ISSN:0975-9646

Access Control for Semantic Data Repository Using Description Logic

[1]Suganyasree.K , [2]Nagajothi.P

[1]M.E,Computer Science and Engineering, [2]Assistant Professor,Computer Science and Engineering
[1,2]K.S.Rangasamy College of Technology,Tiruchengode

Abstract- **To support the authorization access control model and enhance security systems related to the ontology repositories designed an authorization security model enforced on a semantic model's entities and also propagated on their individuals in the OWL database.Itallowed propagation of authorizations based on the semantic relationships among concepts.But access control is not applied to provide the integrity of data.Two level authorization controls (TBox and ABox) are used for securing semantic knowledge. The various sensitivities of data, needs suitable accesscontrol mechanisms pertaining to the semantic repository toensure that only authorized users have access to the information in its entirety.So the access control for the data and information is proposed by using the information which helps the inheritance of relation of individual**

Keywords: **TBox,ABox, OWL, Authorization Control,Semantic repository.**

1. INTRODUCTION

The Semantic web is used to effectively administer and provide interoperability and warehousing between the data and systems, and to get information from the databases and warehouses on the Internet. Specialized repositories referred to as semantic models are used to achieve semantic interoperability among sources of data as well as applications. But repository that is designed to manage semantic model does not deal with the access rights. Semantic data repositories require advancement regarding access control and management of data privileges. In repositories, authorization is secure using the ontology knowledge bases. Suitable access control mechanisms are needed in semantic repository to ensure that only authorized users have access to the information due to the various sensitivities of data. Ontologies and Semantic Web representation languages resource description framework (RDF), OWL are used based on access rights to obtain different answers for same query.

Depending on the nature of the application domain, the concepts can be differentiated by many degrees of sensitivity and should be allowed only to those users with the appropriate authorization privileges. The solution addressed is to design an authorization securitymodel for the semantic model's entities and alsopropagated on their individuals in the OWL database. To provide high secure operations forsafeguarding semantic data repositories two-level access control paradigms (TBoxand ABox) are introduced. TBox access control deals with access to the conceptindividual level using TBox family. ABox access control deals with the individual. TBox and ABox together form the knowledge base.

Authorization mechanism fully supports contentbasedaccess control. The access control is used for the enhancement of the secured authorized access of the data based on concept.It also consider the relation of the individuals with the concepts.

2. OVERVIEW

2.1 Description Logic

Description logic are a family of logic- based knowledge representation that represents knowledge of an application domain using description languages. The language provide a set of constructors namely concept(class) and role(property) descriptions. Description logics are useful and efficient in knowledge representation fitting into the structural provision of RDF, RDF schema, and OWL technologies for reasoning about structured knowledge. A concept denotes a class of object that shares common characteristics and the role denote relationship between object and data values.

A DL knowledge base is composed of two parts: intensional knowledge(TBox) and extensional knowledge(ABox) which is shown in Fig.2.1. TBox describes the general knowledge about the domain and ABox describes the knowledge about a specific situation. TBox and ABox combine together and form the knowledge base. A DL system offers reasoning service that involves the checking of truth value for a statement and complex services. The reasoning service include knowledge base satisfiability, concept satisfiability, subsumption and instance checking. TBox reasoning is not influenced by ABox reasoning. A property, which is a binary relation connecting concepts, is distinguished as an object property and data property. An object property represent the relation between individuals (instances) of two concepts and data property represent the relation between an individual concept and the literal value. Classes are denoted as concepts, while instances of a class are represented as individuals.

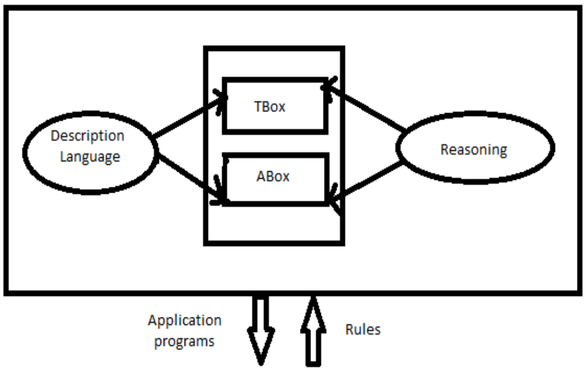

Fig.2.1 Description Logic

2.2 Web Ontology Language

Web Ontology Language(OWL) was used for the greater machine understandability of resources which was built upon the RDF and RDFS. OWL has three expressive sub-languages namely OWL LITE, OWL DL and OWL FULL shown in Fig.2.2. OWL DL is used for the authorizing and access control purpose. Each OWL DL document is same or equal to the RDF document. But both are not considered to be compatible. OWL DL differs from standard description logics in some aspects. In OWL DL object properties relate the individuals to another individuals like nationality. The datatype property relates the individuals to data values. Both property have many in common such as constraints, domains and ranges.

Datatypeproperty (ex:salary
    domain(ex:person)range(xsd:integer))
Objectproperty(ex:nationality
    domain(ex:person)range(ex:country))

OWL DL semantics includes some aspects that are viewed as not usual from the description logic perspective. But as the datatypes are included by OWL the semantics is considered to be similar to the description logic.OWL DL is considered to be the target language which are used in different applications. Some of the properties of RDF are lost while using the OWL DL regarding classes and properties as individuals. Users of OWL DL have the benefit from decidable inference. And has the wide range of tools and infrastructure in an increasing range which includes the sophisticated ontology development environment and the reasoning systems.

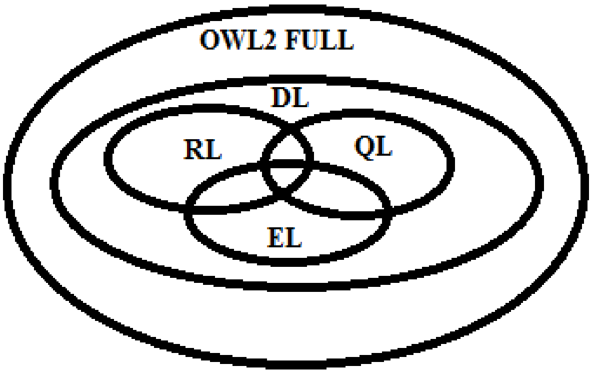

Fig 2.2 OWL

3. Access Control

The term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Types of access control are DAC, MAC, RBAC. RBAC was used in the proposed method. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. It is an approach to restricting system access to authorized users. RBAC is sometimes referred to as role-based security which is given in the Fig.2.3 with the rule assignment relation for roles of user. When defining an RBAC model, the following conventionsare useful:

- S = Subject = A person or automated agent
- R = Role = Job function or title which defines an authority level
- P = Permissions = An approval of a mode of access to a resource
- SE = Session = A mapping involving S, R and/or P
- SA = Subject Assignment
- PA = Permission Assignment
- RH = Partially ordered Role Hierarchy

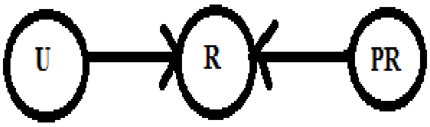

Fig 2.3 Rule assignment relation

In the Fig 2.3 the user role and permission rules assignment relation explains the permission accessed to different users based on the roles. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. When a subject requests an operation on an object in an ACL-based security model, the operating system first checks the ACL for an applicable entry to decide whether the requested operation is authorized. A key issue in the definition of any ACL-based security model is determining how access control lists are edited, namely which users and processes are granted ACL-modification access.

The RBAC access the information based on the role rather than content based retrieval. The higher role authority can now view the details of the lower employees along their retrieval. The lower level authority can retrieve only the details that they require.

4.Conclusion

In the existing system the access control method is used to make sure that only authorized user access the data. The model fully supports content based access control in the existing system. In the proposed system role based access control RBAC is used. In which it supports the role based and concept based access in the organization. The role based is used to access the information from the database based on the comparison of the role. The inheritance relations of a role hierarchy as well as conflict resolution strategies are overcome by using RBAC method. In this method the inheritance relation of an individual is obtained for efficient retrieval and increased authorized information. A more structured model is used to support the detection and handling of conflicting rules. Therefore the information integrity is maintained at a greater level.

REFERENCES:

[1] Abdelhakim Herrouz, Chabane Khentout, Mahieddine Djoudi, “Overview of Access Control Tools,” The International Journal of Engineering And Science, 2013.

[2] Blanquer, V. Hernandez,” Enhancing Privacy and Authorization Control Scalability in the Grid Through Ontologies”, IEEE Transactions on information technology in biomedicine,vol.13,no.1,January 2009

[3] Carlos Vivaracho-Pascual and Juan Pascual-Gaspar,” On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services”,IEEE transacation on Systems, Man and Cybernetics vol.42,no.2 may 2012

[4] Chi-Lun Liu,” Cloud service access control system based on ontologies”,IEEE transaction on secure computing vol.42,no.2,may 2012

[5] Dizza Beimel and Dov Dori,” Situation-Based Access Control:Privacy management via modeling of patient data access scenarios”,IEEE transaction on secure computing.

[6] Kan Yang,” Expressive, Efficient, and Revocable Data Access Control for Multi- Authority Cloud Storage”.IEEE transaction on parallel and distributed system, vol.25,no.7,july 2014

[7] Ma,” Collaborative management of web ontology data with flexible access control”,IEEE transaction on information technology

[8] Rahul Singh and Salam, Member, IEEE transaction on Systems,man, and cybernetics-Part-A:Systems and Humans,vol.36,no.3,may 2006

[9] Simon N. Foley,” Aligning Semantic Web applications with network access controls”, Department of Computer Science, University College Cork, Ireland

[10] Tsung-Yi Chen,” Knowledge sharing in virtual enterprises via an ontology-based access control approach”, Available online at www.sciencedirect.com

[11] Xuan Hung Le,” Evaluation of an Enhanced Role-Based Access Control model to manage information access in collaborative processes for a statewide clinical education program”,journal of biomedical.