A Systematic Literature Review on Extensions to the Role-Based Access Control Reference Model

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

North Carolina State University

Department of Computer Science

890 Oval Drive, Box 8206

Raleigh, NC 27695-2858

Abstract

Context: Since the United States National Institute of Standards and Technology proposed Role-Based Access Control (RBAC) as documented in the RBAC Reference Model in the late 1990's, domain-targeted extensions have been proposed. For example, the mobile domain has identified a need for permission granting and role activation.

Objective: The goal of our work is to aid practitioners and researchers in choosing an RBAC extension model, and in understanding how RBAC extension models are evaluated by providing an assessment of the state of RBAC extension models.

Method: We performed a systematic literature review of RBAC extension models that began with 1,716 papers of which 27 were deemed as primary sources for inclusion.

Results: We identified and classified the RBAC extension models into eight extension categories: Constraint, Context, Organization, Privacy, Task, Spatio-Temporal, Spatial, and Temporal. Only 8 of the 27 papers provided an implementation of their model in the form of an enterprise application or prototype. The primary domains that inspired extensions were the medical domain with 9 of the 27 models, enterprise workflows with 5 of 27, and mobile computing with 5 of 27.

Conclusions: Our literature review shows that all eight of the RBAC extension categories we identified deal with context whereby the privileges provided to a role are environmental depending upon factors such as location or time. RBAC extension model evaluation lacks a consistent set of metrics and evaluation of current models was found to range from providing scenario examples of the model in action to comparison to the RBAC standard. The magnitude and scope of extensions to the RBAC standard suggests a revised standard may be beneficial but in the meantime this work can serve as a starting place for researchers and practitioners.

Keywords: RBAC, access control, systematic literature review

1. Introduction

Software systems use access control mechanisms to determine which subjects can access which resources. Role-Based Access Control (RBAC) is a widely used access control mechanism designed for maintaining and managing an organization's access control based on assigning permissions to roles, and roles to users, instead of assigning the permissions directly to individual users. RBAC is used for securing various applications including web services, database applications, and healthcare applications. In RBAC, roles represent a set of permissions needed to perform a particular job function within an organization. Multiple users who are involved in that specific job function within the organization can then be assigned to a single role to inherit the required access. The ability to logically group users into roles associated with permissions becomes paramount for managing access control as an organization grows and the number of permissions and users scales upward. As permissions can be managed by role instead of by user, RBAC has been shown to significantly reduce complexity of security administration [1]. For example, if a user requires access to resources associated with a manager role within a given organization, security policy administrators need only associate the user with the manager role instead of assigning a set of individual permissions.

The use of RBAC has become popular since the National Institute for Standards and Technology (NIST) first proposed the RBAC standard in 2000 [2]. NIST requested that a unified standard be created by combining the Ferraiolo and Kuhn model [3] with the framework proposed by Sandhu et al. [4]. In 2004, this standard was adopted as ANSI/INCITS 359-2004 approved by American National Standards Institute[1] (ANSI) and the InterNational Committee for Information Technology Standards[2] (INCITS). The development of a standard was inspired by an economic impact study done during the 1990s [5], again in 2002 [1] and later confirmed in 2010 [6]. The study showed the cost savings of RBAC implementation and maintenance. Prior to the development of the RBAC standard, vendors proposed and implemented their own RBAC definition without general agreement on a unified definition of RBAC or RBAC features (e.g., inheritance relationships among roles). The RBAC standard includes the RBAC Reference Model which serves as a basis for defining the scope and functional specifications of RBAC features.

Since the introduction of the RBAC standard, researchers and practitioners have proposed domain-targeted extensions that add one or more features on top of components in the RBAC Reference Model [7]. For example, extensions that target the medical and mobile domains provide dynamic context or privacy around the access control policies. Further, Ni et al. [8] proposed an RBAC extension model to incorporate privacy concerns in to the RBAC Reference Model noting that the RBAC Reference Model is "not designed to enforce privacy policies and barely meet privacy protection requirements" with the introduction of privacy concerns in to the medical domain. These extension models are each building upon and adding features to a standard that was designed to reduce the economic impact experienced by enterprises and to increase interoperability [6].

The goal of our work is to aid practitioners and researchers in choosing an RBAC extension

[1] http://www.ansi.org/

[2] http://www.incits.org/

model, and in understanding how the RBAC extension models are evaluated by providing an assessment of the state of RBAC extension model1s. We established a set of extension categories, examined the state of the art in evaluations of the RBAC extension models, and categorized the motivations that have led to the RBAC extension models. To accomplish this goal, we seek to answer following research questions:

- RQ1: How can RBAC extension models be classified?
- RQ2: How are RBAC extension models implemented by their authors?
- RQ3: How are RBAC extension models evaluated by their authors?
- RQ4: What domains have been targeted by RBAC extension models?
- RQ5: What commonalities exist across RBAC extension models?

We performed a systematic literature review to explore the current body of research in the area of extensions to the RBAC Reference Model. The review began with 1,716 papers, of which 27 were deemed primary sources for inclusion as extension models to the RBAC Reference Model. Our research provides the following:

- A starting place for researchers in the realm of authorization and as a reference guide for discovering the current state of the RBAC extension models.
- A basis for comparison and look up for what extension model to use for developers looking to find a model to fit their access control needs.
- A summary of current evaluation methods used in research on RBAC extension models.

The rest of the paper is organized as follows. Section 2 presents background and the RBAC standard. Section 3 presents methodology and process, which we used in conducting the systemic literature review. Sections 4-8 present analysis and discussion of the research questions. Section 9 discusses issues about the RBAC extension models. Section 10 concludes the paper.

2. Role-Based Access Control Standard

RBAC provides a high level abstraction of permissions management for operations, especially when sharing resources among roles within an organization. In cases where organizations were concerned with adopting RBAC, evaluation and comparison of RBAC technologies developed by different vendors was difficult. To address this issue, NIST proposed a standard for RBAC. NIST's RBAC standard can benefit organizations by lowering the cost of RBAC adoption [6]. The RBAC standard includes three components of RBAC: core RBAC, hierarchical RBAC, and constrained RBAC. Hierarchical RBAC and constrained RBAC are developed by incorporating new features into core RBAC. Each component includes a corresponding RBAC Reference model.

We describe the four entities of these reference models.

- *Users*: A user is defined as a human being. Although the concept of a user can be extended to include machines, networks, or intelligent autonomous agents, the definition is limited to a person in the RBAC standard.

- *Roles*: A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.
- *Permissions*: A permission is an approval to perform an operation on one or more RBAC protected objects in the system.
- *Sessions*: A session is a mapping between a user and an activated subset of roles that are assigned to the user.

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

On the top of the core RBAC Reference Model, the hierarchical RBAC Reference Model adds role hierarchies (RH) as a feature. The role structure in an organization may use a role r_1, which inherits all permissions of another role r_2. Concept of the role inheritance describes the many-to-many mapping role inheritance relations among roles. Therefore, more than one role (e.g., two roles r_1 and r_1') can inherit all permissions of r_2.

The constrained RBAC Reference Model adds separation of duty relations to the core and hierarchical RBAC Reference Models. Separation of duty relations enforce conflicts of interest among roles. The Constrained RBAC model defines two types of constraints placed on the user-role assignments: Static Separation of Duty (SSoD) and Dynamic Separation of Duty (DSD).

- SSoD relations define constraints as a pair ($roleset$, n) statically where no user is assigned to more than n roles from the $roleset$. Suppose roles $Role_A$ and $Role_B$ in $roleset$ conflict with each other and n is 2. A user who is assinged to $Role_A$ cannot be assigned to $Role_B$.
- DSD relations define constraints as a pair ($roleset$, n) dynamically where n is a number, with the property that user session may not activate more than n roles from the $roleset$. For situations where multiple roles can be associated with a single user and n is 2, a user session cannot be assigned to both $Role_A$ and $Role_B$ at the same time.

3. Methodology and Process

We adopted and applied a systematic literature review process following recommendations from Kitchenham and Charter's suggested processes [9]. The systematic literature review process was broken down into four stages and the rest of this section is broken down by each stage. The stages were as follows:

- 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 elimination criteria

Table 1: Paper counts after applying Step 1

	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**

3.1. Step 1: Search Strategy

For the first phase of our systematic literature review, we 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 the stopping criteria were met. Table 1 lists the four search engines along the left most column with the three search terms across the top row along with the papers for each criterion and engine combination. The total column represents the total for each individual search engine with a grand total across all search engines. The combined total represents the net paper total after removing duplicate entries. 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 title 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 are meant to stop after relevant results are no longer being returned by the search engine. After gathering all 12 data sets, we combined the papers into a master list, which includes only distinct papers by systematically comparing the bibliographic information for each. Out of the master list of 1,716 papers, two reviewers conducted a series of elimination rounds to narrow the list of papers and identify primary sources. The two reviewers are denoted by Author 1 and Author 2 where the former is the first author on the paper (Eric) and the latter is the second author on the paper (JeeHyun). Table 2 shows the total number of papers selected by each reviewer 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 conducted 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 on 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 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'?

The title elimination round resulted in Author 1 selecting 305 papers, and Author 2 selecting 176 papers with 149 papers of overlap between the two. All 149 papers found to be in both reviewers lists were kept. The 332 papers found not to be in common were then slated for a second round of review. The second round of review consisted of the reviewers discussing their perception of each paper title as the title related to the elimination criteria and making a joint decision to keep or reject. The second review resulted in 149 rejections and 141 being retained.

3.2.2. Step 3: Abstract Elimination

The second round of elimination was based on reading of the abstracts of papers that survived title elimination. The reviewers 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 an implementation, evaluation, or domain for their model?

The abstract elimination round resulted in Author 1 selecting 86 papers, and Author 2 selecting 102 papers with 51 papers of overlap between the two. All 51 papers found to be in both reviewers lists were kept. The 137 papers found not to be in common were then slated for a second round of review. The second round of review consisted of the reviewers discussing their perception of each the paper abstract as each related to the elimination criteria and making a joint decision to keep or reject based on the joint outcome of the discussion. The second review resulted in 116 rejections and 21 being retained.

Table 2: Elimination Rounds

		Title	**Abstract**	**Content**
Author 1		305	86	46
Author 2		176	102	42
	Overlap	149	51	24
	Disjoint	332	137	64
	Rejected	191	116	61
	Retained	141	21	5
	Num Left	290	72	27

3.2.3. Step 4: Content Elimination

The final elimination round involved reading the entire paper 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. Each reviewer seeks to answer following questions based on the content of the paper:

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

The content elimination round resulted in Author 1 selecting 46 papers, and Author 2 selecting 42 papers with 24 papers of overlap between the two. Between the two reviewers selections, there were 64 papers not in common, of which, 59 were rejected and 5 retained after a second review.

3.3. Extraction

After selection of primary sources, the next step was to extract data from each paper that pertained to our research questions 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 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 extension models and what papers fell into what categories.

4. RQ1: Classification

How can RBAC extension models be classified?

During the paper reading phase, we identified that a variety of common terms were emerging to describe the RBAC extension models. We developed a process by which to build a classification of the RBAC extension models based upon observations during the paper reading phase. For example, the paper “Privacy-aware role-based access control” [8] brings in the notion of privacy explicitly within the title of the paper and the name of their model. Some papers appeared to present a direct pronouncement of their classification, whereas others were less obvious. Thus, we developed a set of guidelines to aide in determining a set of eight categories. In developing these guidelines, we defined each category by a single noun-phrase descriptor. The guidelines were as follows:

- Model Name - Does the name of the model classify itself?
- Self Assessment - Do the authors of the paper directly identify a descriptor for their model within the body of the paper?
- Repetition of Phrase - Does the body of the paper present the same phrase repeatedly when discussing their model?

The previous example paper “Privacy-aware role-based access control” [8] contained “privacy” in the title and in the name of the model leading to the creation of the Privacy category and the subsequent placement of the paper under that category. By comparison, the paper “An extended RBAC model based on granular logic” [10] does not contain a direct categorization in the title or model name. However, in reading the body of the paper, we determined that the paper discussed RBAC extension based on context. In Section 4.1, we offer definitions for each of the eight observed categories.

4.1. Results

We provide a definition for each observed model category based on data extracted from the primary sources and the English definitions for each noun-phrase. Some category descriptors contain abbreviations in parenthesis that match the shortened name found in Table 6 (within Appendix 1) which presents each primary source within it’s designated category.

- **Context**: The extension model integrates contextual information into the RBAC standard model. Context is defined as a user’s current state and environment (e.g., location, time, system resources, network state, network security configuration, etc). The user’s access privileges are dependent upon the values of the current state and environment at any given time.
- **Constraint (Const)**: The extension model provides conditional restrictions on permissions of given roles. The constraint is either static or dynamic. For example, a doctor may modify any medical record for which the doctor is assigned as the designated primary care physician.

This example describes a doctor's permission with a conditional restriction - "only when the doctor is assigned as the designated primary care physician may the doctor modify a particular medical record".

- **Organizational (Org)**: The extension model is concerned with providing mechanisms and entities that allow for RBAC across multiple organizations. Typically, users may have the same role name in different organizations, but may have different access privileges due to departmental variations.
- **Privacy (Priv)**: The extension model provides entities and mechanisms to describe privacy policies, which are legal statements or documents about disclosure or management of personally identifiable information such as name, address, or date of birth.
- **Task**: The extension model provides task entities which are associated with permissions and roles. 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 associated with tasks that are associated with permissions. For example, the employee role is associated with a task to write a report. This task is then associated with a permission.
- **Spatio-Temporal**: The extension model combines the use of either or both spatial (location-based) and temporal (time-based) constraints in specifying access control policies. For example, specific locations permit roles to conduct actions from 8:00 a.m. to 5:00 p.m.
- **Spatial**: The extension model provides spatial (location-based) constraints in specifying access control policies. For example, in organizations, locations are enforced whereas a specific role is permitted to conduct an action. Consider that an employee works only at a specific location. In such cases, a role should allow access to required resources only when the user is in that location. Spatial constraints can integrate with roles, user-role assignments, or role-permission assignments.
- **Temporal (Temp)**: The extension model provides temporal (time-based) constraints in specifying access control policies. For example, in organizations, periodic temporal durations are enforced whereas a specific role is permitted to conduct an action. Consider that a temporal employee works only from 9:00 a.m. to 3:00 p.m. In such cases, the temporal employee role should only be allowed to access required resources during the interval. Temporal constraints can integrate with roles, user-role assignments, or role-permission assignments.

4.2. Analysis and Discussion

The 27 primary sources produced a set of eight hierarchical categories. Table 7 summarizes each primary source under their designated category and furthermore, displays the perceived hierarchy of the categories. Figure 1 shows the hierarchy structure among categories and the counts of primary sources for each. For categories that have sub-categories, the totals of the category and sub-categories is provided as the second number in the figure. The Constraint, Organizational,

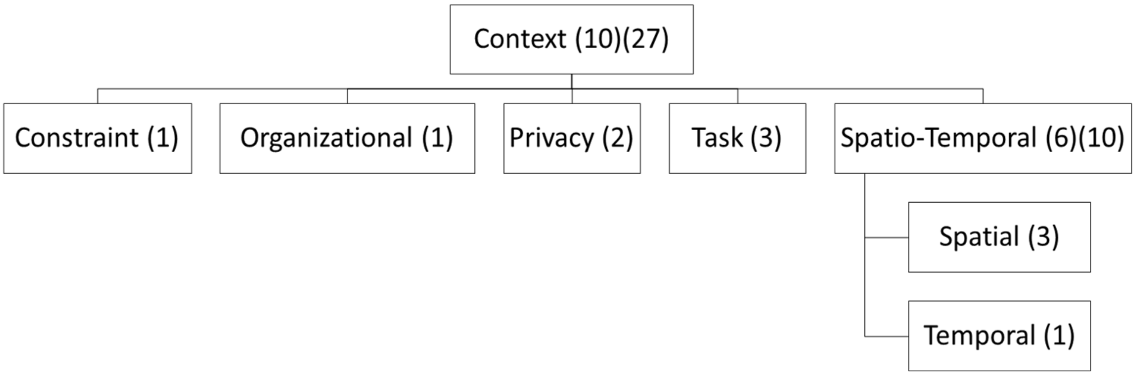

Figure 1: Structure of categories within the RBAC extension models.

Privacy, Task, and Spatial and Temporal categories can be special cases of the Context category. The Spatial and Temporal categories were treated as subsets of the broader category of Spatio-Temporal since this category encompasses them individually and the Spatio-Temporal category was derived from primary sources directly.

When looking across all categories, we noted that each category added specific features on top of the RBAC Reference Model. These features were under the surface adding contextual relationships between the core user, permission and role entities. Thus, we concluded that all categories stemmed from the context category, of which some primary sources were already deemed direct members.

For example, in the case of the Privacy category, the models added entities such as purpose binding to represent within the model data collected for one purpose should not be used for another purpose without user consent [8]. While the new entity provided by the Privacy based models is inspired by domains such as healthcare where privacy is of legal concern, the underlying mechanism that drives purpose binding is providing context around making an access control decision. The system must take into account not just a static set of permissions a user has through their roles, but also the context of the data being accessed as that data relates to privacy policy. In the spatio-temporal models, a users location and the time of day are two factors that can be taken into account when activating a role or verifying a permission. The concepts of location and time are properties of the user and place specific contexts around the role and permission entities.

We found eight categories that exist within the RBAC extension models: Constraint, Context, Organization, Privacy, Task, Spatio-Temporal, Spatial and Temporal. The context category was a superset of all other categories since all categories were found to consider context.

5. RQ2: Implementations

How are RBAC extension models implemented by their authors?

When designing and proposing a model targeted at a feature that is rooted in practical usage by real software systems, implementing the model is evidence that the proposed model can work

Table 3: Implementation types found and the count of primary sources

Implementation Type	Papers	Count
Enterprise	[12] [13] [14]	3
Prototype	[15] [16] [17] [18]	4
None	[8] [10] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36]	20

in practice. The presence of an actual implementation substantiates the robustness of the design and/or the need for the extension. We analyzed the primary sources to see how many proposed models actually had implementations associated with them. We quantified whether the implementation was an enterprise implementation (i.e., an implementation used in a production environment for a real system) or a prototype implementation (i.e., proof of concept to demonstrate the feasibility). In scientific research software life cycle, NuNamaker et al. [11] illustrated three implementation stages: prototype, enterprise (i.e., product), and technology transfer. Researchers often conduct their research by building a prototype implementation. A prototype implementation serves as a proof of concept to verify that certain concepts of proposed RBAC extension models. The prototype implementation demonstrates feasibility. However, this prototype implementation does not represent a deliverable real-world application. Majority of implementations in RBAC research stops with prototyping. After prototypes are successfully demonstrated, researchers make an effort to further develop a prototype implementation into an enterprise implementation. An enterprise implementation is a deliverable real-world application and allows to conduct realistic evaluations of the RBAC extension models. Technology transfer means that the technology of the proposed RBAC extension models are eventually transferred to the public marketplace. We found that none of implementations of the primary sources reach to the stage of the transfer of technology.

5.1. Results

Table 3 shows the breakdown of implementations found within the primary sources. Of the 27 papers surveyed, RBAC extension models in four papers were prototypes developed by the authors whereas RBAC extension models in three papers were claimed to be implemented within a real system. The remaining 20 papers provide no mention of an implementation.

5.2. Analysis and Discussion

The RBAC standard is designed such that when practitioners implemented RBAC into their systems, the RBAC standard demonstrates reasonable assurance being based off a well thought out model. As extensions to the RBAC Reference Mode come along, thought and time would be given to how features and nuances of their models may impact implementation to achieve the same goals as the original standard. The primary sources showed a lack of implementation with over 70% of the models having no notion of attempting to implement them. Prototype implementation shows the feasibility of the RBAC extension models in the four papers. Of the models that produced an implementation within the enterprise world, two were from within the medical domain and one was implemented using web application technologies.

Research on RBAC extension models shows a lack of implementations in the real world scenarios that the models are ultimately designed for.

6. RQ3: Evaluations

How are RBAC extension models evaluated by their authors?

The 27 primary sources were examined for evidence that evaluations of the proposed model were presented by the model authors. Zelkowitz and Wllace [37] proposed evaluation types and methods that are used to validate the claims in the paper. Table 4 illustrates 12 evaluation methods with their corresponding general evaluation types and descriptions. We classified each paper according to the evaluation methods shown in Table 4. For example, Aich et al. conducted project monitoring to show the performance and complexity of their proposed RBAC extension model [13].

6.1. Results

Table 5 shows evaluation methods and criteria. Based on the diverse evaluation methods, 12 models presented no evidence of an evaluation. Fourteen models presented example scenarios and how application of their model would apply and resolve the situation. These methods refer to assertions. Six models provided some form of performance or complexity analysis of their model through project monitoring. The performance and complexity analysis included graphs of the model's time to determine calculate authorization as the number of entities grew, and the size of the role space for the extension model compared to the RBAC Reference Model. Five models provided simulations based on mathematical descriptions and analysis as a way to provide evaluation in the form of completeness. The most widely used evaluation method was assertion, which provides sample scenarios with accompanying workflows of how the extension model would tackle those scenarios.

6.2. Analysis and Discussion

When proposing an access control model, providing an evaluation of the model is a key component in establishing the validity of the model. Further, in the case of extensions to the RBAC Reference Model, the model is accompanied by validation of the model as a stand-alone access control model and in comparison to the model upon which the enhancements are being made. The results show that robust evaluations of extension models are lacking.

The primary source of validation a developer or practitioner may encounter is a qualitative discussion of real-world scenarios and how the proposed model can tackle those situations. For five of the primary sources [17] [23] [25] [34] [38], the model authors conduct field study to provide some discussion of how the RBAC Reference Model is deficient in tackling the scenario. In Table 5, we observe that one paper includes a case study to examine how the proposed model works in practice. Discussions of how an extension model handles a real-world scenario provides developers and practitioners anecdotal evidence at best for what types of situations the proposed model could handle. Further, by not providing a comparison to the RBAC Reference Model, developers may be left implementing a more complex model to address their requirements when

Table 4: Evaluation Types and methods classified by Zelkowitz and Wllace [37]

Evaluation Type	Method	Description
Observational methods	Project monitoring	Monitor project and collect development data
	Case study	Monitor project in depth and collect data with a specific goal for the project
	Assertion	This evaluation uses examples for validation
	Field study	Monitor multiple projects and collect relevant information to compare the projects
Historical methods	Literature research	Examine previously published projects
	Legacy	Examine data from completed projects
	Lessons learned	Examine qualitative data from projects
Controlled methods	Static analysis	Examine structure of dveloped product
	Replicated experiment	Develop mulitple versions of product
	Synthetic environment	Replicate one factor in laboratory setting
	Dynamic analysis	Execute developed product for perormance
	Simulation	Execute product using a model of real enviroment

the RBAC Reference Model would have sufficed. Further, given the nature of access control models as grounded in application to enterprise implementations, case studies of a model in action provide developers with evidence that the model works as intended when applied.

When looking for an enterprise ready access control mechanism, developers must balance usability with security. Two of the primary sources examined provided time-based performance analysis of their extension model compared to the RBAC Reference Model through project monitoring. This inclusion of time analysis provides some assurances to developers that any non-functional requirements surrounding time to compute authorizations compete or beat the RBAC Reference Model. Further, four of the models provided some form of complexity of their model through project monitoring. This complexity analysis plays a key role in the management of the access control mechanism over the course of the models implementation lifetime. As the number of roles, users and additional entities grows, developers will need to ensure non-functional requirements are met that deal with the ability for a system administrator to effectively manage

Table 5: Evaluation methods by primary source

Methods	Criteria	Papers	Count
Project Monitoring	Time-Based Performance	[8] [13]	2
	Complexity Analysis	[17] [25] [30] [31]	4
Case Study	RBAC Model in Practice	[12]	1
Assertion	Example Scenarios of the Model in Action	[10] [14] [15] [16] [17] [18] [19] [20] [21] [23] [32] [34] [36] [35]	14
Field Study	Comparison to Standard RBAC	[17] [23] [25] [34] [38]	5
Simulation	Mathematical Modeling	[27] [29] [30] [31] [36]	5
No Evaluations	Not Applicable	[26] [28] [33]	3

these entities.

RBAC extension model research lacks comprehensive evaluation of the models both in theory and in practice.

7. RQ4: Domains

What domains have been targeted by RBAC extension models?

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. We identified domains presented within the primary sources by looking for example scenarios cast within a particular domain or mention of domain requirements within the body of the paper.

7.1. Results

Table 6 shows domains mentioned and their associated sources.

The predominant domain for which extension models have been generated for is that of the medical domain with 9 of 27 mentioning scenarios or requirements of that industry. Mobile computing and enterprise workflows were each represented by five papers claiming to be influenced by the requirements for access control within these domains. The final set of domains was pervasive computing environments and large-scale organizations with three each and web applications with one. Two papers [10, 30] do not mention domains explicitly since Aich et al. [13] fall under both the medical domain and mobile computing.

Table 6: Domains by primary source

Domain	Papers	Count
Medical Domain	[8] [12] [13] [18] [19] [20] [27] [29] [32]	9
Pervasive Computing Environments	[16] [34] [31]	3
Web Applications	[24] [26]	1
Mobile Computing	[13] [22] [23] [28] [33]	4
Organizations with Many Sub-departments	[14] [21]	2
Enterprise Workflows	[15] [17] [25] [35] [36]	5
None	[10] [30]	2

7.2. Analysis and Discussion

The medical domain produced the largest selection of papers when analyzing the domains influencing the proposals of RBAC extension models. Moreover, we observed that the categories associated with papers identifying the medical domain were not limited to one or two but cut across each of the eight categories except for the Organizational category. The cross-category nature of the medical domain papers appears indicative of the complex nature of medical applications and requirements. Given the growth of the research and development of medical applications over the past decade this result does not appear to be surprising. However, the RBAC standard was originally created to reduce cost and increase interoperability - two goals of current regulation around the standardization of electronic health record systems. The large number of proposed models, and the cross-category result stand in direct opposition of the goals of both the RBAC standard and current regulations.

The RBAC standard has been re-enforced by the economic impact that standardization has had on enterprises needing to apply access control. The inclusion of extension models targeted at the enterprise workflow domain is indicative of the expansion of requirements for enterprises. Developers and researchers would take care when looking at extension models designed to address the newer requirements of enterprise workflows to achieve the same economic implementation and maintainability benefits the RBAC Reference Model presents.

Figure 2 shows domain distribution by 3-year period. We observed that medical and enterprise domain papers constantly appear for every period in Figure 2. For a domain that has roots in medical and enterprise computing, protecting the data of both through access controls is paramount given their ubiquity. Mobile computing has seen a dramatic increase in the number of available devices, operating systems and applications since 1997 when the first smart phone was introduced [39]. Since 2004, the domain analysis results produced five papers that targeted extensions that are designed to address the requirements of mobile computing.

RBAC extension models were found targeting domains such as medical, pervasive computing, web applications, enterprise workflows and mobile computing.

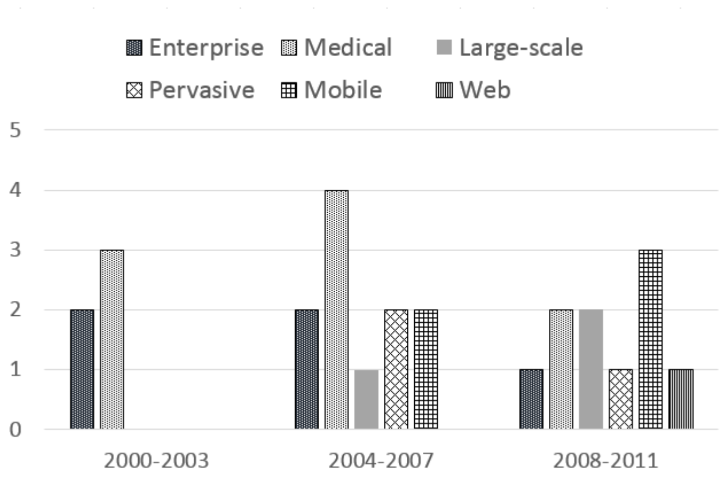

Figure 2: Domain distribution by 3-year period. Y-axis represents the number of corresponding domain papers. X-axis represents 3-year period from 2000 to 2011.

8. RQ5: Generalizations

What commonalities exist across RBAC extension models?

During the paper reading phase, we identified commonalities within the primary sources by looking for formal modeling of extending RBAC extension models.

8.1. Results

The RBAC standard is used in various aspects of computer systems. To reduce efforts for modeling access control used in various applications, researchers often focus on developing generalized core concepts of access control. The authors use formal model to provide high level description of access control model across all categorizations. Formal model of access control provides precise understanding, specification, and analsysi of access control. Formal model [40] of access control can be specified in one of logic expressions such as propositional logic. For example, 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. Aich et al. [13] proposed STARBAC model, which can be expressed in propositional logic. While propositional logic does not support for quantifiers, first-order logic (i.e., predicate logic) extends propositional logic by the use of quantifiers. For example, ESTARBAC model [13] can be expressed in first-order logic.

8.2. Analysis and Discussion

We found that 27 papers of RBAC extensions provide formal model based on logic expressions to describe its extended model. We discuss two widely used logic expressions for access control: propositional logic and first-order logic. Given context, propositional logic is used to evaluate true or false based on specified rules and access control logic. As access control is typically evaluated to either true or false based on predicates, propositional logic is sufficient to describe key ideas and definitions. Propositional logic is suitable for specifying what combination of attributes values a request must satisfy to be authorized to roles. However, propositional logic has limitations. While this logic is simple, this logic does not support for quantifiers and reasoning about RBAC, which helps reduce the administrative complexity of associations such as user- role associations. To support for reasoning of access control, one may describe the RBAC extended models in first-order logic. First-order logic is expressive enough to concisely represent access control systems. Given an RBAC extension model, Samuel et al. [32] proposed verification of the model using a specification language, which is based first-order logic. This logic is sufficient to model RBAC and extended RBAC for reasoning. Moreover, this logic supports for concise and elegant formulation of the Reference Model and its relation.

.

9. Discussion

The research questions we identified, presented results for and analyzed provide a view of the RBAC extension model landscape. By looking across all the research questions we can arrive at cross-cutting concerns and identify areas that may benefit from future work. We discuss motivations behind the RBAC extension models and guidelines for choosing an RBAC extension model.

9.1. Motivations behind the RBAC extension models

While the RBAC Reference Model is considered fundamental in any RBAC systems, the RBAC Reference Model has limitations on providing features such as dealing with context for emerging applications such as healthcare and mobile devices. For example, in cases where the RBAC extension model does not support the notion of specific constraints, the RBAC extension model incorporates additional entities with regards to context/constraints and their relations with existing entities of the RBAC Reference Model. The RBAC extension model provides general agreement on the definition for specific features. The RBAC extension model helps simplify theoretical modeling and practical implementation of features in the model.

During the paper reading phase, we identify motivations of the RBAC extension models by category. We identify motivations by looking for issues regarding why the RBAC reference model was inadequate and how the authors addressed the issues. We describe motivations behind the RBAC extension models by category as follows:

- **Context**: The RBAC Reference Model does not support the notion of context constraints related to changes in environments. Therefore, RBAC belongs to the static access control model, which may not capture changes in environments.

- **Constraint**: The RBAC Reference Model has limitations on its features such as delegation and role hierarchy. For example, partial inheritance in role hierarchy needs to be developed.

- **Organizational**: The RBAC extension model does not handle RBAC administrative tasks efficiently across multiple organizations. The model needs to reduce the administrative complexity of RBAC across multiple organizations.

- **Privacy**: The RBAC extension model does not support the notion of privacy. For example, the model lacks components, constraints, and obligations to handle privacy in RBAC.
- **Task**: The RBAC extension model does not support the notion of a task, team, purpose, and organizational roles, which help specify a business activity in enterprises.
- **Spatio-Temporal**: The RBAC extension model does not support spatial (location-based) and temporal (time-based) constraints, which specify role-assignment, role-activation and permissions based on location and time.
- **Spatial**: The RBAC extension model does not support the notion of spatial (location-based) constraints, which specify role-assignment and permissions based on location.
- **Temporal**: The RBAC extension model does not support the notion of temporal (time-based) constraints, which specify role-assignments and permissions based on time.

We found that motivations for RBAC extension models vary across category. In general, motivations are rooted in adding new entities or relationships to allow authorization flexibility in meeting the demands of emerging requirements.

9.2. Adoption of RBAC Extension Models

To adopt a model in practice, software developers would implement the model in real system environments based on intended use of the models. As shown by RQ5, all primary sources were found to provide an abstract formal representations of their extension model and the model's operation. The presence of an abstract formal representation of the model stands as a starting place for developers to configure intended use (i.e. which subjects can access which resources), and define an access control policy (i.e. which specifies high-level rules such as which subjects can access to which resources).

A formal representation of access control models is a critical step of designing high-level abstraction where which entities are used and how these entities are operated. One of the objectives of a formal representation is to help ensure the correct behaviors through formal verification. Given the formal representation of access control models, software developers may prove of properties (e.g., safety, consistency and completeness) and check whether these properties are satisfied.

While the concept of the Reference Model is clear and can be applicable to any system, it is challenging to implement the security mechanism of RBAC because the Reference Model is can be interpreted in more than one interpretation due to its complexity. To bridge gap between RBAC standard and its implementation, NIST published RBAC Implementation and Interoperability standard (RIIS/ ANSI INCITS-459) in 2011. This standard specifies how to implement RBAC system, which is consistent with NIST RBAC standard. Moreover, this standard describes interoperability specification where one RBAC implementation can be translated to another one.

This standard does not provide a specific guideline for implementation of various RBAC extension models. Moreover, when software developers implemented RBAC extension models, they require clear security requirements of extended role-based access control, which identifies security objectives, intended environments, and assumed threats. Moreover, software developers understand how this RBAC extension model overlaps with other access control models when more than two access control models are integrated into a single system. A survey [6] shows that over 50% of users at organizations with more than 500 employees are given some of their permissions to access resources based on RBAC. To adopt RBAC into a system, organizations often use hybrid approaches, which combine RBAC and access control lists because specific user types, systems, and workflow may not be effective to manage access based on roles. Therefore, when RBAC is extended and combined with other access control models, software developers can provide a formal representation which can serve as support for proof of the model. Then, software developers implement RBAC extension models based on NIST standard of RBAC implementation. Especially, software developers understand intended use of RBAC extension models to meet a new system requirement. For example, for a spatial RBAC model, software developers incorporate additional spatial constraints, which can be either static or dynamic, in practice into the RBAC model.

10. Conclusion

The RBAC extension models were revealed to fall into a number of categories with Const, Org, Priv, 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 identified as being the motivations behind needing extensions to the RBAC Reference 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 extension 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.

11. Acknowledgements

Funding for this work was provided by the Secure Open System Initiative funded by the Department of Defense.

References

[1] B. K. Michael P. Gallaher, Alan C. OConnor, The economic impact of role based access control., http://csrc.nist.gov/groups/SNS/rbac/documents/cost_benefits/report02-1.pdf (2002).

[2] R. Sandhu, D. Ferraiolo, R. Kuhn, The nist model for role-based access control: towards a unified standard, in: ACM workshop on Role-based access control, Vol. 2000, 2000.

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

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

[5] C. E. Y. Charles L. Smith, Edward J. Coyne, A marketing survey of civil federal government organizations to determine the need for rbac security product, http://csrc.nist.gov/groups/SNS/rbac/documents/cost_benefits/seta.ps (1996).

[6] A. C. O'Connor, R. J. Loomis, 2010 economic analysis of role-based access control, http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf (2010).

[7] D. R. Kuhn, E. J. Coyne, T. R. Weil, Adding attributes to role-based access control, Computer 43 (6) (2010) 79–81.

[8] 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.

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

[10] 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.

[11] J. F. Nunamaker Jr, M. Chen, Systems development in information systems research, in: System Sciences, 1990., Proceedings of the Twenty-Third Annual Hawaii International Conference on, Vol. 3, 1990, pp. 631–640.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] S. Haibo, H. Fan, A context-aware role-based access control model for web services, in: Proceedings of the IEEE International Conference on e-Business Engineering, ICEBE '05, 2005, pp. 220–223.

[25] 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.

[26] A. Masoumzadeh, J. Joshi, Purbac: Purpose-aware role-based access control, On the Move to Meaningful Internet Systems: OTM 2008 (2008) 1104–1121.

[27] 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.

[28] I. Ray, M. Kumar, L. Yu, Lrbac: A location-aware role-based access control model, in: Information Systems Security, Springer, 2006, pp. 147–161.

[29] 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.

[30] 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.

[31] 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.

[32] 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, Purdue University.

[33] 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.

[34] 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.

[35] S. Oh, S. Park, Task–role-based access control model, Information Systems 28 (6) (2003) 533–562.

[36] 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.

[37] M. V. Zelkowitz, D. R. Wallace, Experimental models for validating technology, Computer 31 (5) (1998) 23–31.

[38] 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.

[39] J. L. Buck, E. McInnis, C. Randolph, The new frontier of education: The impact of smartphone technology in the classroom.

[40] M. Abadi, Variations in access control logic, in: Deontic Logic in Computer Science, Springer, 2008, pp. 96–109.

[41] H. Zhang, M. A. Babar, P. Tell, Identifying relevant studies in software engineering, Information and Software Technology 53 (6) (2011) 625–637.

[42] B. Kitchenham, P. Brereton, A systematic review of systematic review process research in software engineering, Information and Software Technology 55 (12) (2013) 2049–2075.

12. Appendix

Table 7: Primary sources by classification and properties (Implementation Type / Domain / Evaluation Type(s))

Context	[20] A flexible content and context-based access control model for multimedia medical image database systems, 2001 (None / Medical / Scenario)		
	[24] A Context-Aware Role-Based Access Control Model for Web Services, 2005 (None / Web Applications / None)		
	[15] A context-sensitive access control model and prototype implementation, 2000 (Prototype / Enterprise Workflow / Scenarios)		
	[16] A Context, Rule and Role-Based Access Control Model In Enterprise Pervasive Computing Environment, 2006 (Prototype / Pervasive Computing / Scenarios)		
	[12] A contextual role-based access control authorization model for electronic patient record Motta, 2003 (Enterprise / Medical / Case Study)		
	[17] A Role and Context Based Access Control Model with UML, 2008 (Prototype / Enterprise Workflow / Complexity, Comparison to Standard, Scenarios)		
	[10] An extended RBAC model based on granular logic, 2008 (None / None / Scenarios)		
	[21] Designing an agent-based RBAC system for dynamic security policy, 2004 (None / Organizations / Scenarios)		
	[22] Leveraging Access Control Mechanism of Android Smartphone Using Context-Related Role-Based Access Control Model, 2011 (None / Mobile Computing / Scenarios)		
	[23] CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment, 2009 (None / Mobile Computing / None)		
	Const	[19] A constraint based role based access control in the SECTET a model-driven approach, 2006 (None / Medical / Scenarios)	
	Org	[25] ROBAC: Scalable Role and Organization Based Access Control Models, 2006 (None / Enterprise Workflows / Complexity Analysis)	
	Priv	[8] Privacy-aware role-based access control, 2007 (None / Medical / Time-based Performance)	
		[26] PuRBAC: Purpose-Aware Role-Based Access Control, 2008 (None / Web Applications / None)	
	Task	[14] A Task-Role Based Access Control Model with Multi-Constraints, 2008 (Enterprise / Organizations / Scenarios)	
		[18] Team and Task Based RBAC Access Control Model, 2009 (Prototype / Medical / Scenarios)	
		[35] Task-role-based access control model, 2003 (None / Enterprise Workflows / Scenarios)	
	Spatio-Temporal	[30] STARBAC: Spatiotemporal role based access control, 2007 (None / None / Mathematical Modeling)	
		[31] On spatio-temporal constraints and inheritance in role-based access control, 2008 (None / Pervasive Computing / Mathematical Modeling)	
		[32] A framework for specification and verification of generalized spatio-temporal role based access control model, 2007 (None / Medical / Scenarios)	
		[33] LoT-RBAC: A Location and Time-Based RBAC Model, 2005 (None / Mobile / None)	
		[34] A Spatio-temporal Role-Based Access Control Model, 2007 (None / Pervasive / Scenarios, Comparison to Standard)	
		[13] Role Based Access Control with Spatiotemporal Context for Mobile Applications, 2009 (Enterprise / Medical, Mobile / Complexity Analysis, Time-based performance)	
		Spatial	[27] GEO-RBAC: a spatially aware RBAC, 2005 (None / Medical / Mathematical Modeling)
			[28] LRBAC: A location-aware role-based access control model, 2006 (None / Mobile / None)
			[29] Spatial role-based access control model for wireless networks, 2003 (None / Medical / Mathematical Modeling)
		Temp	[36] A generalized temporal role-based access control model, 2005 (None / Enterprise Workflows / Scenarios)

13. General Breakdown

- Broken literature references in Table 5 We address this issue.
- Tables 3,4,5 are not sorted in any order We manually sort by the order of the paper.
- Additional figures/visualizations would help [TBD] Eric and I would discuss this issue because the reviewer did not clearly which kinds of figures/visualizations would be needed.
- Reference section has incomplete entries We address this comment by looking at the each reference item and find missing entry. We check each entry with ACM or IEEE Bibtex. Consistent formatting will be done as well.
- Spelling, grammar and punctuation flaws We address this by spell check and grammar check (in Latex compiler). In addition, we convert it to MS word for additional spell check and grammar check. After this step, we will conduct manual proof reading.
- Table 6 should be revised to have better structure [TBD] Eric and I would discuss this issue because the reviewer did not clearly mention what's the issue or how to revise Table 6.

14. Background Breakdown

- This section should be shortened to at most 1 page. We address this comment by revising the background section.
- Definitions of static and dynamic separation of duty are incorrect. We find reference of static and dynamic separation of duty from NIST RBAC standard. We refer to ”The NIST Model for Role-Based Access Control: Towards A Unified Standard.”

15. Methodology Breakdown

- Calls into question the ”systematic” nature of the paper.

  We can address this by adjusting our search method to follow an accepted systematic approach as noted in the SLR literature. Notably the Zhang [41] approach mentioned in [42]. In this approach we do a two phase manual + automatic search. The manual phase identifies premier journals and conferences specifically related to our research questions and pulls out the ”quasi-gold standard” set of papers. We derive our search term from this set of papers and use them as an oracle for the precision and sensitivity of our automatic search

- Why the search we chose? Why not others like Springer? Elsevier?

  Looking at the recent work by Kitchenham to review SLRs from 2013 [42], the literature justifies the use of:

  - ACM Digital Library (already included)
  - IEEE Explore (already included)

  Two of the following indexes:

  - SCOPUS
  - EI Compndix
  - Web of Science
  - Google Scholar (already included)

  Journals/Conferences of Access Control:

  - ACM Transactions on Information and System Security (TISSEC)
  - International Conference on Emerging Security Information, Systems and Technologies, SECURWARE
  - International Conference on Information Systems Security
  - International Conference on Network and System Security
  - ACM Symposium on Access Control Models and Technologies (SACMAT)
  - ACM Symposium on Information, Computer and Communications Security
  - Information Security Conference
  - International Conference on Information Security and Assurance
  - International Conference on Information Systems Security
  - International Conference on Information Assurance and Security
  - International Symposium on Policies for Distributed Systems and Networks
  - ACM Conference on Data and Application Security and Privacy

- Where are the search terms?

  We will explicitly enumerate and mention the search term.

- Search process not described

  This will be beefed up with added information from the adjusted search strategy derived from the Zhang method.

- Search terms too generic. Why isn't search focused on research questions?

  Zhang [41] proposes (based on empirical testing) two methods for selecting search terms.

  Subjective - researchers derive search terms based on expert knowledge and the results of the "quasi-gold standard (QGS)" paper set or the use of Kitchenhams suggested population, intervention, comparison, outcomes, context, study designs Objective - researchers use a textual analysis tool aimed at the QGS paper set to derive most commonly used words and word relationships to then build the search term

- No mention of using different syntax for different search engines based on how different engines parse search strings.

  We will note any differences in how the search term is applied for different search engines.

- Type of search: full-text? title? abstract?

  We can address this by only specifically mentioning it for the manual search process since the automatic search will use common search engines.

- Whyat type of papers did the authors target? research? white paper? journal? conference?

  We can address this by only specifically mentioning it for the manual search process since the automatic search will use common search engines.

- Was search restricted to a publication period?

  We can address this by only specifically mentioning it for the manual search process since the automatic search will use common search engines.

- Reports of reviewers agreement/disagreement too coarse. IRR analyses recommended by Kitchenham.

  We'll calculate and use the Cohen Kappa value for this.

- Reasoning for stopping criteria never explained, especially technical limitations and what they are.

  This one may be trickier as a lot of SLRs don't require a stopping criteria due to how the search term is constructed. This item may take care of itself with the adjustments to the process and if not we'll specify the technical limitations for any search engine as the reason for why we ”stopped”.

- Why not use quasi-gold standard for search threshold?

  Zhang method will achieve this.

- No motivation for why ”model” is important as a search term.

  Choice of subjective or objective will handle this justification.

- ”conditional inclusion criteria” not allowed by SLR process

  We can pair down our inclusion/exclusion criteria and move some of the items into the data collection aspect. I noted that a number of SLRs use only a few inclusion/exclusion criteria.

- Corpus too small

  We can add a threat to validity if the corpus is too small and note that the search process followed a systematic approach.

- Question about changing the inclusion/exclusion criteria as not being systematic

  We can justify this more in the text as Kitchenham even mentions being able to iterate some elements as the search proceeds.

- No jutification for deviating from initial procedure

  Changing our methodology to Zhang should take care of this.

- ”inspired by real world example” - what does this mean?

- Table 3/4 inconsistent

- No papers from joournals/conferences related to access control such as SACMAT, missing papers from ACM TISSEC

  We can include these journals as part of the manual QGS approach prior to the automatic search.

- Why the search chain?

  Handled by Zhang.

- Criteria for selecting sources?

  Handled by Zhang method manual and automatic engines listed from Kitchenham.

- Why ”model” in the title is important and not something like ”policy”?

  This can be handled by the derivation of search terms from the subjective/objective method.

16. RQ1 Breakdown

- Not clear how the authors established the common terms. We find the terms by bottom-up approach by looking at the paper and finding common terms that can characterize the paper.

- How did the authors systematically tag the included papers in terms of a content analysis?

- Was this done ad hoc (during paper reading) or as a preparatory step? We address this issue by describing our approach. We do it by bottom-up search to find terms and construct it. Need to find such a method for classification (I don’t think that our approach is ad-hoc if we find it during paper reading).

- Authors defined the classification criteria by observation during paper reading. Same as above.

- The authors defined comparison items by themselves. Are there existing frameworks for comparing access control policies?

  In our SLR, we measure not only access control policies, but also measure approaches of papers. There are some such as ”Hu & Scarfone” metrics to measure access control policies themselves. We may find some papers that describe metrics. However, their metrics are limited to measure a specific property (such as complexity) of a given access control policy.

17. **RQ2 Breakdown**

- How do the answers to this RQ relate to the SLR? We address this issue by checking SLR process to understand what kinds of answers would be expected. Then, we adjust our answers to fit to SLR.

- This section reads like a discussion based on authors intuitions or conjectures We would move this section to discussion section if this one may not fit well to the RQs for SLR.

18. **RQ4 Breakdown**

- Why do the authors only distinguish between enterprise/prototype implementations? In the development process, modeling -¿ research prototype -¿ implementations in the real world systems. Our selected papers dealt with modeling of access control policies. Then, we would like to check whether this model is provided with a prototype and implementation.

- What about distinguishing different ”implementation techniques” ?

- What about other evaluation techniques such as case studies, static and dynamic analysis, formal proofs or controller experiments for example? We find from bottom-up approach.

19. **RQ6 Breakdown**

- Authors suggestion of ”propositional logic” is purely discussion and not backed by any data from the SLR We find reference paper about this propositional logic, which is used for papers collected for us.

20. **Discussion Breakdown**

- Why the ”Hu & Scarfone” metrics? We use this metric to show additional metrics.

- Did the authors perform a prior comparative analysis of different metrics? [TBD]