# Access Control Framework For Social Networking Systems Based On Present Access Control Policies

**Vipin Kumar**[1],

[1]Krisha Institute of Engineering & Technology,

Ghaziabad, 201206,

[1] Ph. D Scholar of Shri Venkateshwara University

Gajraula, J. P. Nagar (UP)

**Dr. Sachin Kumar**[2]

[2]AKG Engineering College,

27th KM stone, Delhi Hapur Bypass Road,

Ghaziabad,

## ABSTRACT:

Social Networking System (SNS) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month. To protect user data, access control has become a central feature of OSN. In order to protect OSN this paper is going to suggest access control framework for social networking systems based on presently available access control model like DAC, MAC, Rule-BAC, Role-BAC, etc.

**Keywords:** SNS, OSN, PL, ACPMPL, PPACP, PPACIE

## I. INTRODUCTION

Currently, web 2.0, advancement of web1.0, is used. Web 2.0 is also called Wisdom Web, people centric web, participative web and read/write web. Web 1.0 deals with static pages produced through HTML while Web 2.0 uses concept of interactivity. Content creation and its sharing is the core of Web 2.0 while Social networking web sites are the extension for Web 2.0 and journey toward Web 3.0 or semantic web. Social Networking System (SNS) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, unprecedented growth in the application of OSNs was observed.. To protectuser data, access control has become a central feature of OSNs

The access control mechanism provides a security approach which permits the authorized user to access the resources and refuses to provide services to non-authorized user [1]. The access control mechanism is the necessary part for various social networking systems (SNS). There are many access control mechanisms available which are described from different aspects, such as RBAC [2], TBAC [3], ABAC [4], and so on.

The RBAC model has been used the most widely due to its flexibility, fine-grained control ability and strong usability, and it introduces roles to decouple users and permissions. Some scholars research the ontology-based RBAC model, but the discussion has only been limited to the RBAC model. The TBAC method models from the tasks in workflow and dynamically manages the permissions through tasks and tasks' status through introducing the context into the access control mechanism [3].The ABAC model annotates the access subject and emissions according to attributes, and the attributes can be considered the generic knowledge which describes the access subjects and permissions.

Various kinds of access control models have provided the security strategies from different aspects, but they can be described as a unified access control model using ontology technology. In this paper, we propose a generic access control framework for social networking system that is most popular now a days as a Facebook, Twitter, & Orkut format and the details are organized.

In Section II we have introduces the impotence of access control framework for SNS, which is the base for the discussion. In Section III we have discussed the related works done in the field of access control framework for SNS; In Section IV we have discussed about proposed generic access control working framework for SNS. This framework is dividing into various layers as explain in section IV; In Section Vwe have discussed about thefuture scope of the research; and at the last Section VI concludes this paper.

## II. IMPOTENCE OF ACCESS CONTROL FRAMEWORK

Over the past decade, online social networks have witnessed phenomenal growth in popularity to an extent that today two thirds of the world's Internet population participates in some form of online social networking. [Nielsen, 2009] This large audience spends a significant amount of time both viewing existing information and contributing new information to the social web. In regards with member communities such as Facebook, MySpace, Orkut, Twitter, and LinkedIn, the data generated is stored with the relevant social network service providers. This data, which is mainly a representation of real life of the members, includes pictures, videos, educational and work profiles, personal contact information, and list of friends and acquaintances. While networking online presents obvious benefits to users, the flaws of the current model of centralized online social networks is raising concerns. The two major issues with the centralized system are emergence of "information silos" which are closed to the outside web and even other social networks as well as lack of user control over dissemination of personal information; a major privacy concern. To solve above mentioned problems, proper access control model or framework is required, but so far present access control models are not according to the need of social networking system. My approach in this paper is to proposed generic access control framework for social networking system based on presently available models.

## III. RELATED WORKS

There are many different approaches and mechanisms for controlling access on online social network, e.g. Discretionary access control (DAC) [5], Mandatory access control (MAC)[5], Role-Based access control (RBAC) [6, 7], Attribute-Based access control [8], etc. Each approach has its own advantages, disadvantages and feasibility scope. Some researchers have tried to combine different access control mechanisms to build more powerful models.

The study of access control mechanisms in Cooperative Systems is not new and was in existence since the birth of e-Collaboration tools in 1980s. Shen et al. [9] studied access control mechanisms in a simple collaborative environment, i.e. a simple collaborative text editing environment.

Zhao [10] provides an overview and comparison of three main access control mechanisms in collaborative environments.

Tolone et al. [11] have published a comprehensive study on access control mechanisms in collaborative systems and compare different mechanisms based onmultiple criteria, e.g. complexity, understandability, ease of use.

Jaeger et al. [12] present basic requirements for role-based access control within collaborative systems.

Gutierrez Vela et al. [13] try to model an organization in a formal way that considers the necessary elementsto represent the authorization and access control policies.

Kern et al. [14] provide architecture for role-based access control to use different rules to extract dynamic roles.
Alotaiby et al. [15] present a team-based access control which is built upon role-based access control.

Periorellis et al. [16] introduce another extension to role-based access control which is called task-based access control. They discuss task-based access control as a mechanism for dynamic virtual organization scenarios.

Toninelli et al. [17] present an approach towards combining rule-based and ontology-based policies in pervasive environments.

Demchenko et al. [18] propose an access control model and mechanism for grid-based collaborative applications.

Massa et al. [19] use the dataset from Epinions.com to do computational experiments on employing global versus local trust metrics. They study the implications of controversial users in product rating community.

Role-based access control (RBAC) is being increasingly recognized as an efficient access control mechanism that facilitates security administration [20]. It can be seen as a newer alternative approach to mandatory access control (MAC) [21] and discretionary access control (DAC) [22], so in other words, RBAC enforces DAC and MAC [23]. RBAC has been proposed as an alternative approach to this traditional access control mechanisms both to simplify the task of access control administration and to directly support function-based access control [24]. Furthermore, it has been recently approved as a standard by the American National Standards Institute (ANSI) and a number of organizations are today applying this standard in specialized domains [25].

A key advantage of the RBAC model is that it simplifies authorization administration by assigning permissions to users through roles. Thus, it adds a layer of abstraction between users and their permissions [26]. RBAC groups individual users into roles that relate to their position within an organization and assigns permission to various roles according to their stature in the organization [27]. Separation of duty and dependence constraints are examples of dynamic constraints and required in most commercial applications, including digital government, E-commerce, healthcare systems, and workflow management systems that can be addressed by using RBAC [28]. As a result of this, today, the RBAC model is one of the most established access models [29]. Because of its relevance, RBAC hasbeen widely investigated and several extensions to it as well as possible applications have been proposed, including TRBAC [30], W-RBAC [31] and GeoRBAC [32] to cite just a few.

New technologies such as Web services or Semantic Web increase the complexity and the dependencies of < [34] because it can define a diverse set of access control policies [35]. Thus, the adaptation of RBAC to new technologies has been a common starting point. As a result access control frameworks have been evolving from OASIS XACML (Extensible Access Control Markup Language) [36] or X-RBACwhich were based on XML to describe the access rights and lacked on machine interpretation; to O-RBAC [37] that adapts RBAC tosemantic webtechnologies by exporting its domain to an ontology specification.

The purpose of this research paper is to design generic access control framework based on presently available access control policies like DAC, MAC, and RBAC etc.

## IV. ACCESS CONTROL WORKING FRAMEWORK

This proposed access control framework is completely based on innovative idea that came in mind after studying related work in this area. OSN (Online Social Network) User is the actor in this framework that interacts with the other OSN Users that may be friends, relatives or unknown users of same SNS (Social Network System).

Web Interface is the second part of this framework that is sub-divided into three parts Authentication, Session and ACPMPL (Access Control Policy Management Programmed Logic). User login is handles by Authentication part and Session management for each individual user is performed in Session part and ACPMPL is the advanced program logic using any server side programming languages like ASP, ASP.NET, JSP, PHP, and etc. for managing PPACP [38] (Parameterized Programmed Access Control Policy).

PPACP [38] layer is responsible to select useful access control model on the basis of parameter that passes from upper layer ACPMPL to PPACP layer. This parameter decides which access control model have to use among presently available model like DAC, MAC, RBAC, X-RBAC, O-RBAC and etc.

PPACIE (Parameterized Programmed Access Control Inference Engine) layer is interface between SNS Database and PPACP to fetch data from SNS Database and pass data to PPACP layer or vice-versa.

SNS Database is RDBMS database that store data related to elements and relations, such as a set of roles, a set of users, a set of permissions, and relationships between users, roles, permissions and etc.

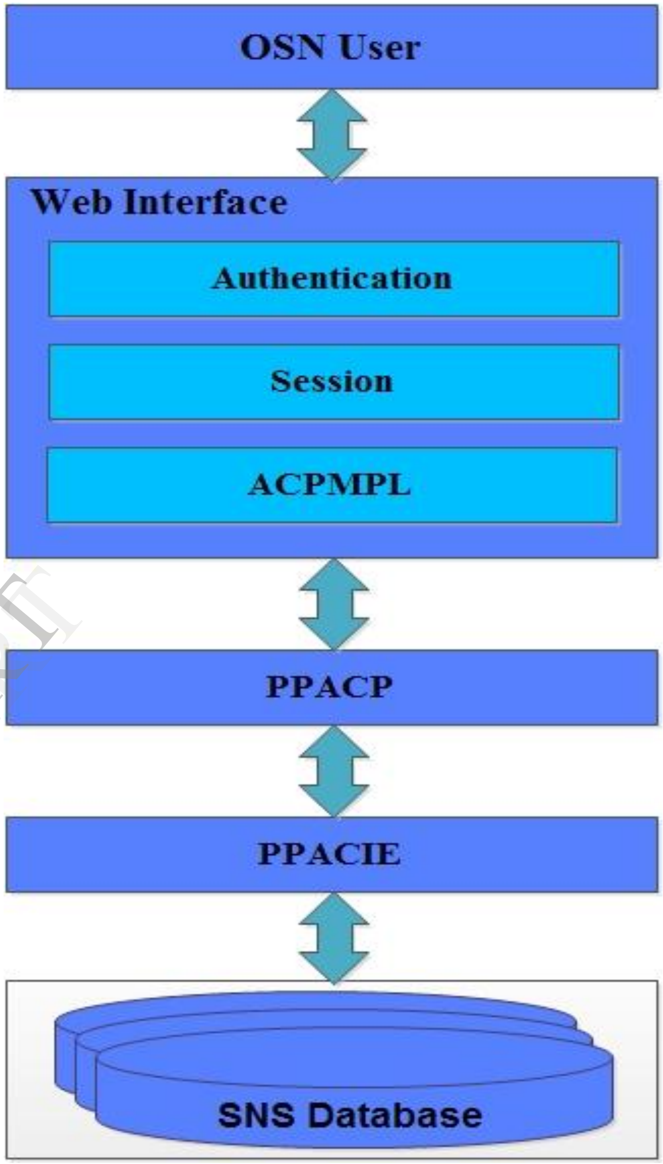

**Fig 1: Proposed Access Control Framework**

## V. CONCLUSION AND FUTURE SCOPE

Online social networking web sites are part of our day to day life now a day; right now we are living in Web 2.0 era and going toward Web 3.0. There various access control models for social networking systems, but not cent percent suitable for it. The proposed framework for access control model can bring the revolution in the field of Social Networking System for Web 2.0 and it can be implemented using presently available access control model. In future, we will propose multi-agent based access control model using semantic web technologies for Web 2.0 as well as for Web 3.0.

## VI. REFERENCES

[1] Long Qin, Liu Peng, Pan Aimin. Research and Implementation of an Extended Administrative Role-Based Access Control Model (1).Journal of Computer Research and Development.2005, 42(5):868- 876.

[2] HUANG Jian, QING Si-Han, WEN Hong-Zi. Timed Role-Based Access Control [1].Journal of Software.2003, 14(11):1945-1954.

[3] DENG Ji-Bo, HONG Fan. Task-Based Access Control Model [J). Journal of Software.2003, 14(1):77- 82.

[4] Ll Xiao-feng, FENG Deng-guo, CHEN Zhao-wu,etal. Model for attribute based access control [J). Journal on Communications.2008, 29(4):90-98.

[5] http://wikipedia.org

[6] Ferraiolo, D.F., Kuhn, D.R.: Role Based Access Control. in 15th National Computer Security Conference. 1992.

[7] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-Based Access Control Models. IEEE Computer, 1996. 29(2): p. 38-47.

[8] Kolter, J., Schillinger, R., Pernul, G.: A Privacy-Enhanced Attribute-Based Access Control System. inDBSec. 2007: Springer.

[9] Shen, H., Dewan, P.: Access Control for Collaborative Environments. in Computer- Supported Cooperative Work Conference. 1992: ACM Press.

[10] Zhao, B.: Collaborative Access Control, in Seminar on Network Security. 2001.

[11] Tolone, W., Ahn, G., Pai, T., Hong, S.: Access control in collaborative systems. ACM Computing Surveys, 2005. 37: p. 29-41.

[12] Jaeger, T., Prakash, A.: Requirements of role-based access control for collaborativesystems, in 1st ACM Workshop on Role-based access control. 1996: ACM Press.

[13] Gutierrez Vela, F.L., Isla Montes, J.L., Paderewski, P., Sanchez, M.: Organization Modelling to Support Access Control for Collaborative Systems, in Software Engineering Research and Practice. 2006.

[14] Kern, A., Walhorn, C.: Rule support for role-based access control, in 10th ACM symposium on Access Control Models and Technologies. 2005: ACM Press
.

[15] Alotaiby, F.T., Chen, J.X.: A Model for Team-based Access Control, in International Conference on Information Technology: Coding and Computing. 2004: IEEE Computer Society.

[16] Periorellis, P., Parastatidis, S.: Task-Based Access Control for Virtual Organizations, in Scientific Engineering of Distributed Java Applications. 2005.

[17] Toninelli, A., Bradshaw, J., Kagal, L., Montanari, R.: Rule-based and Ontology-based Policies: Toward a Hybrid Approach to Control Agents in Pervasive Environments, in Semantic Web and Policy Workshop. 2005.

[18] Demchenko, Y., Gommans, L., Tokmakoff, A., van Buuren, R.: Policy Based Access Control in Dynamic Grid-based Collaborative Environment, in International Symposium on Collaborative Technologies and Systems. 2006: IEEE Computer Society.

[19] Massa, P., Avesani, P.: Trust Metrics on Controversial Users: Balancing Between Tyranny of the Majority and Echo Chambers. International Journal on Semantic Web & Information Systems, 2007. 3(1): p. 39-64.

[20] Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E., Role-Based Access Control Models, IEEE Computer 29 (2) (2000) 38–47.

[21] Joshi, J.B.D., Access- Control language for multidomain environments, IEEE Internet Computing 8(6) (2004) 40-50.

[22] Bell, D. E. &LaPadula, L. J., Secure computer system: unified exposition and MULTICS. Technical Report ESD-TR-75-306, The MITRE Corporation, Bedford, MA, 1976.

[23] Lampson, B. Protection. In Proceedings of the 5th Symposium on Information Sciences and Systems (Princeton, NJ, Mar.) 1974, 437–443
.

[24] Osborn, S., Sandhu, R. and Munawer, Q., Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies, ACM Transactions on Information and System Security 3(2) 2000, 85- 106.

[25] Bertino, E. RBAC models — concepts and trends. Computers & Security 22(6) (2003) 511- 514.

[26] Damiani, M.L., Bertino, E. and Perlasca, P., Data security in location- aware applications: an approach based on RBAC, International Journal of Information and Computer Security 1(1/2) (2007) 5-38.

[27] Bhatti, R., Bertino, E., Ghafoor, A. and Joshi, J.B.D., XML Based Specification for Web Services Document Security, IEEE Computer 37(4) (2004) 41-49.

[28] Wainer, J., Kumar, A. and Barthelmes, P., DW- RBAC: A formal security model of delegation and revocation in workflow systems, Information Systems 32(3) (2007) 365-384.

[29] Shafiq, B., Joshi, J.B.D., Bertino, E. and Ghafoor, A., Secure Interoperation in a Multidomain Environment Employing RBAC Policies, IEEE Transactions on Knowledge and Data Engineering 17(11) (2005) 1557-1577.

[30] Breu, R., Popp, G. and Alam, M., Model based development of access policies, International Journal on Software Tools for Technology Transfer, 9(5) (2007) 457, 470.

[31] Bertino, E., Bonatti, P. and Ferrari, E., TRBAC: a temporal role- based access control model, ACM Transactions on Information and System Security, 4(3) (2001) 191–233.

[32] Wainer, J., Barthelmess, P. and Kumar, A., W- RBAC a workflow security model incorporating controlled overriding of constraints, International Journal of Cooperative Information Systems, 12(4) (2003) 455- 485.

[33] Damiani, M.L., Bertino, E., Catania, B. and Perlasca, P., GeoRBAC: A Spatially Aware Rbac, ACM Transactions on Information and System Security 10(1) (2007).

[34] Sohr, K., Drouineaud, M., Ahn,G.J. and Gogolla, M., Analyzing and Managing Role-Based Access Control Policies. IEEE Transactions on Knowledge and Data Engineering 20(7) (2008) 924-939.

[35] Joshi, J.B.D., Aref, W.G., Ghafoor, A., Spafford, E.H., Security Models for Web- Based Applications, Communications of the ACM 44(2) (2001) 38-72.

[36] Moses, T., OASIS eXtensible Access Control Markup Language 2.0, core specification. OASIS XACML Technical Committee StandarD, 2005.

[37] Wu, D., Chen, X., Lin, J. & Zhu, M., Ontology- Based RBAC Specification for Interoperation in Distributed Environment. First Asian Semantic Web Conference, Beijing, China, September 3-7, 2006, pp. 179-190.

[38] Amit Kumar, Prof. (Dr.) A K Singh; Ontology Based Multi Agent ELearning Model; International Conference on Issues and Challenges in Networking, Intelligence and Computing Technologies, 2-3 September 2011; Page(s): 845-847.