International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-7)

Research Article | **July 2017**

Role-Evolution in Role-based Access Control System

Suganthy. A*
Department of Banking Technology
Pondicherry University, Puducherry, India

Dr. T. Chithralekha (Associate Professor)
Department of Computer Science and Engineering
Pondicherry University, Puducherry, India

Abstract—

Security is a major concern in today's digital world. Role based access control provides a mechanism for protecting the digital information in an organization by assigning roles to the individual user and giving permissions to the assigned roles for accessing any resources. This paper describes the importance of roles in an organization and the evolutionary changes that occurs with respect to the organizational roles. Here the role is defined as an entity and the attributes of the roles have been identified with their related operations. The evolutionary changes that happens to the roles in an organization is identified and evolutionary algorithms have been proposed to handle these changes which helps in simplifying the formulation of access control policies.

Keywords*— *Access control, Role based access control, Access control modelling, Evolution handling, Role Evolution.

I. INTRODUCTION

Securing the Information System is becoming a major challenge in today's Business environment. Access control is a means of controlling the system resources from unauthorized usages. Access control allows an authorized user to access the resources and forbids an unauthorized users from accessing the resources. Access control policies helps to maintain the list of authorized users for every resources in an organization. Access control models used in organizations includes Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC). RBAC method is well suited in multiuser environment where the controlling of the system resources becomes more challenging. In RBAC, every user is given a role and the roles are given permissions for accessing the objects. The three basic security principles supported by RBAC are separation of duty, principle of least privilege and data abstraction [2]. Roles are assigned the limited permissions to support least privilege concept, and no two mutually exclusive roles have the same set of permissions. And the role permissions are abstract in nature thereby supporting data abstraction. With these three basic security principles, it becomes easy for an organizations to protect their resources and RBAC is also more flexible when compared to MAC and DAC.

RBAC method for modelling the access control also reflects the organizational structure and highlights the responsibilities assigned to the users. Every organization in this dynamic environment undergoes changes and these changes should be reflected in the system which models the organizational structure. In RBAC, the organizational supporting systems are modelled with the help of the relationships between users, roles and their permissions. Because of the organizational changes the role-role, user-role and role-permission relations should be updated to reflect the system evolution [3].

RBAC has been standardized by NIST [12] and defined four different models of RBAC as depicted in Fig 1. These models are characterized as flat, hierarchical constrained and consolidated models. The flat model is the one which does not support any hierarchy or constraints and this is referred as the core RBAC model and the other model models are built upon this model. The role hierarchical model is built on the core model with hierarchical relationships among the roles. The constrained model supports the constraints in the role hierarchy and the consolidated model supports both the role hierarchy and the constraints that can be included in the role-permission assignment and user role assignment.

Structural changes in the organization becomes unavoidable due to many reasons like: an employee moves from one designation to the other in the organization, or an employee may quit the job, etc. These changes in the organization reflects the system structure which results in changing the access control rules and constraints of an existing model. The evolving changes in the access control models to reflect the evolving organization changes is often observed in the RBAC models as "Evolutions" [3], [4], [5], [6].

Evolution in access control model consists of changes in the roles that are assigned to a user and due to these changes there may be changes in the permission set. And these changes should not violate the constraints imposed in the organization [4]. Fig 2 depicts an organizational role hierarchy where the top level in the hierarchy indicates the higher designation role than that of the lower levels.

Evolution handling in RBAC is more challenging and is well studied and reported in the paper authored by K.Shantha Kumari, T.Chithralekha [15]. These authors have also published other papers focusing on evolving permissions in access control policies [16]. In continuation with their work, this paper focuses on the changes that takes place with respect to the roles in an organization. This paper is structured as follows: Section 2 focuses on the importance of roles in role based access control systems and formally defines a role. Section 3 gives the role operations that are identified as part of this work and the conclusion and future research work is given in Section 4 of this paper.

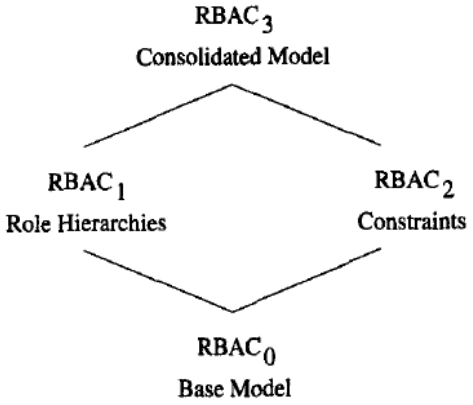

Fig. 1 RBAC Reference Models

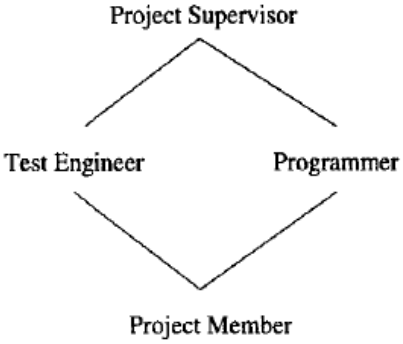

Fig. 2 Organizational Role Hierarchy

II. ROLES IN ROLE BASED ACCESS CONTROL

In the basic RBAC model proposed by R. Sandhu et all [1], a role is defined, based on the organizations roles (ie) a role is assigned in accordance to the employee's position in the organization. Identifying the roles in an organization is a major task in the RBAC systems and the process of identifying roles and their permissions and assigning users to the roles is often termed as role engineering. In an organization, the roles are generally defined based on the job functions [8] and in [7], the author defines the roles as a set of rights and duties. This section defines the role as an entity with the attributes.

Table I Font Sizes for Papers

Name	Name of the role
Description	Description of the role
Permissions	Set of permissions
Children	A list consisting of all the assigned children of the role
Max_Cardinality	Maximum number of children
Parent	Parent of the current role
Relations	with other roles
Constraints	Set of all constraints assigned to the role

A. Role Definition

A role is identified with the attributes as given in table I. A set of properties that a role should possess is also identified and tabulated in Table II. These properties includes: the role operations, the role relations, role constraints, role status and role types. Role operations are briefly explained in section 3. Role relations gives the types of relationship that exists between two roles and these relations are of mutually exclusive, inheritance, association and dependency. If there exists a mutually exclusive relations between two roles it means that the permissions that can be assigned to these two mutually exclusive roles should be different. In other words, there will not be any common permission that exists among these two roles. If two roles have inheritance relationship between them then the parent of the role will inherit all the permissions and constraints of the child role. The association relation is defined as a simple relation between two roles and the dependency relation between two roles is that, one role is completely dependent on the actions that are completed by the other dependent role.

Table III Role and Its Properties

Role Properties	
Role Operations	Create Role
	Add Role
	Delete Role
	Merge Roles
	Split Roles
	Delegate
	Revocation
Role Relations	Mutually Exclusive
	Inheritance
	Association
	Dependency
Role Constraints	Prerequisite
	Permission
	Cardinality / Role Assignment Constraints
Role Status	Active
	Passive
Role Types	Flat Role
	Hierarchical Role

The constraint property of the role tells three different constraints that exists between roles: prerequisite, cardinality and permission constraints. Prerequisite constraint gives the necessary constraints that needs to be verified whenever any operations are to be performed on these roles. The cardinality or the role assignment constraints denotes the maximum number of children assigned for a given role and the permission constraints gives the set of permissions allowed for the given role.

The other properties that exists in a role are the status of the role for the indicating the active or the passive state of the role and the role type indicates the type of relationships that exists between the role: hierarchical or flat.

Based on the identified attributes of the role, a role denoted by R formally defined as follows:

R(Name, Description, Permissions, Children, Max_cardinality, Parent, Relations, Constraints)
Where
Name= Name of the Role
Description = Description of the role
Permissions = Role permissions set
Children = The set of children assigned to the role
Max_Cardinality = Maximum cardinality of the role
Parent = The Parent node
Relations = {R(pi,pj) $\forall$ pi,pj ε Role.Permisssion}
Constraints = {C(pi,pj) $\forall$ pi,pj ε Role.Permisssion}

A permission set (P) is defined as the set consisting of all the permissions of a role and is formally defined as follows:

P(Name, Description, Members, Relations, Constraints) where,
Name = Name of the Set
Description = Descriptions of the permissions
Members = { p_i | p_i is a permission, $\forall$ i}
Relations = {R(pi,pj) $\forall$ i,j }, where R: PxP $\rightarrow${=, <, >} // Defines the hierarchy of permissions
Constraints = {C(pi,pj) | C(pi,pj) =0}, where C: PxP $\rightarrow${0,1} // 0 if mutually exclusive and 1 otherwise

III. ROLE OPERATIONS IN ROLE BASED ACCESS CONTROL SYSTEMS

Role operations indicates the structural changes that takes place in an organization. These structural changes happens when a new employee joins in the organization or an existing employee resigns or leaves the organization and so on. These role operations includes: creating a new role, adding roles, deleting an existing role from the hierarchy, merging two roles that have the similar permissions, splitting a single role to more than one role, the delegation operation which involves in transferring the permissions of a role to the other role and the revocation operation is the one by which the delegated permissions are taken back from a role. Table III gives the role evolutionary operators and briefly describes the consequences of how these operations are affected by the constraints and the relations that exists among these roles.

Table IIIII Role Evolutionary Operations

Operations	Constraints	Relations Affected	Invoking Operations
Add Role	**Prerequisite** Assign the set of permissions to the role No two roles should have the same permission set Assign the level in the role hierarchy where the role needs to be included Include the relationship with other roles **Cardinality Constraint:** The maximum number of roles to be added should not be exceed.	• Cardinality Constraint: Based on this constraint, **merging or split** operation may take place. • Inheritance: the permissions assigned to the new role should be inherited by its parent role. • Mutually exclusive: no two mutually exclusive roles are added in a hierarchical relation (parent-child). Allow only one role to be active at a time	Merge: If the newly added node has the same permission has that of the existing one Split: takes place when the cardinality constraints arises.
Delete Role	Deletion of a role should not introduce any dangling reference. If the deleted role has already delegated any of its roles / permissions then Revocation operations takes place	• Mutually exclusive roles: Not affected • Inheritance: If the role to be deleted is the child role, then assign its permissions to its parent role. If the role is a parent one, then assign its permission and all its child roles to the role above it. • Aggregation: Deleting parent – Assign the child to other node. Deleting Child – Assign its permission to its siblings • Composition: Deleting parent – Assign the child to other node. Deleting Child – Assign its permission to its siblings • Call **Revocation** Operation if necessary	Delegation Add Role
Merge Roles	Hierarchical role: Based on prerequisite and cardinality constraints Prerequisite: Merging should not affect the level of the role in the hierarchy. Cardinality: should not affect the cardinality constraint	• Mutually exclusive roles: Not applicable • Inheritance: o If the roles are merged does not have any child note then assign all its permissions to the newly merged role. o If the roles to be merged have children then assign the permissions and its children to the newly merged role. • Association: merge two roles that have the common permission set in the same level. Delegate and delete the role (Two roles becomes one role) • Dependency operation: delegate and delete • Delegation / Revocation: Perform revocation operation before delegation operation	Delegation and Deletion operation takes place
Split Roles	Based on the cardinality constraints and the permission sets In the root level: The role that needs to be split should not have the same permission.	• Mutually exclusive roles: Not applicable • Inheritance: maintain hierarchy level and parent-child relations	Add node

	Parent node: Add a new node in the same level whose permission set is different		
Delegate	Hierarchical role (Role to Role): Permission Delegation Role Delegation Cardinality Prerequisite	• Mutually exclusive roles: Not applicable • Inheritance: Relationship removal Relationship creation	Add node: If the children of the role to be delegated needs to be assigned to the delegatee role

IV. CONCLUSION AND FUTURE WORK

This paper focuses on the evolutionary changes of roles in role based access control systems. A formal definition for role is given by identifying the role and its attributes. Based on the organizational roles and its changes the role operations are identified and these operations are termed as evolutionary operations. As part of this research, the author is currently working on the algorithms of all the role operations that has been identified.

REFERENCES

[1] Sandhu R, E. Coyne, H. Feinstein, and C. Youmann, "Role-Based Access Control Models", IEEE Computer, 2(29):38-47, 1996.
[2] A. Cenys, A. Normantas and L. Radvilavicius, "Designing role-based access zcontrol policies with UML", Journal of Engineering Science and Technology Review, 2009
[3] Jinwei Hu et al,, "Role updating for Assignments", SACMAT, 10 Proceedings of the 15th ACM symposium on Access control models and technologies, 2010.
[4] M. Koch, L.V.Mancini, F.Parisi-Presicce, "On the Specification and Evolution of Access Control policies", Proceeding of SACMAT'01, Sixth ACM Symposium on Access Control models and technologies, Pages 121-130, Chantilly, Virginia, USA, ISBN: 58113-350-2
[5] Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati, "Over-encryption: Management of Access Control Evolution on outsourced Data", VLDB '07, September 23-28, 2007, Vienna, Austria. Copyright 2007 VLDB Endowment, ACM 978-1-59593-649-3/07/09.
[6] Stefanie Rinderle, Manfred Reichert, "On the controlled evolution of Access Rules in cooperative information systems", Springer 2005.
[7] Longhua Zhang et al, "Rule-based framework for Role-based delegation", SACMAT' 01 Proceedings of the sixth ACM symposium on Access control models and technologies
[8] D.Jonscher, "Extending Access Controls with duties – Realized by Active Mechanisms", Elsiever, 1993
[9] Sejong Oh, Seog Park, "Task-role based access control model", Informations Systems, Elsiever Science, 2003.
[10] Manachai Toahchoodee, Ross M. Mcconnell, "Using Graph Theory to Represent a Spatio-Temporal Role-Based Access Control Model", IJNGC, 2016
[11] R.S Sandhu, D. Ferraiolo, and D. Kuhn, The NIST model for Role-based Access Control: Towards a Unified Standard, Proceedings of the 5th ACM Workshop on Role-based Access Control, Berlin, Germany, July 26-27, 2000.
[12] David F. Ferrariolo, Ravi Sandhu, D. Richard Kuhn and Ramaswamy Chandramouli, Proposed NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, August 2001
[13] Joon S. Park et al, Composite RBAC Approach for Large, Complex Organizations, ,SACMAT'04 ACM Proceedings, 2004
[14] Ninghui Li, Ziging Mao, Administation in Role-Based Access control, ASIAC'07, 2007
[15] K.Shantha Kumari, T.Chithralekha, "Challenges in Modeling Evolving Access Control Policies using Feature Modeling", Journal of Software, Vol. 9, No.5, May 2014.
[16] K. Shantha Kumari, Features Based Model for Handling Evolutions In Role Based Access Control Policies, Presented in Third Doctoral Colloquium at Institute for Development and Research in Banking Technology, Hyderabad, 2013.

