Sociality brings Security in Content Sharing

Mohammad M. R. Chowdhury, Sarfraz Alam and Zahid Iqbal
UNIK-University Graduate Center, Kjeller, Norway
Email: {mohammad, sarfraz, zahid}@unik.no

Josef Noll
University of Oslo, Norway
Email: josef@unik.no

Abstract—Sharing digital contents on the Web has become one of the most popular activities on the Internet. When the contents are sensitive in nature, sharing them online has security implications. Recently social relations are used extensively as access constraints to secure the content sharing. However only relation cannot provide personalized and granular enough access control. To mitigate the problems, this paper proposes an access authorization model incorporating diverse real life social relations and associated attributes such as trust, distance of relations and frequency of interactions. The model comprises of a formal knowledge base and personalized access authorization policies. We implement the model using the capabilities of semantic technologies. The paper also demonstrates practical applications of such model.

Index Terms—access control, ontology, policy, relation, semantic technology

I. Introduction

Today sharing personal contents on the Web is the most interesting application and accounts for about half of the top 10 most visited sites [1]. There are typical content sharing sites such as Flickr, YouTube and social networking sites also provide such facility extensively. The private information and contents are nowadays increasingly available on the Web especially when a user is equipped with sophisticated electronic gadgets. Often users want to make access to his online contents restricted. This is not only user's own requirements but also supported through government legislations. To meet such privacy requirements, content sharing and social networking sites include access control features through relationships.

Nowadays social relations pervade every aspect of our life. Hence representation of diverse social and professional relations in virtual world has become a necessity. The characteristic feature of social relationship is that two or more people coordinate with each other so that their action, affect, evaluation, or thought are complementary [2]. The involvement of so many traits in social relations makes the representation more difficult.

This paper not only tries to encode this complex world of social relations but also provides answers to secure content sharing concerns on the Web through an access authorization model. The model comprises of a knowledge base and personalized access authorization policies. The knowledge base contains diverse social relations and associated attributes such as trust, distance in relations and frequency of interactions. The capabilities of semantic technologies help us realizing the knowledge base and access policies. We used the Web Ontology Language (OWL) [3] to formalize the knowledge base and the Semantic Web Rule Language (SWRL) [4] to represent the access policies. The paper also demonstrates usability of such approach in practical use case scenarios.

The paper is structured as follows. In section II, we provide a brief discussion on the background of security concerns in content sharing applications and current research activities related to these areas. Section III discusses our approach to achieve secure content sharing through an access authorization model. The model is then introduced in detail in section IV. Section V provides a functional architecture of a content sharing application that incorporates the proposed model. The implementation details and results are then elaborated in section VI. In section VII, we demonstrate the applicability of the proposed model in practical setting and the paper concludes with an evaluation of the model.

II. Background and Related Work

A. Content sharing

The current content sharing systems suffer from a number of drawbacks and their popularity has further amplified the problems. The first and foremost is regarding the ownership of individual's information which compromises the privacy of the users [5]. The lack of portability of the information typically requires all information to be registered again in every other content sharing site when one wants to use other sites as well. The copies of the information often remain inconsistent. These sites usually controls the access to information and contents through 'friends' attribute only and thus personalized security is not supported. Nowadays users are increasingly posting and sharing personally created or recorded contents online. To mimic real life sharing model, the content sharing sites need to include as many real life relation and their attributes.

To mitigate some of these problems, we propose maintaining individual's information under his own control through a knowledge base which is assumed to be

doi:10.4304/jcp.5.12.1839-1846

portable and the information can only be disclosed with user's explicit consent. The knowledge also contains personalized access control feature involving real life complexity of relations. The following sections will elaborate these aspects.

B. Semantic access control

Researchers were working over the years to bring the science of semantics to Access Control. Adding semantics to the prominent RBAC [6] model facilitates high level specification of access rights and constraints, and supports delegation and revocation of rights [7], [8]. By incorporating attributes and contextual information, Attribute-Based Access Control [9] and Context-Aware Access Control [10] can support varying granularity. Lately these models were also semantically extended [11], [12]. Now to enhance security in content sharing sites or social networks, we need to make access control social aware and this is the focus of this paper.

In [13], Carminati et al. proposed a social network access control model based on Semantic Web framework using OWL and SWRL. The fine grained access control feature was included through closeness of relation and trust attribute. Closeness was expressed only through several predefined *subclasses* such as best friend, close friend, distant friend. We in this paper extended the notion of fine grained access control further by including closeness through distance values applied upon any relations such as friend, family, relative in addition to trust and frequency of interaction values.

In access control, constraints are often specified through policies. According to Coi et al. [14], well-defined semantics, expressiveness of condition and extensibility are some of the crucial policy specification criteria. Use of OWL and SWRL for formal specification of policies supports these criteria [14]. In [15], authors also suggested expressing the access control policies based on OWL and SWRL citing the lack of formal semantics in XACML [16], a popular policy language.

C. Social access control

Lockr [17] provides an access control scheme based on social relationships that makes sharing personal contents easy by eliminating the need for maintaining site specific copies of one's social networks. What makes this paper different from Lockr is that Lockr has no further granularity in access control. Moreover, Lockr is based on social Access Control List (ACL) that carries the problems related to maintenance and management of the list [18]. This paper is the extension of our earlier work [19] where we proposed a very initial social aware semantic access control model containing relationship and trust only.

III. Our Approach

In this paper security in content sharing is achieved through access control mechanism which is a process of limiting access to the resources of a system only to authorized people or processes [6]. The mechanism has two parts: authentication and authorization. There are currently numerous means of authentication available and hence this paper will not elaborate this issue.

Authentication merely ensures that the individual is he or she who claims to be but says nothing about the access rights. Authorization process makes sure one accesses only what he is allowed to access. This paper proposes an access authorization model composed of a formal knowledge base and access policy. Knowledge base consists of concepts, properties (linking concepts), and instances of the concepts. Policy contains the constraints which are being formulated using the components of the knowledge base. Access authorization is achieved through execution of policies. A policy execution environment derives the authorization decisions. Fig. 1 illustrates the brief overview of the proposed access authorization model. In this paper the whole knowledge base and associated policies may represent a person's (e.g. Alice) Social Graph. Here we assume that the Social Graph is portable and can be imported to different content sharing or social networking sites.

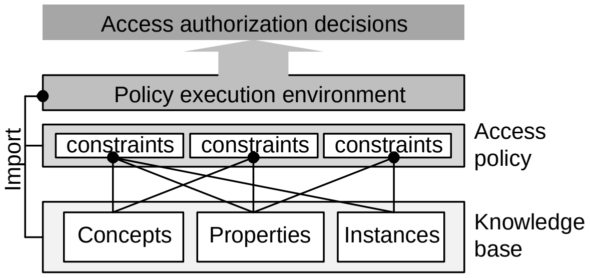


Figure 1. The proposed access authorization model.

Semantic technologies are used to implement the knowledge base and the policies. Semantics mean the explicit interpretation of domain knowledge to make the machine processing more intelligent, adaptive and efficient [20]. Such interpretations are critical for decision making. In this regard, semantic technologies that include standards, methodologies and tools act as the enabler. In this paper, access authorization decisions are derived through automated reasoning process.

IV. Access Authorization Model

A. Knowledge base

A Knowledge base is a repository of information about a particular domain of interest. Among the two different types of knowledge base: human-readable knowledge base and machine-readable knowledge base [21], this paper is aiming the latter one which is having the reasoning capability. Through reasoning new facts can be inferred based on the existing knowledge.

The **concepts** are represented through classes**.** The knowledge base in this paper described four classes: **Subject, Object, Relation,** and **Privilege. Subject** is the people or devices in the interaction. **Objects** are the contents to be shared and **privilege** refers to the access rights. All social or professional relationships are defined through **relation**. Subjects contain attributes such as distance, trust and frequency of interaction. Along with the relation, these attributes are used to formulate the access constraints in the policy.

The real actors of a practical use case scenario (e.g. individuals) are defined through instances and they belong to the classes. A property belongs to a domain and has a range. Syntactically, a domain links a property to a class and range links a property to either a class or a data range [3]. From an instance point of view, a property relates instances from the domain with the instances from the range.

The Ontology which is defined as formal and explicit representation of knowledge was used for representing knowledge base. Among the different ontology languages [24], this work uses the Web Ontology Language (OWL) [3]. Fig. 2 illustrates a breakdown of the knowledge base used here containing classes (nodes), subclasses, instances of classes or subclasses (is), properties (edge between nodes) and data values.

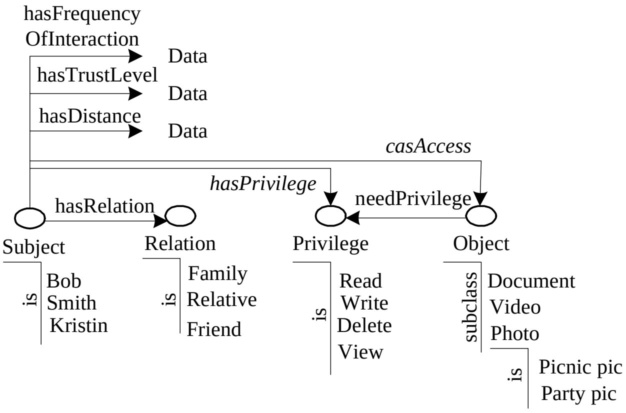


Figure 2. The breakdown of the knowledge base used in this paper.

The ontology is a set of *classes C*, *properties P* and *instances i*. Concepts have *owl:subClassOf* link among them. The semantic scope (SC) of a concept (class) C_i is represented as $SC(C_i)$. Following are the definitions (and examples using the knowledge base in fig. 2) of OWL used in this paper:

Definition 1

owl:subClassOf: $SC(C_1) \subseteq SC(C_2)$, the semantic scope of C_1 is narrower than that of C_2.

Example: $Object \subseteq \{Document, Video, Photo\}$

Definition 2

$\{i_1, i, ...i_n\} : SC(C_1)$, instances $i_1, i_2, ...i_n$ belong to class C_1.

Example: $\{Picnic\,pic, Party\,pic\} : Photo$

Definition 3

$P(i_1, i_2)$ states that i_1 relates with i_2 through the property P. i_2 can be a numeric value in case of datatype property.

Example: *needPrivilege(Partypic, {View, Delete})*
hasTrustLevel(Bob,0.9)

These definitions were used to define the knowledge base shown in fig. 2.

B. Authorization policy

Access authorization is achieved through policies. A policy is broadly defined as a definite course of action to determine present and future decisions. Applying policy is nowadays a prominent approach to protect security and privacy of users, contents and services. Policy specifies: (a) who is allowed to perform, (b) which action, (c) on which objects depending on (i) subject's attributes and (ii) contextual factors.

C. Constraints in authorization policy

Distance represents the closeness of relationships. It is very obvious that when distance increases the trust decreases (fig. 3a). But in real life the situation is rather complex. The distance-trust relationship may not follow a linear path (fig. 3b). For example, A can have more trust on B than C though C is closer to A in terms of biological relationship. The frequency of social interaction may even be used to build trust between individuals.

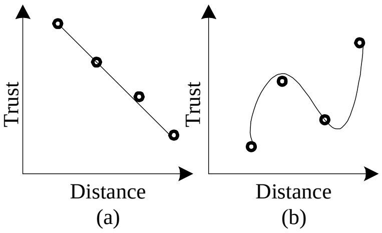


Figure 3. Trust Vs Distance.

Considering all these aspects cardinality constraints of policies are defined using the following tangible components: Relation, Distance, Trust and Frequency of Interaction.

Relation (Rel)

The use of relations as access authorization constraints is very common in social networks. For the time being this paper considers the following relations: friend, relative, and family. Example:

*As Bob is a **relative** of Alice, Bob can see Alice's family picnic pictures.*

Distance (d)

The distance of relations says how one knows another person whether it is a direct relationship ($d = 1$) or indirect one ($d > 1$) through other people. The distance can even be viewed as the degrees of separation. It can be defined either statically or dynamically. This paper considers the following constraints of distance while forming the policy:

- equal to (=)
- greater or equal to ($\geq$)
- less or equal to ($\leq$)

Example:

*As Bob is a **relative** of Alice with* $d = 1$, *Bob can see Alice's party pictures.*

Trust (T)

Trust is statically defined through numeric trust level values on the scale of 0 to 1 (with 0.1 intervals). Both $\geq$ and $\leq$ are used for forming the constraints in the policy. Example:

As Bob is a ***relative*** *of Alice with* ***trust level*** *0.7, Bob can see Alice's party pictures.*

Frequency of Interaction (FI)

It represents the number of social interactions happened in the virtual world for example as simple as number of blog post on each other's sites. In this paper it is measured on monthly basis. For modeling the authorization mechanism we define it statically but in practice this has to be dynamically updated. The system may need to aggregate information gathered from multiple sources. Both ≥ and ≤ are used for forming the constraints in the policies. Example,

As Bob is a ***relative*** *of Alice with* ***frequency of interaction*** *10, Bob can see Alice's party pictures.*

D. Scenarios of constraints

The following two scenarios of constraints are used throughout this paper.

Scenario 1 *The most trusted and nearest family members with whom the frequency of interaction is the maximum.*

$$\mathrm{Re}\,l = Family \wedge T \geq 0.9 \wedge d = 1 \wedge FI \geq 30$$

Scenario 2 *The least trusted and the most distant friends with whom the frequency of interaction is the minimum.*

$$\mathrm{Re}\,l = Friend \wedge T \leq 0.4 \wedge d \geq 4\, FI \leq 1$$

V. Functional Architecture

In order to understand how the proposed access authorization model fits within a content sharing application, this section provides a functional architecture (fig. 4) of such a system briefly describing its core components.

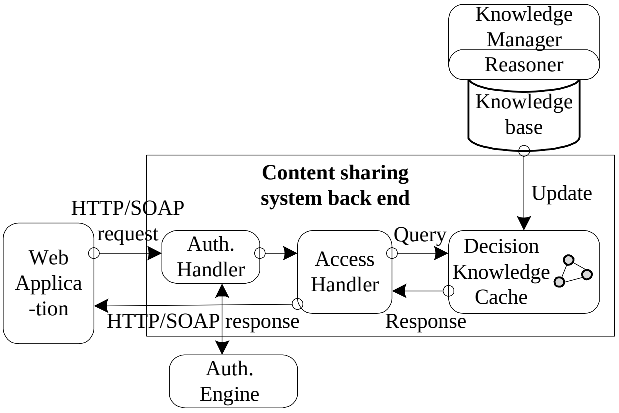


Figure 4. The functional architecture of a content sharing system.

The **knowledge base** is managed and maintained by the **knowledge manager** through an interface. The knowledge manager also facilitates the update of the knowledge-cache through the reasoning process. The rule based **reasoner** in this paper works as the policy execution environment. The **decision knowledge-cache** holds the access authorization decisions derived through reasoning. To avoid real-time decision making, the knowledge-cache is maintained. **Access handler** makes the queries to the cache. User authentication is managed through the **authentication handler**. By incorporating an external authentication engine, the framework ensures the flexibility of using different authentication methods varying simple username/password to mobile phone based authentication. Upon authentication, access handler enforces the access request by processing the requests. It generates the SPARQL [23] queries to the decision knowledge-cache to acquire the list of contents the requester is allowed to access with appropriate privilege. The SPARQL responses are generated in html format and Access Handler forwards these to the **Web Application interface**.

VI. Implementation

This section presents the overview and results of the implementation of the knowledge base, access authorization policies and SPARQL query interface.

A. Knowledge base

The Protégé Ontology Editor was used for encoding the ontology in OWL. Fig. 5 shows the screen shots of OWL classes, properties and instances editor in Protégé. Fig. 6 visualizes the class-subclasses hierarchy and instances of the ontology using Jambalaya plug-in for Protégé. In the ontology, *hasPrivilege and canAccess* are the inferred properties, and the domain and range values of these are filled in through the reasoning process. These represent the access authorization decisions. The proposed knowledge base is a static one and it requires knowledge owner's explicit interactions for modification.

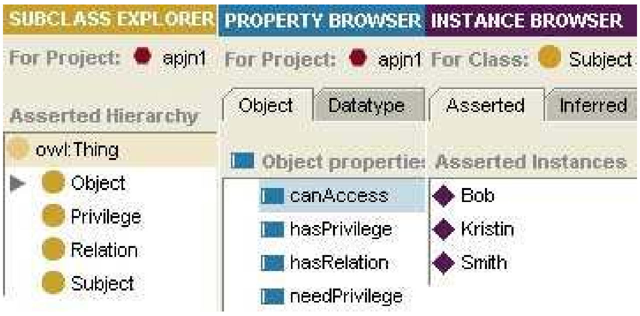


Figure 5. Editor of classes, properties and instances in Protégé.

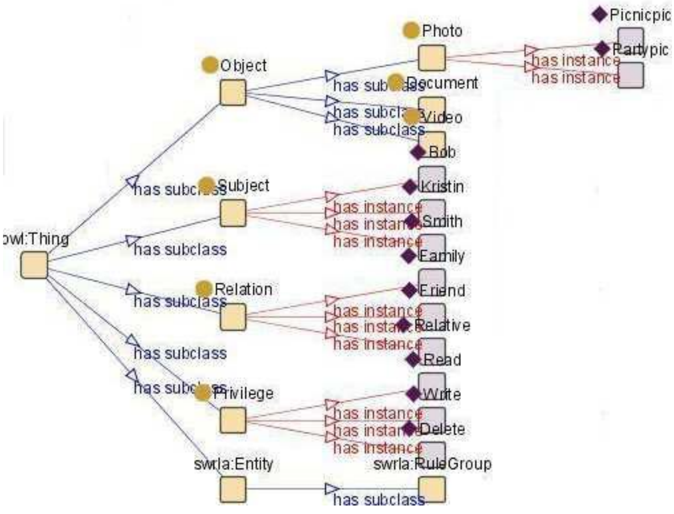


Figure 6. The classes, subclasses and instances of the ontology.

TABLE I.
POLICIES USING SWRL SYNTAX.

Scenario		Policy
1	P1	$has\,Relation(?S, Family) \wedge Privilege(?P) \wedge hasTrustLevel(?S, ?x) \wedge$ $swrlb: greaterThanOrEqual(?x, 0.9) \wedge hasDistance(?S, ?y) \wedge$ $swrlb: equal(?y, 1) \wedge hasFrequencyOfInteraction(?S, ?z) \wedge$ $swrlb: greaterThanOrEqual(?z, 30) \rightarrow has\,Privilege(?S, ?P)$
	P2	$has\,Privilege(?S, ?P) \wedge need\,Privilege(?O, ?P) \rightarrow canAccess(?S, ?O)$
2	P1	$has\,Relation(?S, Friend) \wedge Privilege(Read) \wedge hasTrustLevel(?S, ?x) \wedge$ $swrlb: lessThanOrEqual(?x, 0.4) \wedge hasDistance(?S, ?y) \wedge$ $swrlb: greaterThanOrEqual(?y, 4) \wedge hasFrequencyOfInteraction(?S, ?z) \wedge$ $swrlb: lessThanOrEqual(?z, 1) \rightarrow has\,Privilege(?S, Read)$
	P2	$has\,Privilege(?S, ?P) \wedge need\,Privilege(?O, ?P) \rightarrow canAccess(?S, ?O)$

B. *Access policy*

Ontology through OWL lacks the required expressivity for granting access permissions. Addition of rules with OWL using SWRL [20] can enhance the expressivity of OWL. In this paper the authorization policies are specified with SWRL using SWRLTab plug-in for Protégé.

We will describe two authorization policies which represent two different access scenarios. Each policy is divided into two parts: the first part (P1) decides which privileges a subject will hold during access and the second part (P2) grants permission to subject for accessing specific contents. The logical interpretations (*if-then* statements) of the policies are given using the constraints described in section IV and the following notations: *S* for Subject, *P* for Privilege and *O* for Object.

Scenario 1 Bob is the most trusted and nearest family member of Alice with whom the frequency of interaction is maximum. Alice wants to share (with privilege *Read, Write, Delete*) her party pictures and family picnic pictures with Bob.

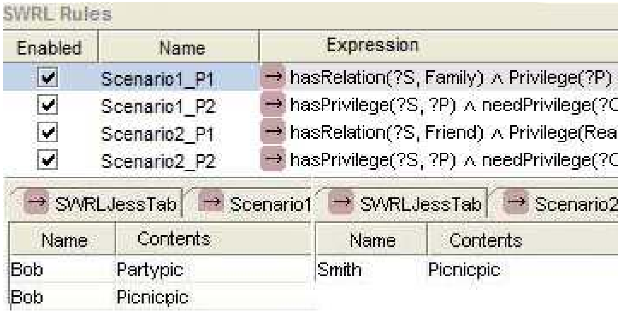
(P1). Decides the privilege
IF
"P" is a Privilege
AND IF
"S" has Relation "Family"
AND "S" has TrustLevel "x"
WHERE "x" IS GREATER THAN OR EQUAL TO 0.9
AND "S" has Distance "y"
WHERE "y" IS EQUAL TO 1
AND "S" has FrequencyOfInteraction "z"
WHERE "z" IS GREATER THAN OR EQUAL TO 30
THEN
"S" has Privilege "P"
(P2). Grants permissions
IF
"S" has Privilege "P"
AND IF
"O" need Privilege "P"
THEN
"S" can Access "O"

Scenario 2 Smith is the least trusted and the most distant friend of Alice with whom the frequency of interaction is minimum. Smith can access Alice's family picnic picture with Read privilege only (no write privilege means Smith cannot comment over the pictures).

(P1). Decides the privilege
IF
"Read" is a Privilege
AND IF
"S" has Relation "Friend"
AND "S" has TrustLevel "x"
WHERE "x" IS LESS THAN OR EQUAL TO 0.4
AND "S" has Distance "y"
WHERE "y" IS GREATER THAN OR EQUAL TO 4
AND "S" has FrequencyOfInteraction "z"
WHERE "z" IS LESS THAN OR EQUAL TO 1
THEN
"S" has Privilege "Read"
(P2). Grants permissions
IF
"S" has Privilege "P"
AND IF
"O" need Privilege "P"
THEN
"S" can Access "O"

Table 1 shows the access policies in SWRL syntax representing the logical interpretations of the policy of each scenario. The policies are executed using Jess rule engine [25] and the results represent the access authorization decisions. SWRLJess Bridge (a java class) allows the rule engine to interact with OWL knowledge base and SWRL rules. Fig. 7 presents the SWRL editor in Protégé and the derived results. It shows that Bob can access (with *Read, Write, and Delete* privilege) both the party and picnic pictures of Alice whereas Smith can only access (with *Read* privilege) picnic pictures. The decision knowledge-cache is updated with these results.

Joseki is an HTTP engine supports SPARQL query


SWRL Rules

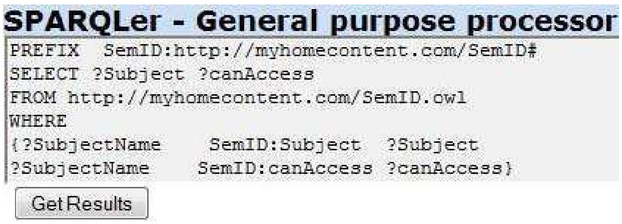
Enabled	Name	Expression
☑	Scenario1_P1	→ hasRelation(?S, Family) ∧ Privilege(?P)
☑	Scenario1_P2	→ hasPrivilege(?S, ?P) ∧ needPrivilege(?C
☑	Scenario2_P1	→ hasRelation(?S, Friend) ∧ Privilege(Rea
☑	Scenario2_P2	→ hasPrivilege(?S, ?P) ∧ needPrivilege(?C

Name	Contents
Bob	Partypic
Bob	Picnicpic

Name	Contents
Smith	Picnicpic

Figure 7. The access authorization decisions of scenario 1 and 2.

processor (called SPARQLer) in a Web Application. Fig. 8 shows snapshot of the installed Joseki instance with SPARQL queries. The queries are generated from the access handler in response to a request from the Web Application.



SPARQLer - General purpose processor

```
PREFIX  SemID:http://myhomecontent.com/SemID#
SELECT ?Subject ?canAccess
FROM http://myhomecontent.com/SemID.owl
WHERE
{?SubjectName    SemID:Subject  ?Subject
?SubjectName    SemID:canAccess ?canAccess}
```

Figure 8. The SPARQLer with SPARQL queries in Web Application.

VII. Application Scenarios

This section demonstrates the applicability of the proposed access authorization model in practical use case scenarios.

A. Content sharing through networked devices

Fig. 9 depicts a connected home scenario which is typically equipped with devices such as mobile phones, computers, Set-top-box (STB), and a TV. A user can utilize the infrastructure to relish personalized content sharing. The STB works as gateway and provides connectivity, management and access to the contents. The entire back end of the system (fig. 4) was built on an STB. The knowledge base and the reasoning process were maintained in an external server. As real-time reasoning over large ontology may not be efficient [22], we propose to adopt an event-based (e.g. modification or addition of knowledge base and policies) or periodical reasoning and thereby the knowledge-cache is updated with the derived access authorization decisions. The users were authenticated using the preregistered Bluetooth MAC address of the devices. The notion of such connected home is already presented in ITEA WellCom project (a European Union project).

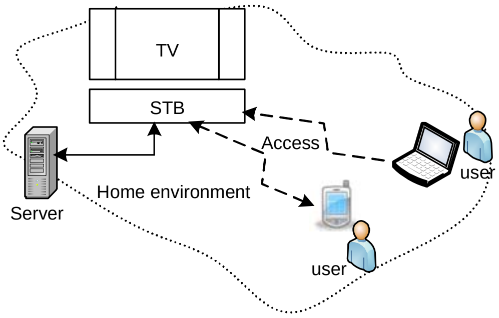


Figure 9. A connected home scenario.

For instance, Alice wants to share a recently recorded TV program with Bob who has similar interests as Alice. Alice already defined an access policy and when someone from her contact group (Friend here) wants to access that specific TV program the system evaluates the policies against the constraints. If the request satisfies the constraints then the system allows access to that particular content. Fig. 10 demonstrates the preferred contents of Bob (close friend of Alice) on the TV screen where English Football was shared by Alice.

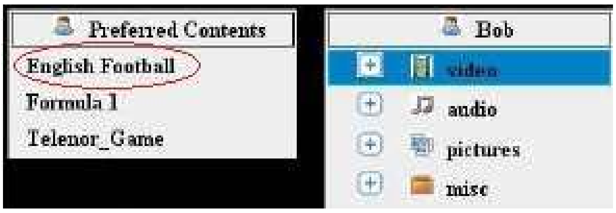


Figure 10. The content is shared with Bob on the TV screen.

B. Content sharing through social networks

This section introduces a very common scenario of a social network. Currently, people use social networks to share contents such as video, audio, pictures etc. People can share and access contents based on their relationships. With the assistance of constraints in the authorization policy, user can have more fine grained control on the contents to enhance security and privacy. Consider the example of social aware school where school has its social graph containing information about students, parents and their staff etc. The school has contents of their annual ceremony and they want to share with parents and staff members. The school publishes the contents on social network and defines access authorization policy based on the constraints (trust, relation, distance). The school's social network evaluates the policy and shares the contents with all members of school social graph who meets the constraints defined in the policy.

VIII. Conclusion

In this paper we proposed a personalized access authorization model that can support fine grained access control to share contents on the Web or at connected devices. The model takes into account the complex real life social relations to formulate access constraints. We implemented the model using the capabilities of semantic technologies.

Though the use of semantic technologies leads to advantages such as human understandability, easier extensibility, machine interpretability and automatic reasoning, there exist some limitations too. Scalability is a big issue for ontology management and reasoning. Real-time reasoning over very large ontology may not yield results in required time. One of the solutions can be to populate the results beforehand in a separate knowledge base and query that knowledge on real time for fetching the decisions. This we used in this paper through a decision knowledge-cache. SWRL brings in some design and use restrictions for example it cannot support 'OR' clauses, explicit universal ($\forall$) and existential quantifiers ($\exists$) which could not make policies more effective and realistic.

The proposed access authorization model contains a knowledge base and user defined access authorization policies. By separating the knowledge base and reasoning process from the system back end, we decoupled the access control part of the system from the content sharing and delivery part. This gives user complete control over his personal information and can contribute in the preservation of user's privacy during content sharing.

In this paper we assumed the knowledge base to be portable. As a future work, we planned to investigate the portability aspects of the knowledge and demonstrate its usability in a practical setting.

ACKNOWLEDGMENT

The authors wish to thank for the supports and contributions from the colleagues at UNIK-University Graduate Center and the SWACOM and ITEA Welcom project.

REFERENCES

[1] The top 500 Sites of the Web, Alexa-The Web Information Company, http://www.alexa.com/topsites/ [retrieved on 22. April 2010]

[2] A. P. Fiske, "Human Sociality", International Society for the Study of Personal Relationships Bulletin, 14(2), 4-9, 1998.

[3] M. K. Smith, C. Welty, and D. L. McGuinness. OWL Web Ontology Language Guide. World Wide Web Consortium Recommendation, 10 February 2004.

[4] Horrocks, P. F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, M. Dean, "SWRL: A Semantic Web Rule Language Combining OWL and RuleML", W3C submission, 21 May 2004.

[5] "Facebook's New Privacy Changes: The Good, The Bad, and The Ugly", The Electronic Frontier Foundation, http://www.eff.org [retrieved on 22. April 2010]

[6] Ravi S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based Access Control Models", IEEE Computer, 29, 2:38-47, February 1996.

[7] Crampton amd H. Khamnhammettu, "Delegation in Role-Based Access Control", in 11th European Symposium on Research in Computer Security, LNCS, Volume 4189/2006, Springer Berlin/Heidelberg, September 2006, pp. 174-191.

[8] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. H. Winsborough, and B. Thuraisingham, "Role based Access Control and OWL", In the Forth OWL: Experience and Directions Workshop 2008.

[9] Hai-bo Shen and Fan Hong, "An Attribute-Based Access Control Model for Web Services", In Seventh International Conferecne on Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2006, pp.74-79.

[10] Young-Gab Kim, Chang-Joo Mon, Dongwon Jeong, Jeong-Oog Lee, Chee-Yang Song, and Doo-Kwon Baik, "Context-Aware Access Control Mechanism for Ubiquitous Applications", Advances in Web Intelligence, LNCS, Volume 3528/2005, pp. 236-242.

[11] T. Priebe, W. Dobmeier, N. Kamprath, "Supporting attribute-based access control with ontologies", in the First International Conferecne on Availability, Reliability and Security 2006, 20-22 April 2006, pp. 465-472.

[12] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila, "A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasie Computing Environements", in the 5th International Semantic Web Conference 2006.

[13] Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, B. Thurainsingham, "A Semantic Web Based Framework for Social Network Access Control", in SACMAT'09, June 3-5, 2009, Stresa, Italy.

[14] J. L. D. Coi and D. Olmedilla, "A review of trust management, security and privacy policy languages", in International Conference on Security and Cryptography (SECRYPT 2008), July 2008.

[15] H. Li, X. Zhang, H. Wu, and Y. Ou, "Design and application of rule based access control policies", in 4th International Semantic Web Conference (ISWC 2005), November 2005, pp. 35-41.

[16] M. Lorch, S. Proctor, R. Lepro, D. Kafura, and S. Shah, "First experience using XACML for access control in distributed systems", in 2003 ACM Workshop on XML security, pp. 25-37.

[17] A. Tootoonchian, K. K. Gollu, S. Saroiu, Y. Ganjali, A. Wolman, "Lockr: Social Access Control for Web 2.0", in the First ACM SIGCOMM Workshop on Online Social Networks (WOSN'08), August 18, 2008, Seattle, Washington, USA, pp. 43-48.

[18] Mohammad M. R. Chowdhury and Josef Noll, "Integrating Social Identity Theory in Access Control", in the IEEE 9th Malaysia International Conference on Communications (MICC 2009), 14-17 Dec. 2009, Kuala Lumpur, Malaysia.

[19] Mohammad M. R. Chowdhury and Josef Noll, "A Social Relation Aware Semantic Access Control", in 12th International Conference on Computer and Information Technology (ICCIT 2009), 21-23 Dec. 2009, Dhaka, Bangaldesh.

[20] Mohammad M. R. Chowdhury, "Semantically Augmented Identity-based Service Access", Doctoral Thesis, University of Oslo, August 2009, ISSN: 1501-7710.

[21] Rajendra Akerkar and Priti Sajja, Knowledge-Based Systems, Jones & Barlett Publishers, MA, USA, 2010.

[22] Mohammad M. R. Chowdhury and Josef Noll, "Secure Connected Home: where the semantic technologies meet the device community", in the Journal of Information Assurance and Security (JIAS), Vol. 4, Issue 5, Special Issue on Privacy and Trust 2009, Dynamic Publishers Inc., Atlanta, USA, pp. 390-402.

[23] Eric Prudhommeaux and Andy Seaborne, "SPARQL Query Language for RDF", W3C Recommendation 15 January 2008.

[24] Asunción Gómez-Pérez and Oscar Corcho, "Ontology languages for the Semantic Web", IEEE Intelligent Systems, Vol. 17, Issue 1, 2002, pp. 54–60.

[25] Jess, the Rule Engine for the Java Platform, http://www.jessrules.com/ [retrieved on 22. April 2010]

Mohammad M. R. Chowdhury received the Ph.D. from the Department of Informatics, University of Oslo in the area of security, privacy and trust. Before that he received the M.Sc. degree in Telecommunication Engineering from Helsinki University of Technology (HUT), Finland in 2002. His current research interests include access control, identity management, personalized service access, and security in Internet of Things.

He is currently working as postdoctoral fellow at UNIK-University Graduate Center, Kjeller, Norway. He was involved in research projects funded by the Norwegian Research Council and the European Union. Dr. Chowdhury has published about 35 scientific articles in journals, books and international academic conferences. He contributed in several international conferences as technical program committee member, session chair and reviewer. Dr. Chowdhury is a member of IEEE Communication Society.

Sarfraz Alam is a PhD candidate at UNIK-University Graduate Center in Kjeller, Norway. He received his M.Sc. degree in the area of Information Security from The Royal Institute of Technology (KTH), Sweden. His research area covers Mobile SOA, Semantic Mobile Services and SOA security and privacy.

Zahid Iqbal is a PhD candidate at UNIK-University Graduate Center in Kjeller, Norway. He received his M.Sc. degree in the area of Information Security from The Royal Institute of Technology (KTH), Sweden. His research area covers Security and Privacy of User Profile, Social Network and Cloud Computing.

Josef Noll is Professor at the UNIK-University Graduate Center and University of Oslo, Norway in the area of Mobile Systems. He is also Chief Technologist in Movation, an innovation company in Norway. He received his Ph.D. from University of Bochum, worked for European Space Agency at ESTEC from 1991-1997, and from 1997-2005 at Telenor R&D. His working areas include mobile authentication, wireless broadband access, personalized services, mobile-fixed integration, and the evolution to 5G system.