attacks succeed, the attacker can establish a friendship connection with the victim's contacts and hence, access their personal information. The simplest attack they present consists of the cloning of existing user accounts and the automated sending of friend requests to the contacts of the cloned victim. In the second, more advanced attack, they show that it is feasible to launch an automated, cross-site profile cloning attack where the victim's contacts are stolen and reestablished in a social network where she is not registered yet.

B. Carminati and E. Ferrari [5] in this paper Topology-based access control is today a de-facto standard for protecting resources in On-line Social Networks (OSNs) both within the research community and commercial OSNs. According to this paradigm, authorization constraints declare the relationships (and possibly their depth and trust level) that should present between the requestor and the resource owner to create the first able to access the required resource. In this paper, they show how topology-based access control can be enhanced by exploiting the collaboration among OSN users, which is the essence of any OSN. The need of user collaboration during access control enforcement arises by the fact that, distinct from old settings, in most OSN services users can reference other users in resources (e.g., a user can be call to a photo), and therefore it is generally not possible for a user to control the resources published by another user. For this reason, they introduce collaborative security policies, that is, access control policies identifying a set of collaborative users that must be involved during access control enforcement. Moreover, they discuss how user collaboration can also be exploited for policy administration and they present an architecture on support of collaborative policy enforcement.

B. Carminati, E. Ferrari, and A. Perego[6]In this article, they propose an access control mechanism for Web-based social networks, which adopts a rule-based approach for specifying access policies on the resources owned by network contributors, and where authorized users are signified in terms of the type, depth, and trust level of the relationships existing between nodes in the network. Different from traditional access control systems, our mechanism makes use of a semi decentralized architecture, where access control enforcement is carried out client-side. Access to a resource is assumed when the requestor is able to testify to being authorized to do that by providing a proof. In the article, besides illustrating the main notions on which our access control model relies, they present all the protocols underlying our system and a performance study of the implemented prototype.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

A. Architecture:

The implementation proof-of-concept Facebook application for the collaborative management of shared data, called MController.

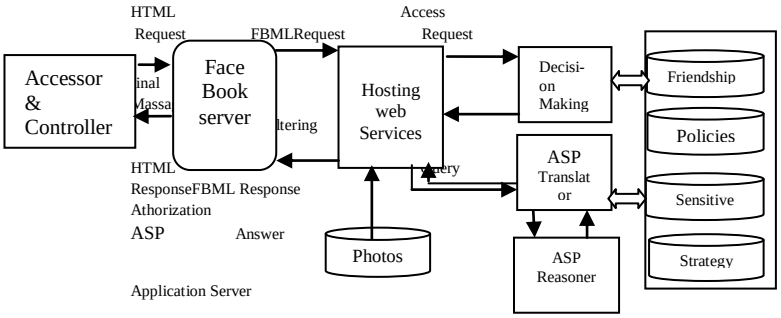

Fig.1 System Architecture

Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to control a shared data item. We are also investigating more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs.

B. Mathematical Model:

MPAC Model: In MPAC model define the following controllers.

Owner: Let *d* be a data item in the space of a user *u* in the social network. The user *u* is called the holder of *d*.

Contributor: Let *d be* a data item published by a user *u* in someone else's space in the social network. The user *u* is called the assistant of *d*.

Stakeholder: Let *d* be a data item in the space of a user in the social network. Let *T*be the set of tagged users homogeneous with *d*. A user *u* is called a stakeholder of *d*, if *u 2 T*.

Disseminator: Let *d* be a data item shared by a user *u* from someone else's space to his/her space in the social network. The user *u* is called a spread of *d*.

We are normally defining our MPAC model as follows.

U= $\{u_1, \ldots u_n\}$: Set of users

G= $\{g_1. . . g_n\}$: Set of Group

P: $\{p_1 \ldots . , p_n\}$ Collections of user profile

Where p_i: Profile of user i ϵ U

RT: Set of Relationship Type

R= {r1. . . rn}: Collection of user relationship sets

Where $r_i$relationship list of user i ϵ U

C= {c1, ... ,cn}: collection of user content sets

ISSN: 2321-8169
4075 - 4080

Where c_i set of contents of user i ϵ U
Where e_{ij} content identifier
D= {d1, ... ,dn}: collection of data set s
Where d_i set of data of a user i ϵ U
CT= {OW,CB,ST,DS}: Set of controller types
UU= {UU_{rt1} , ... , UU_{rtm}}: Collection of unidirectional binary user-to-user relations
Where UU_{rti} UxU pairs of users having relationship type rt_i ϵ RT
UG⊆U x G : Set of binary user-to-group membership relations
UD: Collection of binary user-to-data relations
whereUD_{cti} U x D specifies a set of user, data pairs having controller type ct_i ϵ CT
relation_members(u: U , rt: RT)
={u' ϵ U | (u , u') ϵ UU_{rt}};
ROR_members: $U \xrightarrow{RT} 2^U$each user u ϵ U relation of a relationship rt ϵ RT, denoted as relationship-of-relationship(ROR)
ROR_members(u: U, rt: RT) = {u' ϵ U |u' ϵrelation_member(u,rt)∨(ϵU[u ϵ ROR_members(u,rt)) u ϵ ROR_member(u'',rt)]};

Controllers:
function mapping each date item d ϵ D controller type ct ϵ CT
Controllers(d: D , ct: CT) = {u ϵ U | (u,d) ϵ U D_{ct}};

group_members: $G \rightarrow 2^U$, each group g ϵ G set of users, belong to the group
group_member(g: G) = {u ϵ U | (u , g) ϵ UG} ; groups(u : U) = {g ϵ G | (u,g) ϵ UG}.

relation_members: $U \xrightarrow{RT} 2^U$ function mapping each user u ϵ U with whom he/she has a relationship rt ϵ RT:

1) MPAC Policy Specification:

Accessor Specification: Let ac ϵ U ∪RT G be a user u ϵ U, a relationship type rtϵ RT, or a group g 2 G. Let at ϵ {UN, RN, GN} be the type of the accessor specification (user name, relationship type, and group name, respectively). The accessorfeatures is defined as a set, accessors= {a1; : : : ; an}, where each element is a tuple < ac, at >.
Data Specification: Let dt ϵ D be data item. Let *sl*be a reactivity level, which is a rational number in the range [0,1], assigned to *dt*. The data specification is defined as a tuple *<dt; sl>*.
MPAC Policy: A MPAC Policy is a %-tuple
P = < controller, ctype, accessor, data, effect > ,
Where,
Controller ϵ U : user who can regulate the access of data
Ctype ϵ CT : type of the controller
Accessor: Set of users to whom
Data: represented with a data specification
effect ϵ {permit, deny}: authentication effect of the policy

2)A Voting Scheme for Decision Making Multiparty Control

Decision voting**:** A decision voting value (DV) derived from the policy evaluation is defined as follows,

$$DV = \begin{cases} 0 & if Evaluation(p) = Deny \\ 1 & if Evaluation(p) = Permit \end{cases}$$

Assume all controllers equally.
Resolution value (DV_{ag}) range 0.00 to 1.00
Owner (DV_{ow}) the contributor (DV_{cb}) and stakeholders (DV_{st})
$DV_{ag} = (DV_{ow} + DV_{cb} + \sum_{i\epsilon\, SS} DV'_{st}) X \frac{1}{m}$,
Where SS is the stakeholder set of the shared data item, and m is the number of controllers of the shared data item.
Weighted decision voting scheme is as follows:

$$DV_{ag} = \left(w_{ow} * DV_{ow} + w_{cb} * DV_{cb} + \sum_{i=1}^{n} \left(w_{st}^{i} * DV_{st}^{i} \right) \right) * \frac{1}{w_{ow} + w_{cb} + \sum_{i=1}^{n} w_{st}^{i}}$$

Suppose, where are weight values for owner, contributor, and stakeholders, individually and n is the number of stakeholders of shared data item.
Sensitivity voting**:** A sensitivity score (Sc) (range from 0.00 to 1.00) for the data item can be calculated based on following equation:

$$Sc = \left(SL_{ow} + SL_{cb} + \sum_{i\epsilon\, SS} SL_{st}^{i} \right) * \frac{1}{m}$$

3) Threshold-Based Conflict Resolution

The final decision is made automatically by OSN systems with this threshold-based conflict resolution as follows:

$$Decision = \begin{cases} Permit, & if\, DV_{ag} > Sc \\ Deny, & if\, DV_{ag} > Sc \end{cases}$$

4) Strategy-Based Conflict Resolution with Privacy Recommendation

Introduce following strategies for the purpose of resolving multiparty privacy conflict in OSNs:
Owner-overrides:
Set $w_{ow} = 1, w_{cb} = 0, and w_{st} = 0$

 ISSN: 2321-8169
4075 - 4080

$$Decision = \begin{cases} Permit, & if\, DV_{ag} = 1 \\ Deny, & if\, DV_{ag} = 0 \end{cases}$$

Full-consensus-permit:

$$Decision = \begin{cases} Permit, & if\, DV_{ag} = 1 \\ Deny, & otherwise \end{cases}$$

Majority-permit:

$$Decision = \begin{cases} Permit, & if\, DV_{ag} \geq 1/2 \\ Deny, & if\, DV_{ag} < 1/2 \end{cases}$$

5)Logical Definition of Multiple Controllers and Transitive Relationships

Logical definition of multiple controllers is as follows

i) The owner of a data item can be represented as:

$$OW(controller, data) \leftarrow UD_{ow}(controller, data) \wedge U(controller) \wedge D(data)$$

ii) The contributor of a data item can be represented as:

$$CB(controller, data) \leftarrow UD_{CB}(controller, data) \wedge U(controller) \wedge D(data)$$

iii) The stakeholder of a data item can be represented as:

$$ST(controller, data) \leftarrow UD_{ST}(controller, data) \wedge U(controller) \wedge D(data)$$

iv) The disseminator of a data item can be represented as: $DS(controller, data) \leftarrow UD_{DS}(controller, data) \wedge U(controller) \wedge D(data)$

6)Logical Policy Specification

The translation module converts a multiparty authorization policy,accessor specification at=RN

$$(controller, ctype, \{< ac_1, RN >, \ldots\ldots < ac_n, RN >\} < dt, sl >, effect)$$

Into an ASP rule

$$decision(controller, effect) \leftarrow \bigvee_{1 \leq k \leq n} ac_k(controller, X) \wedge ctype(controller, data) \wedge U(controller) \wedge U(X) \wedge D(dt).$$

The translation module converts a multiparty authorization policy,accessor specification at=UN

$$(controller, ctype, \{< ac_1, UN >, \ldots\ldots < ac_n, UN >\} < dt, sl >, effect)$$

Into a set of ASP rules

$$decision(controller, effect) \leftarrow \bigvee_{1 \leq k \leq n} U(ac_k) \wedge ctype(controller, data) \wedge U(controller) \wedge D(dt).$$

The translation module converts a multiparty authorization policy,accessor specification at=GN

$$(\text{controller}, \text{ctype}, \{< \text{ac}_1, \text{GN} >, \ldots\ldots < \text{ac}_n, \text{GN} >\} < \text{dt}, \text{sl} >, \text{effect})$$

Into a set of ASP rules

$$decision(controller, effect) \leftarrow \bigvee_{1 \leq k \leq n} UG(ac_k, X) \wedge ctype(controller, data) \wedge U(controller) \wedge U(X) \wedge D(dt).$$

7) Logical Representation of Conflict Resolution Mechanism

Voting scheme are represented in ASP rules as follows:

$$decisionvoting(C) = 1 \leftarrow decision(C, permit).$$
$$decisionvoting(C) = 0 \leftarrow decision(C, deny).$$
$$aggregationweight(K) \leftarrow K = sum\{weight(C): controller(C)\}.aggregationdecision(N) \leftarrow N = sum\{decionvoting(C) * weight(C): controller(C)\}.aggregationsensitivity(M) \leftarrow M = sum\{sensitivityvoting(C) * weight(C): controller(C)\}.$$

Threshold-based conflict resolution mechanism is represented as:

$$aggregationdecision(N) \wedge aggregationsensitivity(M).$$
$$decision(controllers, deny) \leftarrow notdecision(controllers, permit).$$

IV. RESULTS AND DISCUSSION

Following figure showing that after registration user account is created.

Fig 2: User Account Window

The following figure showing window of the Friend list including Friend and Non friend.

Fig 3: Friend and Non Friend window

 ISSN: 2321-8169
4075 - 4080

The following figure showing when user want to filter there inbox message or comment then if any one write some abuse are related word then it is filtered and shows warning message in red border message.

Fig 4: Filtered Block window

The first graph shows the difference between image shares from all or only tagged friend.

Fig 5: No. of tag user v/s total user

The second graph show comment words total count and filter message count, this is our proposed method

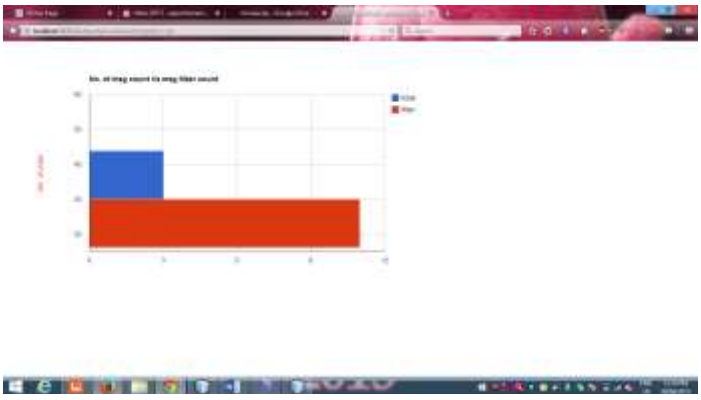

Fig 5: No. of total message count v/s filter message count

V. CONCLUSION

Collaborative management OSNs in a novel solution for shared data. An MPAC model, a multi-party policy specifications plan and policy evaluation system was designed with. In addition, we represent and our proposed an approach to logic model is presented. A proof-of-concept implementation of our solution called MController has been discussed also, followed the system evaluation and usability study.To this end, we are associated with multiple users sharing OSNs data to enable an approach. The planto systematically integrate the notion of trust and reputationinto our MPAC model and investigate a comprehensive solution to with collusion attacks for providing a robust MPAC service.In addition, we have our access control model that allows us to analyze various tasks on our models to take advantage of the features of existing logic solvers allows for a logical representation exists. We also have our vision is a proof of concept prototype Facebook as part of an application and evaluation of usability studies and provide our system method.

VI. ACKNOWLEDGMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Mrs.Shanthi K.Guru for her exemplary guidance, monitoring and constant encouragement throughout the course of this project. I also take this opportunity to express a deep sense of gratitude to my Head of the Department Mrs. M.A.Potey, PG Coordinator Mrs.S. S.Pawar, for her cordial support, valuable information and guidance. Thanks to all those who helped me in completion of this work knowingly or unknowingly like all those researchers, my lecturers and friends.

REFERENCES

[1] G. Ahn and H. Hu, “Towards Completing a Formal RBAC Model inReal Systems,” Proc. 12th ACM Symp. Access Control Models andTechnologies, pp. 215-224, 2007.

[2] G. Ahn, H. Hu, J. Lee, and Y. Meng, “Re-presenting and Reasoningabout Web Access Control Policies,” Proc. IEEE 34th Ann.Computer Software and Applications Conf. (COMPSAC), pp. 137-146, 2010.

[3] A. Besmer and H.R. Lipford, “Moving beyond Untagging: PhotoPrivacy in a Tagged World,” Proc. 28th Int’l Conf. Human Factors inComputing Systems, pp. 1563-1572, 2010.

[4] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, “All YourContacts Are Belong to Us: Automated Identity theft Attacks onSocial Networks,” Proc. 18th Int’l Conf. World Wide Web,pp. 551-560, 2009.

[5] B. Carminati and E. Ferrari, “Collaborative Access Control in Online Social Networks,” Proc. Seventh Int’l Conf. CollaborativeComputing: Networking, Applications and Worksharing (Collaborate-Com), pp. 231-240, 2011.

[6] B. Carminati, E. Ferrari, and A. Perego, “Rule-Based AccessControl for Social Networks,” Proc. Int’l Conf. On the Move toMeaningful Internet Systems, pp. 1734-1744, 2006.

[7] B. Carminati, E. Ferrari, and A. Perego, “Enforcing Access Controlin Web-Based Social Networks,” ACM Trans. Information andSystem Security, vol. 13, no. 1, pp. 1-38, 2009.

[8] E. Carrie, “Access Control Requirements for Web 2.0 Security andPrivacy,” Proc. Workshop Web 2.0 Security & Privacy (W2SP), 2007.

[9] J. Choi, W. De Neve, K. Plataniotis, and Y. Ro, “Collaborative FaceRecognition for Improved Face Annotation in Personal PhotoCollections Shared on Online Social Networks,” IEEE Trans.Multimedia, vol. 13, no. 1, pp. 14-28, Feb. 2011.

[10] J. Douceur, “The Sybil Attack,” Proc. Int’l Workshop Peer-to-PeerSystems, pp. 251-260, 2002.

 ISSN: 2321-8169
4075 - 4080

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

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

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

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

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

Authors

Bhushan Nanche received the B.E.degree in Information Technology from D.Y.Patil College of Engineering and Technology, Kolhapur in 2008 and has 7 years of teaching experience. He is currently working System Administrator at D.Y. Patil College of Engineering Akurdi, Pune and pursuing Master degree in Computer Engineering from Savitribai Phule Pune University.

Mrs.Shanthi K.Guru received the BE degree in Electronics and Telecommunication from Madras University in 1994 and ME in Electronics and Telecommunication from University of Pune in 2012 and has 13.7 years of teaching experience. She is currently working as Assistant Professor at D.Y. Patil College of Engineering, Akurdi, Pune.