International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

An Ontological Representation of an Adaptive Access Control Mechanism for Enterprise Cloud

Amardeep Kaur, Amandeep Verma

Abstract: ***With the increased development of cloud computing, access control is of paramount importance as a security concern. Numerous access control approaches exist in various published works. Among such prevalent approaches, Role Based Access Control (RBAC) model for enterprise cloud is scope of the present study. Nowadays, resource management, along with the primary aspect of security concern, is also addressed by the access control policies through restricting the allocation of the computing resources based on the roles assigned to the users. Keeping in view of the upcoming peak-load requirements or certain constraints, the policies may have ineffective resource allocation which leads to over/under-utilization of the resources over a period of time. So, an adaptive access control mechanism is desired that can vary their policies dynamically for resource allocation depending upon the ongoing requirements, for its efficient utilization. This is presented in the form of an adaptive access control mechanism (AACM) that aims to effectively utilize the computing resources in the enterprise cloud. It will aid in identifying the over- and under-allocation of the computing resources defined as access control policies and redefine these policies so as to ensure efficient and effective usage of the enterprise cloud resources. In this paper, this novel approach to access control mechanism for the enterprise cloud is represented using ontologies developed in Protégé. This is developed by identification of the underlying concepts and their interrelationships through properties, in the enterprise cloud. The presented ontology is for the sake of knowledge representation to represent knowledge and facts.***

Keywords: Adaptive Access Control Model, Enterprise Cloud, Knowledge Representation, Ontologies.

I. INTRODUCTION

Cloud computing is an architecture that provide on-demand network access to pooled configurable computing resources and makes ubiquitous computing possible [1]. A computing environment of an enterprise that is protected by the firewall to offer the SaaS, PaaS and IaaS to its users is termed as Enterprise Cloud Computing. Access control is an important security concern in the cloud environment. It contains configured access permissions and privileges defined as an access security policy. This is accountable to control the activities of genuine users. Enough capability and flexibility in these access control policies is desired to encounter the unforeseen and volatile behaviors. Operational and situational knowledge regard factors like resource usage, access pattern and user behaviour that can affect the policies for an efficient and effective access control system.

In conventional IT environment, in order to fulfill the needs of peak load requirement of a given application, more computing resources are assigned by the resource allocation mechanism [2]. In most of the instances, such criteria for resource allocation lead to the underutilization of computing resources that occurs due to the over allocation of resources. Moreover, due to certain constraints, the under allocation of resources may lead to over utilization of such resources. This necessitates a mechanism to adapt the access control model with the current operational environment in order to avoid over allocation or under allocation of resources for its optimum and efficient utilization. The cloud environment which is very dynamic and highly reactive in nature, demands for the adaptation of policies to ongoing changes in the observations for access control [3]. So, an adaptive access control decision system is desired. This can be attributed by adjusting itself to the changing environment by keeping track of the access and denial of resources, along with their utilization, to affect the future access decisions.

The intent of the study in progress is to develop a novel approach to the access control mechanism that will help in the maximizing the utilization of the allocated resources of cloud. This model will aid in identifying the excess or lack of the cloud resources defined as in access control policies for various roles, if exists, and then optimizes the allocation. The suggested mechanism has applicability where access control policies, in addition to their primary concern of providing security, are also accountable for making better utilization of the resources by controlling the resource allocation process. A stated model in abstract form is depicted in paper [4]. The current paper is an attempt to have semantic representation of that model using ontologies.

Nowadays, ontologies have their applications in diverse areas. Managing the knowledge, content and document, integration of information are some of the other areas of applications of ontologies, apart from traditional application of it in semantic web. Ontology as a general vocabulary provides a means of sharing information of interest among researchers [5].

Manuscript received on January 02, 2020.
Revised Manuscript received on January 15, 2020.
Manuscript published on January 30, 2020.
*Correspondence Author
Amardeep Kaur*, Department of Computer Science, Punjabi University Regional Centre for Information Technology and Management, Mohali, India. E-mail: amardeep_tiet@yahoo.com
Amandeep Verma, Department of Computer Science, Punjabi University Regional Centre for Information Technology and Management, Mohali, India. E-mail: vaman71@gmail.com

It comprises of characterizations that can be interpreted by machine about the basic entities in the stated area along with the relations. It puts down the essentials to model a domain by depicting the fundamental provisos and associations that constitutes the vocabulary of the stated area. Such rudiments facilitate to system developers into implying knowledge bases, developing services, and coalescing knowledge bases and services to generate bigger systems.

Development of ontology is analogous to definition(s) of entire data set and their composition for further programs to use.

The intended audience for this paper is researchers involved in addressing the domain of efficient utilization of cloud resources. Furthermore, the researchers working on ontological representation of models, in domain of their research topic may use it as a reference for their work.

The paper is divided into five sections. Section II refers various application areas where ontological representation has been used for their work. Section III describes the ontological representation of AACM. Section IV presents the results and discussions and Section V concludes the paper.

II. RELATED WORK

Review of literature reveals the number of areas where ontology is used for model representation and it has proven its worth. Ontology is more realistic approach to describe the world as it yields a representation that strongly imitates the real world under study. The characterization and usage of an enterprise architecture framework is primarily represented as domain ontology [6]. A role based access control using OWL is presented in the study [7]. A blend of domain and task ontology on the basis of crop cultivation standards is represented in [8]. Knowledge representation through the use of ontologies is exemplified in the paper [9]. The characteristics of ontology modeling were considered to demonstrate the ontology based information retrieval [10]. The knowledge representation about the environment of processing task or methods is represented in [11].

III. ONTOLOGICAL REPRESENTATION OF AACM FOR ENTERPISE CLOUD

An abstract representation of the adaptive access control mechanism (AACM) [4] is trivially revised and hereby represented as an ontology.

A set of concepts, *C* and their properties, represented as set P, constitute ontology *O.* A concept, represented as a class, is a collection of instances. The relationship among individuals as well as data is depicted as a property. The object property specifies the relationship among concepts and datatype property associate instances of concepts to a data literal. Every defined property must have a domain and a range. In case of object properties, both are ontology classes whereas in case of datatype properties, the domain consists of classes and range are data types such as integer, time, etc. Such properties may be constrained by certain restrictions.

The present study use ontological engineering for the representation of AACM for cloud computing.

A. The Concepts

The identified concepts in the study are represented as classes. The sub-concepts that are more precise than the parent concept are depicted as subclasses.

B. The Properties

The relationships are depicted as OWL properties represent and are binary in nature. The object properties map an individual to another individual whereas datatype properties map an individual to a data literal.

As enterprise is the core term in enterprise cloud, so a precise definition of the enterprise is desired. As far as the present study is concerned, the enterprise is defined as E = {USER, RESOURCE} where USER is the finite set of users and RESOURCE is the finite set of available resources in the enterprise. For enterprise cloud, the resources are the computing resources and the users are the cloud users. The classes for USER, RESOURCE and other supporting concepts are shown as ontology in **Fig. 1**. There are 27 classes in all.

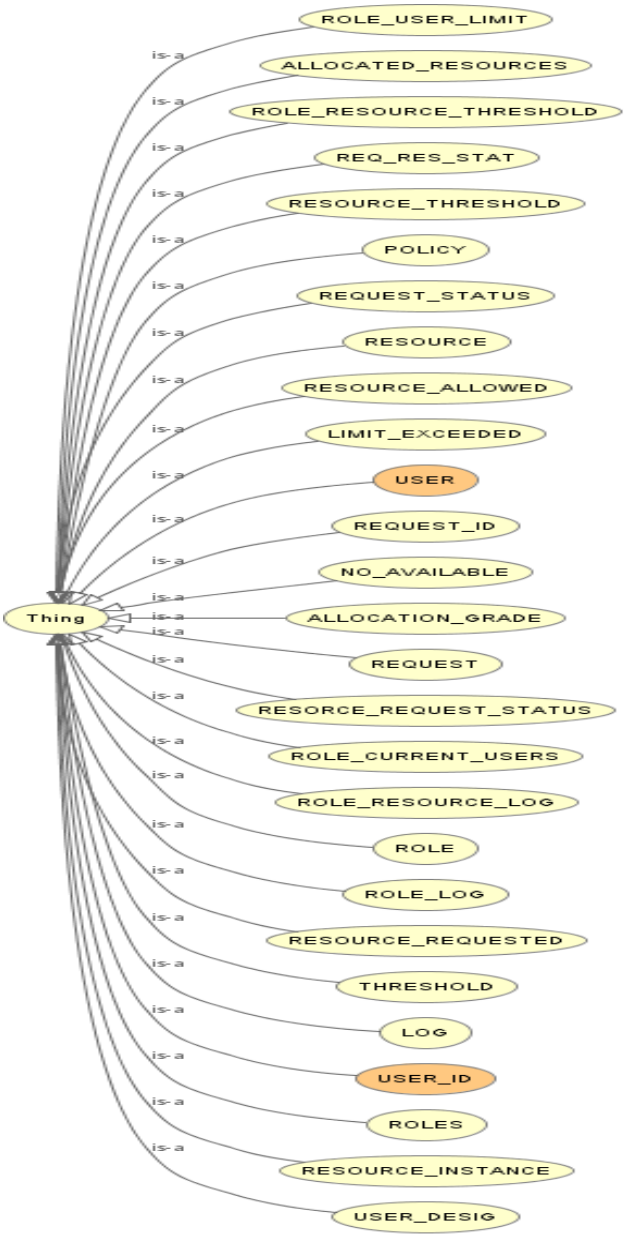

Fig. 1 Concepts of AACM as an Ontology

The main classes and their description are shown in Table-I.

Table- I: Main Classes in AACM Ontology

Concepts	Description
USER	The end user of the services provided by the enterprise cloud
ROLES	A set of possible roles assigned to every user on the basis of user credentials
REQUEST	A request initiated by user to use services offered by cloud
LOG	A log book to record the outcomes of every request
ROLE_LOG	Another log to record the outcomes of every role
ROLE_RES_THRESH	Threshold value on resources for every role

A code segment of OWL code for class declaration is shown in **Fig. 2**.

```
<Declaration>
    <Class IRI="#REQUEST"/>
</Declaration>
<Declaration>
    <Class IRI="#REQUEST_ID"/>
</Declaration>
<Declaration>
    <Class IRI="#REQUEST_STATUS"/>
</Declaration>
<Declaration>
    <Class IRI="#REQ_RES_STAT"/>
</Declaration>
<Declaration>
    <Class IRI="#RESORCE_REQUEST_STATUS"/>
</Declaration>
<Declaration>
    <Class IRI="#RESOURCE"/>
</Declaration>
```

Fig. 2. Code Segment of OWL Code for Class Declaration

The ontological representation for the USER class is shown in **Fig. 3**. The user is defined by a unique id, designation, additional charges (if any), a set of roles with the restriction of atleast one role and the allocated resources for each assigned role at a given instance of time. The dotted lines represent the relationship of the user with other concepts.

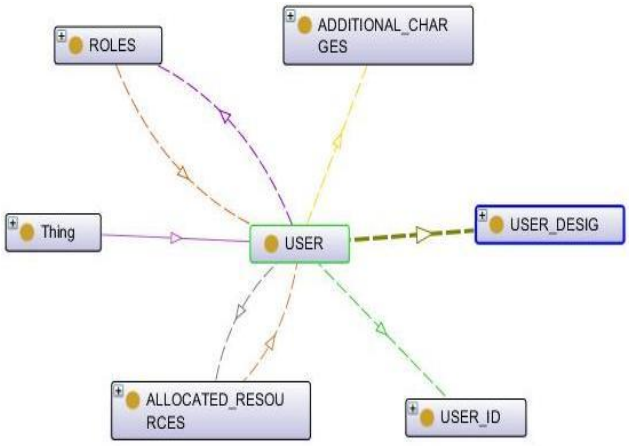

Fig. 3 Ontology of USER

The object properties of USER concept is shown in Table- II. The domain, range and restriction is shown along with. Among the listed properties, many of these are asymmetirc, irreflexive and non-transitive in nature.

Table- II: Object Properties of USER Concept

Property	SubProperty	Domain	Range	Restriction
hasUserProperties	hasUserId	USER	USER_ID	Exactly 1
	hasUserDesig	USER	USER_DESIG	Exactly 1
	hasRoles	USER	ROLES	Some ROLES, Min 1
	hasAdditionalCharge	USER	ADDITIONAL_CHARGES	Min 0
	hasAllocatedResources	USER	ALLOCATED_RESOURCES	Min 0
isUserProperties	isIdentityOfUser	USER_ID	USER	Exactly 1
	isDesigOfUser	USER_DESIG	USER	Some
	isRoleOfUser	ROLES	USER	Some
	isAdditionalChargesOf	ADDITIONAL_CHARGES	USER	Some
	isAllocatedResourcesTo	ALLOCATED_RESOURCES	USER	Some

A code segment for declaration of object properties is shown in **Fig. 4**.

```
<Declaration>
    <ObjectProperty IRI="#hasInstanceForResAllow"/>
</Declaration>
<Declaration>
    <ObjectProperty IRI="#hasInstances"/>
</Declaration>
<Declaration>
    <ObjectProperty IRI="#hasInstancesForRoleResLog"/>
</Declaration>
<Declaration>
    <ObjectProperty IRI="#hasLimitExceeded"/>
</Declaration>
<Declaration>
    <ObjectProperty IRI="#hasLogProperties"/>
</Declaration>
<Declaration>
    <ObjectProperty IRI="#hasNoAvailable"/>
</Declaration>
<Declaration>
    <ObjectProperty IRI="#hasPolicyProperties"/>
</Declaration>
```

Fig. 4 Code Segment of OWL code for Object Property

The REQUEST concept and their relationship with the other concept defined in the ontology is shown in **Fig. 5**. The REQUEST is identified by a unique id, with the information about the user in terms of their id and role, as well the resources requested with their names and number of instances.

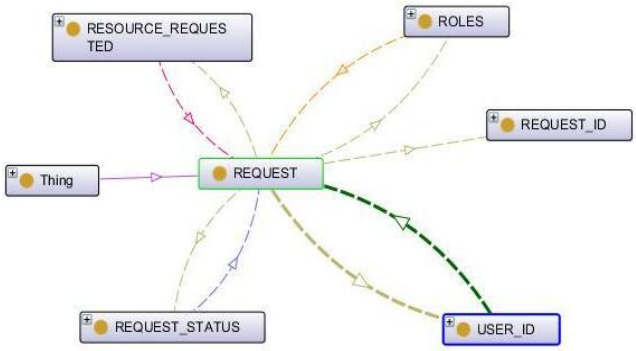

Fig. 5 Ontology of REQUEST concept

The description of the object properties that contains the REQUEST concept either as a domain or as a range is specified in Table- III. The restrictions and information about the super property is also listed.

Table- III: Object Properties of REQUEST Concept

Property	SubProperty	Domain	Range	Restriction
hasRequestProperties	hasRequestId	REQUEST	REQUEST_ID	Exactly 1
	hasRequestStatus	REQUEST	REQUEST_STATUS	Exactly 1
	hasResourceRequest	REQUEST	RESOURCE_REQUESTED	Some Resources
	hasRoleForRequest	REQUEST	ROLES	Exactly 1
	hasUserIdForRequest	REQUEST	USER_ID	Exactly 1
isRequestProperties	isIdentityofRequest	REQUEST_ID	REQUEST	Exactly 1
	isIdentityOfUserOfRequest	USER_ID	REQUEST	Min 0
	isRequestedResourceOfRequest	RESOURCE_REQUESTED	REQUEST	Exactly 1
	isRoleOfRequest	ROLES	REQUEST	
	isStatusOfRequest	REQUEST_STATUS	REQUEST	

A LOG concept which is used to record all the relevant information about the request is maintained. Its relationship with the relevant concepts is described in the **Fig. 6**. The log has information about the user identity, request identity, role of the respective user, current status of the request, and the description of each requested resource.

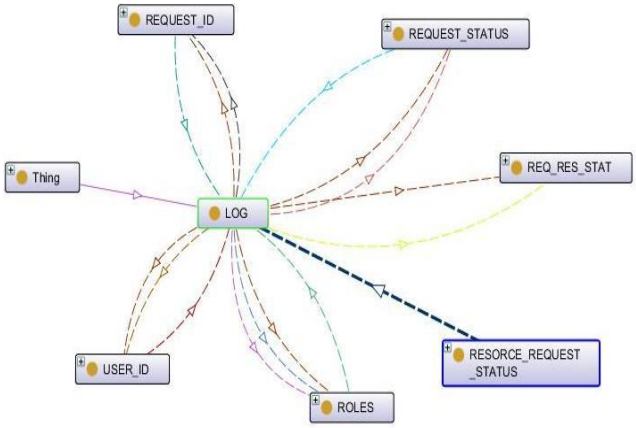

Fig. 6 Ontology of LOG Concept

Object properties of LOG concept is shown in Table- IV. It has all the properties like user id, request id, role, status of the requested resource, which are required for further analysis of the request for resource allocation.

Table- IV: Object Properties of LOG Concept

Property	SubProperty	Domain	Range	Restriction
hasLogProperties	hasUserIdForLog	LOG	USER_ID	Some
	hasRequestIdForLog	LOG	REQUEST_ID	Exactly 1
	hasRoleForLog	LOG	ROLES	Some
	hasReqStatForLog	LOG	REQUEST_STATUS	Some
	hasReqResStatForLog	LOG	REQ_RES_STAT	Some
isLogProperties	isRequestIdInLog	REQUEST_ID	LOG	
	isRoleOfLog	ROLES	LOG	
	isStatusOfRequestedResources	RESOURCE_REQUEST_STATUS	LOG	
	isStatusOfRequestInLog	REQUEST_STATUS	LOG	
	isUserIdOfRequestInLog	USER_ID	LOG	

The POLICY concept with other required concepts for the specification of the policies is shown in **Fig. 7**. The policies define the resource and their number of instances for each role.

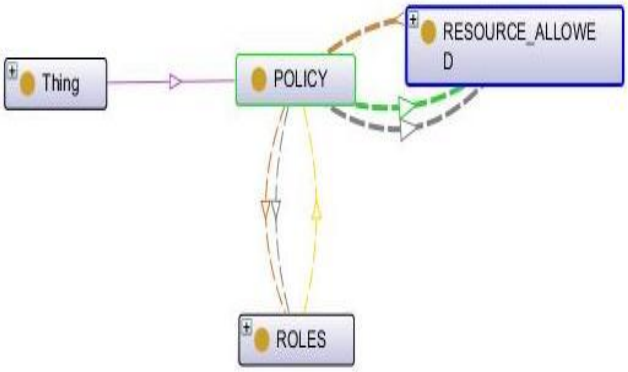

Fig. 7 Ontology of POLICY Concept

The linkage of POLICY with concepts ROLES, RESOURCE_ALLOWED through object properties is described in Table- V.

Table- V: Object Properties of POLICY Concept

Property	SubProperty	Domain	Range	Restriction
hasPolicyProperties	hasRolesForPolicy	POLICY	ROLES	Universal
	hasResAllowForPolicy	POLICY	RESOURCE_ALLOWED	Some
isPolicyProperties	isAllowedResourceInPolicy	RESOURCE_ALLOWED	POLICY	
	isRoleInPolicy	ROLE	POLICY	

As the RESOURCE concept is fundamental in this ontology, it is related with a number of other concepts like RESOURCE_REQUESTED, ROLE_RESOURCE_LOG, REQ_RES_STAT. These inter-relationships as an ontology is represented in Fig 8.

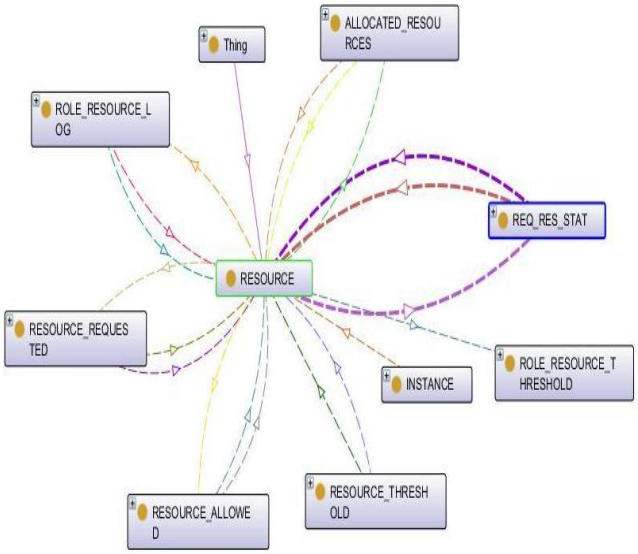

Fig. 8 Ontology of RESOURCE Concept

The object properties with RESOURCE either as a domain or as a range is represented in Table- VI.

Table- VI: Object Properties of RESOURCE Concept

Property	SubProperty	Domain	Range	Restriction
hasResourceProperties	HasInstances	RESOURCE	INSTANCE	Some
hasAllocatedResourcesProperties	hasResourceForAllocRes	ALLOCATED_RESOURCES	RESOURCE	
isResourceProperties	isInstanceOfResource	INSTANCE	RESOURCE	

The detailed information about RESOURCE_REQUESTED concept as an ontology is shown in Fig 9. The requested resource has the information about the name of the resource and the number of instances requested for that resource.

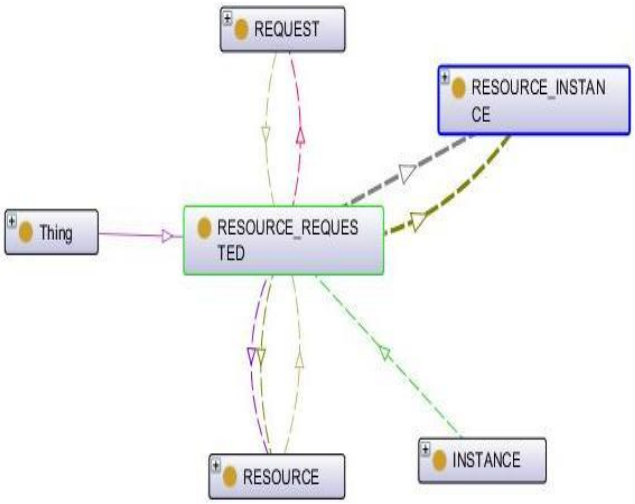

Fig. 9 Ontology of RESOURCE_REQUESTED

The object properties relating to RESOURCE_REQUESTED and the RESOURCE_INSTANCE, RESOURCE are represented in Table- VII.

Table- VII: Object Properties of RESOURCE_REQUESTED

Property	SubProperty	Domain	Range	Restriction
hasResourceRequestProperties	hasResInstForResReq	RESOURCE_REQUESTED	RESOURCE_INSTANCE	
	hasResourceForResReq	RESOURCE_REQUESTED	RESOURCE	
isResourceRequestProperties	isInstanceForResRequest	INSTANCE	RESOURCE_REQUESTED	
	isResourceForResRequest	RESOURCE	RESOURCE_REQUESTED	

The concept ROLES i.e. the name of all the roles, the concept user limit for a given role and the concept number of users currently in a given role with their inter-relationship to ROLE concept is shown in Fig 10.

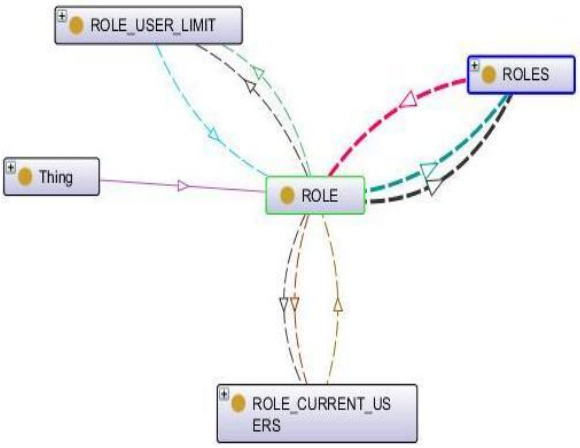

Fig. 10 Ontology of ROLE Concept

The object properties relating ROLE with other concepts in terms of domain, range and restriction is shown in Table- VIII.

Table- VIII: Object Properties of ROLE Concept

Property	SubProperty	Domain	Range	Restriction
hasRoleProperties	hasRoleCurrentUsers	ROLE	ROLE_CURRENT_USERS	Exactly 1
	hasRolesForRole	ROLE	ROLES	Universal
	hasRoleUserLimit	ROLE	ROLE_USER_LIMIT	Exactly 1
isRoleProperties	isCurrentUsersInRole	ROLE_CURRENT_USERS	ROLE	
	isRolesInRole	ROLES	ROLE	
	isUserLimitInRole	ROLE_USER_LIMIT	ROLE	

A ROLE_LOG concept that has the information about the resource in terms of ALLOWED, UNAVAILABLE and BEYOND_LIMIT for each resource in every role is shown in Fig 11.

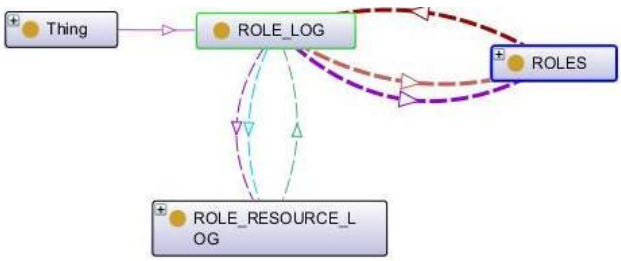

Fig. 11 Ontology of ROLE_LOG Concept

Table- IX shows the object properties associated with ROLE_LOG concept.

Table- IX: Object Properties of ROLE_LOG Concept

Property	SubProperty	Domain	Range	Restriction
hasRoleLogProperties	hasRoleForRoleLog	ROLE_LOG	ROLES	
	hasRoleResLogForRoleLog	ROLE_LOG	ROLE_RESOURCE_LOG	
isRoleProperties	isLogOfRoleResource	ROLE_RESOURCE_LOG	ROLE_LOG	
	isRoles	ROLES	ROLE_LOG	

The ROLE_RESOURCE_LOG in terms of availability, non availability and limit exceeded as ontology is represented in Fig 12.

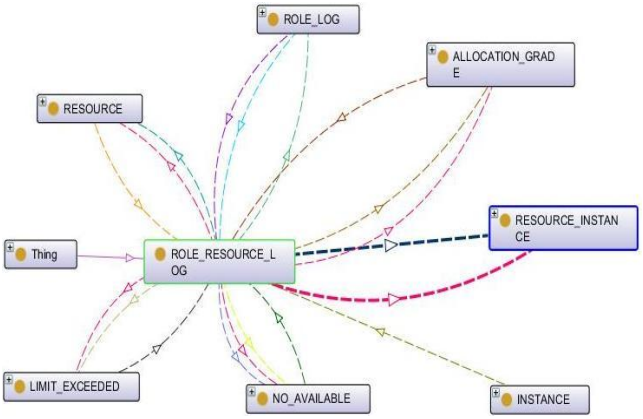

Fig. 12 Ontology of ROLE_RESOURCE_LOG

Object properties of ROLE_RESOURCE_LOG is shown in Table- X. It has five properties that have this concept as a domain and five properties having it as a range.

Table- X: Object Properties of ROLE_RESOURCE_LOG

Property	SubProperty	Domain	Range	Restriction
hasRoleResourceLog	hasAllocationGrade	ROLE_RESOURCE_LOG	ALLOCATION_GRADE	Some
	hasInstancesForRoleResLog	ROLE_RESOURCE_LOG	RESOURCE_INSTANCE	Some
	hasLimitExceeded	ROLE_RESOURCE_LOG	LIMIT_EXCEEDED	Some
	hasNoAvailable	ROLE_RESOURCE_LOG	NO_AVAILABLE	Some
	hasResourceForRoleResLog	ROLE_RESOURCE_LOG	RESOURCE	Some
isRoleResourceLogProperties	isAllocationGradeOf	ALLOCATION_GRADE	ROLE_RESOURCE_LOG	
	isInstancesOf	INSTANCE	ROLE_RESOURCE_LOG	
	isLimitExceeded	LIMIT_EXCEEDED	ROLE_RESOURCE_LOG	
	isNoAvailableOf	NO_AVAILABLE	ROLE_RESOURCE_LOG	
	isResourceOf	RESOURCE	ROLE_RESOURCE_LOG	

As shown in Fig 13, the threshold values for all resources in every role is specified as concept ROLE_RESOURCE_THRESHOLD.

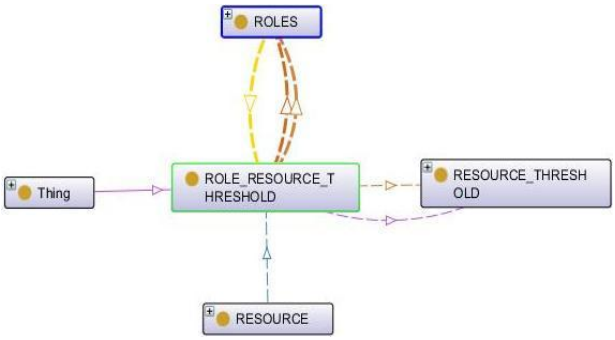

Fig. 13 Ontology of ROLE_RESOURCE_THRESHOLD

Object Properties shown in Table- XI are related with the ROLE_RESOURCE_THRESHOLD Concept. It is associated with ROLES and RESOURCE concept.

Table- XI: Object Properties of ROLE_RESOURCE_THRESHOLD

Property	SubProperty	Domain	Range	Restriction
hasRoleResourceThreshold	hasResThreshForRoleResThreshold	ROLE_RESOURCE_THRESHOLD	RESOURCE_THRESHOLD	
	hasRoleForRoleResThreshold	ROLE_RESOURCE_THRESHOLD	ROLES	
isForRoleResourceThreshold	isResourceForRRT	RESOURCE	ROLE_RESOURCE_THRESHOLD	
	isRoleForRRT	ROLES	ROLE_RESOURCE_THRESHOLD	

Finally, the inter-relationship of the ROLES with already defined concepts is shown as ontology in Fig 14. It is evident from the representation that ROLES is associated with most of the concepts of this ontology.

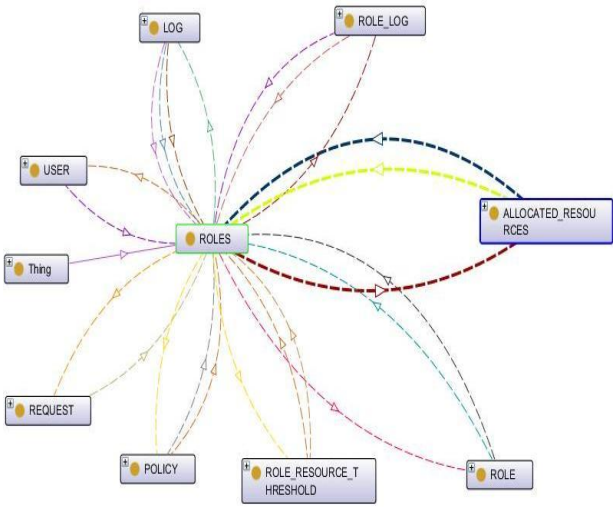

Fig. 14 Ontology of ROLES Concept

The data properties used in the ontology are shown in Table- XII.

Table- XII: Data Properties of AACM ontology

Property		Domain	Range
hasUserProperties	hasUserId	USER_ID	positiveInteger
	hasUserDesig	USER_DESIG	positiveInteger
hasRoleProperties	hasRoleCurrentUsers	ROLE_CURRENT_USERS	Exactly 1 integer
	hasRoleUserLimit	ROLE_USER_LIMIT	Exactly 1 integer
hasInstances		INSTANCE	positiveInteger
hasRequestId		REQUEST_ID	positiveInteger
hasLimitExceededValue		LIMIT_EXCEEDED	positiveInteger
hasNoAvailableValue		NO_AVAILABLE	positiveInteger
hasThresholdValue		THRESHOLD	positiveInteger

C. The Individuals

Some of the individuals defined for the current ontology are shown in Table- XIII.

Table- XIII Individuals defined for REQUEST_STATUS and RESOURCE_REQUEST_STATUS class

Class	Individuals
REQUEST_STATUS	ACCEPTED
	COMPLETED
	DISCARDED
	PROCESSING
	WAITING
RESOURCE_REQUEST_STATUS	ALLOW
	BEYOND_LIMIT
	UNAVAILABLE

The ontologies represented here have been developed using Protégé.

IV. RESULTS

The ontology for an adaptive access control mechanism (AACM) is presented. In totality, it is represented by 12 ontologies. The object properties as well data properties (if any) are also tabulated along with the constraints on these properties. The domain, range and type of property are also tabulated.

The developed ontology represents a mechanism for an adaptive access control for enterprise cloud. The purpose to use ontology for presenting the mechanism is the comprehensiveness of this means of knowledge representation. The novelty in the suggested mechanism is to use the access control mechanism for efficient resource allocation in addition to its primary concern of security. The effectiveness in resource allocation can be achieved by controlling the over and under allocation of resources. This purpose can be realized by making the access control policies adaptive to the user(s) request behaviour for a period of time.

V. CONCLUSION

The representation of the mechanism as an ontology has begun with the identification of the concepts and their interrelationships. The relationships among concepts are represented by object properties and the relation of concepts to data literals are shown by data properties. The constraints on such properties are tabulated. The individuals as concrete instances of the concepts are also listed.

The advantage of this ontology is for the researchers and the developers working in the said area. As ontology is a formalized and standardized way of knowledge representation, so this can easily be used for implementation in live applications.

REFERENCES

1. Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing," *J. Inf. Secur. Appl.*, vol. 19, no. 1, pp. 45–60, 2014.
2. W. Lin, J. Z. Wang, C. Liang, and D. Qi, "A threshold-based dynamic resource allocation scheme for cloud computing," *Procedia Eng.*, vol. 23, pp. 695–703, 2011.
3. R. A. Shaikh, K. Adi, and L. Logrippo, "Dynamic risk-based decision methods for access control systems," *Comput. Secur.*, vol. 31, no. 4, pp. 447–464, 2012.
4. A. Kaur and A. Verma, "An Abstract Model for Adaptive Access Control in Cloud Computing," in *Proceedings of International Conference on Recent Advancement on Computer and Communication*, 2018, vol. 34, pp. 269–277.
5. R. Mizoguchi, "Tutorial on ontological engineering," *New Gener. Comput.*, vol. 21, no. 4, pp. 365–384, 2003.
6. D. Man, "Ontologies in Computer Science," *Didact. Math.*, vol. 31, no. 1, pp. 43–46, 2013.
7. T. Finin *et al.*, "ROWLBAC - Representing Role Based Access Control in OWL," in *Proceedings of the 13th ACM symposium on Access control models and technologies*, 2008, vol. 35, pp. 73–82.
8. D. Li *et al.*, "An ontology-based knowledge representation and implement method for crop cultivation standard," *Math. Comput. Model.*, vol. 58, no. 3–4, pp. 466–473, 2013.
9. P. M. Santos and A. J. Rover, "Knowledge representation through ontologies: an application in the electronic democracy field," *Perspect. em Ciência da Informação*, vol. 21, no. 3, pp. 22–49, 2016.
10. K. Munir and M. Sheraz Anjum, "The use of ontologies for effective knowledge modelling and information retrieval," *Appl. Comput. Informatics*, vol. 14, no. 2, pp. 116–126, 2018.
11. R. Gayathri and V. Uma, "Ontology based knowledge representation technique, domain modeling languages and planners for robotic path planning: A survey," *ICT Express*, vol. 4, no. 2, pp. 69–74, 2018.

AUTHORS PROFILE

Amardeep Kaur is a faculty member in the subject of Computer Science at Punjabi University Regional Centre for Information Technology and Management, Mohali. She has done her B.E. (CSE) from Thapar University, Patiala and M.E.(CSE) from Panjab Engineering College, Chandigarh. She is currently pursuing her PhD in Computer Engineering. The area of research is the development of mechanism of access control for effective resource allocation in enterprise cloud. She is credited with various publications in journals and as well in the proceedings of international and national conferences. She has guided a number of M.Tech (CSE) students for their research dissertations.

Dr. Amandeep Verma is a faculty member in the subject of Computer Science at Punjabi University Regional Centre for Information Technology and Management, Mohali. He is B.E. (CSE), M.Tech.(CSE), and PhD in Computer Engineering. His area of specialisation is the application of ontological engineering, access control, digital image processing and natural language processing. He has number of research paper publications in various reputed international journals and proceedings of the international conferences.