Relation-based Access Control through Semantic Rules

Najeeb Elahi, Mohammad M. R. Chowdhury, and Josef Noll
UniK-University Graduate Center, Post Box 70, N-2027 Kjeller, Norway.
Email: {najeeb,mohammad,josef}@unik.no

***Abstract*—Web based social communities are one of the most widely used applications nowadays. Ubiquitous computing and access capabilities leverage the evolution of highly dynamic social communities. Recently, security and privacy concerns within these communities have increased significantly. This paper addresses these challenges by controlling access to community resources exploiting Semantic Web technologies. In this regard, a conceptual community framework and its access control mechanisms are formalised using the Web Ontology Language. Access to the resources is controlled by defining differential access rights based on the relationships between the individuals and the communities. Instead of an explicit definition, some additional facts of the mechanisms are inferred by executing Semantic Web rules using the Jess rule engine over the designed ontology. These information are then passed back into the ontology to enrich the existing ontology.**

***Index Terms*—Access Control, Rule, Semantics.**

I. Introduction

UBIQUITOUS computing and connectivity together with extensive diffusion of portable devices allow users to access information/resources/services anytime and anywhere even when they are on the move. However, these access scenarios demand security and privacy assurance which is not a trivial job in today's increasingly connected systems. In this regard, Professor Dr. Eugene Spafford said [1],

> The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.

This paper focuses on the security and privacy provisions in a social community environment through access control mechanisms. The always-online connectivity together with the necessities of information exchange and collaborative work recently boost the participation to web-based social communities manifold. This has become the hub of information and resource sharing among friends. Online communities hold the resources in electronic repositories, to which the user can add content or download it through user friendly interfaces. At the beginning, the community resources were open to all of its members. But recently security and privacy concerns in the Internet have increased significantly. This has been addressed by adding a security layer in online communities through "only visible to friends". Still, it requires more levels of restrictions.

Nowadays social networks are one the most widely used platform of online communities. According the the report from ComScore in July 2007[1], few famous social network sites like MySpace, Facebook, Friendster, Orkut, Bebo etc. are enjoying about 65 million daily visitors and the growth rate is 50% to 300%. These sites rely on the keyword based search queries (syntactic matching) and non-semantic personalisation. In the access control, they lack granularity in the levels of restrictions. The traditional access control mechanism requires more efforts in its modifcation. These limitations can be overcome by using semantic technologies. Semantics promises information consistency and information processing by using ontologies to model the social community structure and its access control mechanisms. Adding semantics can facilitate the machine interpretability and automated processing of these information and mechanisms.

This paper proposes an access control mechanism in social communities exploiting the benefits of Semantic Web technology. It restricts the unauthorised persons to access community resources and increase the system's confidentiality and integrity. Design and maintenance of access constraints are a challenging job in such a highly dynamic environment where access rights and community member profiles are keep changing. Our access control mechanism adopts an ontological approach using the Web Ontology Language (OWL). Access to the resources is controlled by defining differential access rights based on the relationships between the individuals and the communities. Instead of explicit definition, some additional facts of the mechanisms are inferred by executing Semantic Web rules using the Jess rule engine over the designed ontology. These information are then passed back to the ontology to enrich the existing ontology.

The paper is organised as follows. The next section discusses the use case scenario and the problem statements. Section III briefly describes the generic architecture of the proposed system. Section IV introduces the Web Ontology Languages. Detailed descriptions of the ontology representing the community and access control mechanisms are in section V. In Section VI, we introduce the rule language and the results of the inference based on the proposed ontology. The next section contains overview of the related works. The paper concludes with the conclusion and some comments on the future work.

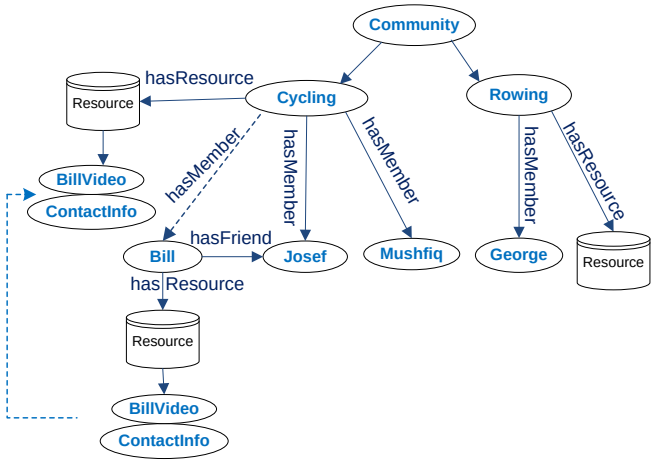

Fig. 1. The use case scenario.

II. Use case scenario

Fig. 1 demonstrates our use case scenario which describes a specific online community environment where unauthorised users are denied to access community resources. The community has public and private resources. When someone joins the community along with his resources, he can declare these as private or public. It is apparent that access requests to private resources need to comply with the access control mechanism. For the remaining part of the paper, resources will mean the private resources of the community. The use case introduces different levels of access rights. The rights are designed based on the requester's relationship with the community/community members. In this paper, we emphasise three situations.

- The requester is not only a member of the community but also a friend of the resource owner.
- The requester is only a member of the community.
- The requester does not belong to the community.

In fig. 1, there are two communities: Cycling and Rowing. Josef and Mushfiq belong to Cycling community, and the Rowing community has George as member. Each community has resources which are uploaded to the community from the repositories of the individual members. Bill is a friend of Josef and interested in cycling. He joins the community and makes some of his resources (for example, his mobile contact and videos) available to the community. As Josef is already defined as a friend of Bill (in Bill's profile), he will get enhanced access. In the proposed architecture, we are going to implement the following access scenarios based on three situations described underneath.

- Josef can access Bill's video with full access privilege, as he is not only the member of the same community but also a friend of Bill.
- Mushfiq can access Bill's video with but limited access privilege, as Mushfiq is only the member of the same community.
- George cannot access Bill's video as he is neither a friend of him nor a member of the Cycling community.

[1]ComScore, Social Networking Goes Global, http://www.comscore.com/press/release.asp?press=1555 [accessed on Jan. 14, 2007]

Full access means the requester can even download the videos or photos and can modify in case the resources are documents. Similarly, with limited access a requester cannot have these capabilities and only limited to resource visibility. The community contains public resources which are visible only to its members, and private resources where access control is maintained according to the above scenarios.

III. Generic Architecture

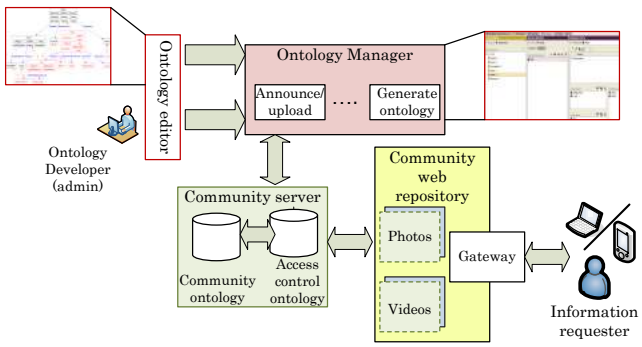

Fig. 2. Generic architecture of the proposed community.

Fig. 2 illustrates the generic architecture of the proposed community which consists of a community server and a web repository along with a webpage. The webpage shows a restricted resource link which is active only when the access requester meets the necessary requirements. The community server will contain the community and access control ontologies. The community members' information and repository entries are maintained centrally. The administrator of the community manages the ontology through an ontology manager. In this paper, it is assumed that members are authenticated to the community through some secure means (e.g. username & password). Thus we are focusing only on the community and access control ontologies, which are further described in section II. The following sections introduces ontologies and provides the reasons for our choice of technology.

IV. Web Ontology Language (OWL)

In this section, We introduce Web Ontology Language which is used to represent the proposed community and access control mechanisms.

A. Introduction to OWL

Semantic Web is an extension of the World Wide Web where both data and its explicit meaning can be effectively processed by computer programs [4]. Semantic Web is merging the existing Web technologies with knowledge representation formalisms in order to establish an infrastructure allowing data to be processed, filtered and discovered more effectively on the Web. Semantic Web encloses the ideas for interoperability that go beyond the traditional programming. Ontologies define unambiguous formal semantics which allows the common access to the information. Ontology is used

to capture the knowledge about a domain of interest in the form of concepts and their relationships. Different ontology languages are available, focussing on different aspects. The Web Ontology Language[2] is suggested by the World Wide Web Consortium (W3C). OWL is a markup language formally derived from the DAML+OIL web ontology language and mainly intended to achieve sharing, publishing and reasoning about the information on the web. OWL builds on RDF and RDFS and provides more vocabulary for describing concepts and properties (e.g. relations between concepts, cardinality, equality, richer typing of properties, etc). There are three species of OWL: OWL Lite, OWL DL and OWL Full and these are designed to be layered according to their increasing expressiveness. We decide to use OWL DL to represent our scenario. OWL DL provides the computation competence and decidability required in our scenario, though it does not allow the full freedom of expressiveness as compare to OWL Full.

B. Description logic for OWL

OWL DL is meant to supports users who want a maximum expressiveness without losing computational efficiency and decidability. It comprises all OWL language constructs with restrictions and it is based on the Description Logics (hence the suffix DL). These are the decidable parts of the First Order Logic[3] and are therefore amenable to automated reasoning. It makes sure that all its entailments are computable and the computation will finish in finite time. In order to achieve more expressivity and decidability, we use Semantic Web Rule Language (section VI-A) which is designed as an extension of OWL DL.

V. Ontology description for community and access control

In this section we present the social community ontology. We describe the main concepts and the realisation of these concepts to make the ontology uncomplicated and but comprehensible which is illustrated in fig. 3.

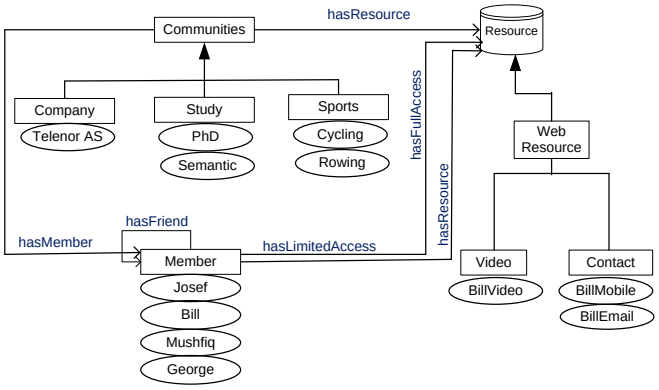

Fig. 3. The description of the ontology using classes, properties and instances.

[2]OWL Overview: http://www.w3.org/TR/owl-features/

[3]First Order Logic (FOL), http://en.wikipedia.org/wiki/First-order_logic

A. Defining the community through classes

We define a community as a set of members who share a common interest. *Communities* might be further divided into professional, educational, social or sports communities. Every community has its own resource that can be visible within the communities. *Member* of the community have control of their own resources, they are free to modify or delete them.

A member of a community is a person who is authenticated and has a certain role in the community. Members might be subscribed to different communities and will probably have different roles in the communities. They can add, edit and share the community or personal resources according to their access rights. For the secure system in a social community ontology, a member can't exist without any subscription. A member has to join at least one community. This is implemented by the restriction below.

```
<owl:Restriction>
<owl:someValuesFrom rdf:resource="#Community"/>
  <owl:onProperty>
   <owl:ObjectProperty rdf:ID="hasCommunity"/>
  </owl:onProperty>
</owl:Restriction>
```

Resources belong to the members and to the communities. Members have different access rights to the particular resources. Such resources might be content in form of documents, pictures, audio, video files and the contact information about members or it might be services provided by members or the community. Contact information can be used for dispatching the access request to the mobile phone.

B. Relations and access rights

In our usage scenario properties are playing vital roles to achieve the access goals. Fig. 3 illustrates the properties and their relationships with concepts. We anticipate that the ontology will answer who can have access, what kind of access he has and which resources he can access. The solution is provided based on the access requester's relationships with the community and its members. *hasFriend* is a symmetric property by nature which defines the relationship between two members. The *hasLimitedAccess* and *hasFullAccess* properties define the specific access rights. These take *Member* and *Community* as domain and *Resources* and *Community* as respective range. *Community* and *Member* form the relationship with the *Resources* using the*hasResource* property. *hasMember* relates the members to the community.

C. Realising the ontology

Fig. 3 shows the instances of the concepts in ellipses. A limited number of instances are added for modelling our use case scenario. Instances of the *Members* are defined here simply as their names and we presume that the system has already authenticated them through some means. Instances of the resources are defined so that they belong either to the communities or a member. According to the use case scenario (section II), we define Cycling and Rowing as instances of the *Community*.

Later in section VI we are going to enhance the expressivity of OWL using a reasoner based on rule language. Reasoning in OWL (Description Logics) is based on what is known as the open world assumptions (OWA). The OWA means that we cannot assume something does not excist until it is explicitly stated that it does not exist. Therefore, we have to explicitly define that all instances of the *Member*s are different from each other. Moreover, we also declare that *Community*, *Member* and *Resource* are disjoint concepts so that an individual can not be the instance of more than one of these classes. These limitations remain there even after the addition of rules, as the semantic web rule language is an extension of OWL DL.

VI. Enhancing expressivity of OWL

Besides semantically enhanced resource description over the Web, another main benefit of semantics is semantic inference over the knowledge base with logic foundation. The semantic inferences can be used for extracting more implicit information. The reasoning capability makes the semantic technology so attractive to apply in the context of access control. In the social community scenario, the access rights over the resources can change dynamically. This can be a perfect field where reasoning can extract the useful information to evaluate the access privileges.

A. Using Semantic Web Rule Language

Recent work has given attention to adding rules to OWL to provide an additional layer of expressivity. The Semantic Web Rule Language (SWRL[4]) is one of the widely used rule languages in conjunction with the OWL ontologies. SWRL is based on a combination of the OWL DL and OWL Lite sublanguages with the Unary/Binary RuleML[5] sublanguages of the Rule Markup Language. SWRL enables Horn-like rules expressed in terms of OWL concepts to reason about OWL individually. In our framework a SWRL rule is used to infer new instantaneous knowledge from exiting OWL knowledge base. SWRL rule specification provides a convenient way to choose reasoning mechanism and does not impose restrictions on how reasoning should be performed with SWRL rules [3]. Users are free to use a verity of rule engines to reason with the SWRL rules stored in an OWL knowledge base. We chose the Jess reasoning engine[6] for performing inference because of its great compatibility with Protege-OWL platform.

B. Enhancing the knowledge base

We have developed a social community ontology that allows SWRL rules to be used to query and infer the new knowledge from OWL ontologies. SWRL helps to combine the domain level specification of the system data and run-time operational data requirements of the system [2]. SWRL rules are used to reason the OWL individuals using its classes and properties. Execution of the rules given below will answer the following questions:

- Who has full access over individual's resources?
- Who has limited access over individual's resources?
- What is the action when an anonymous (who does not belong to the same community and not even a friend of resource owner) person requests to access individual's resources?
- How can only the members of a community have access to its public resources?

We use the Jess inference engine to execute these rules and thus to get inferred knowledge. As a first step the Jess engine converts the relevant OWL knowledge and SWRL rules to Jess knowledge. Then the engine executes the rules and at the end the inferred facts can be exported back to the OWL knowledge base. All these actions are user driven. The SWRL rules are formulated as follows:

- SWRL Rule 1: who has full access over individual's resources?
  $Members(?personA) \wedge$
  $hasResources(?personA, ?resA) \wedge$
  $hasMember(?Comm, ?personA) \wedge$
  $hasFriend(?personA, ?personB) \wedge$
  $hasMember(?Comm, ?personB) \longrightarrow$
  $hasFullAccess(?personB, ?resA)$
- SWRL Rule 2: who is restricted to limited access over individual's resources?
  $Members(?personA) \wedge$
  $hasResources(?personA, ?resA) \wedge$
  $hasMember(?Comm, ?personA) \wedge$
  $notFriend(?personA, ?personB) \wedge$
  $hasMember(?Comm, ?personB) \longrightarrow$
  $hasLimitedAccess(?personB, ?resA)$
- SWRL Rule 3: forward anonymous person's request to the resource owner mobile phone.
  $Members(?personA) \wedge$
  $Members(?personB) \wedge$
  $notFriend(?personA, ?personB) \wedge$
  $hasMember(?Comm, ?personA) \wedge$
  $notMember(?Comm, ?personB) \wedge$
  $hasMobile(?personA, ?mobileA) \longrightarrow$
  $dispatchRequest(?mobileA)$
- SWRL Rule 4: All community member can access community's public resources.
  $hasMember(?Comm, ?Member) \wedge$
  $hasResources(?Comm, ?resComm) \longrightarrow$
  $hasFullAccess(?Member, ?resComm)$

The asserted facts from Jess are transported into the OWL knowledge to fill the corresponding relationships. Rule 1 checks whether the requester is a friend of the resource owner and member of the same community. We have explicitly defined in our ontology that Josef is a friend of Bill and also sharing the same community. Therefore by rule 1, Josef is eligible to have full access to Bill's resources. Fig. 4 illustrates the results of successful execution of rule 1. These relationships have not been explicitly defined (empty circle in fig. 5) during the design of the ontology. Therefore the

[4]Proposal of Semantic Web Rule Language by W3C members, http://www.w3.org/Submission/SWRL/

[5]The Rule Markup Initiative, http://www.ruleml.org/

[6]Jess Rule Engine, http://herzberg.ca.sandia.gov/jess/

existing ontology needs to be updated with these new facts. Fig. 5 shows that the asserted facts are updated back to the knowledge base (filled in circle in the figure) using the Jess export facility.

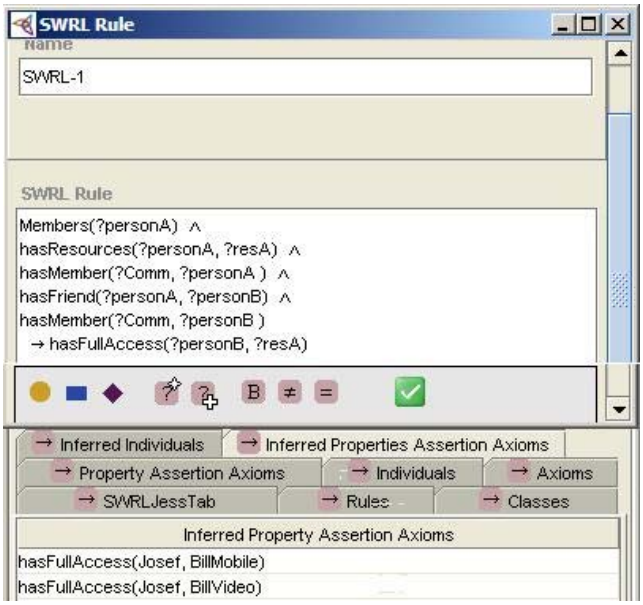

Fig. 4. Results of rule 1: Josef can access Bill's video with full access privilege.

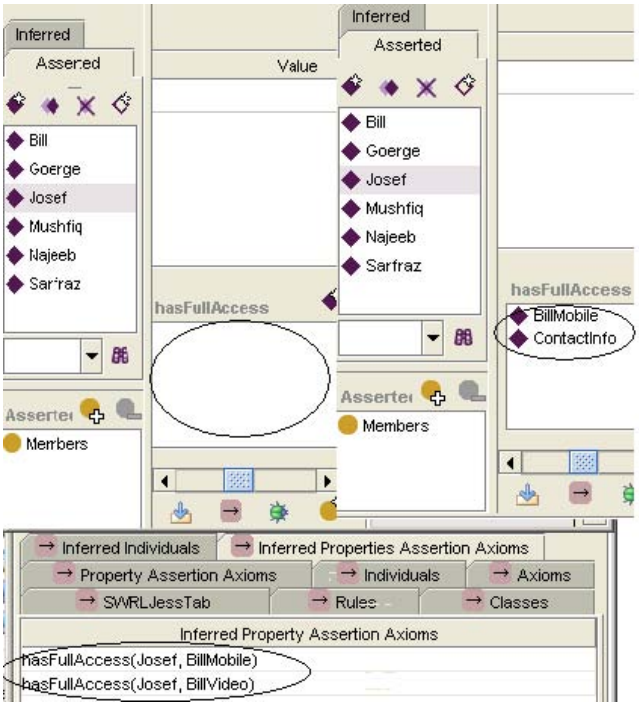

Fig. 5. Results of the rule 1 are exported back to the existing knowledge base.

Rule 2 answers which person can get the limited access to the resources, here the rule checks whether the requester belongs to the same community of the resource owner but is not a friend of him. As expected, Mushfiq gets the limited access to Bill's video (fig. 6). Rule 3 answers the access request querry of the requester who is not a friend of the resource owner and not even shares a single community with him. These requests are dispatched to the resource owner's mobile phone for his explicit permission. The proposed community ontology has provision to store its member's mobile contact information. Finally, rule 4 asserts that all the community members have full access over the public resources of the specific community they belong to. Our results shows that the inferred knowledge

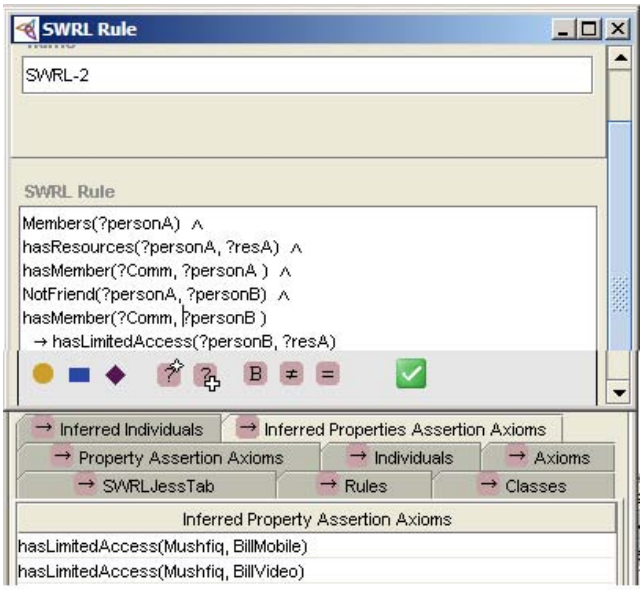

Fig. 6. Results of the rule 2: Mushfiq gets limited access to Bill's video.

is as expected (fig. 7).

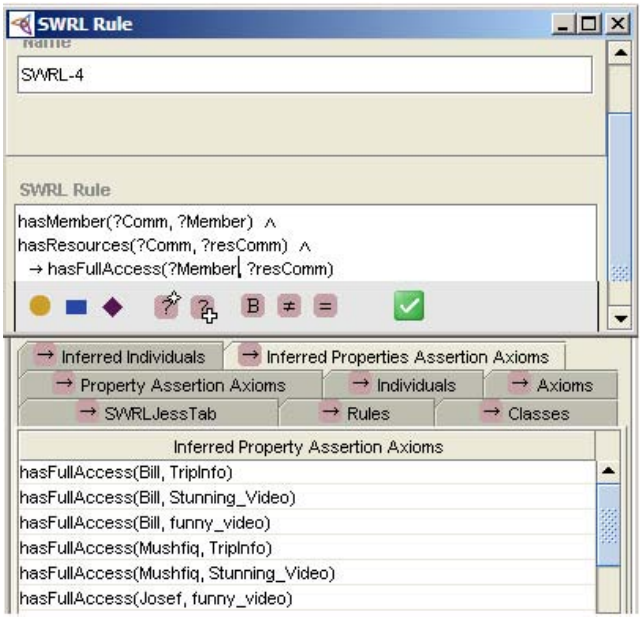

Fig. 7. Results of the rule 4: All the community members have full access to its public resources.

VII. Related Works

The significance of adding privacy-enhancing technologies (PET) in virtual community networks is overwhelming [5],

[6]. This paper suggests to exploit Semantic Web technology to ensure security and privacy in virtual communities through access control mechanism. We believe that ontologies together with the rules can provide an underlying security platform in this area. This section introduces some of the other initiatives in the relevant area and compares them with our proposed solution.

Among the access control technologies, Access Control List (ACL) is widely used. The semantics of ACLs have been proven to be insecure in many situations. Instead of maintaining a centralized ACL, a trust based group has been proposed to delegate access rights [7], [8] where FOAF (friend of a friend[7]) based social networks acted as a mean for the delegation. A private key based signature scheme was proposed to ensure the privacy of networks and users. But such scheme requires secure distribution and maintenance of keys. A similar concept of trust or reputation has also been used by [9] to create and access communities. A distributed trust management approach is also considered as one of the main components to secure the Semantic Web [10]. They intended to provide access to community resources and privacy solutions only by means of trust/reputation management. Trust is affected by various factors and therefore difficult to quantify. The generation of trust between users requires considerable computational complexity.

FOAF uses RDF technology[8]. In this paper, we use OWL which facilitates greater machine interpretability of the Web content than that supported by XML, RDF, and RDF Schema (RDF-S) by providing additional vocabulary along with a formal semantics. It also maintains decidability and computational efficiency. The expressivity provided by OWL is limited by tree like structures [11]. This means that knowledge cannot be inferred from indirect relations between entities. Integration of rules with the ontology enhances its capability to infer new knowledge.

In [12] the authors also suggested expressing access control policies based on OWL and SWRL. The solution was limited to the definition of OWL ontology and declaration of SWRL rules. They predicted the use of an engine to deduce more information by additng rules. In [13] a Semantic Based Access Control Model was presented which considers semantic relations among different entities in decision making process. Here SWRL was also applied to enhance the expressiveness of the authorisation rules but without the rule engine support. The superiority of the proposed work is, it includes a rule execution environment which is realised through the use of a rule engine. It also facilitates the export of new inferred facts back to the ontology which further enriches it.

VIII. Conclusion and future work

Web based social communities are one of the most widely used applications nowadays. This paper addresses the challenges of controlling access to community resources. Traditional access control mechanisms require the semantic enhancement to define complex constraints based on various factors like relationships and roles. The inference capabilities of Semantic Web technology allow us to avoid explicit definitions of some indirect relationships. In the proposed solution, we address the access control scenarios in social community context where relationships with the individuals and the community determine the access restrictions to community resources. All these knowledge are represented in an ontology using OWL DL. Semantic rules are added on top of the ontology wich provides it the sufficient exprissivity and decidability to infer the indirect relationships.

In this paper we assume a centralised community architecture. Such an architecture might not be scalable and individual's privacy can be compromised. As a future work, we are now concentrating on developing a distributed mechanism of the social community architecture. We also believe that the inclusion of the mobile phone can provide a channel for explicit authorisation to anonymous access requester.

[7]FOAFRealm project, http://www.foafrealm.org/

[8]RDF builds on URI and XML technologies. The specifications provide a lightweight ontology system.

Acknowledgement

This work was supported in part by the Norwegian Research Council in the SWACOM project and the ITEA WellCom project.

References

[1] E. H. Spafford, director of the Purdue Center for Education and Research in Information Assurance and Security, Selected Quotes, http://homes.cerias.purdue.edu/~spaf/quotes.html [accessed on Jan. 4, 2007]

[2] M. J. O'Connor, S. W. Tu, A. K. Das, and M. A. Musen. Querying the Semantic Web with SWRL. The International RuleML Symposium on Rule Interchange and Applications (RuleML2007), Orlando, FL, Springer Verlag, 2007.

[3] M.J. O'Connor, H. Knublauch, S. W. Tu, B. Grossof, M. Dean, W.E. Grosso, and M.A. Musen. Supporting Rule System Interoperability on the Semantic Web with SWRL. Fourth International Semantic Web Conference, Galway, Ireland, 2005.

[4] T. Berners-Lee, J. Hendler, and O. Lassila. The semantic web. Scientific American, 2001.

[5] C. M. Chewar, D. Scott McCrickard, and John M. Carroll. Persistent virtual identity in community networks: Impact to social capital value chains. Technical Report TR-03-01, Computer Science, Virginia Tech, 2003.

[6] G. J. Walters. Privacy and Security: An Ethical Analysis. Computers and Society, 2001, pp. 8-23.

[7] S. R. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and Hee-Chul Choi. D-FOAF: Distributed Identity Management with Access Roghts Delegation. 1st Asian Semantic Web Conference, Beijing, China, 2006.

[8] S. R. Kruk, A. Gzella and S. Grzonkowski. D-FOAF Distributed Identity Management based on Social Networks. In demo session of ESWC 2006.

[9] H.-C. Choi, S. R. Kruk, S. Grzonkowski, K. Stankiewicz, B. Davis, and John G. Breslin. Trust Models for Community-Aware Identity Management. Identity, Reference and the Web IRW2006, WWW2006 Workshop, Scotland, May 23, 2006.

[10] T. Finin and Anupam Joshi. Agents, Trust, and Information Access on the Semantic Web. ACM SIGMOD, vol. 31, issue 4, Special Issue: Special section on semantic web and data management, December 2002, pp. 30-35.

[11] B. Motik, U. Sattler, and R. Studer. Query Answering for OWL-DL with Rules. International Semantic Web Conference 2004, SpringerLink, 2004, pp. 549-563.

[12] H. Li, X. Zhang, H. Wu, and Y. Qu. Design and Application of Rule Based Access Control Policies. International Semantic Web Conference Workshop on Semantic Web and Policy, 2006, pp. 34-41.

[13] S. Javanmardi, M. Amini, R. Jalili, and Y. Ganjisaffari. SBAC: Semantic Based Access Control. The 11th Nordic Workshop on Secure IT-systems, Linkøping, Sweden, October 2006, pp. 157-168.

Najeeb Elahi is Scientific Assistant at the University Graduate Center at Kjeller (UniK), Norway in the area of Social Community. He worked in Digital Enterprise Research Institute (DERI) Ireland and his main focus was Semantic Web.

Mohammad M. R. Chowdhury is PhD candidate at the University Graduate Center at Kjeller (UniK), Norway in the area of User Mobility and Service Continuity. He received is MSc from Helsinki University of Technology in Radio Communication. His current areas of interest include identity, identity management, identity representations, identity based service interactions, and seamless user experience in heterogeneous wireless networks.

Josef Noll holds a professor stipend from the University of Oslo in the area of Mobile Services. Working areas include Mobile Authentication, Wireless Broadband Access, Personalised Services, Mobile-Fixed Integration and the Evolution to 4G systems. He is also Senior Advisor at Movation, Norway's leading innovation company for mobile services. He received his Ph. D. from the University of Bochum (D), worked for the European Space Agency at ESTEC from 1991-1997, and from 1997-2005 at Telenor R&I.