International Journal of Computer Engineering & Technology (IJCET)
Volume 9, Issue 5, September-October 2018, pp. 201–213, Article ID: IJCET_09_05_023
Available online at
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=9&IType=5
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

ROLE-CENTRIC RBAC MODELS – A LITERATURE REVIEW

Suganthy A
Department of Banking Technology,
Pondicherry University, India

Dr. V. Prasanna Venkatesan
Professor, Department of Banking Technology
Pondicherry University, India

ABSTRACT

Protecting the system resources from vulnerable access is more challenging in today's digitalized environment and identifying a suitable mechanism for access control is more critical. Access control based on Roles is more suitable for the organizational resources and this paper explores the role based access control (RBAC) models. RBAC models are based on the concept that the system resources are accessed based on the roles by which the user of the system access the system resources and every role in the system is associated with certain permissions. This paper identifies the requirements where the RBAC models needs to be extended to support the security of the systems. Such models are referred in this paper as Role-Centric extended models and the application of these extended models are explained in this paper along with the research opportunities.

Key words: RBAC Models, Applications of RBAC, Extensions to RBAC, Role-Centric RBAC Models.

Cite this Article: Suganthy A and Dr. V Prasanna Venkatesan, Role-Centric RBAC Models – A Literature Review. *International Journal of Computer Engineering and Technology*, 9(5), 2018, pp. 201-**2**13.
http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=9&IType=5

1. INTRODUCTION

Protecting the System resources is a challenging task in the present business condition. Access control helps the organization to control their assets from unapproved usages. Access control enables an approved user to access the assets and prohibits an unapproved user to access the assets. The policies in access control helps in maintaining the proper usages of the assets in any organization.

There are many models that can be applied to control the system resources. The widely used access control methods for protecting the system resources are Mandatory Access Control (MAC) and Discretionary Access Control (DAC). In MAC, the system administrator

assigns the permissions to the users of the system depending on the level of security that is required for each of the resource. The most suitable application of MAC policies are in the Military organization where the security policies are strictly administered by the administrator. In DAC, an object is accessed by a user with the type of the permissions that are given to the user while creating an object. An example for DAC is the UNIX system, where the owner of the object define the read, write and execute permissions to every file created by him. But these two access control models were not powerful and flexible to control the organizational resources where the access to the resources are controlled by the users with different levels of control rights.

The third type of access control model is "Role Based Access Control" introduced by the research community in 1992 to cope up with the organizational requirements for controlling the system resources [21]. RBAC model is appropriate in multiuser systems where the controlling of the assets becomes more challenging. In RBAC model, the users are assigned with roles and the roles are given permissions to access the objects in the system. RBAC model support the three security principles: least privilege, separation of duties and data abstraction. Roles are assigned the limited permissions to support least privilege concept, separation of duties constraint is supported by imposing the rules on roles that "no two mutually exclusive roles have the same set of permissions". The data abstraction principle is supported in RBAC by means of the permissions assigned to the roles. The RBAC models with their principles helps the organization to achieve their security goals in a better way when compared to the other two models defined previously.

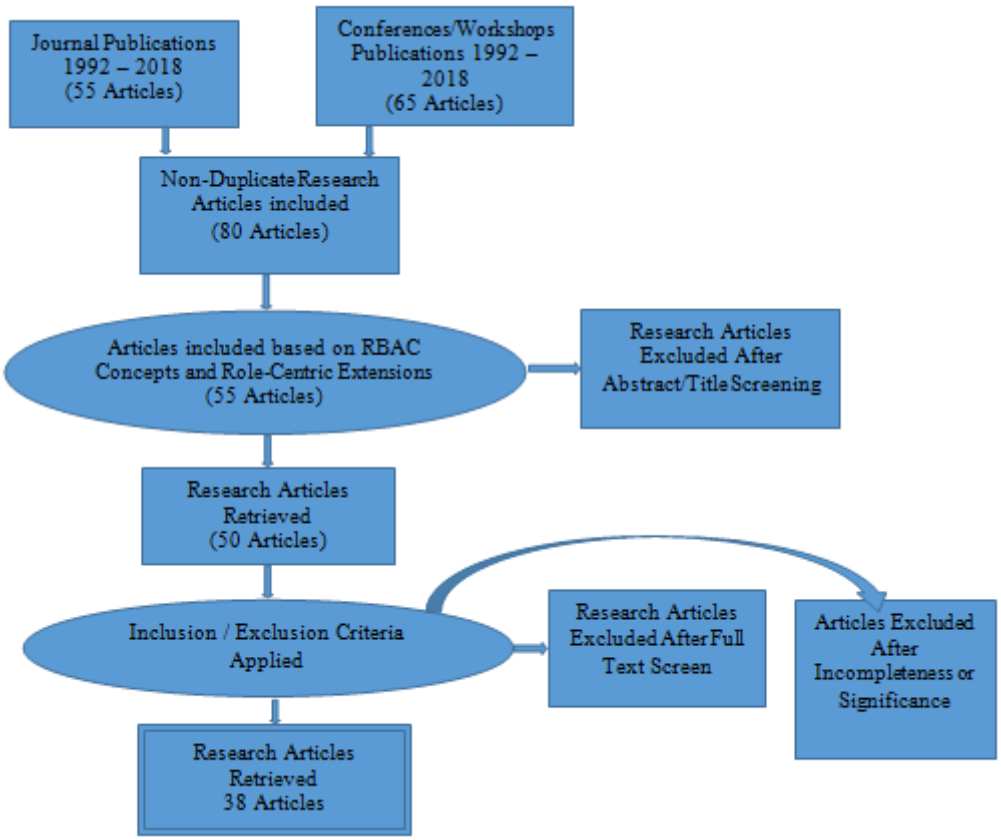

Figure 1 Flow Diagram of the Review Process

The objectives of this review work is to make a comprehensive study on the research papers available in the research on the concepts of RBAC models and the extensions to RBAC models; and nearly hundred and twenty papers were collected as part of this work on

various aspects of RBAC models from various reputed data sources including the Journals, the Conferences and the Workshops. The collected articles were screened in different levels based on the criteria: relevance to the subject of review, completeness of the article and significance to the study. From the initial level of screening, nearly eighty articles were selected; the initial screening in the first phase includes the removal of the duplication of the concepts explained in the article. After the initial level of screening, a series of other criteria's were applied and around 38 articles were taken for this review process. The flow diagram of the review process under consideration is depicted in Figure 1. The articles included in this study were taken from the research community contributed by the researchers since 1992, the period when the basic concept of RBAC was first introduced. Since 1992, the researchers worked on establishing the core concepts and principles of RBAC models and to standardize it. The histogram in Figure 2 shows the number of publications that has been taken for the study after screening in the given period.

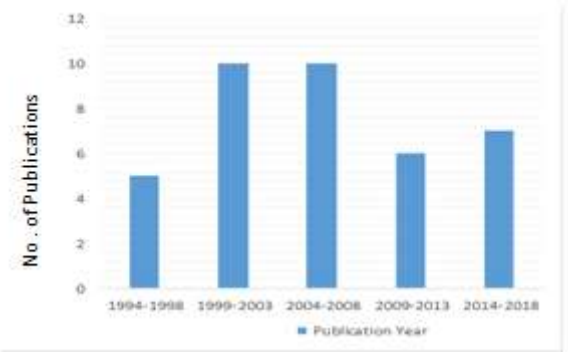

Figure 2 Histogram showing the number of Publications taken for this study in the given period

Figure 3 gives a model which has been followed in this research work to outline the research objectives and the scope of this study is limited and focused on the following aspects:

- *RBAC Concepts and Standards:* This research objective is first aimed in understanding the concepts and principles of RBAC models and to identify the standards that has been widely approved by the research community.
- *RBAC Extended Models:* The second objective of this paper is to focus on the limitations of the core RBAC models, and from the literature, it is identified that the core model of RBAC is not sufficient to support the specific requirements that are necessary for certain applications. Accordingly, the core RBAC model is extended to support the application or domain specific requirements. This study covers the extended Role-centric RBAC models to support the limitations of the core model.
- *Applications of RBAC Models*: The third objective is to identify the domains and applications which employs RBAC models and its extensions.
- *Recent Developments in RBAC Models*: Identifying the recent development in the field of RBAC is the other objective of this research paper.
- *Research Opportunities*: This paper also explores the research opportunities in various aspects of RBAC models.

The remaining sections of this paper is structured as follows: section 2 gives the core RBAC models and their standards. Section 3 narrates the literature review that has been carried out to study the need for the extension of the RBAC models and section 4 gives the list of applications where this RBAC models and its extensions were successfully employed.

Section 5 and 6 gives the recent developments in this field and the research objectives respectively and section 7 concludes the paper.

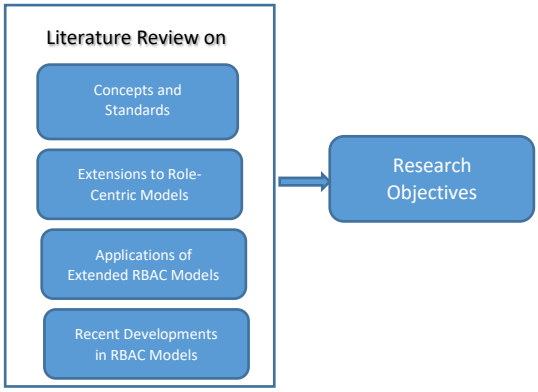

Figure 3 Proposed Research Objective Model

2. RBAC AND ITS STANDARDS

The basic model of RBAC is depicted in Figure 4 and this model shows the three major components: user, role and the permissions. A user in the RBAC model is defined as a person who uses the system and the roles are associated to every user. The role is defined as a job or a function in an organization and the roles are assigned permissions. The permissions are the one which controls access to the system resources. In RBAC model, when a user wants to access certain resources in the system, the user takes up the role and the role's permission defines the control of access to the user. And there exists three types of relationships between these RBAC components: the user-role, role-role and role-permissions and the RBAC systems are modelled with the help of these relationships. The user-role relation defines the roles that an user in the system can take. There exists a many-to-many relationship between the user and the role but at any point of time an user can activate only one role. The role-role relationship defines the hierarchical relationship that exists among the roles and the role-permission relations defines the set of permissions that can be assigned to the roles.

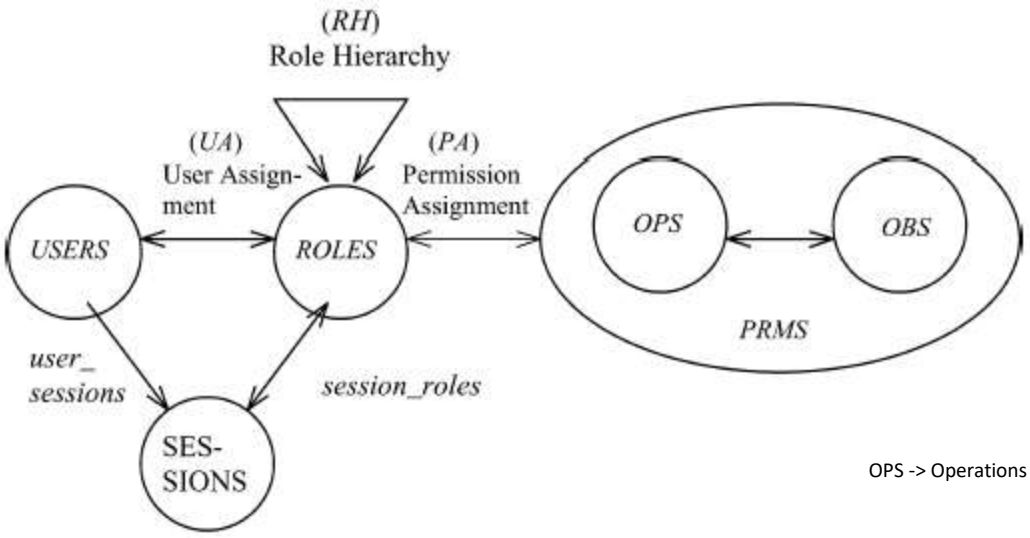

Figure 4 Traditional Role Based Access Control Model [Adopted from NIST Standard]

A standard for RBAC models has been developed by NIST [1] and they have characterized four unique models of RBAC as portrayed in Table 1. These models are described as flat model, hierarchical model, constrained model and consolidated model. The

flat model is considered as the core model in RBAC and forms the basis for other models. The hierarchies and constraints in the components are not supported in this flat model. Inclusion of role hierarchies in the flat model forms the hierarchical model and inclusion of constraints in the flat model forms the constrained model. The consolidated model is one which includes both role hierarchies and the constraints.

Table 1 NIST Standards For RBAC

RBAC Models	
Model Name	**Features**
Flat Model	Users, Roles, Permissions, Sessions
Hierarchical Model	Hierarchical Roles
Constrained Model	Constraints
Consolidated Model	Role Hierarchies and Constraints

The traditional RBAC models proposed earlier controls the system resources by statically defining the access permissions to the roles for controlling the system resources. But, the applications in today's environment requires dynamic assignment of permission to the roles based on the environmental changes. Accordingly, the RBAC concept is extended to support the features required in the dynamic environment. Based on the requirements of the applications, to support for other concepts like location, time and context the RBAC model is extended and a number of researchers have used these extended versions of the basic RBAC models. These extended models were briefly discussed in the next section.

3. EXTENSIONS TO RBAC MODELS

Extensions to RBAC models were proposed over a period of time to support the dynamic changes that occurs in the modern applications. This section briefly explains few of the extensions to RBAC models proposed by the research communities. The RBAC models are basically classified as Role-centric and Attributed-centric models. The Role-centric RBAC models are the extensions made to the core RBAC models for supporting specific features required by the system. In Attribute-centric models, the users are assigned attributes and the access to the resources by an user depends on the set of attributes associated to that user. A role may be one of the associated attribute to a user [12], [17].

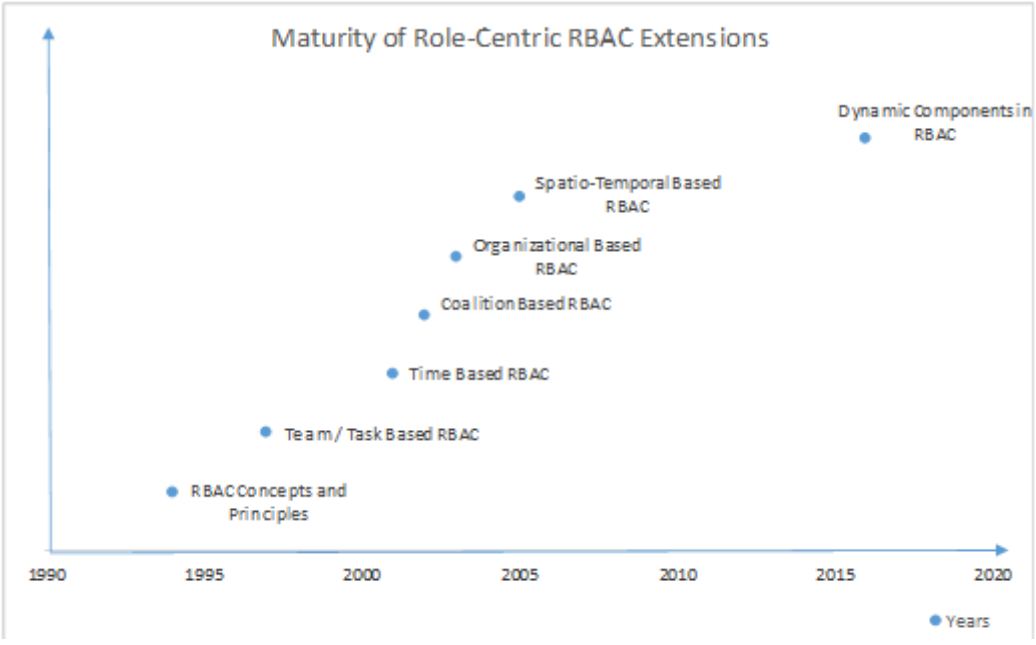

Figure 5 Maturity of Role-Centric Extended RBAC Models

As part of this work, a review was conducted to identify the role-centric extended models and the results of the development to the Role-centric RBAC model over a period of time is given in the Figure 5.

In the core RBAC model, a set of permissions are assigned to the role, and the user assigned to the role is given access based on the permission that the role has. The difficulty with this method arises when more than one user takes the same role and wanted to access different resources at different point of time. To explain this situation in more detail, let us take a system for managing the Hospital, the roles identified in the system are (Doctors, Nurses, Patients) and the resources are the records containing the medical reports for each Patient. If there are two units (Day and Night) in the Hospital and each unit is taken care by a Doctor responsible for that unit and the Doctor comes in shift basis. The requirement of the system is that if a user comes in Day time and takes the Doctor role then the user is allowed to view the records of the patients coming in Day time only and the other user who comes during the night time is permitted to access the records of the patients staying in the hospital during the night time. In this example, the permissions required for a role depends on the time the user is assigned the role. Similar situation arises were the roles are assigned permission based on the location from where the role is activated and to handle all there specific requirements made by the system, the core RBAC model requires to be extended. These specific requirements are captured by the researchers in their research, and came up with the required extensions to the core RBAC models and these Role-centric extensions are explored in the figure 6 and Table 2 gives the details of the constraints or the extended features supported by each of these models. The details of these role-centric RBAC extended features are as follows:

***Location-Based RBAC*:** There are situations to restrict the permissions to access certain resources depending on the place from where the resources are accessed by the users by taking up the roles. For example, an organization may allow their employees to work from their home but still wanted to restrict certain critical information to be accessed from their home. In such situation access to these critical information will be protected based on the location from where the employee sends the request. These type of location-based access requirements were captured and addressed by the author Damiani et al., in 2007 [3] who proposed an extension to RBAC model called GEO-RBAC model by adding location information to the standard RBAC model. In this model, the users and the resources were assigned a location information. The activation of a role by the user depends on the location from where the user activates it and the location associated to the resource affects the permissions to access the resources.

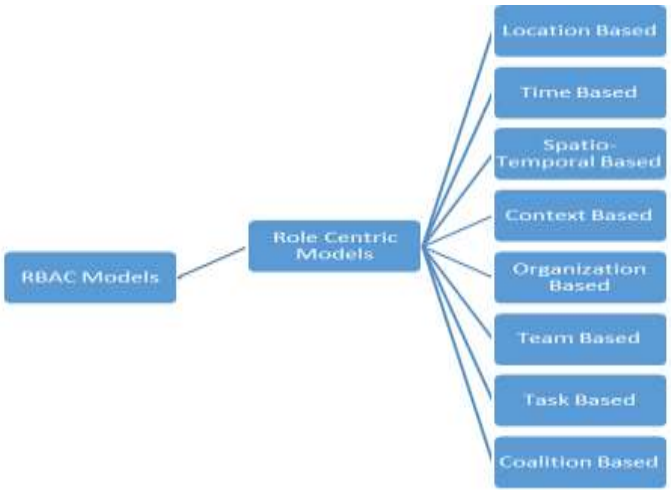

Figure 6 RBAC – Role Centric Extended Models

***Time-Based RBAC*:** As explained in the Hospital System, the time-based role activation services are required and an extension to time-based RBAC (TRBAC) model was proposed by the researchers in [4], [5] and a generalized temporal RBAC model (GTRBAC) is described [6] for supporting the periodic enabling/disabling of roles based on the time the role is activated.

***Spatio-Temporal based Access Control*:** There are situations where the time and the location component together forms the basis for accessing certain resources. Let us consider an example of online shopping portal which gives an offer on a particular time period for specific countries. To verify the eligibility criteria for the order to get the offers, the system needs to check the time and the country location from where the order is requested. The spatio-temporal based control systems considering both time and location for accessing the system resources are well described by the authors in their research articles [8], [9], [10], [11], [15].

***Context-Based RBAC*:** There are situations where only location and time of access cannot determine the access to certain resources. In such conditions, in addition to location and time, context of the role while accessing the resources is required [25]. The RBAC model is extended to support for the context in which the role is activated. These context were modelled based on the events which enables the role to be activated in the environment, the location from where the role is activated or based on time in which the role is activated [18]. The context and semantic based model is proposed and used by the researchers in their research to access the resources [19], [20]. In [24], the author has explained a context-based model for managing the workflow systems.

***Organization-Based RBAC*:** The authors in their research article in [2], identified the difficulties in expressing the hierarchical relationships of roles in RBAC (ie), when the organizational roles are defined using role hierarchy, the roles represented using the role hierarchy is ambiguous in nature. In his research work, the author has proposed a model called "Organization-Based Access Control (ORBAC)" to overcome the limitations of the inheritance relations that is faced in the existing RBAC models, by considering the organizations and the context. An administrative model of ORBAC based on temporal context has been proposed in [23].

Team, Task and Coalition-based Access Control: In the modern applications there are situations where the users come together to form a group or team to complete a task [28], [38]. These type of collaborative work is identified and a model to support these activities were designed by a set of authors in their research work. E. Kohen et el., proposed a model called "Coalition-Based Access Control (CBAC)" where a set of organizations comes together to do their activities.

Table 2 Comparative Analysis Of Role-Centric Rbac Models

RBAC/ Extended RBAC Models	Constraints supported by the RBAC Models			
	Location	Time	Context	Collaborative Environment
Location-Based RBAC Models	Yes	No	No	No
Time-Based RBAC Models	No	Yes	No	No
Spatio-Temporal RBAC Models	Yes	Yes	No	No
Context-Based RBAC	Yes	Yes	Yes	No
Organization-Based RBAC Models	No	Yes	Yes	No
Task, Team and Coalition-based RBAC Models	No	No	No	Yes

4. APPLICATIONS OF RBAC AND ITS EXTENDED MODELS

Though the concept of RBAC is widely used in many applications, there are situations where the core concept of RBAC could not support for the changes that occur in the dynamic

environment. The applications supporting the dynamic changes in the environment needs to have certain additional features that could be added in the core RBAC model. This section briefly explains about the applications where the RBAC concept is required to be extended and Table 3 summarizes the supported applications for each of these models.

The author in research paper [18] describes the requirement of context-based access control system for communicating the process related activities to all the concerned people in the manufacturing environment. Another application which explains about the use of context-based RBAC is "Mobile office application" [8]. This paper explain about a framework "UbiCOSM", proposed by the author which provides ubiquitous services using extended RBAC model. Accessing resources in the home requires contextual information which is described with the help of "Smart intercom services" application in [9]. In [24] the author explains about the security requirements of workflow in an organisation by proposing a context sensitive model to RBAC.

The resources in certain web applications developed for hospital-medical application system and museums requires controlling the users to access the resources based on the time and from the place from where they are accessing the resources. These types of location and time based applications were discussed in [22].

Table 3 Applications of RBAC Extended Models

RBAC Extended Model	Applications	Extended Features	Reference
Context-Based RBAC	Manufacturing	Communicating process related activities that occur in the manufacturing domain.	[18]
	Mobile Office Application	Accessing the office resources from ubiquitous environment.	[8]
	Securing Smart Intercom Services	Protecting access to the resources in the home	[9]
	Security aspect in work flow based information system	Handling security requirements in various levels in an organisation	[24]
Time and location based	Hospital – Medical Information System	Limited Access to patients records by doctors, patients and organizational staffs	[22]
	Museum – Web Application System	Controlling access to the resources in the Museum (rooms)	[22]
Attribute-Based Access Control	Securing the storage of Cloud Data	Encrypting the data to be stored in the Cloud and controlling the access.	[26], [27]
	Cross Domain Access in SOA	Attributes are assigned to subjects, Resources and Environment	[29]
Task-RBAC	Logistics Management System (LMS)	The functions to be carried out in LMS is divided into atomic task and the operational permissions are assigned to the task.	[28]

5. DEVELOPMENTS IN RBAC MODELS

This section briefly explains the research advancements of RBAC models and Table 4 summarizes the notable research developments in the RBAC models. The first aspect to be considered in RBAC development is the standardization of the model. Since the emergence of RBAC, it has been recognized and accepted as primary model for supporting the access

control in an organization and a consensus standard of this model has been recognized by the major standards organization NIST [1].

The second development in RBAC is the theoretical or conceptual understanding of the model. Though MAC and DAC came into existence prior to RBAC, both these models can be easily integrated within the RBAC framework [30]. The third development that needs to be considered in the RBAC model is the contextual understanding which indicates the applicability of the model in different domains. Based on the applicability of the standard RBAC model, the need for its extensions to support specific functions forms the fourth development in RBAC models.

The other developments in RBAC models is from the administrative side to consider other major aspects in employing RBAC models in different applications like identifying the roles, assigning roles to the users and specifying the access control policies for a given application. Roles are identified using Role Engineering methods and there are a number researches available in this area to identify the roles using role mining techniques [34], [35]. Once the roles are identified for a given application, the roles are assigned to the users of the application and these assignment criteria are subject to the administrative policies.

Specification of the RBAC policies for an organization is the other important aspect that needs to be considered while following the RBAC model. The research communities are following different notations to represent these access control policies in their RBAC models. The authors in their research articles [36] and [37] proposed a language for specifying the access control policies.

Table 4 Developments in RBAC Models

Research Developments in RBAC Models			
Developments in RBAC	**Questions to be raised**	**Support from Research for the questions raised**	**References**
Standardization	Is there a common standard available to support RBAC models	Consensus model to standardize RBAC was developed by NIST	[1]
Conceptual Understanding	How RBAC is related to DAC and MAC?	Both DAC and MAC can be integrated within RBAC framework.	[30]
Contextual Understanding	Where RBAC is practically applied?	Helps to understand the policies. IT can be implemented using different architectures	[31]
Extensions to RBAC	How Application specific constraints are supports in RBAC models?	Application specific constraints like location, time, context, organization, team task and coalition are supported by extending the standard model of RBAC	[3], [4], [5], [18], [19], [20], [24], [2], [23], [28]
Administering RBAC	How to assign roles to users? How to specify RBAC policies?	RBAC administrative models are supported to identify and assign roles to users using Role Engineering methods. And RBAC policies are specified using specific languages	[32], [33]

6. RESEARCH OPPORTUNITIES

This section explores the research opportunities in RBAC that has been identified during this research survey. The research developments in RBAC raises various questions that leads to further research in this area. In the modern technological environment the objects that needs to be secured increases dramatically and the access mechanism should cope up to the current requirements. In today's dynamic environment, the business model is changing and the application supporting the business requirement behaves differently for the same user. It means based on the user's role and responsibility the access permissions for the resources in the organization needs to be limited. Though RBAC models allows a limited access control mechanism there are few areas in which this model needs to be explored. The following are the research areas that can be explored further in RBAC based on [8], [20], [24], [25], [38]:

***Support for Dynamic Changes*:** With the advancements in the field of Information Technology like Cloud and IOT, the support for the dynamic changes with the roles and responsibilities are inevitable and the RBAC models requires to be improved to adapt to the scalability of the users, roles and the resources.

***Context Sensitive*:** The standard RBAC model defines the role as a static component and the permissions that are assigned to the role is also predefined. The problem with this model is the limitations that exists in the application of standard RBAC model in the context sensitive environment. With the changes in the environment, the roles and responsibilities of the users are changing which requires the permissions to be updated periodically. The RBAC models needs to be extended for its support the applications in the context sensitive environment.

***Standardized Framework*:** Though RBAC models are widely used in a variety of applications, a standard framework supporting the organizational roles to access the organizational resources is lacking and there is a need for standardizing a RBAC-based framework.

***Security Metrics*:** The other research opportunities in this area is measuring the level of security of the resources in the organization when the resources are protected using RBAC models. The evaluation metrics of the RBAC models are required as this will help in identifying the required features for improving the security of the resources.

7. CONCLUSIONS

This paper explained the concepts of the RBAC models and the need for extending the standard model to support the application specific features to maintain security in this dynamic environment. The applications supporting the extended features in RBAC model that has been developed by the research community is also briefly explained in this paper. The recent developments in the field for RBAC is identified and forms the basis for framing the research question and gives hope for further research in this area. From this study it is identified that RBAC models are best suited for the applications which allows multiple roles to be interacted with the application. The drawback with the basic RBAC model is that it requires all the permissions to be assigned with the user, when the user takes up a role but, this static assignment of permissions to the roles are not enough to support the applications which requires other specific criteria which are dynamic in nature. The support for dynamism in permission assignment to the roles are carried out by extending the basic RBAC models and this paper explained in detail about the Role-centric extensions to the RBAC models. Further, this work can be extended by analyzing the support of the extended RBAC models in multiple contextual applications.

REFERENCES

[1] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-Based Access Control Models. IEEE Computer 29(2), 38–47 (1996)

[2] Kalam, A. A. E., Benferhat, S., Miege, A., Baida, R. E., Cuppens, F., Saurel, C., Balbiani, P., Deswarte, Y., and Trouessin, G. "Organization based access control". In Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks (2003), POLICY '03, IEEE Computer Society, pp. 120.

[3] Damiani, M. L., Bertino, E., Catania, B., and Perlasca, P. GEO-RBAC: A spatially aware RBAC. ACM Trans. Inf. Syst. Secur. 10, 1 (Feb. 2007).

[4] Elisa Bertino And Piero Andrea Bonatti And Elena Ferrari, "TRBAC: A Temporal Role-Based Access Control Model", ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, Pages 191–223.

[5] James B D Joshi, Elisa Bertino, Arif Ghafoor, "Temporal Hierarchiesand Inheritance Semantics for GTRBAC", in Seventh ACM Symposium on Access Control Models and Technologies (SACMAT 02), Monterey, California, USA, June 2002.

[6] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor. A generalized temporal role-based access control model. Knowledge and Data Engineering, IEEE Transactions on, 17(1):4–23, 2005.

[7] E. Kohen, R. K. Thomas, W. Winsborough, and D. Shands, "Models for Coalition-Based Access Control (CBAC)," in Seventh ACM Symposium on Access Control Models and Technologies (SACMAT 02), Monterey, California, USA, June 2002.

[8] A Corradi, R Montanari, and D Tibaldi. Context-based access control for ubiquitous service provisioning. In Proceedings of COMPSAC'04, pages 444–451, Washington, DC, USA, 2004. IEEE Computer Society.

[9] M J. Covington, W Long, S Srinivasan, A K. Dev, M Ahamad, and G D. Abowd. Securing context-aware applications using environment roles. In Proceedings of SACMAT'01, pages 10–20, New York, NY, USA, 2001. ACM

[10] Song Fu and Cheng-Zhong Xu. Coordinated access control with temporal and spatial constraints on mobile execution in coalition environments. Future Generation Comp. Syst., 23(6):804–815, 2007.

[11] M. Kumar and R. Newman. STRBAC - An approach towards spatio-temporal role-based access control. In Communication, Network, and Information Security, pages 150–155, 2006.

[12] Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. Attribute-based access control. Computer, (2), 85–88, IEEE Computer Society, 2015.

[13] R. K. Thomas. Team-based access control (TMAC): A primitive for applying role-based access controls in collaborative environments. In Proceedings of the Second ACM Workshop on Role-based Access Control, pages 13–19, Fairfax, Virginia, November 1997.

[14] W. Wang. Team- and role-based organizational context and access control for cooperative hypermedia environments. In Proceedings of ACM Hypertext '99, pages 37–46, Darmstadt, Germany, February 1999.

[15] S. M. Chandran and J. B. D. Joshi. Lot-rbac: A location and timebased rbac model. In A. H. H. Ngu, M. Kitsuregawa, E. J. Neuhold, J.-Y. Chung, and Q. Z. Sheng, Proceedings of WISE'05, volume 3806 of LNCS, pages 361–375. Springer, 2005.

[16] R. K. Thomas and R. Sandhu. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. In Proceedings of

the IFIP WG 11.3 Workshop on Database Security, pages 166–181, Lake Tahoe, California, August 1997.

[17] Arjumand Fatima, Yumna Ghazi, Muhammad Awais Shibli and Abdul Ghafoor Abassi, Towards Attribute-Centric Access Control: an ABAC versus RBAC argument, Security Comm. Networks 2016; 9:3152–3166, 2016 John Wiley & Sons, Ltd.

[18] Kosmas Alexopoulosa, Sotiris Makrisa, Vangelis Xanthakisa, Konstantinos Sipsasa, Aggelos Liapisb, George Chryssolourisa, Towards a role-centric and context-aware information distribution system for manufacturing, The International Scientific Committee of the 8th International Conference on Digital Enterprise Technology - DET 2014 – "Disruptive Innovation in Manufacturing Engineering towards the 4th Industrial Revolution", Published by Elsevier B.V.

[19] Toninelli, A., Montanari, R., Kagal, L., & Lassila, O. (2006). A semantic context-aware access control framework for secure collaborations in pervasive computing environments. In The Semantic Web-ISWC 2006 (pp. 473–486). Springer.

[20] Tran, N. A. & Dang, T. K. (2007). A novel approach to fine-grained content-based access control for video databases. In Database and Expert Systems Applications, 2007. DEXA'07. 18th International Workshop on (pp. 334–338).: IEEE.

[21] Sandhu RS, Samarati P. Access control: principle and practice. IEEE Communications Magazine 1994; 32 (9): 40–48.

[22] Clara Bertolissi, Maribel Fern´andez, Time and Location Based Services with Access Control, 978-2-9532443-0-4, 2008 ESRGroups France

[23] Ouarda Bettaza, Narhimene Boustiab, Aicha Mokhtaric, "Dynamic delegation based on temporal context", 20th International Conference on Knowledge Based and Intelligent Information and Engineering Systems, Procedia Computer Science, 2016

[24] Goran Sladi´c, Branko Milosavljevi´c, and Zora Konjovi´c, "Context-sensitive Access Control Model for Business Processes", ComSIS Vol. 10, No. 3, June 2013

[25] Muhammad Nabeel Tahir, "C-RBAC: Contextual Role-Based Access Control Model", Ubiquitous Computing and Communication Journal, Volume 2, Number 3, 2008.

[26] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage", IEEE Transactions On Information Forensics And Security, VOL. 10, NO. 11, NOVEMBER 2015

[27] Xuejiao Liu, Yingjie Xia, Shasha Jiang, Fubiao Xia, Yanbo Wang, "Hierarchical Attribute-based Access Control with Authentication for Outsourced Data in Cloud Computing", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013

[28] Yingying Yu, Yan Chen, Yuqin Wen, "Task-Role Based Access Control Model in Logistics Management System", IEEE, 2013

[29] Ni Dan, Shi Hua-ji, "Attribute Based Access Control (ABAC)-based cross-domain access control in service-oriented architecture (SOA)", International Conference on Computer Science and Service System, 2012.

[30] Osborn, S., Sandhu, R. and Munawer, Q.: Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. ACM Trans. on Information and System Security, V. 3, No 2, (May 2000) 85–1 06

[31] Sandhu, R.: Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC Way. Proc. 5th ACM Workshop on RBAC, Berlin. (July 26–2 8, 2000) 111–11 9

[32] Ezedin Barka and Ravi Sandhu: Framework for Role-Based Delegation Models. Proc. 16th Annual Computer Security Applications Conference, New Orleans (Dec., 2000)

[33] Sandhu, R.: Role Activation Hierarchies. Proc. 3rd ACM Workshop on Role-Based Access Control, Fairfax, Virginia. (October 22–2 3, 1998) 33–4 0

[34] A. Colantonio, R. Di Pietro, and N. V. Verde, "A business-driven decomposition methodology for role mining. Computers & Security, 2012.

[35] Zhongyuan Xu, Scott D. Stoller, "Algorithms for Mining Meaningful Roles", SACMAT'12, June 20–22, 2012, Newark, New Jersey, USA.

[36] Hitchens, M. and Varadharajan, V.: Tower: A Language for Role Based Access Control. Int. Workshop on Policy, Bristol, UK, January 2001, Springer LNCS 1995

[37] Damianou, N., Dulay, N., Lupu, E., and Sloman, M.: The Ponder Policy Specification Language. Int. Workshop on Policy, Jan. 2001, Springer LNCS 1995

[38] Federica Paci, Anna Squicciarini, Nicola Zannone, "Survey on Access Control for Community-Centered Collaborative Systems", ACM Computing Surveys, Vol. 51, No. 1, Article 6, 2018. https://doi.org/10.1145/3146025