ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

User to User Relation Based Online Access Control to Overcome Multiparty Conflict in Social Media

Supriya H. Karkare, Dr. S. A. Ubale

ME Student, Department of Computer Engineering, Zeal College of Engineering and Research, Savitribai Phule Pune University Maharashtra, India

Professor, Department of Computer Engineering, Zeal College of Engineering and Research, Savitribai Phule Pune University, Maharashtra, India

ABSTRACT: Users and resources in online social media areconnected socially by different kind of relationship. In specific,user to user relationships creates the basis of the Online SocialNetwork(OSN) structure, and plays a significant role in specifyingand enforcing access control. Single users and the OSN providerneed to be capable of specification which access can be allowed inorder of existing relationships. Proposed system presents a noveluser to user relationship based access control model for OnlineSocial Network(OSN) systems that utilizes regular expressionformat for such policy specification. Access control policies onusers and resources are assigned in the form of requested action,multiple relationship types, the starting point of the analysis,and the number of nodes on the path. This present multipath checking mechanism to determine whether the requiredrelationship path between users for a given access request exists.We validate the feasibility of our approach by implementing aprototype system and evaluating the performance of DFS-basedand BFS-based path checking algorithms.

KEYWORDS: UURAC, Tag, Anomaly Detection, Authentication,Authorization .

I. INTRODUCTION

Background-Online social network is enormouslygrowing with content uploading most of user generated content platforms. Photos, videos, blogs, web links and other kinds of information are uploaded, shared and commented by OSN users. Different types of user interactions, including chatting, private messaging, poking, social games, etc., are also embedded into these systems. Present theoryadds more features that need to be supported in access control solutions for OSN systems.[6] OSN users may want to express their own preferences on how their own or related contents should be exposed. A system wide access control policy such as we find in mandatory and role-based access control, does not meet this need.[5] Access control in OSNs further differs from discretionary access control in that users other than the resource owner are also allowed to configure the policies of the related resource. Furthermore, those users accessing application, e.g. parent to child, may want to control the accessing user's actions. Therefore, the OSN system needs to collectively utilize these individualized policies from users related to the accessing user or the target, along with the system-specified policies for control decisions. User and resource as a target Unlike traditional user access where the access is against target resource, activities such as poking and friend recommendations are performed againstother users.Notification of a particular friend's activities could be bothersome and a user may want to block it. This type of policy is captured asincoming action policy. Also, a user may want to control her own or other users' activities. For example, a user may restrict her own access from all violent content or a parent may not want her child to invite her co-worker as a friend. This type of policy is captured as an outgoing action policy.[7] In OSN, it is necessary to support policies for both types of actions.[5]Typically, the number of users in an OSN is very large and the amount of resources they own is usually even larger. Moreover,the relationships among users are changing frequently anddynamically. A user may not be able to know either theuser name space of the entire network or all her

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

possibledirect or indirect contacts.[4] Therefore, it is infeasible for herto specify access control policies for all of the possibleaccessing users. [3]Even if she knows them all, it takes enormousamount of time for her to explicitly specify policiesfor all of them one by one as in discretionary access control.Role-based access control does not fit well in this situationeither, because privileged user groups are different for eachuser. Thus different users' privileged user groups cannot beassigned to a unified set of roles. Overall using traditionalaccess control approaches is cumbersome and inadequatefor OSN systems.[2]

Motivation-Online social network gives platform for people connect, interact and share information with each other. Access control in online social media presents many features different from traditional access control. In required and role based access control, a system wide access control policy is managed by the security administrator. In systematic access control, the resource owner design access control policy. But, in OSN systems, users required to usual access to their application resources and activities related to them. Thus access in OSNs is related to user specified policy rights. Other than the resource owner, some related users like a tagged in a photo owned by another user, parent of a user may also expect some control on how the resource or user can be explored. To prevent users from accessing unwanted or inappropriate content, user-specified policies that regulate how a user accesses information need to be understands in authorization policy as well. So that, the system needs to gather these single partial policies, from both the accessing users and the target users, along with the system-specified policies and fuse them for the collective control decision. In OSN, access to resources is controlled by the relationships between the accessing user and the controlling user of the target found in the social user graphs constructed. This type of relationship based access control (to which this system refer as ReBAC) takes into account the existence of a particular relationship or a particular sequence of relationships between users and shows access control policies in terms of such user-to-user (U2U) relationships.This system additionally performs social media conflict detection to resolve multiparty conflicts. This system proposed a computational mechanism for social media that, given the single privacy preferences of each user included in an item, is able to find and resolve conflicts by applying a different conflict solution method based on the follower users' may be willing to make in different situations.[4] Also present a user study comparing this computational mechanism of conflict resolution and already existing approaches to what users would do themselves manually in a number of situations. The results obtained suggest our proposed mechanism importantly outperformed other previously proposed techniques in order to the number of times it matched participants' behavior in the study.[3]

II. LITERATURE SURVEY

In this work, Ubale S. A, ApteSulabha studied MAC, DAC and RBAC access control re different implementations. Also listed the advantages and disadvantages of these models. Y. Cheng, J. Park, and R. Sandhuintegrates attribute based policies into user relationship based access control. This attribute aware ReBAC improves access control capacity and allows fine -grained access controls which is not available in ReBAC. The policy specification language for the user to user relationship-based access control (UURAC) model proposed in is extended to enable such attribute-aware access control. Proposed methodology presents an improved path checking algorithm for checking existence of the required attributes and relationships in for allowing access [2]. In this work a formal access control model that is used to confirm ideas from relationship based access control and a two stage method for evaluating policies. These techniques are defined using path conditions, which are similar to regular expressions. We define semantics for path conditions, which we use to develop a rigorous method for evaluating policies. Proposed system presents the algorithm needed to check policies and create its complexity. At last, Proposed system elaborate the advantages of our model using an example and describe a preliminary implementation of our algorithm [3].

This survey explores what it takes to improve the applicability of ReBAC to application domains other than social media conflict. This work also design an structural ReBAC model to capture the essence of the paradigm, that is, authorization decisions are based on the relationship between the resource owner and the resource access or in a social media network maintained by the protection system. A reliability of the model is that it asses the contextual form of relationships. We devise a policy language, based on modal logic, for composing access control policies that support delegation of trust [4]. This work takes a first step in deepening the understanding ofthis access control paradigm, by proposing an access control technique that creates and generalizes the privacy preservation methodology of Face book.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Proposed model can be started into a family of Face book style social media application, each with the identified by different access control mechanism, so that Face book is but one formulation of the model. This states that the model can be formulated to defined policies that are not currently supported by Face book but uses rich and natural social importance. It describes the design space of privacy preservation mechanisms for Face book style socialmedia network application, and lays out a formal framework for policy analysis in these systems [5].

The increased social media application security provided by Web 2.0 technologies needs to a review of what we consider private" and what we consider personal" information, and will subsequently drive a new way of limiting and monitoring the information that we release online. Web 2.0 applications are designing large, complex number of things from personal data and so we need new approaches to describe and execute access control on that data [6]. H. Hu and G.-J. Ah proposes approach for collaborative privacy management of shared information in OSNs. Specifically, we provide a systematic approach to identify and resolve privacy conflicts for collaborative data sharing. Social media conflict resolution indicates a compromise between privacy protection and data sharing by modulating privacy risk and sharing loss [7].

In this work, H. Hu, G.-J.Ahn and J. Jorgensen formulate access control model to capture the essence of multiparty authorization requirements, with a multiparty policy features scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model that allows us to deal with new the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof of ownership protocol of this approach as part of an application in Face book and gives usability study and system evaluation of our method [8]. A key and novel feature of our architecture, however, is that it is possible to remove access from a user without assigning new keys to other users or re-encrypting existing cipher texts. We achieve this by creating a proxy that participates in the decryption process and enforces revocation constraints. The proxy is cheaply trusted and cannot decrypt cipher texts or provide access to former revoked users. This work design simple architecture and construction, provide performance evaluation,and prototype application of our approach on Facebook[9] .

Y. Cheng, J. Park, and R. Sandhu Proposed an approach is relationship based access control system for OSNs that includes not only U2U relationships but also user to resource (U2R) and resource to resource (R2R) relationships. In addition to this, while most access control approach for OSNs only focus on controlling users normal usage activities, our model also achieve controls on users administrative policies. Authorization policies are defined in terms of patterns of relationship paths on social graph and the hop count limits of this path. The new policy featured language shows features of hop count ignoring of resource related relationships, permits more flexibility and explorative mechanism. We also provide simple specifications of conflict resolution policies to resolve possible conflicts among authorization policies. Autonomous agents usually wraps personal information defines their principals, and therefore they play a important role in protection of privacy. Additionally, autonomous agents themselves can be applied to improve the privacy of computer applications by taking benefits of the intrinsic features they assigns, such as artificial intelligence, pro activeness, self government, and the like. This article features the problem of preserving privacy in computer applications and its relation to having freedom to acts as agents and Multi-agent Systems. It also surveys privacy-related survey in the field of Multi-agent Systems and identifies open challenges to be faced by future research [10].

III. PROPOSED SYSTEM

Proposed system modulates users and resources in online social media are connected by different kinds of relationships. In this case, user-to-user relationships form the basis of the OSN structure, and play aimportant role in specifying and enforcing access control. Single users and the OSN provider should be enabled to specify which access can be granted in terms of existing relationships. In this system proposes a novel user-to-user relationship-based access control (UURAC) model for OSN systems that utilizes regular expression notation for such policy specification. Access control policies on users and resources are designed in forms of requested action, multiple relationship types, the starting point of the evaluation, and the number of hops on the path. Proposed system present two path checking algorithms to determine whether the required relationship path between users for a given access request exists.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

In this first step for detecting and resolving privacy conflicts in Social Media that is based on current evidence about privacy negotiations and disclosure driving factors in Social Media and is able to adapt the conflict resolution strategy based on the particular situation. The intermediate firstly inspects the individual privacy policies of all users involved looking for possible conflicts. If conflicts are found in, the mediator proposes a solution for each conflict according to a set of concession rules that model how users would actually negotiate in this domain

IV. MATHEMATICAL MODEL

Online Access control based on User to User relationship (MATHEMATICAL MODEL)

Let us consider S as a system for Authentication and authorization for industrial authentication

S= {……

INPUT:

- Identify the inputs

F= {f_1, f_2, f_3 ……,f_n| 'F' as set of functions to execute commands.}

I= {i_1, i_2, i_3…|'I' sets of inputs to the function set}

O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets}

S= {I, F, O}

I = {user credential and user relation from path extraction}

O = {User Access control}

F = {policy matching,

User role assignment, User to User path computation .Multiparty conflicts detection

}

Above mathematical model is NP-Complete

Given an user n ∈ N, her groups G_n, her individual privacy policy $P_n =< A, E >$, and a user t ∈ T; we define the action function as:

$$act(P_n, t) = \begin{cases} 1\ if \exists G \in G_n : t \in G \wedge \in P_n.A \wedge t \notin P_n.E \\ 1\ if \exists G \in G_n : t \in G \wedge \notin P_n.A \wedge t \in P_n.E \\ 0\ Otherwise \end{cases}$$

Note that the definition of this function will vary according to the access control model used, but it will be defined in a similar way. That is, the idea is to be able to know, given a target user t, whether the privacy policy will grant/deny t access to the item regardless of the access control model being used. In particular, we assume that the available actions are either 0 (denying access) or 1 (granting access).

Given a set of negotiating users N and a set of target users T; a target user t ∈ T is said to be in conflict iff∃a,b∈N with individual privacy policies P_a and P_b respectively, so $V_a[t] \neq V_b[t]$

Further, we say that the set of users in conflict C ⊆T, is the set that contains all the target users that are in conflict.

Input:

N = {negotiating users}

$P_{n1}, \ldots, P_{nk}$ = {privacy policies}

T = {target users}

Output:

C = {conflict}

Recall groups are disjoint. Otherwise, the complexity is $O(|\cup|^4)$.

Conflict Resolution:

Given user n ∈ N, her preferred privacy policy P_n, the maximum tie strength value δ, a conflicting target user c ∈ C, the willingness of user n to accept changing her most preferred action for c is a function: $W: N \times C \longrightarrow [0,1]$

$$W(n,c) = \frac{1}{2} \cdot \left(\frac{|\ \delta - I_n(c)\ |}{\delta + I_n(c)} + \frac{|\ \delta - S_n\ |}{\delta + S_n} \right)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

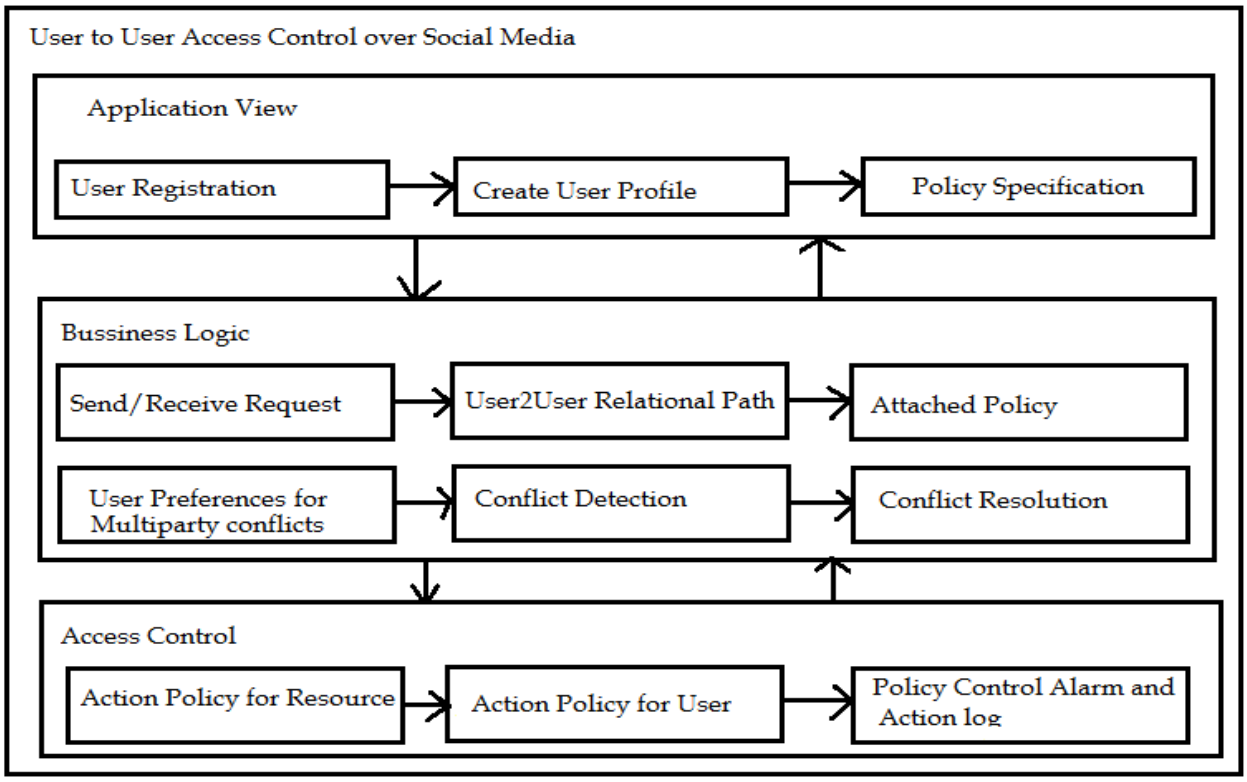
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

V. SYSTEM ARCHITECTURE



VI. ALGORITHMS USED

Proposed algorithm specifies how the access evaluation procedure works. When an accessing user a requests an action against target user user t, the system will look up user a action policy, user t action policy and the system specified policy corresponding to action. When user a requests an action against a resource resource t, the system will retrieve all the corresponding policies of rt. Although each user can only specify one policy per action per target, there might be multiple users specifying policies for the same pair of action and target. Multiple policies might be collected in each of the three policy sets: AUP, TUP/TRP and SP.

Algorithm1. User action Authentication (user $_a$, action, target)
Step 1: (User Policy Assignment)
Step 2: if target ==u_t then
AUP is user a policy for action,
TUP is user t policy for action,
SP system's policy for action
Step 3: else
AUP is user a policy for action,
TRP is resource t policy for action,
SP is system's policy for action,
(resource.typename, resource.typevalue)
Step 4: (User Policy authentication)
Step 5: for all policy in AUP, TUP/TRP and SP do

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Generate graph models (start, path rule) from policy
Step 6: for all graph model extracted do
Step 7: Determine the starting node, specified by start, where the path evaluation starts
Step 8: Determine the evaluating node which is the other user involved in access
Step 9: Extract path rules path rule from graph rule
Step 10: Find every path spec path, hop count from path rule
Step 11: Path-check each path spec using Algorithm 2
Step 12: Check combined result based on conjunctive or disjunctive connecting path specs and negation on individual path nodes.
Step 13: Collect final result from the result of each policy.

VII. RESULT ANALYSIS

Online user to user access control system is implemented using path associated communicating party (user to user). Furthermore, proposed system enhancement this work for avoiding multiparty conflict in social media environment.

a. RESULT TABLE

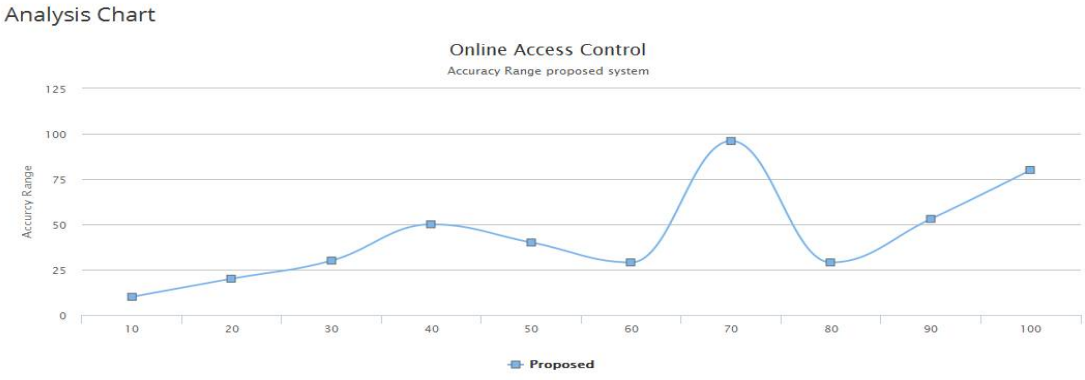
Proposed user to user relationship based access control leads to social media control by user policy. User relationship extracted based on user to user path.

Attributes	**Existing**	**Proposed**
Access rule	Path Rule	Path, User , Action grant
User Policy	Limited User Policy	Share, Upload, Download, Tag, Like
Security	Improvement needed	Improved
Algorithm	DFS, BFS	User to User Hop Count

b. PERFORMANCE MEASURES

1. Accuracy:-

Online access control system based on user to user relationship by hop count between path of source and destination users. Proposed system shows accuracy of path extraction based access control level in the system.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

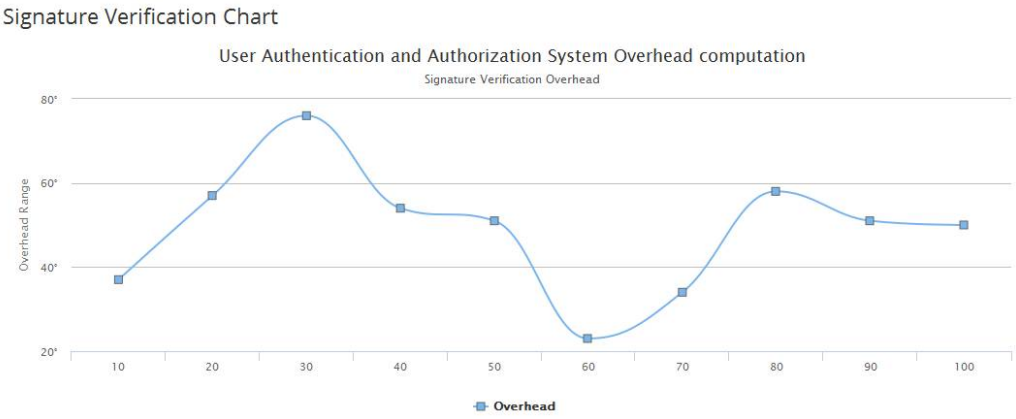
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

2. Signature Verification:-

In online social network user to user access control is managed by digital signature based policy as response action to user request. Following graph shows that signature generation overhead while verification of user policy grant. Digital signature verification can be applied at various level of authentication such as at time of login, add post, download, user tagging in friend list.



VIII. CONCLUSION

Proposed system designs an User to User RelationshipAccesControl(UURAC) model and a regular expression withpolicy preferences as security setting. Proposed methodologyused DFS-based and BFS-based path checking algorithmsand analyzed the complexity for the algorithms. This workbelieves the proposed model in this paper provides a solidfoundation for more advanced ReBAC solutions in thefuture. This work proposes a new model, namely URRAC,which experiments user to resource and resource to resourcerelationships as well as. This experiment implements anattribute-aware UURAC model that incorporates attributebasedpolicies to Relationship Based Access Control(ReBAC).In order to contribute this system, proposes approach fordetecting and resolving privacy conflicts in Social Media thatis based on current empirical evidence about privacy conflictsfor compromise and disclosure driving factors in SocialMedia and is able to adapt the conflict resolution strategybased on the particular situation. The Proposed approachprovides a solid foundation from the user perspectives.

REFERENCES

[1] Ubale S. A, ApteSulabha, ”Analysis of DAC MAC RBAC Access Control based Models for Security”, International Journal of Computer Applications, Volume 104 No.5, October 2014.
[2] Y. Cheng, J. Park, and R. Sandhu, ”Attribute-aware relationship based access control for online social networks,” in Proc. 27th Data Appl. Secur. Privacy, 2014, pp. 292306.
[3] J. Crampton and J. Sellwood, ”Path conditions and principal matching: A new approach to access control,” in Proc. 19th ACM SACMAT, 2014, pp. 187198..
[4] P. W. Fong, ”Relationship-based access control: Protection model and policy language,” in Proc. First CODASPY, 2011, pp. 191202.
[5] P. W. Fong, M. Anwar, and Z. Zhao, ”A privacy preservation model for facebook-style social network systems,” in Proc.Comput. Secur.ESORICS, 2009, pp. 303320.
[6] C. Gates, ”Access control requirements for Web 2.0 security and privacy,” IEEE Web 2.0, 2007.
[7] H. Hu and G.-J.Ahn, ”Detecting and resolving privacy conflicts for collaborative data sharing in online social networks,” in Proc. 27th ACSAC, 2011, pp. 103112.
[8] H. Hu, G.-J.Ahn, and J. Jorgensen, ”Multiparty access control for online social networks: Model and mechanisms,” IEEE Trans.Knowl. Data Eng., vol. 25, no. 7, pp. 16141627, May 2013.
[9] S. Jahid, P. Mittal, and N. Borisov, ”Easier: Encryption-based access control in social networks with efficient revocation,” in Proc. 6th ACM Symp. Inf., Comput.Commun.Secur., 2011, pp. 411415.
[10] Y. Cheng, J. Park, and R. Sandhu, ”Relationship-based access control for online social networks: Beyond user-to-user relationships,” in Proc. IEEE PASSAT, 2012, pp. 646655.