A Systematic Literature Review on Extensions to Role Based Access Control

Eric D. Helms, JeeHyun Hwang, Tao Xie, Laurie Williams

North Carolina State University

Department of Computer Science

890 Oval Drive, Box 8206

Raleigh, NC 27695-2858

Abstract

Context: Since the introduction of the role based access control (RBAC) standard in the late 1990's, RBAC has become an increasingly popular access control mechanism for applications such as web applications, mobile computing and databases. RBAC restricts access to resources based on the identity of subjects connected to logical groupings of permissions. The introduction of computing into new domains has led to proposals for extensions to the standard RBAC model; for example, defining additional constraints among roles, adding context or defining new heirarchy relationships.

Aim: Our work aims to aid researchers looking to expand on the body of knowledge surrounding extensions to RBAC need a starting place to prevent re-invention of the wheel and developers needing to find and select an access control mode based on their project requirements. *The goal of this work is to provide practioners an assessment of the current extensions to RBAC to aid with choosing a model that meets their requirements, and researchers with insights into the state of RBAC extension models and how they are evaluated.*

Method: We conducted a systematic literature review by collecting and synthesizing relevant research papers in the area of RBAC extensions. The review we performed yielded 1716 papers, of which 29 were deemed primary sources for inclusion as model extensions to the RBAC standard model. The papers we collected were from electronic digital libraries IEEE, Google Scholar, CiteSeerX and ACM based on a set of exclusion and inclusion criteria. We performed a comparative analysis of the primary sources to find relationships among extended models and to analyze the state of RBAC extension evaluations.

Results: Our results showed that extensions to RBAC fall into a number of categories that in turn all fall under the single category of context based extensions. We look into the motivations behind RBAC extensions and the domains that are leading factors in developing these newer models. We also quantify the current evaluation methods used when RBAC extension models are presented to the research community.

Conclusions: The extensions to RBAC fall into a number of categorizations with Organization, Privacy, Resource, Task, Spatio-Temporal, Spatial and Temporal falling under the general category of context. Domains, such as healthcare and mobile computing, were idenitfied as motivations behind the development of extensions to the RBAC model. Our literature review showed that the state of RBAC model evaluation could benefit from the research community given most model evaluations seen within the papers were based on hypothetical situations with little to no case studies or implementations in practice.

Keywords: RBAC, access control, systematic literature review

1. Introduction

Innovation and the use of RBAC into new domains has led to scenarios that, by some accounts, the standard RBAC model cannot handle. For example, Ni, Q. and Bertino, E. et al [4] state that RBAC is "not designed to enforce privacy policies and barely meet privacy protection requirements" with the introduction of privacy concerns in domains such as healthcare. Thus, a series of extensions to the standard RBAC model have appeared in the literature, each adding one or more features. However, as researchers often develop their own specialized extended models of RBAC, their research cannot be generalized or compared with other research work appropriately.

Role based access control (RBAC) was first introduced in the 1990s when the National Institute for Standards and Technology (NIST) requested that a unified standard be created by combining the Ferraiolo and Kuhn model [1] with the framework proposed by Sandhu, et al [2]. The development of a standard was inspired by an economic impact study done during the 1990s and later confirmed in 2011 [1]. In an RBAC model, roles represent a group of users who are involved in a specific job function in an organization. RBAC assigns permissions of specific actions on resources to roles instead of individual users. Therefore, in order to gain roles' permission on specific resources, users acquire appropriate roles first. RBAC is a generalized access control approach used for various applications including web services, database applications, and healthcare applications. RBAC has advantages in maintaining and managing organization's security policies. For example, if a user is to access manager role's resources within a given organization, security policy administrators simply add the user to be associated with the manager role.

The goal of this work is to provide practioners an assessment of the current extensions to RBAC to aid with choosing a model that meets their requirements, and researchers with insights into the state of RBAC extension models and how they are evaluated. With respect to our goal, the authors addressed the following research questions:

- What categorizations exist within extensions to RBAC?
- What are the motivations behind extensions to RBAC?

[1] `http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf`

- Do the extensions to RBAC have corresponding implementations?
- How are extensions to RBAC evaluated theoritically and in practice?
- What domains have extensions to RBAC been created for?
- What commonalities or generalizations exist across all categorizations?

The authors performed a systematic literature review designed to explore the current body of research in the area of extensions to the core RBAC model. The review we performed yielded 1716, of which 29 were deemed primary sources for inclusion as model extensions to the RBAC standard model. This review is intended to serve as a starting place for researcher's looking to tackle new problems in the realm of authorization and prevent re-invention of the wheel. For developer's looking to find a model to fit their seemingly unique access control needs, this review will provide a basis for comparison and easy look-up for what extension based model to use. Further, the review provides insight into the state of evaluation, or lack thereof, within the RBAC extension model community.

Our research provides contributions to the community in the following ways:

- Summarizes current extended RBAC research work and its contributions.
- Guides a direction for a standard of extended RBAC. Understanding the categorization and the motivation of the existing research results helps decide a standard of extended RBAC.
- Identifies the research challenges in the areas of security policies and suggest a future extension of RBAC.
- Identifies the deficiencies in RBAC extension evaluation.

The rest of the paper is organized as follows. Section 2 covers background and the core RBAC model. Section 3 lays out the process used in conducting the review. Section 4 discusses the categorization break down of the papers. Section 5 analyzes the rest of the research questions. Section 6 contains the final conclusions.

2. Core Role Based Access Control

Since the basis for our review is extensions to the core model, we will describe the core model, associated entities and other terminology encountered across the space of our review. The NIST RBAC model proposed by Ferraiolo et al. [1] and later adopted as the official standard for RBAC by the International Committee for Information Technology Standards (INCITS) consists of four basic entities:

- a set of *Users*: A user can be a person or an agent.
- a set of *Roles*: A role is a collection of permissions to perform a specific job function in an organization.

- a set of *Permissions*: A permission refers to an access mode that can be exercised on an object in the system and a session relates a user to possibly many roles.
- a set of *Sessions*: In each session, a user can be assigned to some of the roles, only when the corresponding role is enabled for activation for that time.

In RBAC, a user can exercise a permission only if the user is assigned to a role. In addition to the four basic components, two functions are defined: the user role assignment (UA) and the role permission assignment (PA) functions. UA models assignment of users to roles. PA models assignment of permissions to roles.

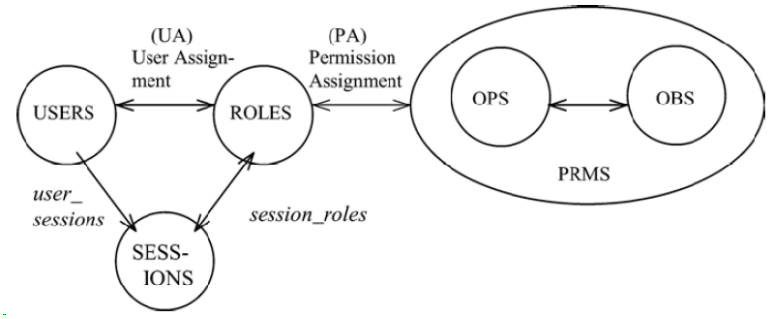

Figure 1: RBAC Core Diagram in NIST RBAC model [1].

Figure 1 presents an overview of core RBAC model diagram where elements and their relations are described. Let "USERS", "ROLES", "OBS", "OPS", "PRM", and "SESSIONS" denote users, roles, objects, operations, permissions, and sessions, respectively. Permissions are associated with possible users' pre-defined operation on an object (e.g., execute a file). Note that, at user or role activation, a session associated with user or role is established.

3. Process

The authors adopted and applied a systematic literature review following recommendations from Kitchenham's suggested processes [3]. The systematic literature review process was broken down in to four stages and the rest of this section is broken down by each stage. The stages were:

- Step 1: Development of a search strategy
- Step 2: Elimination of papers based on title criteria
- Step 3: Elimination of papers based on abstract criteria
- Step 4: Elimination of papers based on content and matching to elimination criteria

	RBAC	**role based access control**	**role-based access control**	**Total**
Google Scholar	651	213	435	1299
ACM Portal	500	20	720	1240
IEEExplore	200	40	230	470
CiteSeerX	100	100	150	350
Totals	1451	373	1535	3359
Combined				**1716**

Table 1: Paper counts after applying search strategy

3.1. Step 1: Search Strategy

For the first phase of our systematic literature review, the authors developed a search strategy for finding papers. The search strategy was executed by an automated comprehensive search taking as input a set of academic search engines and a list of search terms. The search was performed by applying each search term to each engine incrementally until a stopping criteria was met. Table 2 lists the four search engines along the left most column with the three search term across the top row along with the papers for each criteria and engine combination. The search algorithm was performed as follows:

1. Call to search engine with current search position and current search term.
2. Parse results and extract paper title, authors and year of publication.
3. Compare results against stopping criteria:
    - If the size of the result set is greater than or equal to 1000 then stop.
    - If the last ten results did not contain the search term phrase within the tite then stop.
4. If stopping criteria not met, increment search position and go back to step one.

The result set size stopping criteria was chosen due to a technical limitation of some search engines. The stopping criteria related to the last ten titles is meant to stop after relevant results are no longer being returned by the search engine. After gathering all 12 data sets, the authors combined the papers into a master list by systematically comparing the bibliographic information for each. The master list of 1716 papers was used to perform a series of elimination rounds to narrow the list of papers and identify primary sources. Table **??** shows the total number of papers selected by each author for each round and how many papers from the disjoint set for each round survived to the next round.

3.2. Steps 2-4: Elimination Rounds

The elimination rounds were performed based on reading of the title, abstract and finally the paper itself. While each elimination stage had a unique set of criteria for elimination the general procedure for elimination for the researchers was as follows.

- The two first authors independently classified papers as relevant, irrelevant or uncertain based off elimination criteria
- Those papers marked as relevant by both reviewers were kept and those marked irrelevant by both were thrown out.
- Papers marked as relevant, or irrelevant by a single reviewer were combined with all papers marked as uncertain and discussed by both reviewers. From this discussion, papers were either thrown out or kept until the next round of the review.

3.2.1. Step 2: Title Elimination

The first round of elimination was performed by strict examination based on the title. Each author was tasked with deciding on elimination by answering the following questions:

- Did the title contain a reference to 'role based access control' or 'RBAC'?
- Did the title contain a reference to 'model'?

3.2.2. Step 3: Abstract Elimination

The second round of elimination was based on strict reading of the abstracts of papers that survived title elimination. Researchers read each abstract and evaluated relevancy based off:

- Does the abstract mention a proposed model?
- Does the abstract mention extension of role-based access control?
- Does the abstract mention either an implementation, evaluation or domain for their model?

3.2.3. Step 4: Content Elimination

The final elimination round involved taking the entire paper into consideration and answering five questions that would serve as the basis for elimination. The data collected by answering these questions served as the basis towards answering the research questions. The questions each reviewer attempted to answer based on the content of the paper was:

1. Does this model extend the core model? (Exclusion)
2. Do the researchers give evidence that RBAC needs extension? (Inclusion)
3. Was the paper and subsequent model inspired by a real world example? (Conditional Inclusion)

		Title	Abstract	Content
Eric		305	86	46
Hwang		176	102	42
	Overlap	249	51	24
	Disjoint	232	137	64
	Rejected	208	116	59
	Retained	41	21	5
	Total	290	72	29

Table 2: Elimination Rounds

4. Did the researchers offer any evaluation of the proposed model? If yes, how did they do one? If no, why? (Conditional Inclusion)
5. Did the authors implement their model? (Inclusion)

Question 1 was a definitive exclusion criteria as any paper that failed in the affirmative was rejected. Questions 3 and 4 were marked as conditional includes given that they were connected in making a decision. A paper that met Question 3 but not 4, or met 4 but not 3 would be included since in some cases the real world examples served as research evaluations and without this conditional include the paper list size would be too small to be significant.

4. Categorization

After selection of primary sources, the next step was to extract data from each paper that pertained to our research questions in order to look for trends. The first step was to take the individual data generated from the final elimination round and organize this information around the research questions. During the paper reading round, and resulting data, the fact that the papers were logically falling into a number of categorizations became evident. Thus, the first step undertaken was to answer the question of what categories exist for the RBAC model extensions and what papers feel into what categories. Each paper deemed a primary source and the papers associated categorization are shown in Table 3.

4.1. Research Question 1

What categories exist within RBAC extensions?

The primary sources contained either within the title, or by multiple references within the body of the text a reference to a quantifier for the type of extension their model was. For example, the paper "Privacy-aware role-based access control" [4] contained "privacy" in the title leading to the papers categorization of Privacy. By comparison, the paper "An extended RBAC model based on granular logic" [5] does not contain a direct categorization in the title or model name, but in reading the body of the paper the authors assessed that this paper was context based. The authors offer definitions for each categorization and their characteristics based on the primary sources and the English definitions for each.

- Constraint: Access control model in this category extends constraints, which are conditional restrictions on permissions of given roles. This constraint is either static and dynamic. For example, a doctor can modify any medical record for which the doctor is assigned as the designated primary care physician. This example describes doctor's permission with conditional restriction, "only when the doctor is assigned as the designated primary care physician".

- Context: Access control model integrates context information. In access control, context often refers to user's current state and environment information (e.g., location, time, system resources, network state, network security configuration, etc) which may affect user's access privileges.

- Organizational: Organizational access control is concerned with access control associated with multiple organizations. Typically, users may have the same role name in different organizations, but may have different access privileges due to different local variations.

- Privacy: Access control model can be extended to describe privacy policies, which are legal statements or documents about disclose and management of personally identifiable information such as name, address, data of birth, etc.

- Resource: Access control model can be extended to handle any system resources (e.g., a file, printer, terminal, database record, etc) in a flexible way.

- Spatial: Spatial constraints are location-based constraints in specifying access control policies. For example, in organizations, locations are enforced while a specific role is permitted to conduct an action. Consider that part-time employee works only in specific location. In such cases, the part-time employee role should access required resources only when the user is in the location. Spatial constraints can incorporate either on roles, user-role assignments, or role-permission assignments.

- Spatio-Temporal: Spatio-temporal constraints are combination of spatial (location-based) and temporal (time-based) constraints in specifying access control policies. For example, specific locations are enforced while a role is permitted to conduct an action from 8 am to 5 pm.

- Task: A task is a fundamental unit of a business activity. Different from core RBAC, in task-role-based access control model, roles are not directly associated with permissions. Roles are first associated with tasks, which are associated permissions. For example, the employee role is associated with a task, which is to write a report. Then, this task is associated with a permission.

- Temporal: Temporal constraints are time-based constraints in specifying access control policies. For example, in organizations, periodic temporal durations are enforced while a specific role is permitted to conduct an action. Consider that part-time employee works only from 9:00 a.m. to 3:00 p.m. In such cases, the part-time employee

role should access required resources during the interval. Temporal constraints can incorporate either on roles, user-role assignments, or role-permission assignments.

5. Motivations

5.1. Research Question 2

What are the motivations behind RBAC extensions?

Core RBAC model provides an abstraction of authorization model based on user role assignment (UA) and the role permission assignment (PA). Since this simple model may not provide a fine-grained access control for sophisticated security mechanism, a variety of extended RBAC models have been proposed over the years to meet security requirements. When administrators design a model, it is important to capture an important abstraction to help the model to be enforced in a system.

- Core RBAC model needs additional contextual information and constraints to develop fine-grained policies in practice.
- Core RBAC does not incorporate context. Therefore, RBAC belongs to static access control model, which may not capture changes in environments.
- Core RBAC does not support for various constraints such as temporal and spatial constraints to design sophisticated policies on demand.
- Core RBAC does not provide an abstraction to additional user-defined attributes (e.g., task and team) and their association with existing attributes.
- Core RBAC has limitation on delegation and role hierarchy. For example, partial inheritance in role hierarchy needs to be developed.
- Model needs to incorporate additional contextual information and constraints to develop fine-grained policies in practice.
- Model needs to incorporate additional attributes such as task, team, purpose, organizational roles and collaborative activities over existing attributes. Moreover, new association between attributes are introduced.
- Model needs to improve existing features such delegation and role hierarchy to meet fine-grained access control.

6. Implementations

6.1. Research Question 3

Do the extension models have corresponding implementations?

When designing and proposing a model targeted at a feature that is rooted in practical usage by real software systems, bringing the model to life is strong evidence that the

proposed model can work in practice. The concept of authorization, and access control is rooted in a business need. Thus, any access control model needs to be feasible in the real world not just on paper. We analyzed the primary sources to see how many proposed models actually had implementations associated with them. And quantified the type of implementation. Whether the implementation was for a real system, for a prototype and/or used in a production environment.

Of the 29 papers surveyed, there was a lack of implementation with 21 of the paper providing no mention of a implementation or prototype. Of the remaining 8 papers that did mention an implementation, half were simply prototypes developed by the authors while the other half were claimed to be implemented within a real system.

7. Evaluations

7.1. Research Question 4

How are extension to RBAC evaluated theoritically and in practice?

Providing evaluation of a proposed model is a key component in establishing the models validity. The papers were examined for evidence of evaluations ranging from performance to mathematical accuracy to application to real world scenarios. Further, for each proposed model, the reviewers looked for evidence that the authors made comparisons between their own model and the base model as they pertained to claims made by the authors of why their model is needed. The quantifiable evaluations looked for were:

- Time-based Performance [4], [6]
- Complexity analysis [7], [8], [9], [6]
- Comparison to standard RBAC [7], [10], [8], [11], [12]
- Mathematical modeling [**?**], [13], [14], [9], [15]
- Example scenarios of the model in action [16], [17], [18], [19], [7], [5], [**?**], [10], [12], [20], [12], [15], [21], [22], [23]
- Experimental analysis of the model
- Case study of the model in practice [24]

Based on the diverse evaluation criteria, 12 models presented no evidence of an evaluation. 8 models presented example scenarios and how application of their model would apply and resolve the situation. 6 of the models provided some form of performance or complexity analysis of their model. This included graphs of the model's time to determine authorization as the number of entities grew, and the size of the role space for the extension model compared to standard RBAC. 4 models provided mathematical descriptions and analysis as a way to provide evaluation in the form of completeness.

The most widely used evaluation method was providing sample scenarios with accompanying workflows of how the extension model would tackle those scenarios. Much is left to the reader to assume of these types of evaluations, as the authors do not explicitly state or show how the standard model is deficient in tackling said scenarios.

8. Domains

8.1. Research Question 5

What domains have RBAC extensions been created for?

Business needs have historically driven RBAC research and development. The primary mode of evaluation for model extensions has been the presentation of business scenarios in various domains and how the model uniquely handles those particular scenarios. Thus, looking for trends in the domains used in the example scenarios might serve to illuminate a trend worth further examination into the reason for the explosion of RBAC extensions.

Upon examination of the primary sources, the most prevalent domains were:

- What domains or scenarios serve as inspiration for these extensions?
- Medical domain
- Pervasive computing environments
- Mobile devices
- Large-scale organizations with many sub-departments
- Enterprise, organization workflows

9. Generaliations

9.1. Research Question 6

What commonalities or generalizations exist across all categorizations?

Core or any extended role-based access control is used in various aspects of computer systems. In order to reduce efforts for modeling access control used in various applications, researchers often focus on developing generalized core concepts of access control. We found that propositional logic is used to describe access control model across all categorizations. Propositional logic is concerned with propositions and their logical relationships. In propositional logic, simple (i.e., atomic) or compound condition at given context is evaluated to true or false based on specified rules and access control logic. Researchers are concerned to extend limited set of propositions specific to core RBAC to meet real-world scenarios such as dynamic constraints, temporal, or spatial constraints. However, semantic meanings of such propositions are various based on researchers' intention.

10. Conclusion

The extensions to RBAC were revealed to fall into a number of categorizations with Organization, Privacy, Resource, Task, Spatio-Temporal, Spatial and Temporal falling under the general category of context. The categories each had properties specific to their implementation, but were seen to generalize to being specialized instances of context tailored to the entities or actions the categories covered. A number of domains were idenitfied as being

the motivations behind needing extensions to the core RBAC model. The domains, such as healthcare, presenting new challenges the previous models were not required to design for. Our literature review showed that the state of RBAC model evaluation needs focused from the research community given most model evaluations seen within the papers were based on hypothetical situations with little to no case studies or implementations in practice.

References

[1] D. Ferraiolo, D. Kuhn, Role based access control, in: 15th National Computer Security Conference, Oct 13-16, 1992, pp. 554–563.

[2] R. Sandhu, E. Coyne, H. Feinstein, C. Youman, Role-based access control models, Computer 29 (2) (1996) 38–47.

[3] B. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering.

[4] Q. Ni, E. Bertino, J. Lobo, C. Brodie, C. Karat, J. Karat, A. Trombeta, Privacy-aware role-based access control, ACM Transactions on Information and System Security (TISSEC) 13 (3) (2010) 24.

[5] H. Jian-min, L. Xi-yu, Y. Hui-qun, T. Jun, An extended rbac model based on granular logic, in: Granular Computing, 2008. GrC 2008. IEEE International Conference on, IEEE, 2008, pp. 261–264.

[6] S. Aich, S. Mondal, S. Sural, A. K. Majumdar, Transactions on computational science iv, 2009, Ch. Role Based Access Control with Spatiotemporal Context for Mobile Applications, pp. 177–199.

[7] Y. Bao, J. Song, D. Wang, D. Shen, G. Yu, A role and context based access control model with uml, in: Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for, 2008, pp. 1175 –1180.

[8] Z. Zhang, X. Zhang, R. Sandhu, Robac: Scalable role and organization based access control models, in: Collaborative Computing: Networking, Applications and Worksharing, 2006. CollaborateCom 2006. International Conference on, 2006, pp. 1 –9.

[9] L. Chen, J. Crampton, On spatio-temporal constraints and inheritance in role-based access control, in: ASIACCS: ACM Symposium on InformAtion, Computer and Communications Security, 2008, pp. 205–216.

[10] D. Zou, L. He, H. Jin, X. Chen, Crbac: Imposing multi-grained constraints on the rbac model in the multi-application environment, Journal of Network and Computer Applications 32 (2) (2009) 402–411.

[11] Y. Zhao, Y. Zhao, H. Lu, A flexible role-and resource-based access control model, in: Computing, Communication, Control, and Management, 2008. CCCM'08. ISECS International Colloquium on, Vol. 2, IEEE, 2008, pp. 75–79.

[12] I. Ray, M. Toahchoodee, A spatio-temporal role-based access control model, in: Proceedings of the 21st annual IFIP WG 11.3 working conference on Data and applications security, 2007, pp. 211–226.

[13] F. Hansen, V. Oleshchuk, Spatial role-based access control model for wireless networks, in: Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, Vol. 3, IEEE, 2003, pp. 2093–2097.

[14] S. Aich, S. Sural, A. K. Majumdar, Starbac: spatiotemporal role based access control, in: Proceedings of the 2007 OTM confederated international conference on On the move to meaningful internet systems: CoopIS, DOA, ODBASE, GADA, and IS - Volume Part II, OTM'07, 2007, pp. 1567–1582.

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

[16] M. Alam, M. Hafner, R. Breu, A constraint based role based access control in the sectet a model-driven approach, in: Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, PST '06, 2006, pp. 13:1–13:13.

[17] S. K. Tzelepi, D. K. Koukopoulos, G. Pangalos, A flexible content and context-based access control model for multimedia medical image database systems, in: Proceedings of the 2001 workshop on Multimedia and security: new challenges, Sec '01, 2001, pp. 52–55.

[18] D. G. Cholewka, R. A. Botha, J. H. P. Eloff, A context-sensitive access control model and prototype implementation, in: In: Information Security for Global Information Infrastructures: IFIP TC 11

Sixteenth Annual Working Conference on Information Security, Kluwer Academic Publishers, 2000, pp. 341–350.
[19] X. Huang, H. Wang, Z. Chen, J. Lin, A context, rule and role-based access control model in enterprise pervasive computing environment, in: Pervasive Computing and Applications, 2006 1st International Symposium on, 2006, pp. 497 –502.
[20] E. B. Arjmand Samuel, Arif Ghafoor, A framework for specification and verification of generalized spatio-temporal role based access control model, Tech. Rep. CERIAS Tech Report 2007-08.
[21] L. Yao, X. Kong, Z. Xu, A task-role based access control model with multi-constraints, in: Networked Computing and Advanced Information Management, 2008. NCM'08. Fourth International Conference on, Vol. 1, IEEE, 2008, pp. 137–143.
[22] W. Zhou, C. Meinel, Team and task based rbac access control model, in: Network Operations and Management Symposium, 2007. LANOMS 2007. Latin American, IEEE, 2007, pp. 84–94.
[23] S. Oh, S. Park, Task–role-based access control model, Information Systems 28 (6) (2003) 533–562.
[24] G. Motta, S. Furuie, A contextual role-based access control authorization model for electronic patient record, Information Technology in Biomedicine, IEEE Transactions on 7 (3) (2003) 202 –207.
[25] S. Haibo, H. Fan, A context-aware role-based access control model for web services, in: e-Business Engineering, 2005. ICEBE 2005. IEEE International Conference on, IEEE, 2005, pp. 220–223.
[26] W. Yamazaki, H. Hiraishi, F. Mizoguchi, Designing an Agent-Based RBAC system for dynamic security policy, in: Proceedings of the 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE '04, 2004, pp. 199–204.
[27] H. Jian-min, L. Xi-yu, Y. Hui-qun, T. Jun, An extended RBAC model based on granular logic, in: Granular Computing, 2008. GrC 2008. IEEE International Conference on, 2008, pp. 261 –264.
[28] N. Thein, et al., Leveraging access control mechanism of android smartphone using context-related role-based access control model, in: Networked Computing and Advanced Information Management (NCM), 2011 7th International Conference on, IEEE, 2011, pp. 54–61.
[29] A. Masoumzadeh, J. Joshi, Purbac: Purpose-aware role-based access control, On the Move to Meaningful Internet Systems: OTM 2008 (2008) 1104–1121.
[30] S. M. Chandran, J. B. D. Joshi, Lot-rbac: a location and time-based RBAC model, in: Proceedings of the 6th international conference on Web Information Systems Engineering, WISE'05, 2005, pp. 361–375.
[31] M. Damiani, E. Bertino, B. Catania, P. Perlasca, Geo-rbac: A spatially aware rbac, ACM Transactions on Information and System Security (TISSEC) 10 (1) (2007) 2.

11. Appendix

Context	A constraint based role based access control in the SECTET a model-driven approach, 2006 [16]		
	A flexible content and context-based access control model for multimedia medical image database systems, 2001 [17]		
	A Context-Aware Role-Based Access Control Model for Web Services, 2005 [25]		
	A context-sensitive access control model and prototype implementation, 2000 [18]		
	A Context, Rule and Role-Based Access Control Model In Enterprise Pervasive Computing Environment, 2006 [19]		
	A contextual role-based access control authorization model for electronic patient record Motta, 2003 [24]		
	A Role and Context Based Access Control Model with UML, 2008 [7]		
	An extended RBAC model based on granular logic, 2008 [5]		
	Designing an agent-based RBAC system for dynamic security policy, 2004 [26]		
	An extended RBAC model based on granular logic, 2008 [27]		
	Leveraging Access Control Mechanism of Android Smartphone Using Context-Related Role-Based Access Control Model, 2011 [28]		
	CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment, 2009 [10]		
	Org.	ROBAC: Scalable Role and Organization Based Access Control Models, 2006 [8]	
	Priv.	Privacy-aware role-based access control, 2007 [4]	
		PuRBAC: Purpose-Aware Role-Based Access Control, 2008 [29]	
	Res.	A Flexible Role- and Resource-Based Access Control Model, 2008 [11]	
	Task	A Task-Role Based Access Control Model with Multi-Constraints, 2008 [21]	
		Team and Task Based RBAC Access Control Model, 2009 [22]	
		Task-role-based access control model, 2003 [23]	
	Spatio-Temporal	STARBAC: Spatiotemporal role based access control, 2007 [14]	
		On spatio-temporal constraints and inheritance in role-based access control, 2008 [9]	
		A framework for specification and verification of generalized spatio-temporal role based access control model, 2007 [20]	
		LoT-RBAC: A Location and Time-Based RBAC Model, 2005 [30]	
		A Spatio-temporal Role-Based Access Control Model, 2007 [12]	
		Role Based Access Control with Spatiotemporal Context for Mobile Applications, 2009 [6]	
		Spatial	GEO-RBAC: a spatially aware RBAC, 2005 [31]
			LRBAC: A location-aware role-based access control model, 2006 [12]
			Spatial role-based access control model for wireless networks, 2003 [13]
		Temp.	A generalized temporal role-based access control model, 2005 [15]

Table 3: Primary sources grouped by categorization