Scientific Journal of Impact Factor (SJIF): 4.72
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 3, March -2017

ACCESS CONTROL FOR ON-LINE SOCIAL NETWORKS USING ReBAC BEYOND USER-TO-USER RELATIONSHIP

[1]Mr. Nilesh. Waskar, [2]Prof. M. D. Ingle

Department of Computer Engineering, Jscoe, Hadapsar, Pune
Department of Computer Engineering, Jscoe, Hadapsar, Pune

Abstract — *User to user (U2U) relationship based access control has become the most common approach for modeling access control in online social network(OSN), where authentication is typically made by mapping between the accessing user and the resource owner based on existence U2U relationship. We propose new ReBAC model for OSN that contains different types of relationships and utilizes regular expression notation for specification, namely UURAC (User to User Relationship- Based Access Control). In this model, Authorization polices are defined as patterns of relationship path and the hop count limit of path on social graph. Now days OSN application allow different types of user activities that cannot be controlled by using U2U relationship. To enable including all user activities for ReBAc mechanism, we develop the URRAC (User to Resource Relationship-Based Access Control) model to manipulate User to Resource (U2R) and Resource to Resource (R2R) relationship for authorization. Most of the today's access control solution for OSNs focus on controlling normal usage activities for user, our new URRAC model also captures controls of user's administrative activities*

Keywords- *Authorization Policy***,** *OSN models, Policy Specifications, Privacy issues, Security issues.*

I. INTRODUCTION

Online social networks (OSNs) have become everywhere in daily life and have extremely changed how people connect, interact and share information with each other. Online social networks (OSNs) have been rapidly evolving since the last decade and now have billions of users in the worldwide. A recent survey found that 79% of online adults use a social network of same kind[11]. Many existing OSNs provide convenient environments for user and share large amount of information with other user for a multitude of purposes. The sharing and communications are based on social connection among users, namely relationship. Most users in OSNs to keep in touch with Know colleagues, they share a large amount of sensitive or private information about each other, including contact information, education information, pictures, video, and comments and so on. Some of this information is made public without security and privacy of user data consideration. Security and privacy in OSNs have increasingly gained attention from both media and research community [12, 13].

These security and privacy high light the need for effective access control that can protect data from unauthorized user access in OSNs. Access Control in OSN is typically based on the users relationship in the social graph. That is granting rights an accessing users based on the existence of certain type of direct and indirect relationship between accessing user and controlling users of the target. Many existing OSN system enforce the limited relationship based access control mechanism, in that users have ability to choose from predefined policy, such as Public, Private, Friend list providing users options to manages the distinctly privileged user groups. These proposals explore more flexible and expressive solution than provided by the current commercial ONSs, such as supporting multiple relationship types in policy languages. In the commercial and academic solution have a common characteristics is that they focus on user to user (U2U) relationship between accessing user and the resource owner, and assume ownership is the only existence of user to resource (U2R) relationship. However, this is not sufficient to mapping many user activities found in the today's OSN application, where users can performance action that creates relationship between users and resources other than ownership. For example, tagging a friend on photo will create U2R relationship between the photo and tagged user which may allow friends of tagged user to access the photo. Hence the tagged user may want to control other related users access to photo. Likewise, users actions can establish Resource to Resource (R2R) relationships such as photo under the same album, comments to a blog post etc. For this purpose, it is necessary to exploit U2R and R2R relationship in addition to U2U relationship for authorization polices and decisions. Moreover, in traditional access control model (discretionary access control, mandatory access control, role-based access control etc) authorization decisions are primarily based on identities and attributes of subject and objects, where attributes may include group or role memberships, access control list, capability lists and security labels etc. However, this approach of identity and attribute based fail to provides scalability and dynamicity of OSNs.

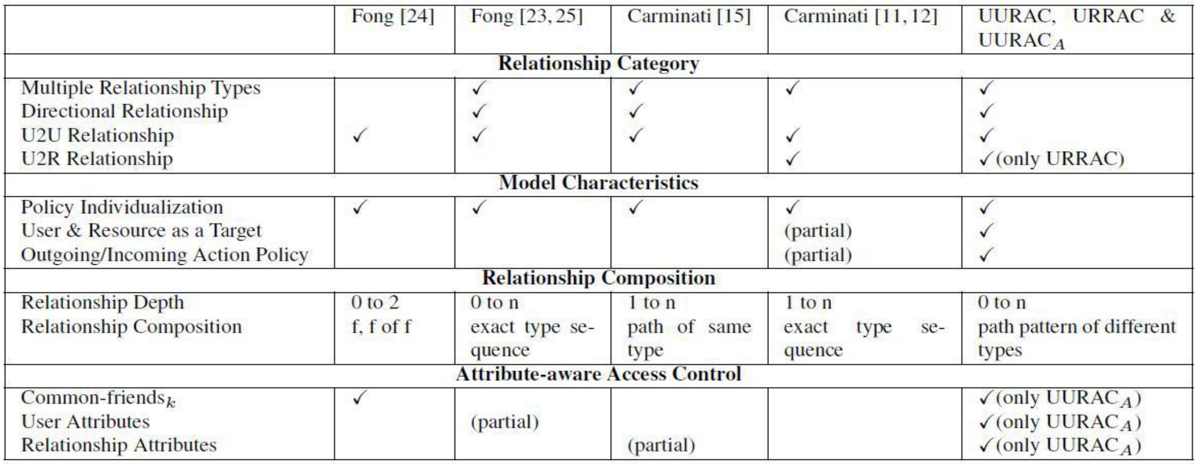
Instead, access control in OSNs is typically based on the relationship between user and resource on social graph. So the relationship-based access control (ReBAC) mechanism has emerged for OSN [14, 15]. In ReBAC, Resource owners without knowing the user name space of the entire network or all their possible direct or indirect contacts, specifies access control of their information based on their relationship with others. Accordingly, relationship-based access control has been recognized as a key requirements for security and privacy in OSNs, has been commonly adopted in real world OSN system. The proposed model includes users normal usages activities as well as the administrative activities. The U2U relationship based access control model is extended by including U2U, U2R and R2R relationship on users administrative activities.

II. REVIEW OF LITERATURE

In This section, We provide brief overview on the security and privacy issues in OSNs, and examine existing access control and privacy preservation solutions for OSNs. In this paper[1], author introduce security issues in OSNs into four categories : privacy breaches, spam and phishing attacks, Sybil attacks and malware attacks. User share a large amount of information with other users in OSNs using different services, such information makes privacy breach very easy to happen form OSN providers, other users and third party applications.OSN system keep all updated information. Thus, users have trust on OSN providers to protect and not misuse the data. Many OSNs allows third party applications to run on their platforms and provides user additional functionalities. During installation of third party application users grant permission to it. Hence, those applications get access more information than they actually need for proper functioning. This shows that a suitable and effective access control mechanism is required for protecting users data from unauthorized access.

In this paper [3], author introduce how the resource owner and access user are in a particular kind of relationship. Typically, an OSN can be modeled as a graph, where node correspond to users and edges denotes corresponds to users and edges denotes relationship between users. In traditional access control system, authorization decision is based on unary predicates of users, and access user have certain identity and role. So in many OSNs there exits non-mutual relationships of different types resource and access user. In many healthcare and education application domain, authorization decision is based on part type of relationship between the resource owner and access user. This need is noticed, we examine how role based access control model have been pushed limits to achieving with this demand. An OSN is collection of different types of users and resources connected by set of relationships. This system usually provides different services of user for both the maintenance of existing and new connections with other users. Based on such relationship, users can identify contacts of their contacts or get notification contacts. In Fong et al [6], proposed a formal ReBAC model for social computing application, which employs a modal logic language for policy specification and composition. Fong [7] et al later extended the policy language and studied its expressive power. These two models allow multiple relationship types and directional relationship. A formal model for access control in Face-Book like system was developed by Fong et al [5], which treats access control as two-stage process, namely reaching the search listing of the resource owner and accessing the resource, respectively.

In [9, 10], Carminati et al proposed an access control framework which utilizes relationships among users and resources as the basis for access control and employs the Semantic Web Rate Language (SWRL) to define authorization, administration and filtering policies. Our URRAC model proposed in this work offers more complete policy administration by addressing policy management and conflict resolution. Fig 1. Summarize the salient characteristic of the model discussed above.



	Fong [24]	Fong [23, 25]	Carminati [15]	Carminati [11, 12]	UURAC, URRAC & UURAC_A
Relationship Category					
Multiple Relationship Types		✓	✓	✓	✓
Directional Relationship		✓	✓		✓
U2U Relationship	✓	✓	✓	✓	✓
U2R Relationship				✓	✓(only URRAC)
Model Characteristics					
Policy Individualization	✓	✓	✓	✓	✓
User & Resource as a Target				(partial)	✓
Outgoing/Incoming Action Policy				(partial)	✓
Relationship Composition					
Relationship Depth	0 to 2	0 to n	1 to n	1 to n	0 to n
Relationship Composition	f, f of f	exact type sequence	path of same type	exact type sequence	path pattern of different types
Attribute-aware Access Control					
Common-friends_k	✓				✓(only UURAC_A)
User Attributes		(partial)			✓(only UURAC_A)
Relationship Attributes			(partial)		✓(only UURAC_A)

Fig. 1. Comparison of Access Control Model

III. SYSTEM OVERVIEW

In this following, we define an access control model OSNs with access control policy conflict resolution polices in terms of existing relationship between user and resources in the system.

3.1 Model Definition :-

The Model describe five categories of components include Accessing User (Ua), Action, Target, Access Request and policy shown in Fig 2. We assume that set of user as U, which includes accessing user (Au) and Target user (Tu) with collection of session for each user. S is the current sessions, which is composed by accessing session (As) and Target session (Ts). Also consider set of resources R, including target session (Ts), objects (o) and access control policies (P). We can write Action function for access users against Target as ACT = act 1, act 2...act n.
This represents the set of OSN supported actions, which provides the access modes of users, execute in the system. The action can be performed in two forms as the active form and passive form. Each action defined in active from with accessing user (Ua) as the actor and users as targets. For each action act i, the passive from act i^{-1} represents the action from the targets perspective. Policy defines the rules according to which authorization is regulated show in Fig 1. Policies can be categorized into user- specified and system specified polices with respect to who defines the policies.

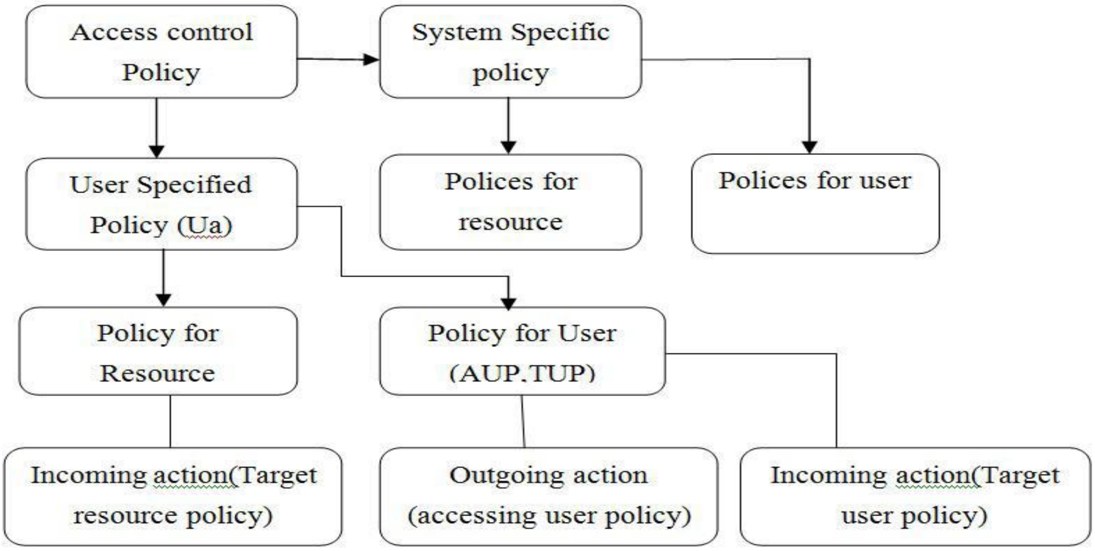

Access control Policy
System Specific policy
User Specified Policy (Ua)
Polices for resource
Polices for user
Policy for Resource
Policy for User (AUP,TUP)
Incoming action(Target resource policy)
Outgoing action (accessing user policy)
Incoming action(Target user policy)

Fig. 2. Model Components

IV. SYSTEM ANALYSIS

Given the social graph showed in Figure 3, below we analyzed how access control of these examples can be realized within the model

4.1. Run into a new known friend in a photo.

Harry and fred both belong in different environment. fred realizes that Harry and he both commented on Georges photo, so he decides to poke her to say hello: (fred, poke, Harry) The comments from Harry and fred are connected through Georges photo with two R2R relationships. freds policy says that he is free to poke his colleague commenter, while Harry allows her colleague commenter to poke her. The system provides many kinds of participating users (e.g. videos, comment, like, share, etc.) to poke each other.

4.2. View a tagged friends photo.

George and Alice are friends of Harry, but not friends of each other. Harry posted a photo and tagged Alice on it. Later, George sees the activity from his news feed and decides to view the photo: (George,read,Photo2).
In this example, George is trying to access a resource through his friend Alice. Whether his request can be granted or not depends on the corresponding policies from the target resource and the system. Here the Harry and Alices authorization policies are clearly in conict, which needs to be resolved. Conflict resolution system policy (read) says that owners policy takes precedence over tagged users, so the decision module will ignore Alices policy and only consider Harrys policy. A system may Conflict resolution system policy (read) with conjunction or disjunction of the owners and tagged users policies for different decisions.

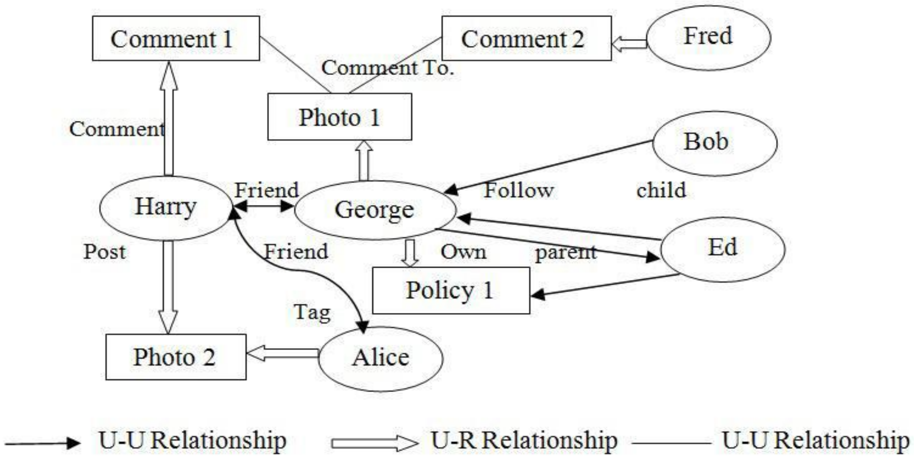


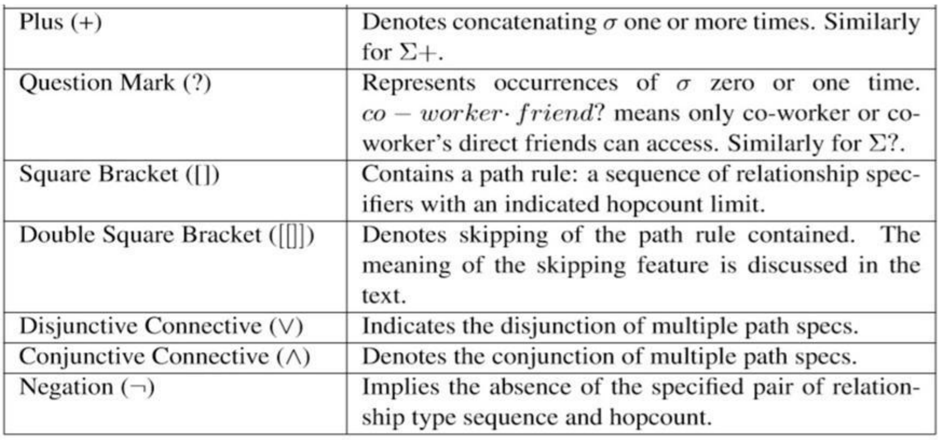
Fig. 3. A URRAC Sample Social Graph

4.3. Friend recommendation.

Harry is a friend of George, Bob follows George, while Harry and Bob are in the different environment. George would like to recommend Harry and Bob to be friends: (George, suggest friend, Harry, Bob) The access request contains Harry and Bob, so we need target user policies from both of them. Bob can suggest friends for his contacts within two hops. Harray welcomes friend recommendation from her direct friends, while Bob allows his friends of friends to do that.

4.4. Policy Specifications.

The different notations used in the policy specification language are show in Fig 4, this notations familiar with typical regular expression notation in the addition of hop count limits and skipping. There are several types of access control policies including accessing user policy, accessing session policy, target user policy, target session policy, object policy, and system specified policy. Here, system specified policies include authorization policies and conict resolution policies. While the user-specified authorization policies deals with the potential conicts of interest in the system-specified conict resolution policy.

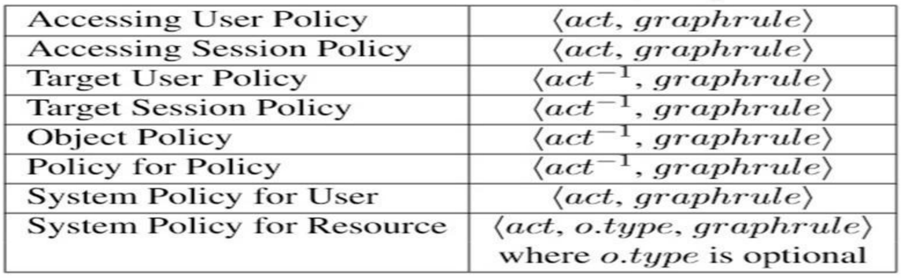


Plus (+)	Denotes concatenating σ one or more times. Similarly for $\Sigma+$.
Question Mark (?)	Represents occurrences of σ zero or one time. $co - worker \cdot friend?$ means only co-worker or co-worker's direct friends can access. Similarly for $\Sigma?$.
Square Bracket ([])	Contains a path rule: a sequence of relationship specifiers with an indicated hopcount limit.
Double Square Bracket ([[]])	Denotes skipping of the path rule contained. The meaning of the skipping feature is discussed in the text.
Disjunctive Connective ($\vee$)	Indicates the disjunction of multiple path specs.
Conjunctive Connective ($\wedge$)	Denotes the conjunction of multiple path specs.
Negation ($\neg$)	Implies the absence of the specified pair of relationship type sequence and hopcount.

Fig. 4. URRAC Policy Specification Notation

4.5. Policy Specifications.

Different formats of authorization policies are shown in Fig 5. Accessing User Policy and Accessing Session Policy are represented as a pair <act, graph rules> and control Behavior of how an access requester in access. Here, act represents the requested action and graph rule denotes the access rule based on social graph. Target User Policy, Target Session Policy, Object Policy are show how others can perform access on the target, so they use passive form act 1 rather than act because the target is always the entity to be accessed, whereas graph rule has the same meaning as in the previous policies.



Accessing User Policy	$\langle act, graphrule\rangle$
Accessing Session Policy	$\langle act, graphrule\rangle$
Target User Policy	$\langle act^{-1}, graphrule\rangle$
Target Session Policy	$\langle act^{-1}, graphrule\rangle$
Object Policy	$\langle act^{-1}, graphrule\rangle$
Policy for Policy	$\langle act^{-1}, graphrule\rangle$
System Policy for User	$\langle act, graphrule\rangle$
System Policy for Resource	$\langle act, o.type, graphrule\rangle$ where $o.type$ is optional

Fig. 5. URRAC Authorization Policy Representations

V. IMPLEMENTATION STATUS

In this section, we present some of the results obtained from our performance studies on the two path-checking algorithms. We implemented the algorithms in .net, and designed two sets of experiments to test the execution of an access request evaluation using algorithms. The social graphs to be tested are stored in sql server databases on the testing machine . We designed different policies and accessing requests that would require the access control decider to gather necessary information and measured the time take to complete a path checking over the graph and return a result to the decider.

VI. PERFORMANCE MEASURES

When designing the experiments, we take into account two parameters of the graphs: hop count (depth) and degree (width). Although the total number of nodes in the system may influence the performance and scalability of graph systems, in our system not to explore the whole graph but the paths with limited hops stemming from one node. Therefore, the all nodes are not important with respect to the performance. In fact, it is the hop count limit and the number of edges to be explored at each hop that contribute most to the size of the problem, and hence the performance of our system.

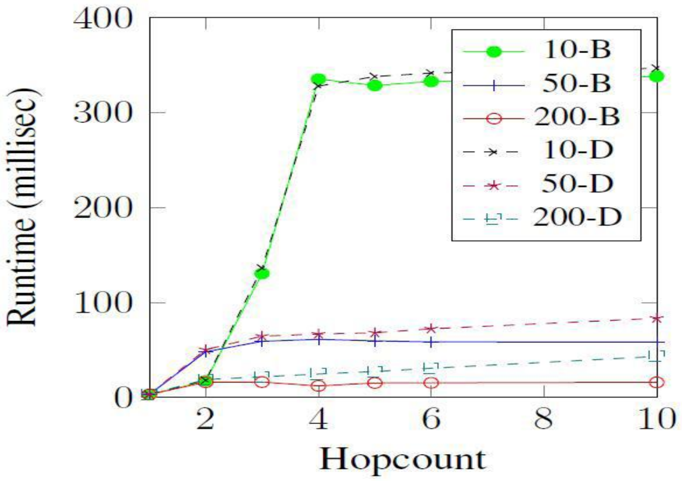


*Fig. 6. True-case scenarios: *-patterns*

Figure 6 illustrates the results of the first set of experiments. We compare the BFS and DFS algorithms using policies with different hop count limits in both the true-case and false case scenarios. shows how the average running time changes with respect to increase in hop count limit. To make a more comprehensive comparison, in this particular test, we apply the following values 10, 50 and 200 to the number of neighbors for each user. *-pattern paths are known to be more flexible than enumeration paths in path-checking.

As shown in Figure 7, when hop count limit increments, the time cost by the BFS algorithm increases significantly, due to the fact that it will not take the next hop without finishing search on all edges at the current level; whereas a greater hop count does not worsen the performance of the DFS algorithm

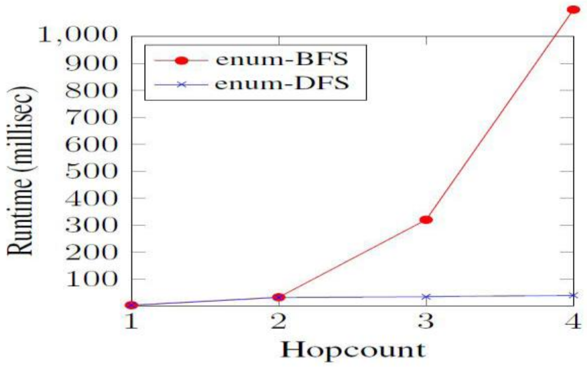


Fig. 7. True-case scenarios: enum-patterns

VII. CONCLUSION

In this paper work, we proposed a U2U relationship-based access control (UURAC) model for OSNs based on policy specification language as a regular expression, which gives greater generality and exibility in policy specification than prior models did. Due to the sparseness nature in social graph, given the constraints on relationship types and hop count limit, the complexity of the algorithms can be reduced. We also further included U2R and R2R relationships in policies and developed URRAC model that provides near grained access control for users usage and administrative access. Specially, we introduced the skipping of some relationship path expression in policy specification in order to offer more expressive policies. The decision modules of the system determine authorizations by retrieving different policies from the access session, the target and the system, and then making a collective decision. Conict resolution policies are applied to address policy conicts

To improve the versatility of ReBAC, it is possible to capture some unconventional relationships found in OSN systems, including temporary relationships and one-to-many relationships. The attribute-aware ReBAC model also needs to be adjusted accordingly to express the attributes of such new relationships. we considered system-specified conict resolution policy to resolve conicts between authorization policies. Since the system is the only one responsible for making policy, such conict resolution will be unambiguous and will not conict with itself. A further potential area of research is to design user specified conict resolution policy. This would allow more exible and near-grained control, as the policy is specified by users and applies to a smaller context.

REFERENCES

[1] Hongyu Gao, Jun Huang, Jingnan wang, and Yan chen, security issuesin online social network.Internet computing, IEEE 2011.

[2] J. park.R.Sandhu and Y.cheg A user- activity-centric framework for access control in online social networks. Internet computing IEEE, sep-oct 2011.

[3] David F. Ferraiolo, D,Richard Kahn and Ramaswamy chandramouli. Role-Based Access Control Artech house 2nd edition 2007.

[4] Evangelos Aktoudianakis, Jason Crampton, Steve Schneider, Helen Treharne, and Adrian Waller.Policy temp lates for relationship-based access control. In Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, pages 221228. IEEE, 2013.

[5] Philip W L Fong, Mhd Anwar and Zhen Zhao. A privacy preservation model for face-book-style social network system, in computer security, springer 2009.

[6] Philip W L Fong, Relationship based access control : protection model and policy language ACM, 2011.

[7] Philip W L Fong and Ida Siahaan. Relationship-based access control policies and their policy languages. In Proceedings of the 16th SACMAT, pages 5160. ACM, 2011.

[8] Barbara Carminati, Elena Ferrari, and Andrea Perego. Enforcing access control in web-based social networks. ACM Transactions on Information and System Security (TISSEC), 13(1):6, 2009.

[9] Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantar cioglu, and Bhavani Thurai singham. A semantic web based framework for social network access control. In Proceedings of the 14th SACMAT, pages 177186. ACM, 2009.

[10] Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantar cioglu, and Bhavani Thurai singham. Semantic web-based social network access control. Computers and security, 30(2):108115, 2011.

[11] Maeve duggan and Aaron smith. Pew internet Report 2016 and social media update 2013.

[12] Hongyo Gao, jun Hu, Tuo Huang, Jingna Wang and Yan Chen . Security issues in online social networks. Internet computing threads IEEE 2011.

[13] Danah m. Boyd and Nicole B.Ellison social network sites: Definition, history and scholarship. Journal of computer-Mediated communication 2007.

[14] Philip W L Fong relationship based access control: protection model and policy language. In proceedings of the first CODASPY ACM, 2011.

[15] Philip W L Fong and ida siahaan. Relationship-based access control policies and their policy languages. In proceeding 16th SACMAT ACM,2011