International Journal of Review and Research in Applied Sciences and Engineering (IJRRASE)
Vol3 No.1. PP 1- 6 March 2013 ISSN: 2231-0061

A Framework for Fine-Grained Access in Semantic Web Services by using Policy-Based Semantic Access Control

M.Ramalingam
Dept. of Computer Science and Engineering,
Mailam Engineering College, Mailam – 604304, Tamil Nadu, India
rammalingamm2005@gmail.com

Dr.R.M.S. Parvathi
Principal & Professor, Dept. of Computer Science and Engineering
Sengunthar College of Engineering, Tiruchengode – 637 205, Tamilnadu, India

Abstract

A semantic access control mechanism is used to provide access permission to the authorized users. Some access control models think about the rich semantic relations between the requested and the availing services. They will not filter out the services that do not met both the service providers' policies as well as the users' policies, because they offer only coarse-grained access. To solve this problem, a new framework is proposed. The framework consists of two separate Ontology, namely service ontology and policy ontology, to maintain the semantic information of policies that are submitted by users and service providers and the semantic information of services, a service locator for identifying the exact services and an access control engine for offering access to the users. The framework is implemented. Its performance is analyzed using precision, recall and F-score measures. Hence it proves that the framework is effectual in providing fine-grained web services using policy based semantic access control.

Keywords: **web services, framework, ontology, fine-grained, semantic access, access control mechanism, policy, service.**

I. INTRODUCTION

The World Wide Web has rapidly grown. This makes difficult to identify, locate, access and preserve information to be available for users. The content of the World Wide Web is often processed through natural language by humans. Semantic Web concept introduced by Tim Berners-Lee is used to solve the problems in accessing and processing the information of WWW [1]. In the semantic web, where the information is given correct sense, allowing computers and user to work in better association [5]. **S**emantic web based systems of future will be more scalable, adaptable, extendable, and interoperable as compared to the current web based systems. These upcoming systems will consist of smaller independent systems. These can work together if they are supported by ontology [4]. Each providing access to diverse contents is expected to work in cooperation, and so interoperability between the smaller systems is essential.

In Ontology domain where the knowledge is human understandable, but machine-readable format comprising of entities, attributes, relationships, and axioms. It is used as a standard knowledge representation for the Semantic Web [13]. For the future success of Semantic Web Services, it is important to create flexible and expansible security architecture for the current generation of Web Services [9]. Security issues for semantic web services are becoming more important for nowadays [15]. A highly distributed knowledge repository [20] is a major issue. It is to be considered for the security of semantic web is how to control access to sensitive and confidential information (access control) present in the Semantic Web. Ontology-based semantic information retrieval is a hotspot of current research [13].

The access control is used to ensure every access to a system and its resources are restricted based on a set of predefined policies. Access Control Policies are security necessities that represent how access is managed, what data can be accessed by whom, and in what conditions that data can be accessed. These policies are forced by a mechanism. It verifies the user's access requests and makes allow/decline decision for providing access to web services [19]. Semantic Web service providers execute the access control policies in order to limit access to their services to only eligible users [10]. Concurrently, the access control policy is checked and request is granted or rejected according to the policy statement associated with the user, before permitting a user to access the service [17].

A semantic aware access control mechanism should assure that only authorized users to be granted an access right and each qualified user must able to access all

the resources that he/she is authorized for. Usual access control models such as Mandatory Access Control, Discretionary Access Control and Role-Based Access Control are failed to address these issues. They do not consider the rich semantic relations in the data model under the Semantic Web [14]. A main issue to be considered during the progress of proper access control models is to limit access to Web services to only authorized users. In addition, security technologies frequently used for Web sites and traditional access control models are inadequate. Some of such literary works are briefly reviewed. To solve the problem, we propose a framework, which is described in this paper with necessary illustration. The experimentation results are also discussed in this paper.

II. RELATED WORKS

A semantic-aware attribute-based access control model to deal with the security problems in Web services, where the Attribute-based access control is combined with the Semantic Web technologies has proposed by Haibo Shen [22]. SABAC could provide managerially scalable alternative to identity-based authorization techniques and it has provided a semantic interoperability for the access control to Web services. SABAC has provided an access to services according to the attributes of the related entities, and has employed a Shibboleth service to handle the discovery issue of the sensitive attributes. Moreover, the ontology of the resources and users has been represented by SABAC using the Web Ontology Language standard and an extensible Access Control Markup Language has been used as the policy language.

Robinet is an ontology data management system, to perform the management of ontology data on web sites. Some important issues for web ontology data management has described by Jie Lu et al. [23]. They have intended the structure of the system and developed a Web ontology data management model which enables an effective access control mechanism. The proposed model has added some rules into the robinet system for using the semantics of ontology for controlling the access to ontology data. The rule-based access control mechanism has been implemented and experimental results have shown the performance of the proposed scheme.

A Secure Ontology approach has proposed by Angel Garcia-Crespoa et al [24]. It comprises a three-fold strategy, namely, ontology for access control, a logical declarative structure and software architecture.

A context management system has developed by Anand Dersingh et al [25]. It uses a semantic web approach as a basic method to model and describe the semantics of the contexts. Their approach has been validated by a proof of concept implementation that has the performance results of the context management system as it responds to a change of the situation. The current contexts have been stored in a semantic knowledge base by the system and the stored context has been utilized by a semantic access control system for creating access control policies and for evaluating policies at run time.

A semantic-based, context-aware, and multi-domain enabled framework implementing a semantic-based access control mechanism for Semantic Web by Moussa Amir Ehsan et al [26]. The access control framework was based on the multi-authority version of deontic logic (MADL) and description logic (DL) model, which consider the semantic relationships between different entities. Considering this model, the framework has embedded that the Semantic Web having some have common characterized domains, which each contain an authority and a security agent. The framework has handled the Semantic Web context by categorize and relating it by means of ontology. Their method has been designed using the semantic technologies, which make it fully compatible with the environment.

A flexible fine grained access control model using semantic web tools has proposed by Barbara Carminati et al [27]. They have also presented the architecture of the framework. In addition, they have proposed authorization, admin and filtering policies that rely on trust relationships between different users, and were modeled using OWL and SWRL.

A semantic-based context-aware access control framework has presented by Moussa A.Ehsan et al [28]. In order to use the context information in the framework, they have proposed context ontology to signify contextual information and use it in the deduction engine. They have demonstrated that in what way the access control framework handles the contextual information with their context ontology. The proposed ontology has classified the context of a semantic web environment and showed the elements of contextual information and their relationship in an abstract level.

III. A FRAMEWORK FOR FINE-GRAINED ACCESS OF SEMANTIC WEB SERVICES

Here we proposed a framework for policy-based semantic access control mechanism to provide fine-grained access of semantic web services. Figure 1 shows the generalized view of the proposed framework. In this framework, two separate ontologies are been made use of to facilitate policy-based semantic access. One is Service Ontology which is used to maintain the semantic information of the available services. The other is Policy

Ontology which maintains the semantic information of polices held by all the service providers.

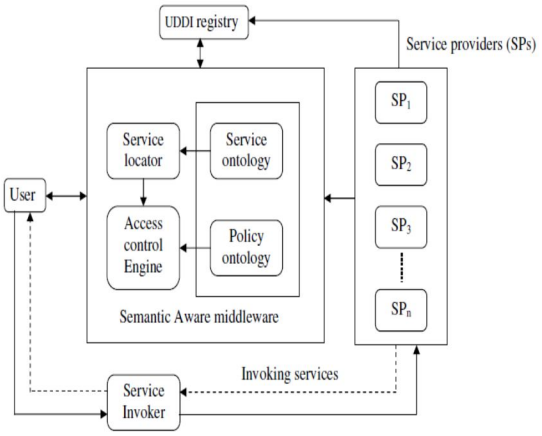


Figure 1: Proposed Framework for Fine-Grained Semantic Web Services Access Control

The semantic aware middleware takes the responsibility of determining semantic web services and provisioning policy-based fine-grained access to the discovered semantic web services. The middleware is comprised by three major blocks, namely, Service locator, Access control Engine and a Block of ontologies. The Block of ontology is a middleware block. This is comprised of the two ontologies, service ontology and policy ontology.

Based on the semantic information of the services available in the service ontology, the Service locator locates the semantic web services from the Universal Description, Discovery and Integration (UDDI) registry that are requested by the user. It is used to provide fine-grained access of the web services, a policy matching process has to be done. The framework is designed in such a way that the Access Control Engine (ACE) performs the policy matching process so as to provide the access for web services without any contravention of the service providers' policy as well as the requesters' policy.

The policy ontology plays a vital role in the policy matching process as the ACE obtains each service provider's policies from the ontology. UDDI registry and the policy ontology are online to any new service provider. Service providers can move in and out of the UDDI registry dynamically over time. In the proposed work, we consider a case with *n* service providers registered in the UDDI registry. Initially, all the Service Providers publish their services in the UDDI registry. Once the services are published, their semantic information are obtained from the UDDI registry and maintained in the service ontology. In the mean time, each service provider will place their policies in the semantic aware middleware that have to be maintained in the policy ontology. In the process of locating semantic services for the user request, service locator plays the major role with the support of service ontology.

The user who wants a service requests the semantic aware middleware with a query and a user policy. In the semantic aware middleware, the service locator holds the query of the user and the ACE keeps the user policy. Once the request is received, the Service locator traverses through the service ontology and recognizes all the semantic description for the given query. Based on the obtained semantic description, the service locator locates all the SP_j:$j=1,2,\ldots,n$, whose services are semantically related to the given query. Once the service locator pinpoints all the SP_j who provide services semantically related with the user query, they all are conveyed to the ACE and then the policy matching process is done.

ACE checks whether the policy of the SP_j is violated by the user credential or not. Also, the ACE checks whether the user policy is satisfied by the SP_j's service or not. After the completion of the policy matching process, ACE has fine-grained *SP*s whose service policies are not violated by the user credential and none of their services violate the user policy. The queried user obtains the access rights of the *SP*s who can provide the fine-grained web services from the ACE. With the aid of the provided access rights, the user contacts the service invoker for gaining uninterrupted access to the concerned web services.

IV. RESULTS AND DISCUSSION

A database of web services was created and it was assumed that it was published in the UDDI registry. Some 3 requests were given to the proposed framework and the results were analyzed using precision-recall values. The requested keyword, the obtained web services and restricted web services, their count are given in Table 1.

Table 1: Access control results by the proposed fine grained semantic access framework

Keywords / Parameters	Kid	News	Ontology

Number of related services	9	18	4
Number of retrieved services	1	2	1
Number of access denied services	2	1	1

Based on the access restricted/offered web services, precision, recall and F-score values are determined. In our case, the precision and recall values are determined using the following formula

$$precision = \frac{Total\ number\ of\ relevant\ access\ offered\ web\ services}{Total\ number\ of\ access\ offered\ services} \quad (1)$$

$$recall = \frac{Total\ number\ of\ relevant\ access\ offered\ web\ services}{Total\ number\ of\ relevant\ services} \quad (2)$$

$$F-score = 2 * \frac{precision * recall}{precision + recall} \quad (3)$$

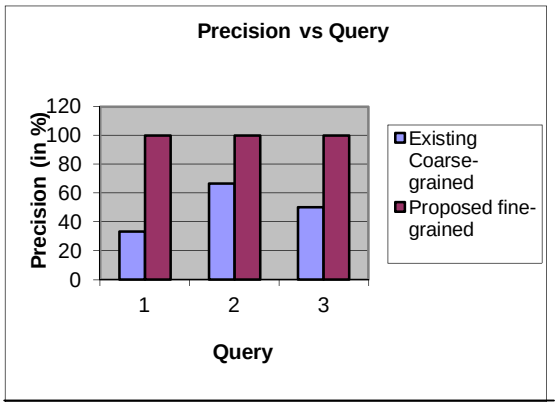
The precision, recall and F-score values that are determined using Eq. (1), (2) and (3) for three different queries are tabulated in Table II. Moreover, the precision, recall and F-score values for conventional coarse-grained semantic access mechanism are also tabulated in Table III. Eventually for pictorial visualization, a comparison chart is affixed in Figure 2.

Table 2: measures for proposed fine-grained access control framework

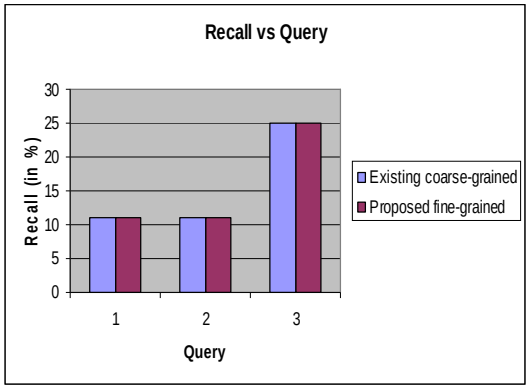
Query	Precision	Recall	F-score
1	1	0.11	0.20
2	1	0.11	0.20
3	1	0.25	0.40

Table 3: measures for coarse-grained access control framework

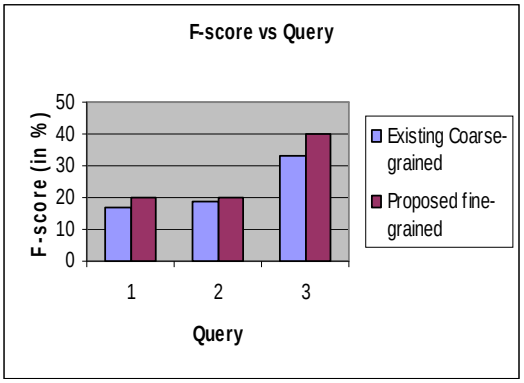
Query	Precision	Recall	F-score
1	0.33	0.11	0.17
2	0.67	0.11	0.19
3	0.50	0.25	0.33



(i)



(ii)



(iii)

Figure 2: Comparative chart between proposed fine-grained access control mechanisms and conventional coarse-grained access control mechanism.

The proposed fine-grained semantic access achieves higher performance. Though the recall performance is similar for both the mechanisms, the proposed fine-grained semantic access mechanism shows higher precision values over the conventional coarse-grained mechanism by 66.6%, 33.3% and 50% for the three queries, kid, news and ontology, respectively. The proposed semantic access mechanism also achieves higher F-score

values of about 3.3%, 0.95% and 6.6%. The proposed fine grained semantic access control mechanism is 50% more precise and achieves 3.65% more F-score.

V. CONCLUSION

We proposed a framework for fine-grained access of the web services with access control mechanism. The control mechanism performed authorization in two aspects, one is to check whether the service provider satisfies the user policies or not and other is to check whether the user satisfies the service providers' policies or not. As per the aforementioned the authorization, the access was presented for the requested services. The services were located based on the semantic information that is stored in the ontology. Different user requests were given to the framework and the precision and recall values were determined from retrieved services. From the results, it was found that the proposed framework achieved a remarkable precision and recall values.

REFERENCES

[1] Cecilia Ionita and Sylvia L. Osborn, "Specifying an Access Control Model for Ontologies for the Semantic Web," *Lecture Notes in Computer Science*, pp. 73-85, November 15, 2005.

[2] Alexander Maedche and Steffen Staab, "Ontology Learning for the Semantic Web," *IEEE Intelligent Systems*, Vol. 16, No. 2, pp. 72-79, 2001

[3] Karim Heidari, Serajodin Katebi and Ali Reza Mahdavi Far, "New Methods for E-Commerce Databases Designing in Semantic Web Systems (Modern Systems)," *World Academy of Science, Engineering and Technology*, Vol. 51, 2009

[4] Minal Bhise, "Automation of Semantic Web based Digital Library using Unified Modeling Language," *International Journal of Recent Trends in Engineering*, Vol. 1, No. 2, 2009.

[5] R. Garcia-Castro, A. Gomez-Perez and O. Munoz-Garcia, "The Semantic Web Framework: A Component-Based Framework for the Development of Semantic Web Applications," *in proceedings of 19th IEEE International Conference on Database and Expert Systems Application*, pp. 185-189, 1-5 September, Turin, 2008.

[6] Francisco Echarte, Jose Javier Astrain, Alberto Cordoba and Jesus Villadangos "Self-adaptation of Ontologies to Folksonomies in Semantic Web," *World Academy of Science, Engineering and Technology*, Vol. 43, 2008

[7] A. Uszok, J.M. Bradshaw, R. Jeffers, M. Johnson, A. Tate, J. Dalton, S. Aitken, "Policy and contract management for semantic web services," *in Proceedings of Semantic Web Services Symposium*, Stanford, California, 2004.

[8] Diego Zuquim Guimaraes Garcia and Maria Beatriz Felgar de Toledo, "Web service security management using semantic web techniques," *in Proceedings of the ACM symposium on Applied computing*, pp. 2256-2260, March 16 - 20, Fortaleza, Ceara, Brazil, 2008.

[9] A. Barbir, "Web Services Security: An Enabler of Semantic Web Services," *in Proceedings of Business Agents and the Semantic Web*, 2003.

[10] Sudhir Agarwal and Barbara Sprick, "Specification of Access Control and Certification Policies for Semantic Web Services", *In proceedings of the 6th International Conference on Electronic Commerce and Web Technologies*, vol. 3590, pp. 348-357,Copenhagen, Danemark, 2005.

[11] Lalana Kagal, Massimo Paolucci, Naveen Srinivasan, Grit Denker, Tim Finin and Katia Sycara, "Authorization and Privacy for Semantic Web Services", *IEEE Intelligent Systems*, vol.19, No.4, pp.50 - 56, 2004.

[12] Shin Moonsoo and Jung Mooyoung, "MANPro: mobile agent-based negotiation process for distributed intelligent manufacturing," *International journal of production research* Vol. 42, No. 2, pp. 303-320, 2004.

[13] Jun Zhai, Yiduo Liang, Yi Yu and Jiatao Jiang, "Semantic Information Retrieval Based on Fuzzy Ontology for Electronic Commerce," *Journal Of Software*, Vol. 3, No. 9, pp. 20-27, DECEMBER 2008

[14] S. Javanmardi, M. Amini and R. Jalili, "An Access Control Model for Protecting Semantic Web Resources," *in proceedings of the 2nd International Semantic Web Policy Workshop*, pp. 32-56, Georgia, USA, 2006.

[15] Mariemma I. Yague, Antonio Mana, Javier Lopez and Jose M. Troya, "Applying the Semantic Web Layers to Access Control," *in proceedings of the 14th International Workshop on Database and Expert Systems Application*, pp. 622, September 01 - 05,2003.

[16] Noorollahi Ravari, Morteza Amini and Rasool Jalili, "A Temporal Semantic-Based Access Control Model," *in the 13th International CSI Computer Conference*, pp. 559–568, Kish Island, Iran, 2008.

[17] Vijay Srinivas Agneeswaran, Rammohan Narendula and Karl Aberer, "Peer-to-Peer Issue Tracking System: Challenges and Solution," *in proceedings of Software Engineering (Workshops)*, pp. 77-81, 2008.

[18] U.U.S.K. Rajapaksha and N. Kodagoda, "Semantic Web Search and Ontology Ranking Algorithm," *in*

proceedings of Semantic Web Search, Vol. 2, pp. 25-29, 2008

[19] "Requirements-based Access Control Analysis and Policy Specification (ReCAPS),"

[20] Jian Li and William K. Cheung, "Query Rewriting for Access Control on Semantic Web," *in proceedings of the 5th VLDB workshop on Secure Data Management*, pp. 151-168, Auckland, New Zealand, 2008

[21] Bhavani Thuraisingham, "Security standards for the semantic web," *Computer Standards & Interfaces*, Vol. 27, No. 3, pp.257-268, 2005

[22] Haibo Shen, "A Semantic-Aware Attribute-Based Access Control Model for Web Service," *in proceedings of the 9th International Conference on Algorithms and Architectures for Parallel Processing*, pp. 693 - 703, June 08 - 11, Taipei, Taiwan, 2009.

[23] Jie Lu, Chao Wang, Guangquan Zhang and Jun Ma, "Collaborative management of web ontology data with flexible access control," *Expert Systems with Applications*, 26 November, 2009

[24] Angel Garcia-Crespoa, Juan Miguel Gomez-Berbis, Ricardo Colomo-Palacios and and Giner Alor-Hernandez, "SecurOntology: A semantic web access control framework," *Computer Standards & Interfaces*, 28 October, 2009.

[25] Anand Dersingh, Ramiro Liscano and Allan Jost, "Utilizing Semantic Knowledge for Access Control in Pervasive and Ubiquitous System," *Proceedings of the IEEE International Conference on Wireless & Mobile Computing, Networking & Communication*, pp. 435-441, October 12 - 14, 2008

[26] Moussa Amir Ehsan, Morteza Amini and Rasool Jalili, "A semantic-based access control mechanism using semantic technologies," *in proceedings of the 2nd international conference on Security of information and network*, October 06 - 10, Famagusta, North Cyprus, 2009.

[27] Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu and Bhavani Thuraisingham, "A semantic web based framework for social network access control," *in proceedings of the 14th ACM symposium on Access control models and technologies*, pp. 177-186, June 03 - 05, Stresa, Italy, 2009.

[28] Moussa A. Ehsan, Morteza Amini and Rasool Jalili, "Handling Context in a Semantic-Based Access Control Framework," *in proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops* , pp. 103-108, May 26 - 29, 2009.