INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue1)

Available online at: www.ijariit.com

Accessing Social Networking Sites using Semantic Web

Aamir Junaid Ahmad
Department of Computer Science & Engineering,
Maulana Azad College of Engineering & Technology
Patna, India.
aamir.junaid@yahoo.com

Sabina Priya Darshini
Department of Information Technology,
Birla Institute of Technology
Mesra, India.
sabinapriyadarshini@yahoo.co.in

Abstract— the popularity of Social Networking Sites (SNSs) has revolutionized human interaction. Social Networking Sites are means for people to have a social connection with other people with similar interests. A social networking site creates network communication among the user community. It stores user information which can be used for reaching people of similar interest. Though social networking site serves for communication purposes among special interest groups, they do not have a searching option where we can search people or group with certain features. A person can be searched only if we know the name of the person.

Here we present a method using Semantic Web to represent and process social network information so that user-queries can be better answered. This paper addresses some of the current limitations of accessing social network data and the semantic approach to overcome those limitations.

Keywords— SNS, KB, SKB, Ontology, Semantic Web, Social Web, Web Ontology Language OWL, RDF, JENA.

I. INTRODUCTION

Social Network Sites (SNSs) are platforms that allow people to publish details about themselves and to connect to other members with similar interests of the network. Improving the SNSs data access is the first step toward addressing the existing security and privacy concerns. Most of current SNSs implement very basic access control systems. SNSs make a user able to decide which personal information will be accessible by other members by marking a given item as public, private, or accessible by their direct contacts. Some online social networks, for example, Facebook support the option "selected friends" which is easy to be implemented, but they lack flexibility [1]. In fact, the available protection settings do not allow users to easily specify their access control requirements, furthermore, existing solutions are platform specific and they are hard to be implemented for various different online social networks.

To address some of these limitations, we propose an access control system based on semantic web technologies. Our main idea is to encode social network-related information by means of ontology. We suggest a model to represent user profile using semantic web ontology.

We model a Knowledge Base (KB) with ontology. The main advantage for using ontology for modelling SNS data is that relationships among many different social network concepts can be naturally represented using OWL and many inferences about such relationships could be done automatically. An access control mechanism can then be implemented by exploiting this knowledge. Security policies are defined as rules. The security settings of each user can be encoded by security policies by means of ontology, obtaining the Security Knowledge Base (SKB). Security policies are important because many users don't want their data to be accessed by others. As a result, the access control policies can be enforced by simply querying the authorizations, that is, the SKB. The query can perform by an SPARQL query and the ontology is serialized in RDF. In this paper, we model a social

network access control system using semantic web technologies. We also assume that a centralized reference monitor hosted by the social network manager can enforce the required policies. Our approach depends on extensible ontology which could be implemented to various online social networks by modifying the ontology in our KB. Semantic web tools allow us to define more fine-grained access control policies than the ones provided by current SNSs.

Organization

In Section 2 we present the objective of our work. In Section 3 we present other related work on Data Access Methods using Semantic Web. In Section 4 we discuss our methodology that will be used for data access using semantic web and the security enforcement for our model. In Sections 5 we discuss the architecture of our model. Finally we conclude this paper in Section6.

II.OBJECTIVE

The objective of this research is to make searching meaningful by using semantic web tools and technologies for creating more effective modern social networking websites. This will help the developers to create, reuse, and link profiles and contents on social media sites so that the users can get the best result of their complex queries.

Semantics can help social websites by using agreed upon semantic formats to describe people, content objects and the connections that bind them all together, social media sites can interoperate by appealing to common semantics. Developers are already using semantic technologies to develop the ways in which they create, reuse, and link profiles and content on social media sites. Social networks can serve as rich data sources for semantic applications. The easy-to use Social Web provides a vast store of continually updated information, as well as emergent data about an individual's interest, professional activities and friends.

This will help the developers to create, reuse, and link profiles and contents on social media sites so that the users can get the best result of their complex queries. Present social networking sites do not give result for queries such as "Find list of Assistant Professors in CSE departments of different Engineering Colleges of North India in the age group of 30 years to 40 years."

The Semantic Web tools and technologies can be used to find meaningful results for such queries.

III.RELATED WORK

Some of the other proposals of an access control mechanism for online social networks are works by Kruk et al. (2006)[3] , Ali et al. (2007)[4] and Carminative et al. (2008). [5]

The D-FOAF system (Kruk et al., 2006) is primarily a Friend of a Friend (FOAF) ontology-based distributed identity management system for social networks, where access rights and trust delegation management are provided as additional services. In D-FOAF, relationships are associated with a trust level, which denotes the level of friendship existing between the users participating in a given relationship. As far as access rights are concerned, they denote authorized users in terms of the minimum trust level and maximum length of the paths connecting the requester to the resource owner.

In the work by Ali et al. (2007), authors adopt a multi-level security approach, where trust is the only parameter used to determine the security level of both users and resources.

In the work by Carminati et al. (2009b), a semi-decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in SNSs is presented. The model allows the specification of access rules for online resources, where authorized users are denoted in terms of the relationship type, depth, and trust level existing between nodes in the network.

Compared to existing approaches, we use semantic web technologies to represent much richer forms of relationships among users, resources and actions. For example, we are able to represent access control rules that support relationship hierarchies. By using OWL reasoning tools, we can infer a “close friend” is also a “friend” and anything that is accessible by friend could be also accessible by a “close friend”. Our solution can be implemented by different online social networks by modifying the underlying KB.

Semantic web technologies have been recently used for developing various policy and access control languages for domains different from SNSs. For example, in the work by Tonti et al. (2003) [6], authors compare various policy languages for distributed agent based systems that define authorization and obligation policies. In the work by Fin in et al. (2008) [7], OWL is used to express role-based access control policies. In the work by Yague et al. (2005)[8], authors propose a semantic access control model that separates the authorization and access control management responsibilities to provide solutions for distributed and dynamic systems with heterogeneous security requirements. None of these previous work deals with the access control issues related to online social networks. Among the existing works, the one by Elahi et al. (2008)[9] is the most similar to our proposal. Compared to the work of Elahi et al. (2008), we provide a much richer OWL ontology for modelling various aspects of online social

networks. In addition, we propose authorization, administrative and filtering policies that depend on trust relationships among various users.

In our previous work [10] we have discussed about the different tools that are available for developing systems based on Semantic Web. In this work we have proposed a model based on these topics to access data from SNSs.

IV.METHODOLOGY

In this section we have discussed the methods and the steps that will be followed in this research to find a solution for perfect result in queries by users of Social Networking sites.

Despite their early popularity, users have later discovered a number of drawbacks to centralized social networking services. First, the information is under the control of the database owner who has an interest in keeping the information bound to the site. The profiles stored in these systems cannot be exported in machine process able formats and therefore the data cannot be transferred from one system to the next. Second, centralized systems do not allow users to control the information they provide on their own terms. These problems have been addressed with the use of Semantic Web technology. The Friend-Of-A-Friend (FOAF) project is a first attempt at a formal, machine process able representation of user profiles and friendship networks. FOAF profiles should be created and controlled by the individual user and shared in a distributed fashion. Much like the way web pages are linked to each other by anchors, these profiles link to the profiles of friends by using the rdfs.

In the recent past, Facebook has made changes to its method of defining the relationships between friends on the network. Now, instead of defining link types that are visible to others, each individual has the ability to create meaningful lists. Friends can then be added into as many lists as a user chooses. These lists can then be used to control visibility to status updates, wall posts, etc. However, there is no way to define a hierarchy of these lists. For instance, if one was to create a 'Classmates' list and then a 'Colleague' list, there is no way to create a 'Merged' list, without individually adding each individual person to that third list.

We represent a friendship using the n-ary relation pattern where each friendship is an instance of a class, which we call Friends. This allows us to maintain separate information about each friendship. Specifically, we maintain a Trust Value for each friendship. This allows us to determine a specific strength of a friendship, even when compared to those in the same class.

In our model a reference monitor evaluates a request by looking for the security settings granting or denying the request. A user can grant/set Public-accessible to all, Private-accessible to only close friends or Protected-accessible to all friends. This permission can be set using the Trust Value attribute of each user. Exploiting this principle in the proposed framework implies retrieving the authorizations/prohibitions by querying the SKB ontology. Thus, for example, to verify whether a user's data is accessible for others, it must have read privilege, Public or Protected on data o, and there must be an ontology in the SKB. This implies that before any possible requests evaluation all the rules encoding security policies have to be evaluated. For this reason, before policy enforcement it is required to execute a preliminary phase to populate the SKB with the inferred security, by executing all the rules encoding security policies. Once security settings are found to be OK, data access can be carried out. In particular, access control and filtering policies are evaluated upon an access request being submitted.

The submitted rule has to be inserted in the system if there exists a profile setting by the user allowing or denying access to others. In general, a security setting can be modelled as a triple (u, p, d), which means that a user u grants security p to access data d from his profile. To evaluate this request the framework has to verify whether there exists a read permission p on data d by the user u.

V.ARCHITECTURE

In our system, we model a layer on top of social network application with the following Semantic Web tools.

1. RDF data store

We use a general RDF triple-store to hold the underlying data.

Due to user friendly interface and its availability, we should use MySQL as the database engine. We note here that an RDF[11] data store differs from a relational database in that there is no database method of ensuring that constraints are maintained on the ontology as a whole, such as making sure that a defined Person has a name. Because we condense the actions of a social network, we assume that this is handled programmatically at a higher layer.

2. Reasoner

Any reasoned that supports SWRL rules can be used to perform the inferences described in this paper. However, we can chose SweetRules3 because it interfaces with JENA and has a rule-based inference engine, which meant that we could use both forward and backward chaining in order to improve the efficiency of reasoning for enforcing our access control policies.

3. RDF/OWL engine

For the RDF/OWL interface, we chose to use the JENA API. We use this to translate the data between the application and the underlying data store. JENA [12] has several important features that were considered in its use. It supports OWL-DL reasoning

which we could use to verify that the data is consistent with the OWL restrictions on the ontology. The OWL restrictions are simple cardinality and domain/range constraints such as every person has to have a name and must have at least one public data or data with read privilege. To enforce these constraints, we plan to have the application layer pass the statements to be entered about an individual until all have been collected. We can then have JENA to insert these statements into the database and then check the new model for consistency. If there are any constraints that have been violated, then we pass this information back to the social network application and have it gather the required information from the user.

CONCLUSION

In this paper, we have proposed an extensible online social network access control model based on semantic web tools. The architecture of a framework in support of this model has also been presented. Further work could be conducted in the area of determining a minimal set of access policies that could be used in evaluating access requests in a further attempt to increase the efficiency of these requests.

Additionally, we have shown that existing social networks need some form of reasonable data partitioning in order for semantic inference of their access control to be reasonable in its speed and memory requirements, due to constraints on the memory available to perform inference. Additionally, further work can be used in determining the best method of representing the individual information of a person in a social network to determine if a hybrid semantic/relational approach or a pure approach offers the best overall system.

ACKNOWLEDGMENT

The authors would like to thank all faculty and students of Maulana Azad College of Engineering & Technology, Patna who have shown interest and supported in this research. We are also thankful to our family members without whom this work would not be possible.

REFERENCES

[1] Ali B, Villegas W, Maheswaran M. A trust based approach for protecting user data in social networks. In: Lyons KA, Couturier C, editors. CASCON. IBM; 2007. p. 288e93.

[2] Horrocks I, Boley H, Patel-Schneider P, Tabet S, Grosof B, Dean M. Swrl: asemanticwebrule language combiningOWLand ruleml. Available at, http://www.w3.org/Submission/SWRL; 2004.

[3] Choi HC, Kruk SR, Grzonkowski S, Stankiewicz K, Davids B, Breslin JG. Trust models for community-aware identity management; 2006. IRW2006/WWW2006 Workshop.

[4] Ali B, Villegas W, Maheswaran M. A trust based approach for protecting user data in social networks. In: Lyons KA, Couturier C, editors. CASCON. IBM; 2007. p. 288e93.

[5] Carminati B, Ferrari E, Perego A. Security and privacy in social networks. In: Encyclopedia of information Science and Technology. 2nd ed., vol. VII. IGI Publishing; 2008. 3369e3376.

[6] Tonti G, Bradshaw JM, Jeffers R, Montanari R, Suri N, Uszok A. Semantic web languages for policy representation and reasoning: a comparison of KAoS, rei, and ponder. In: Fensel D, Sycara KP, Mylopoulos J, editors. International semantic web Conference. Lecture notes in Computer Science, vol. 2870. Springer; 2003. p. 419e37

[7] Finin TW, Joshi A, Kagal L, Niu J, Sandhu RS, Winsborough WH, et al. R OWL BAC: representing role based access control in OWL. In: Ray I, Li N, editors. SACMAT. ACM; 2008. p. 73e82

[8] Yague MI, Gallardo Marı´a-del-Mar, Mana A. Semantic access control model: a formal specification. In: ESORICS: European Symposium on research in Computer security. LNCS,Springer-Verlag; 2005.

[9] Elahi N, Chowdhury M, Noll J. Semantic access control in web based communities; 2008:131e6. Computing in the Global Information Technology, 2008. ICCGI'08. The Third International Multi-Conference on.

[10] Aamir Junaid Ahmad and Sabina Priyadarshinin, Use of Semantic Web - Tools and Technologies for Social Networking; IJERT, Vol. 3 Issue 7, July - 2014

[11] The RDF Query Language (RQL). http://139.91.183.30:9090/RDF/RQL/.

[12] Jena – a Semantic Web framework for Java. http://jena.sourceforge.net/

