# An Ontological Approach for User Profile Based Access Control System

Kalla. Madhusudhana,
Professor, Department of CSE,
CVR College of Engineering, Hyderabad, India.
kallamadhu1@yahoo.com

***Abstract*—The Conventional Role-based Access Control (RBAC) systems evaluate access permissions depending on the identity/role of the users. However, this approach does not incorporate semantic information concerned to users, which could have an impact on access decisions. The basic idea of this paper is to use ontological approach to enable target users to have access to heterogeneous sources of information with intricate semantic relations in educational domain. Here, we proposed user-profile based policy approach in which user profile represented in ontological format so as to meet the semantic relations among different users, and between data objects, so as to enables expressing much more fine-grained access control policies. This work aims at creating a user profile ontology that incorporates concepts and properties used to model the user profile. We have developed ontology to realize the framework and need to demonstrate the framework through considering university administrative system as a case study.**

***Keywords- User profile, ontology, Access Control, Educational Domain***

## I. INTRODUCTION

Information Security (IS) is a non-trivial problem that usually comes in different levels of abstraction. In the context of securing access to computer systems, access control is governed by one or several access control models. Different access control models rely on such operations as authentication or authorization to manage user access to the resources that would otherwise be accessible to potentially unauthorized users.

User-Profile based access control approaches in the context educational domain exploit user identity/role information to determine the set of access permissions. Therefore, it is essential to have a flexible specification of access control polices based on semantic relations among different types of users and among data objects. Modeling security policies based on semantic relations among types of users, becomes an important issue in the design of future access control models.

Access control policy is a means of assigning access rights based on set of rules and provides access control mechanism. Based on the above aspects, we introduce user-profile ontology for modeling access control (AC) policies that take into account the relevant semantic based information, in the context educational domain. The proposed model enables expressing much more fine-grained access control policies.

Since knowledge resources are captured in ontology, the access control policies need to semantically express them [1]. Most of the existing works propose solutions aiming to alleviate the limitations of standard access control models. In contrast, we proposed a generic ontology-based solution that captures the user profile information and their roles using ontology. By introducing the concept of semantic-dependent role activation, the association of users to roles can be achieved.

## II. RELATED WORK

An ontology based access control research in social network area and other domains is still in its early stages. Early access control solutions for Social network systems (SNSs) propose trust-based access control policies that are inspired by research developments in trust and reputation computation in social networks. FOAF-Realm5 is one of the earliest approaches that tried to quantify the “knows” relations in the context of FOAF (Friend Of A Friend) ontology.

The closest work to this paper is probably the Semantic Web-based access control framework by Carminati et al.[2], which also leverages OWL and SWRL. They define three types of policies, namely, access control policy, filtering policy, and admin policy.

Ryutov et al. [3] propose a rule-based access control model for semantic networks, based on the constrained first order logic. The authors have implemented this model in a Resource Description Framework (RDF)-like framework.

Reddivari et al. [4]propose a rule-based model and architecture, called RAP. Access control policy written using Jena framework rules, and supports both permit and prohibit predicates, similar to Ontology-based Social Network Access Control (OSNAC) features.

Damiani et al. [5] propose a semantically enhanced extension of XACML as well as reference architecture for policy enforcement. They extend XACML with an operator to trigger requests for object metadata from a semantic environment. Subject metadata is used for the access control decision as delivered by the requester and used the RDF for specification of metadata, thus not providing the richness of OWL; furthermore, reasoning on subject metadata is not possible.

Masoumzadeh, [1] proposed Ontology-based Social Network Access Control (OSNAC), an ontology-based access control model based on Semantic Web standards that empowers the individual users of a social networking system to express fine-grained access control policies on their related information.

Stan, Johann, et al., [6] proposed ontology-based user profile model that allows users to have a situation-aware social network, by controlling how reachable they are for specific categories of people in a given situation.

The relationship-based access control model proposed by [7,8] but they have different goals that focus on relationship in OSN (Online Social Network) with proposed access control.

## III. ACCESS CONTROL MODEL

Intuitively, access control is to permit or deny the access of a particular resource by a particular entity. Usually, the entity applied for the access is called a subject; the resource is called an object and the way to access is called an operation.

The access control relies at the very least on triple comprising elements from three sets:
S – a set of subjects (those entities who want to gain access);
O – a set of objects (those entities that may be accessed, also known as resources);
P – a set of access actions or invocations.

A triple $\alpha = (s; p; o) \in S \times P \times O$ represents an access right or authority of subject " s " to access object " o " using action " p ". One of the common representation of the authority triples is so-called Lampson's matrix that is often constructed with elements " s " forming the matrix rows, elements " o " forming the matrix columns, and elements " p " being expressed as values of particular cells.

The assignment $(s; p; o) \rightarrow \{T, F\}$ could take the form of (s; p; o; T) or (s; p; o; F) as permit/deny policy stored in an access control system.

**Algorithm**: Access Control Decision

```
//Data: s: Subject; o: Object; p: Permission; f: boolean; KB: set of w;
//Input: Subject s, Operation p, Object o
//Output: boolean
{
if (s,p,o,F) exists in KB
then
        return false;
 else
        if (s,p,o,T) exists in KB
        then
                return true;
        else
                return false;
        end
end
}
```

## IV. ONTOLOGY BUILDING

An ontology is an explicit specification of concepts and relationships that can exist between them. This set of objects, and the describable relationships among them, are reflected in the representational vocabulary. The set of relations such as subsumption is-a and meronymy part-of describe the semantics of the domain.

An ontology is a triple: O = (C, P, R ) C is a set of concepts, P is a set of concept properties, and R is a set of binary relationship(hasPersonalInformation, is-a, hasFaculty, etc) as shown in Tadle.1.

The process of building the user Profile ontology, based on ontology engineering principles, user ontology captures rich metadata about the user's profile including characteristics, preferences, etc.

## V. USER-PROFILE ONTOLOGY

The ontologies used in relation with user profiles are mostly limited to taxonomies of user interests [9] and it is commonly employed nowadays to enhance usability as well as to support personalization, adaptivity and other user-centric features. Bearing in mind that for most applications profiling is not restricted to user interests but also encompasses other user characteristics such as education, expertise, Responsibility, etc., the user characteristics that encompasses with user profile is mainly concerned to the domain where the user-profile ontology is used. Based on the above aspects, we introduce policy ontology with rich metadata about the employee's profile.

TABLE I. BASIC ELEMENTS OF USER-PROFILE IN EDUCATIONAL ORGANIZATION

| Profile | Relation | Example: Objects |
|---|---|---|
| **User** | hasPersonalInformation | Name, Contact, Address, etc |
| | hasAcademicInformation | Department, Experience, Research Area, etc |
| | hasInstitutionRelatedInformation | Faculty, Nonteaching Staff, Student, etc |
| | | |
| **Institutional** | hasFaculty | Dean, Head, Professor etc |
| | hasNonteachingStaff | Secretary, Technician, Officer, etc |
| | hasStudent | Graduate, Master, Researcher |

In order to provide an explicit specification of the conceptual model, based on the Table1, we defined an ontological approach. That represents core concepts accompanied with the three categories of user information such as Personal, Institutional, and Academic. As shown in Figure 1, the ontology was implemented using Protege [10].

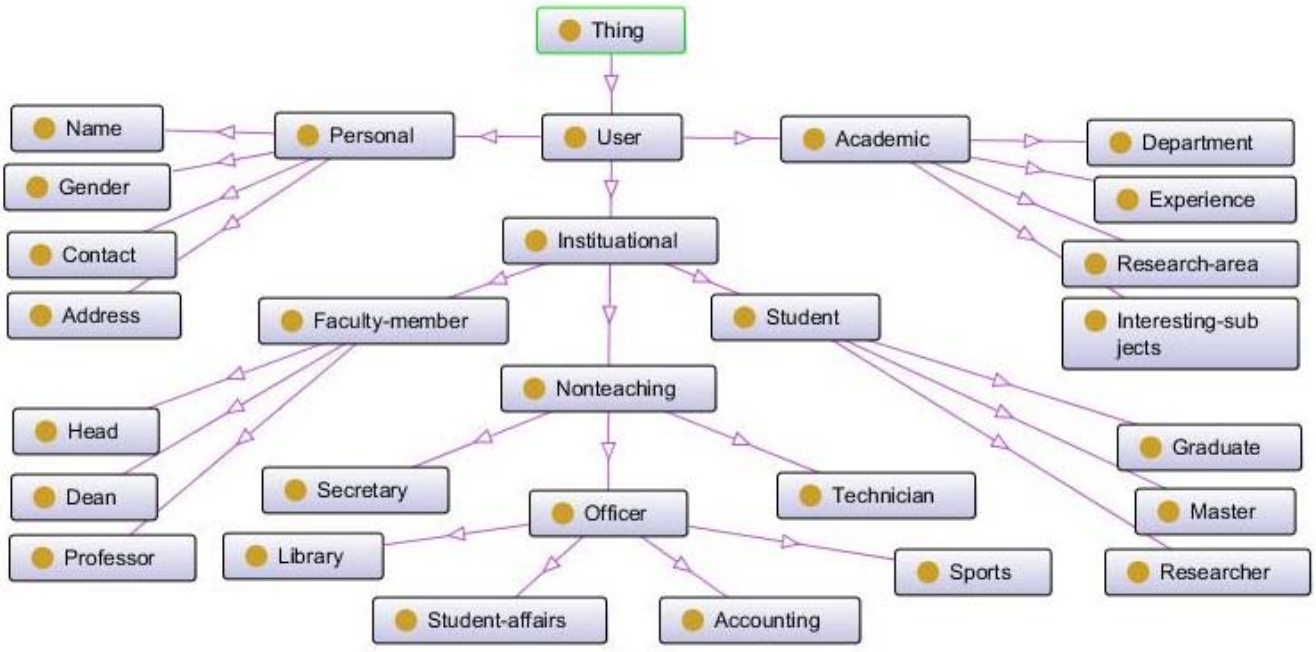


Figure 1. Proposed Ontology for Access Control Mechanism in Educational Organization

Here, we are considering Ontology-based Access Control (OBAC) model for a university domain. In OBAC, the profiles are assigned to users through their personal information, if any change happens in the user's personal information then profile changes without any administrative task and policies related to this new profile will be executed. Thus, OBAC has no administrative tasks expense and does not deal with state changes in user's data [11].

## VI. DESIGN CONSIDERATIONS

Several models have been proposed to address the access control policies, but these cover managing of global policies of organizations. Our goal is to provide a way in which semantic based access control policies can be specified which incorporate user role and activity in educational organization. Figure.2 is our proposed access control model that extend traditional role-based access control model.

In the RBAC policy model, the access permissions are not assigned directly to the particular users, but to the users' roles [12]. In proposed technique, role is not directly mapped to permission. Role is mapped to task that consists of several roles. User is categorized by user domain that is defined by organization's department. The user profile ontology with semantic relationships reflects organization hierarchy and only administrator can change registered relationship. The Ontology Based Decision Engine (OBDE) considers user's relationship and surrounding user information to decide permission assignment and delegation. The proposed model is to create, modify and query with semantically-rich policies. Figure.2 gives a brief example of personalized OBAC model for a university domain. The ontological structure of some individual profile relations of university domain can be seen in previous section.

User-Profile Ontology Base (UO): U represents a set of users and their inter relations. The users are service requesters whose access requests are being controlled. U= {u1, u2, u3,…um}

Roles (R): R represents a set of roles. The roles reflect users' job functions within the organization. R = fr1, r2, r3, … rn}

Resources (Res): Res represents a set of resources. The resources are the objects protected by access control that represent the data container.Res = {res1, res2, res3,…. reso}

Ontology Based Decision Engine: receiving a request from the Access Control Policy Base, and determine whether the Resource should be permitted to access by the concerned user.

Semantic Based Access Control Policy Base: This includes the explicit authorization rules that are defined in Semantic Web Rule Language (SWRL) by security administrators of system.

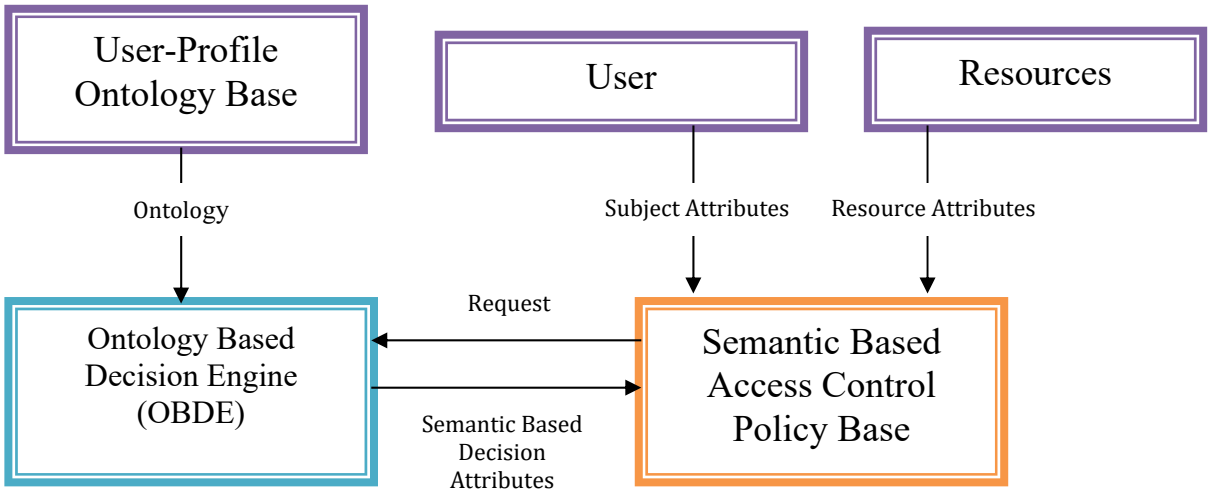


Figure 2. Application scenario of the Access Control Model

## VII. CONCLUSION AND FUTURE WORK

This work is an attempt to develop an access control model by using an ontological approach that incorporates concepts and properties of uses in Educational domain. This is ongoing work and there is much more to be done. It is important to note that the overall approach shown here can, in principle, also be applied to any other domain with similar features.

The future research that derive from the work developed in this paper, we plan to study the interoperability issues that arise in access control and evaluate whether our ontology-based mechanism may provide a suitable solution to interoperate between rules and entities of different scenarios. As future work, to demonstrate the practical applicability, a general system prototype implementing our framework will be developed to build the semantic based access control application through considering university administrative system as a test bed environment.

## REFERENCES

[1] Masoumzadeh, Amirreza, and James Joshi. "Osnac: An ontology-based access control model for social networking systems." In Social Computing (SocialCom), 2010 IEEE Second International Conference on, pp. 751-759. IEEE, 2010.

[2] Carminati, Barbara, 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. ACM, 2009.

[3] Ryutov, Tatyana, Tatiana Kichkaylo, and Robert Neches. "Access control policies for semantic networks." In Policies for Distributed Systems and Networks, 2009. POLICY 2009. IEEE International Symposium on, pp. 150-157. IEEE, 2009.

[4] Reddivari, Pavan, Tim Finin, and Anupam Joshi. "Policy-based access control for an RDF store." In Proceedings of the Policy Management for the Web workshop, vol. 120, no. 5, pp. 78-83. 2005.

[5] Damiani, Ernesto, Sabrina De Capitani di Vimercati, Cristiano Fugazza, and Pierangela Samarati. "Extending policy languages to the semantic web." In ICWE, vol. 2004, pp. 330-43. 2004.

[6] Stan, Johann, Elod Egyed-Zsigmond, Adrien Joly, and Pierre Maret. "A user profile ontology for situation-aware social networking." In 3rd Workshop on Artificial Intelligence Techniques for Ambient Intelligence (AITAmI2008). 2008.

[7] Fong, Philip, Mohd Anwar, and Zhen Zhao. "A privacy preservation model for facebook-style social network systems." Computer Security–ESORICS 2009 (2009): 303-320.

[8] Carminati, Barbara, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham. "Semantic web-based social network access control." computers & security 30, no. 2 (2011): 108-115.

[9] Golemati, Maria, Akrivi Katifori, Costas Vassilakis, George Lepouras, and Constantin Halatsis. "Creating an ontology for the user profile: Method and applications." In Proceedings of the first RCIS conference, no. 2007, pp. 407-412. 2007.

[10] Gennari JH, Musen MA, Fergerson RW, Grosso WE, Crubézy M, Eriksson H, Noy NF, Tu SW. The evolution of Protégé: an environment for knowledge-based systems development. International Journal of Human-computer studies. 2003 Jan 31;58(1):89-123.

[11] Özgü, C. A. N., Okan BURSA, and Murat Osman ÜNALIR. "Personalizable Ontology Based Access Control." Gazi University Journal of Science 23, no. 4 (2010): 465-474.

[12] Kayes, A. S. M., Jun Han, Wenny Rahayu, Md Islam, and Alan Colman. "A Policy Model and Framework for Context-Aware Access Control to Information Resources." arXiv preprint arXiv:1703.02162 (2017).