Role Based Access Control Using Description Logic

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

[1]K.S.Rangasamy College of Technology
Tiruchengode
[2]K.S.Rangasamy College of Technology
Tiruchengode
[1]visitpnagajothi@gmail.com
[2]suganyacse92@gmail.com

Abstract— **Among the sources of data semantic interoperability is achieved using Semantic models. Semantic models combine the data and information that it relates two or more domains. The confidential information that need to be secured from the user while providing the knowledge based on the request is made even more difficult as the user may be able to apply logic and reasoning to infer confidential information from the knowledge being provided. Through an inference policy engine the individuals in the OWL database are propagated in which an authorization security model enforced on a semantic model's entities is proposed. A TBox family provide TBox access control and ABox label-based access control for facts in the domain knowledge the effects of access control are reported experiments to evaluate reasoning and modularization. The access control is proposed by using the information which helps the inheritance of relation of individual for the data and information.**

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

I. INTRODUCTION

The Semantic Web is used to enable users to retrieve and share by combining information more easily and effectively administer the data and provide interoperability between the systems. Semantic repositories are much like the web servers in which it integrates the inference engines characteristics and DBMS. The repositories are designed. Repository is used as the location for storage of data and information often for safety and preservation. It is used for the authorization purpose but it lacks in the area of access rights. Access control and management of data privileges require advancements in the semantic data repository. In repositories, authorization is secure using the ontology knowledge bases. Access control mechanisms are needed to ensure that only authorized users have access to the information in the repository. To obtain different answers for the same query the access rights uses resource description framework (RDF) and web ontology language (OWL).

Depending on the application domain nature, the access rights can be differentiated by various degrees of constraints and allowed only to certain authorized users with certain privileges. The designing of an authorization security model can address the solution using the semantic reasoner authorization for the semantic model's entities which is propagated based on the individual. The security model uses two level access control paradigm namely TBox and ABox for safeguarding semantic data repositories. The authorization model only supports content based access control. The access control deals with concept based access control using TBox and ABox. TBox and ABox combine together to form the knowledge base. Authorization mechanism only deals with the authorization purpose whereas for the enhancement of the secured authorized access of the data the access control mechanism is used in which the relation of the individuals are also considered with the concepts.

II. RELATED WORK

The authorization control for the confidential information or the data is the emerging issue in the day to day life. Several techniques were proposed that protects the information integrity in different methods were analyzed.

The query rewriting and axiom filtering [5] are two approaches used to solve the problem of inferring the secret knowledge which is made to be the confidential information by using the logical reasoning. The query rewriting modify the given user query in a way that returns the result that is allocated for the role of the user. The axiom filtering manages the access control for the secret information based on the roles.

The policy language [3] proposed a security framework for the information using the distributed policy management. It worked based on the action and condition in which the agents are used for the policy management. The policy rule check on the conditions which are classified into simple and complex condition to secure the data and the action varies according to the condition.

RBAC [7] proposed a new concept of security for the information maintained based on the roles. The roles are used to define the authorization of the user and furthermore it manages the level of access control. RBAC maintains the integrity of the information by using the security principles. It provides access to data based on the user roles and permissions assigned to them.

III. SEMANTIC REASONER

To envelope the semantic descriptions the semantic repositories uses the reasoner to expand the functionality and to derive the results from the given set of facts. The reasoner is software nothing but that is used to infer the results from a known set of facts. The semantic reasoner carries the main role in the inference engine in the ontology that uses the description logic. The semantic reasoner uses the first order predicate logic for the reasoning process which is carried out by either forward chaining or backward chaining. It works with the help of predicates and the quantification. The predicate refers to the entity and consider it as input and after checking produces the output if it found to be true else it deny the output if it is false. The predicates use the IF-THEN rule to check the condition on the entity and derive a conclusion from the known facts. The quantification of condition in the description logic is done using the universal and existential quantifier.

The syntax and semantic are the key parts of the first order logic in which the syntax deals with the symbols and the semantic provides the meaning of the syntax in an efficient and easy way. Here the rule based knowledge representation and reasoning is used to infer the results in a proper way. The semantic reasoner is used on the process of the ABox in which it applies the syntax as only the authorized user accessing the information and performs verifying of the users role and their allowable access using that limit it finds and retrieve the information that may be pooled to the user in an efficient way. If the user is permitted to be allowed to receive the basic details then only it will allocate the desired information to the user. The semantic reasoner is used to retrieve different answers for the same query for the different users. It is used to infer and secured access for the confidential information which is used to control or make secure of the information loss and leakage of data.

A. Description Logic

Description logic is used to represents knowledge of an application domain using description languages which are referred as the family of logic based knowledge representation. The language provide a set of constructors namely concept (class) and role(property) descriptions. Description logics are used for the concept based access of the information based on the individual roles using the TBox and ABox.

TBox is referred as the terminological component in which it deals with the user whether they are authorized or not and extensional knowledge (ABox) which are used to retrieve information based on the reasoning which is shown in Fig.1. TBox describes the general knowledge about the domain and ABox describes the knowledge about a specific situation. The Tbox checks and regulate access to the concepts and their relations based on the authorization policy. It secures the semantic system with the building blocks such as subject, role and permissions. If the user passes on from TBox then it bridge to the ABox control. ABox is the assertional part that captures the facts in an application domain. In the ABox it allows access based on the clearance level in which it allows the access to ABox triples which consist of subject, predicate and object is only allowed if the user's level dominates the ABox individual level. DL system offers reasoning service that involves the checking of truth value for a statement and complex services. TBox reasoning is does not influenced by ABox reasoning. It uses the property, which are binary relations that connect concepts. It uses an object property that is used to represent the relation between individuals (instances) of two concepts whereas the relation between an individual concept and the literal value are represented using data property.

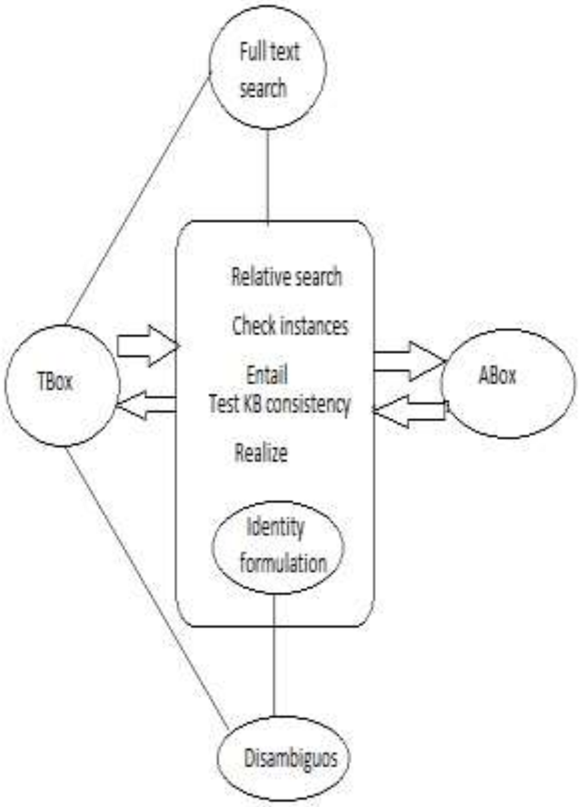

Fig.1 Description Logic

In the description logic the TBox control evaluation algorithm is used for authorization process in which it takes the access request and permission rules set as the input. The method carries out in the way by getting rules to the permission rules with the relevant rules which has the condition of it is not equal to null or empty set. It uses the IF-THEN function in the algorithm for authorization. The second step involves the assigning permissions through the hierarchy using Ck as the superclass and the Cki as the subclass shown as below

```
for each Ck do
    permission = action on Ck;
    for each Cki ChildOf(Ck) do
      if Cki has no permission then
         permission(Cki) = permission(Ck);
      end if
    end for
end for
```

After the permission is assigned through the hierarchy new rules will be generated in which it is evaluate with positive rule and then finally it generate the users role view. It then bridge to the ABox access control which uses the evaluation rules technique with the EVALUATION function with the parameters Treq and Tper. The parameter represents the request and permission. It checks whether the permission concept is null if so then it exits else it switch over to other rule by evaluating the range. And in the viewing analysis result algorithm it is used to analyze the obtained result using the VIEWANALYZE function as shown below

```
function VIEWANALYZE(View)
      if View=null then
          return emptyset;
      else
          function ABoxObjects(View,Li)
      endif
end function
```

B. *Inference Engine*

To retrieve new information from the existing knowledge base inference engine uses the logical rules. The expert system has the inference engine component on the knowledge base. It works either in forward chaining or backward chaining to obtain the required result. The new facts are asserted from the existing facts using the forward chaining. While in backward chaining goal is the starting point which works backward to determine what facts must be asserted.

In this the query given by the user is accessed to retrieve information using either forward chaining or backward chaining in the ontology. It uses the IF-THEN rule for both the forward and backward chaining. It uses the description logic for searching the information. when a query is placed, the inference engine begin search by using query extension in which it briefly expands the query and search for the query related answers and then in the syntax analysis it checks with the syntax of the query and analyse it in the database and finally it compiles the answer with the help of the reasoner as shown in Fig.2. The reasoner checks the query with the user role whether they are permitted to access the confidential information if they are permitted then it provides the user with the required answer. If they are not permitted to allow all the content of the resources then it provides only the allowable information restricted to the user from the database.

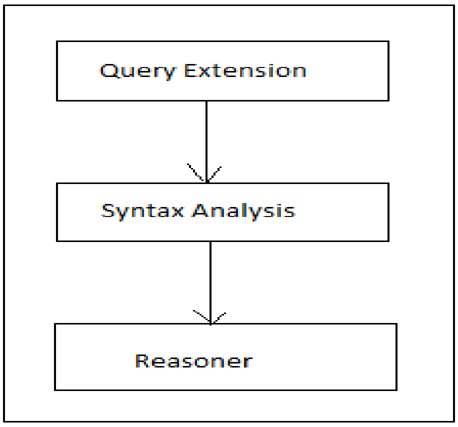

Fig 2 Inference engine

IV. ACCESS CONTROL

The access control is the selective restriction to some resources. The two analogous mechanism of the access control are locks and login credentials. Three types of access control which can be used are DAC, MAC, RBAC. Here role based access control (RBAC) was proposed with the help of login credentials. The user who is allowed to enter where and when is controlled using the access control system. Once the user is permitted as the authorized user the role based access control assigns the access of data content to the user based on their roles with the help of ontology. This approach provides restriction of system access to the authorized users. After login of the user once they request for some information it search over the ontology for the access rights and restricted amount of data according to individual access rights using the inference engine. The role-based security access of the confidential data is done using RBAC. In the RBAC model, the following conventions are used such as subject, Role which defines an authority level and Permissions that is an approval of a mode of access to a resource.

The RBAC access the information for the queries based on the role rather than content based retrieval. In OWL the RBAC represents roles as classes in which the superclass roles are dominated by its subclass roles with several steps. The first step was defining the roles with role name and active role name for every individual. After defining the roles it then provides the hierarchy for the defined roles which helps to assign the permission for static and dynamic duty constraint. The hierarchy for the roles are assigned with the syntax assigned are shown below.

```
<RoleName>rdfs:subclassof <SuperRoleName>
```

In this the subclass is given as the rolename and the superclass is given as the super rolename.The higher level role authority can view all the details of the data whereas the lower employees can retrieve only the details that they are allowed by using the role activation rule which is given as the

```
{ ?ACTION a ActivateRole;
```

```
            Subject ?SUBJ;
            Object ?ROLE.
    ?SUBJ a ?ROLE.
    ?ROLE activeForm ?AROLE.
    ?AROLE rdfs:subClasOf ActiveRole.
  } =>{ ?ACTION a permittedRoleActivation;
             Subject ?SUBJ; object ?ROLE.
              ?SUBJ a ?AROLE }.
```

In the role activation rule the first action carries the activate role for the subject. It checks with the subject corresponding role by using active form of the class. It defines the subclass of the active role and defines the access control for the role of the individual subject. And the action of permitted role activation is carried out if the subject matches the corresponding roles that have the access rights. If the rule fails then it returns the result as deny role activation or not permitted role activation in which the user is denied the access rights for certain confidential information. It limits the access control of the user by relating and comparing with their assigned roles. Roles as classes are preferred to the roles as values because the roles as values do not use the DL semantics but mostly uses the rules.

An experiment that examined the efficiency of the SDC algorithm in clustering topics in Web forum and analysed how the limitation of the eps-neighborhood of a point (eps) and the minimum number of points required for being a neighbourhood (MinPts) influence the performance. Both eps and MinPts are the significant parameters formative the density for clustering. The micro accuracy and macro accuracy are used as the metrics to measure the performance of SDC and benchmark with the performance of DBSCAN.

The interactive boundary allow users to select forum participants as focus nodes by sorting their in-degrees and out degrees, adjust the parameters of fisheye view and fractal view to explore the neighbourhood of focus nodes, and clean less relevant nodes, as well as select the topics extract by the proposed clustering algorithm.

V. CONCLUSION

In the existing system the authorization 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 to support the concept based access to the data based on the individual roles in the organization. In the role based the information is accessed from the database based on the comparison of the role. The inheritance relations of a role hierarchy are overcome by using RBAC method. In this method the inheritance relation of an individual is obtained for efficient retrieval and increased authorized information. The information is accessed based only on the user access level provided for them. Therefore the information integrity is maintained at a greater level.

VI. REFERENCES

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

[2]Anupam Joshi, Kagal,”A Policy Based Approach to Security for the Semantic Web”, 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]Heiner,” Query Based Access Control for Ontologies”,IEEE transaction on secure computing.

[6]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]Ravi Sandhu,”Role Based Access Control Models”, IEEE transaction on information technology, vol.30,no.5, May 2010.