Access Control Framework for Social Network System using Ontology

Vipin Kumar
Krishna Institute of Engineering & Technology,
Ghaziabad, 201206,
Ph. D Scholar of Shri Venkateshwara University
Gajraula, J. P. Nagar (UP)

Sachin Kumar, Ph.D
AKG Engineering College,
27th KM stone, Delhi Hapur Bypass Road,
Ghaziabad,

ABSTRACT
In recent years, we have seen unprecedented growth in the area of Online Social Networking (OSN) that is still keeping on day by day. Social networking websites such as Facebook, Google+, and Twitter are using widely by people to share personal and public information with friends, coworkers, colleagues, family and even with strangers .Facebook, one of the most popular social network sites, has million of active users and billions of pieces of content or data that use daily like web links, news stories, blog posts, notes, photo albums, etc. shared each month. To protect such kind for huge or big data or information need more secured and flexible access control model. There are so many access control policies are available for controlling online social network, but all social networking sites like Facebook or Twitter has their own access control mechanism that is not standard and still not more secured or flexible. To protect such kind of publically oriented user data need more dynamic access control model. In order to protect OSN, in this paper an innovative or dynamic access control framework for social networking systems using semantic web ontology has been proposed which addresses the protection of semantic-rich information in a knowledge base ontology

Keywords
SNS, MABOM, TBAC, ABAC, RBAC

1. INTRODUCTION
Now a days we are using Internet 2.0, advancement of web1.0. 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 websites such as Facebook, Google+, and Twitter are designed to enable people to share personal and public information with friends, coworkers, colleagues, family and even with strangers. In recent years, unprecedented growth in the application of OSNs was observed. To protect user data in such types of sites, 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, an innovative or dynamic access control framework for social networking systems using ontology has been proposed which addresses the protection of semantic-rich information in knowledge base ontology

This paper is partitioned in 8 sections; Section 1 is the introduction to the problem. Section 2, introduces the impotence of access control framework for SNS, which is the base for the problem. Section 3 shows the importance of the related works done in the field of access control framework for SNS. Section 4 shows and explain about the presently running Access Control Framework architecture.

Section 5 propos an innovative or dynamic access control framework for social networking systems using ontology which addresses the protection of semantic-rich information in knowledge base ontology

Section 6 shows and explain the proposed prototyped SNS Ontology, This section also used to explain the classes' relationship diagram, relationship among classes and individuals, and assertions implemented in SNS Ontology by using world known software Protégé.

Sections 7 explain about the future scope of the research and conclusion of the paper. And at last Section 8 shows all references used in this paper

2. 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 online social networking presents

obvious benefits to users, the flaws of the current model of centralized online social networks are 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 propose an access control framework using ontology for social networking system.

3. 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 (ABAC) [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 on multiple 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 elements to 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. It can be seen as a newer alternative approach to mandatory access control (MAC) and discretionary access control (DAC), so in other words, RBAC enforces DAC and MAC. 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. 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.

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. 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. 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.

As a result of this, today, the RBAC model is one of the most established access models. Because of its relevance, RBAC has been widely investigated and several extensions to it as well as possible applications have been proposed, including TRBAC [20], W-RBAC [21] and GeoRBAC [22] to cite just a few.

New technologies such as Web services or Semantic Web increase the complexity and the dependencies, because it can define a diverse set of access control policies. 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) [23] or X-RBAC which were based on XML to describe the access rights and lacked on machine interpretation; to O-RBAC [24] that adapts RBAC to semantic web technologies by exporting its domain to an ontology specification.

The purpose of this research paper is to design an innovative access control framework using semantic web ontology.

4. PRESENTLY RUNNING ACCESS CONTROL FRAMEWORK ARCHITECTURE

There are many ways to represent presently using access control framework architecture, here figure 1 use to represent currently running access control framework architecture, in this architecture user is the actor that make request to SNS using Internet via Web Browser as shown in figure 1. Web Browser is the user interface that used by user to interact with SNS.

SNS represents social networking websites like Facebook, Orkut, and Twitter etc. that directly make connection with database managed by DBMS or RDBMS. This interaction between database layer and SNS may be implemented using Client/Server architecture or distributive DBMS architecture

And at last Database layer represent the data or Meta data used in SNS. This data may be stored using any database management software like MSSQL, Oracle, and MySQL etc.

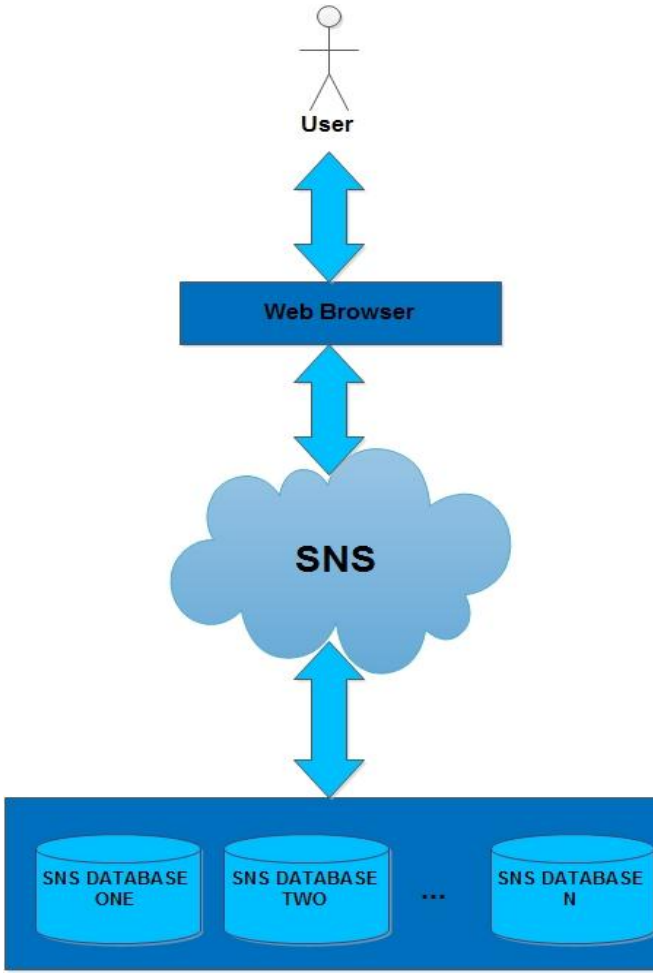

Figure 1: Present SNS Model

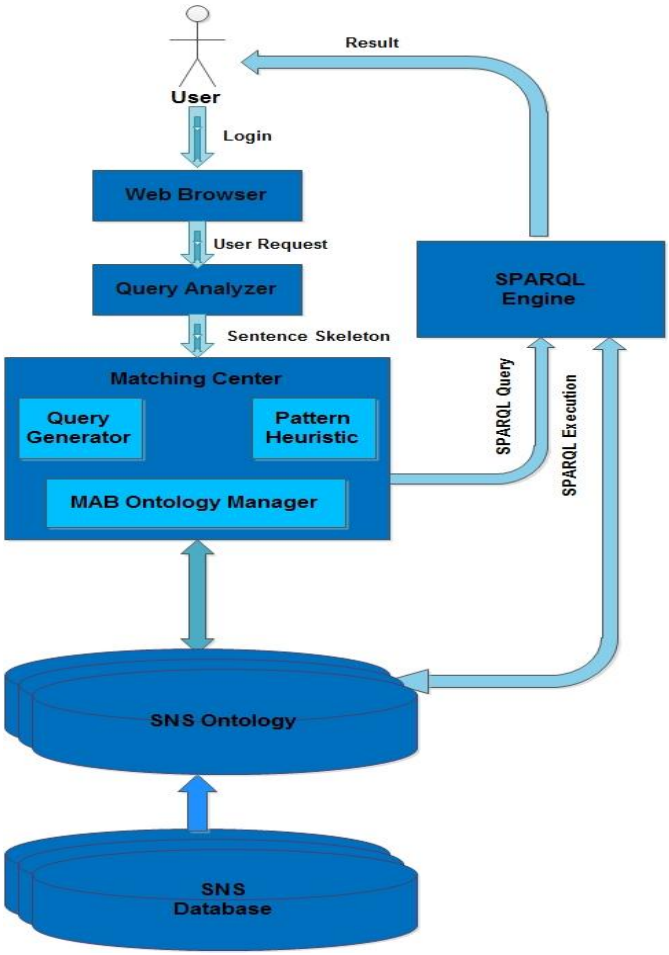

Figure2: Proposed Access Control Framework

This approach is very simple or straight forward that have less flexibility or security which is more suitable for Web 2.0, but may not be suitable for Web 3.0 or Semantic Web (third generation web).

In this paper, we purposed a new access control framework which is more suitable for Semantic Web environments

5. PURPOSED ACCESS CONTROL FRAMEWORK ARCHITECTURE

This proposed access control framework is completely based on innovative idea that came in mind after studying related work in the area of OSN (Online Social Network)

User is the actor in this framework that interacts with the other OSN Users via web browser that may be friends, relatives or unknown users of same SNS (Social Network System) on Internet.

Query Analyzer Interface gets request from user via Internet and send request to Multi-agent based Ontology Manager in sentence skeleton form. On the base of sentence skeleton send by query analyzer, MABOM generate query using query generator and pattern heuristic and then send that query to SPARQL engine

SPARQL is a recursive acronym for the SPARQL Protocol and RDF Query Language. SPARQL is a structure query language for RDF as SQL is a structure query language for DBMS or RDBMS. SPARQL engine execute query send by MABOM from SNS Ontology and send result of that query to user that made request earlier for the specific query.

Ontology is a data model that represents knowledge as a set of concepts within a domain and the relationships between these concepts. In short Ontology is simply data management that why, here SNS Ontology represent semantic web ontology that have relationship, rules, assertions and regulation among classes, object properties, data properties and individual.

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.

6. SNS ONTOLOGY

6.1 Introduction

According to Thomas Gruber, Ontology is an explicit specification of conceptualization. It uses to represent knowledge, meta-data, rules and assertions.

For creating SNS Ontology, we have used Protégé; Protégé is a free, open source ontology editor and knowledge-based framework that is supported by a strong community of developers and academic, government and corporate users, who are using Protégé for knowledge solutions in areas as

diverse as biomedicine, intelligence gathering, and corporate modeling.

6.2 SNS Ontology Classes Graphical Representation

We propose Social Networking Systems Ontology (SNS Ontology) that models the key entities and their relationships that typically found in SNS; partly because we could not find an appropriate ontology representation in the literature that we studied. Based on this, we elaborate and discuss various scenarios regarding our proposed access control model. Note, however, that our access control model is not tied or limited to this specific ontology. It can be implements for any ontology.

The current version of the SNS Ontology comprises of 14 classes and 15 object properties. Figure 3 shows graphical representation of relationship among classes in SNS Ontology.

The Thing is the root class of all classes in SNS Ontology, with three immediate descendants classes are: DigitalObjects, Persons, and Events.

The DigitalObjects class models any object with digital properties. The Persons class models human users in the context of Social Networking. The DigitalObjects class is specialized by sub-classes such as Notes, Photos, Wall, and Annotation. The Notes class represents a textual content or data. The Wall class models the posting board on the homepage ofa currently login person, such as the one Facebook or Orkut provides. The Annotation class represents special digital objects that instead of directly representing a content, annotate one object (e.g., a wall, a photo, etc.) using another object (e.g., a textual comment, a person, etc.). The two objects are related to an annotation object, using properties Annotates and AnnotatesWith, respectively.

Annotation class itself is specialized by Comment, Tag, and WallPost. Comment class annotates an object with a note. PhotoPersonTagclass is a specialized tag that annotates a photo with a person. WallPost class annotates a wall with an object, e.g., a photo or video. We choose to represent annotation as a concept, rather than a relation, in order to be able to capture more semantics regarding it. For instance, it is usually important to know who has tagged a person in a photo; that might be different from the owner and the tagged person.

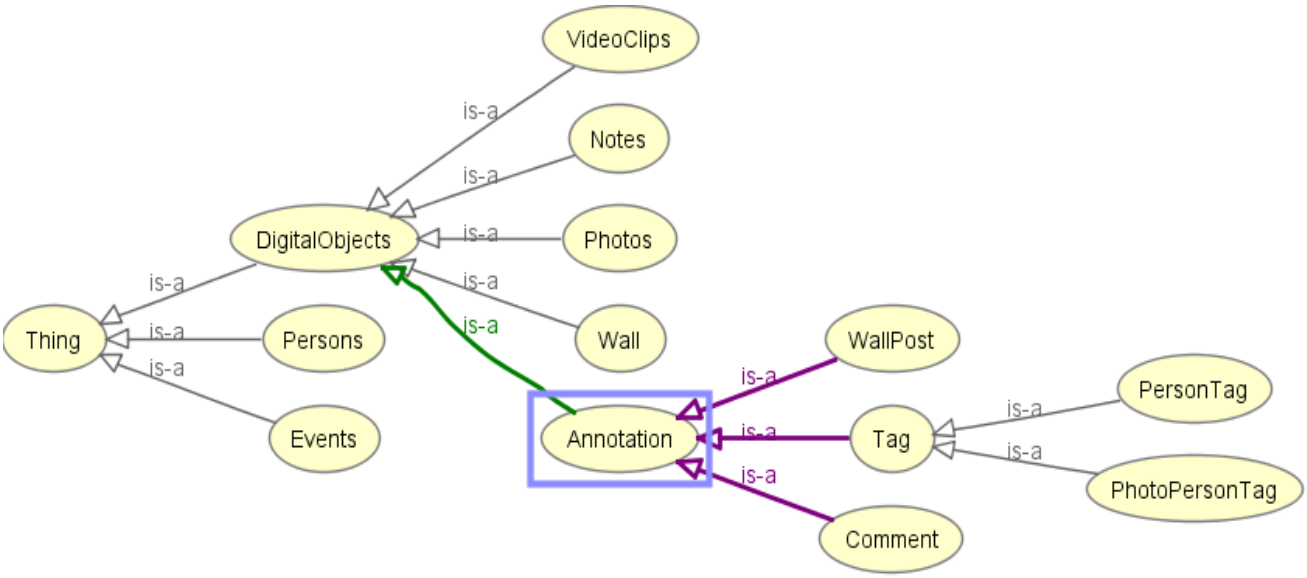

Figure 3: SNS Ontology Classes

6.3 SNS Ontology Graphical Representation

In this section, three figures are used to different perspective of this ontology. Figure 4 shows OntoGraph representation to show relationships among classes and objects. Figure 5 shows the OntoGraph representation to show the annotation or rules implemented in ontology & at last but not the least Figure 6 shows OntologyNavigOwl graphical representation to show node in proposed ontology designed. All these figures show that in this Ontology models, there are 14 classes, 24 individuals & each class have 4 individuals. Comment class has 4 individuals like comment1, comment2, comment3 & comment4. Event class has 4 individuals like event1, event2, event3 & event4. Notes class has 4 individuals like note1, note2, note3 & note4. Persons class also has 4 individuals like person1, person2, person3 & person4. Photos class has 4 individuals like photo1, photo2, photo3 & photo4 and at last VideoClips class has 4 individuals like video1, video2, video3 & video4. Figure 4 also shows relationships and assertions among all classes and individuals used in SNS Ontology

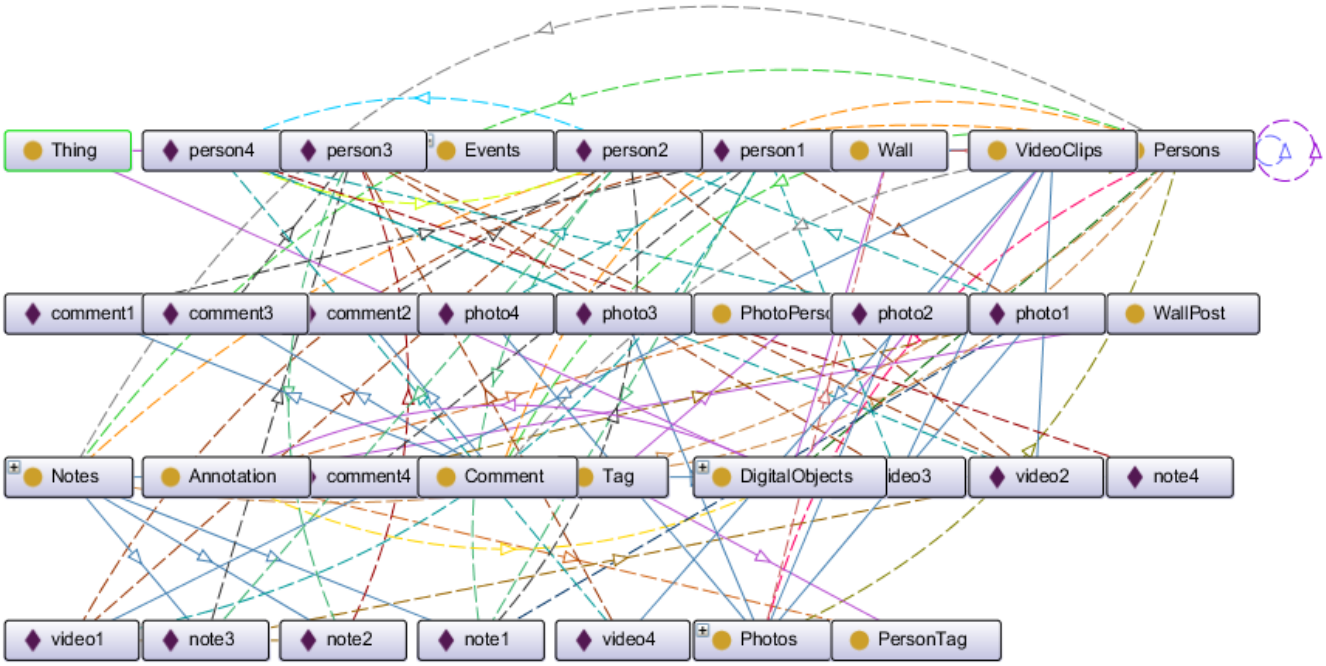

Figure 4: SNS Ontology OntoGraph Representation

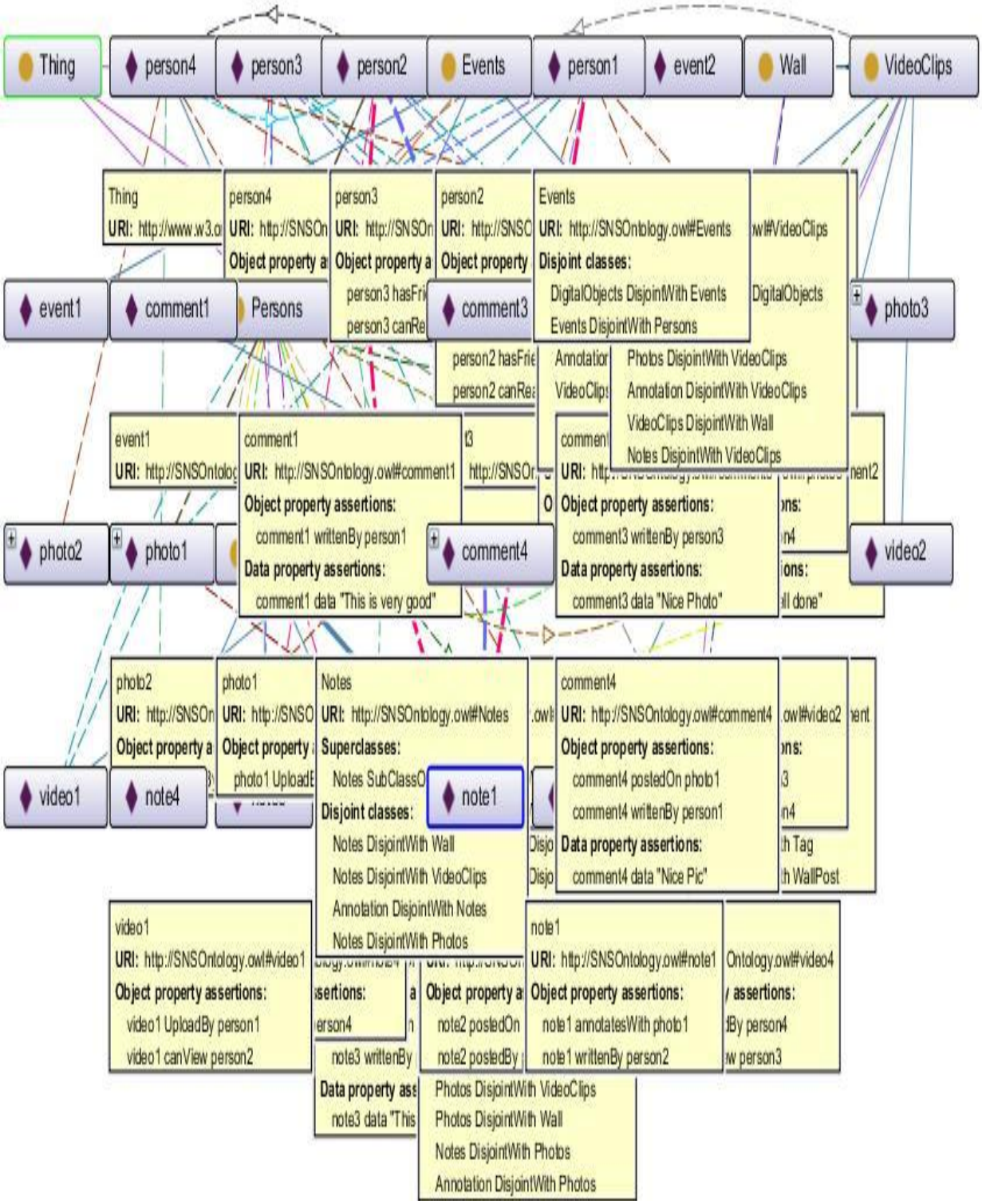

Figure 5: SNS Ontology Annotations Representation

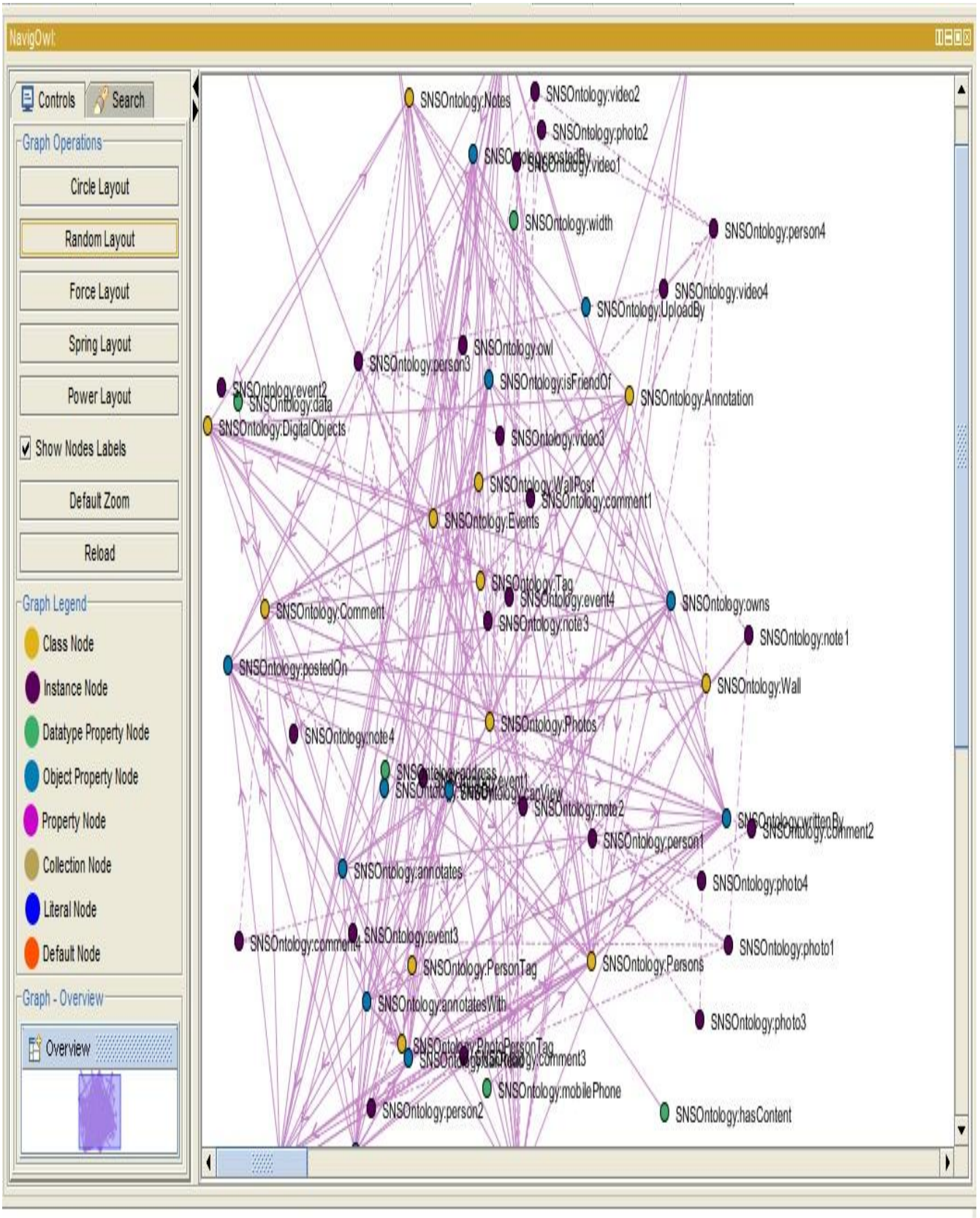

Figure 6: SNS Ontology NavigOwl Representation

6.4 Rules or Assertions Used In SNS Ontology

In this ontology we have asserted 34 rules as prototyped just for running this access control framework model. In this paper we have used RDF format to represent our rules. Resource Description Framework (RDF) is a framework for representing information about resources in a graph form. Since it was primarily intended for representing metadata about WWW resources, it is built around resources with URI.

Information is represented by triples **subject-predicate-object** in RDF. Table 1 show the assertions or rules implemented in this ontology.

S.NO	ASSERTIONS in P(S,O) Format
1	writtenBy(comment1, person1)
2	writtenBy(comment2, person2)
3	writtenBy(comment3, person3)
4	writtneBy(comment4, person1)
5	postedOn(comment4,photo1)
6	writtenBy(note1,person1)
7	annotatesWith(note1, photo1)
8	postedOn(note2,video1)
9	postedBy(note2,person3)
10	postedOn(note3,video2)
11	writtenBy(note3,person3)
12	postedBy(note4,person4)
13	canRead(person1,note1)
14	canView(pserson1,photo1)
15	canView(person1,video1)
16	canRead(person2,note1)
17	canView(person2,video2)
18	hasFriend(person2,person4)
19	canRead(pserson2,note3)
20	canRead(person3,note2)
21	hasFriend(person3,person1)
22	isFriendOf(person4,person2)
23	uploadBy(photo1,person2)
24	uploadBy(photo2,person4)
25	uploadBy(photo3,person4)
26	uploadBy(photo4,person1)
27	uploadBy(video1,person1)
28	canView(video1,person2)
29	uploadBy(video2,person4)
30	canView(video2, person3)
31	uploadBy(video3,person1)
32	canView(video3,person3)
33	uploadBy(video4,person4)
34	canView(video4,person3)

Table 1: SNS Ontology Assertions

7. CONCLUSION AND FUTURE SCOPE

In this paper, we have proposed an innovative access control framework for SNS using ontology, an ontology based access control model based on Semantic Web standards that empowers the individual users of a social networking system to express fine-grained access control policies on their related information. We proposed prototype ontology for SNSs to further demonstrate our approach. The key idea in this model is to express the policies on the relations among concepts in the social network ontology. We have also implemented a framework prototype of the proposed model in order to show the applicability of our approach. Although this model provides powerful access control features to the users of the SNSs, even savvy users of such systems should not have to be able to compose access control policy rules manually. An SNS employing this framework may simply provide a user interface similar to the current practices, but with more flexible options to its user; then, provide the access control engine with policy rules corresponding to the user choices.

In future research, we will explore ways to improve this aspect in our implementation, and theoretically analyze the complexities introduced by ontological data and each policy component; we are also going to test this ACF (Access Control Framework)in Java language based on Jena Semantic Web Framework for proper authenticity.

8. RESULAT ANALYSIS

We have conducted this test on the access control engine by submitting SPARQL queries on Protégé. The engine successfully returns only the authorized information that is expected according to the sample access control policy rules. We also developed a data generator that randomly populates SNS ontology. Table 1 shows the performance results of the prototype access engine based on the following input parameters: the number of users, friendship links, photos, and maximum number of people had been tagged in a photo. Since the inference engine that Protégé provides only works in memory, we were not able to run the experiment for very large ontologies. Our experiments show that the first access control inference is relatively expensive. However, subsequent access checks are performed almost instantaneously. This is because in the first round the inference model caches some of the inferred axioms, which enhances performance for subsequent inference. In fact, the first access check can be considered as part of the initialization phase, which can be triggered with a dummy access request.

Table1: Prototype Performance Results

Data Generation Parameters				Access Times (in second)		
User	Photo	Tag/ Photo	isFriendOf	Initial	First	Subsequent
20	6	6	50	2.3	0.4	0.004
50	30	10	150	4.8	36.0	0.004
80	60	20	180	6.2	176.2	0.006
110	70	20	210	12.4	2116.2	0.008
130	80	30	500	18.3	4321.8	0.008

8. REFERENCES

[1] Long Qin, Liu Peng, Pan Aimin. Research and Implementation of an Extended Administrative Role-Based Access Control Model. 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. Journal of Software.2003, 14(11):1945-1954.

[3] DENG Ji-Bo, HONG Fan. Task-Based Access Control Model. 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. 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 collaborative systems, 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] 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.

[21] 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.

[22] 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.

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

[24] 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.