Linköping University | Department of Computer and Information Science
Master’s thesis, 30 ECTS | Informationsteknologi
2023 | LIU-IDA/LITH-EX-A--2023/003--SE

Access Management in Organizations

– A Comprehensive Study and Scenario-based Analysis

Åtkomsthantering inom organisationer - En omfattande litteraturstudie och scenariobaserad analys

Emily Berghäll
Anna Bergström

Supervisor : Alireza Mohammadinodooshan
Examiner : Niklas Carlsson

Linköpings universitet
SE–581 83 Linköping
+46 13 28 10 00 , www.liu.se

Abstract

Access management is an important part of the security of an organization as it limits access to sensitive material such as code and files. Therefore, access management can be a vital part of preventing leaks of information in regard to company-sensitive information or information about employees or users.

A technique that can be used to handle access management is the use of access control models. This thesis conducts a literature study and scenario-based evaluations of 12 access control models with the aim of creating recommendations and a roadmap for choosing access control models for different organizations. The most common factors of the chosen access control models are adaptability, flexibility, and high security. The 12 chosen access control models were chosen because they were deemed the best fit for organizations in the technology industry. Other models could be chosen depending on the industry or environment, which will yield different results but the roadmap can still be tailored.

The scenario-based organization focuses on five main parameters within the evaluation: attribute definition, economy, control authorities, organization, and security. These are determined by taking the average of the sub-parameters of each main parameter, this is done for each access control model resulting in a total average. The scenarios conducted are of differently-sized organizations namely: small, growing, and large. For each scenario, the main parameters were weighted which resulted in new averages which in turn resulted in recommendations for each scenario.

The results present recommendations for each scenario both in the form of a single access control model that can be used but also in the form of access control model combinations that can help reach more of the priorities parameters for each scenario. Further, the thesis can be viewed as a roadmap for organizations that can be tailored to fit individual needs and priorities by altering the parameter weights.

Acknowledgments

We would like to express our gratitude to our external supervisors Fredrik Gryvik, Björn Wallebäck, and Ronny Kuylenstierna for their guidance and encouragement. We also would like to thank the experts that were consulted for the important insights for this thesis.

Additionally, we would like to express our gratitude to our examiner, Niklas Carlsson, and our supervisor, Alireza Mohammadinodooshan, at Linköping University, for their consultation and feedback. Lastly, we would like to thank our opponent Roger Öncu for the valuable feedback.

Contents

List of Figures

List of Tables

1 Introduction

Access management is an important part of managing security in the system, for organizations within the technology industry, that work with devices such as computers. Access management is the process of managing permissions and actions of authorized users within an IT environment using policies to ensure that roles and permissions are followed [20].

Access management can be realized through the adaptation of access control models, which helps monitor ongoing operations and limit access of users to improve security within the organization. Typically, within access control models, access to resources is assigned depending on users' roles or attributes.

The work with access management and the choice of an access control model is important as the choice of a non-suitable model can cause major vulnerabilities for organizations. However, as of today, it can be difficult to find guidelines that help simplify the process of choosing an access control model. Therefore, this thesis will conduct a literature study and a model evaluation of access control models, with the aim of providing recommendations that can aid organizations' choice of access control model.

1.1 Aim

This thesis aims to present a scenario-based evaluation of access control models used within the technology industry. Specifically, this thesis compares the parameters of different access control models to conclude how the models adapt in different scenarios based on different-sized organizations and their needs. It will conclude with a recommendation of what access control model is best suited for each organization respectively.

1.2 Research questions

Through a comprehensive literature study and comparison of access control models and practices within the technology industry, this thesis aims to answer the following research questions:

1. What access control models are suitable for organizations within the technology industry?

2. How can organizations proceed to choose an access control model?
3. What access control models are best suited for different-sized organizations?

1.3 Approach

This thesis presents a literature study consisting of the discovery of potential access control models suitable for the technology industry as well as parameters such as attributes, economical factors, flexibility, etc., to present an analysis that ends with a recommendation of a suitable model. The analysis is in the form of an evaluation that measures and compares the different parameters and models against each other. The analysis also contains a scenario-based evaluation before a recommendation can be made for each scenario.

1.3.1 Delimitations

This thesis introduces some delimitations to control the settings of the study, as well as the scope. To begin with, it is important to recognize that choosing an access control model is not a complete security solution, albeit an important part of the solution. This thesis, however, only focuses on access control models, and all other parts of the security solution are assumed to be secure.

To create the frames of the thesis a baseline assumption is made that the organization is using RBAC as the current access control model, before the evaluation and the possible implementation of a new access control model. If another access control model were to be used as the baseline it could potentially yield different results.

Another delimitation made is that only 12 access control models were used in the report, despite there being a great deal more models out there. This is because the sample size would be too great otherwise. Further, when comparing the compatibility between the access control models, most research found is in connection to ABAC and RBAC which reflects in the analysis.

1.4 Contributions

The main contributions of this thesis are a literature study of 12 access control models, both role-based models, and other models, as well as an evaluation based on parameters and different organizational scenarios to create more tailored results. The results for the different scenarios, lead to recommendations of which access control models to use for different organizations.

1.5 Thesis outline

The remainder of this thesis is structured as follows. Chapter 2 explains core concepts and the results from the literature study. Chapter 3 contains findings from other papers on the same topics. In Chapter 4, the method, both for the literature study and the evaluations, alongside the parameters used, is described. Further, in Chapter 5, the literature-based model evaluation is presented using tables, followed by the organization-based evaluation in Chapter 6. The results are then discussed in Chapter 7, together with a discussion about the method used and the work in a wider context. Finally, in Chapter 8 the conclusions are presented with final recommendations for different organizations.

Abbreviations

Abbreviation	Definition
ABAC	Attribute-Based Access Control
ATRBAC	Administrative Temporal Role-Based Access Control
CapBAC	Capability-Based Access Control
DRBAC	Dynamic Role-Based Access Control
FBAC	Function-Based Access Control
GTRBAC	Generalized Temporal Role-Based Access Control
PARBAC	Priority Attribute Role-Based Access Control
PBAC	Policy-Based Access Control
RBAC	Role-Based Access Control
RRBAC	Resource and Role hierarchy Based Access Control
TBAC	Topic-Based Access Control
TRBAC	Temporal Role-Based Access Control

2 Background

In this chapter, a background for the thesis is presented, which introduces basic concepts and terms, as well as theory on the different access control models researched as part of the literature study.

2.1 Roles and permissions

A role can be seen as a job function within an organization, it can represent either competence, authority, or duty assignments rotated through multiple users [19]. Roles are used to provide a basis for the dividing of permissions for an organization and users are assigned to the roles corresponding to their job responsibilities and qualifications. Therefore, a role defines the individuals with access to specific resources and to what extent.

Permissions that are connected to a role rarely change over time, compared to the individuals behind the roles, which makes it a simpler way of handling permissions to resources as a new user is instead assigned to a preexisting role [19]. This also allows users to move within the organization and permissions will change according to their new role.

Further, using roles, rather than groups, for permission management eases the administrative aspects of access control within the organization since groups are a collection of users, but not a collection of permissions, and a role is a collection of both users and permissions [19]. Hence, the main difference between a group and a role is that for roles the users have permission, whereas groups consist of only users.

2.2 Least privilege

Least privilege is an aspect of access control that aims to lessen the risk of over-authentication of a user, meaning when the user has more permissions than needed in that role [19]. The objective of using least privilege is that a user with a specific role should only have permissions that are required for that role. The need-to-know principle could be considered a synonym for least privilege and is described as the guaranteeing that the user does not have too few or too many permissions suitable for their role [7]. In other words, least privilege means that a user should not have more permissions than necessary to perform their duties.

2.3 Separation of duty (SoD)

Separation of duty (SoD) is a form of restraint made to prevent a single user from obtaining control over the system or misusing it [1]. It also maintains a least privilege basis. For example, a user should not be allowed to both create and approve requests as it can be an internal security risk for the company.

In SoD, there can occur clashing in conflicts of interest. For example, if an end-user performs actions while active in a session where the user does not have permission, although the user might have the needed permission in other sessions [1]. There are different approaches to resolving conflict of interest issues, one method involves creating more dynamic access control models based more on permissions than roles to avoid such issues on both administrator and end-user levels.

2.4 Access control

Access control is a security technique used to determine what actions a legitimate user can perform in a system, and is used to prevent actions that could lead to misusage or security vulnerabilities [20]. All resources in a system can be seen as data stored in objects, the most fundamental aspect and crucial requirement of access control is the protection of these objects.

Access control needs to coexist with other security services as it is not a complete security solution [20]. This is because it only focuses on the actions of legitimate users, rather than also providing authorization and auditing. The authorization of users is performed separately to ensure the legitimacy of the identity. Further, access control also needs to coexist with auditing, which logs all users' requests and activities to be able to analyze the behaviors of said users. For the notion of access control, it is assumed that the users are legitimate and that the auditing is performed separately from the access control model.

Further, access control can present varying flexibility due to different policies used [20]. The flexibility impacts the ability of access control to adapt to specific organizations. The main reason for the importance of flexibility is that, even though how important access control is for an organization, if it is ill-fitted for the organization it will not be as beneficial.

2.4.1 Policies and mechanisms

The distinction between a policy and a mechanism is important for access control, as it is what defines security [20]. A policy is a high-level guideline that dictates how access is controlled and how access decisions are determined. No policy is deemed better than another policy, but some policies e.g. ensure more protection than others while others provide more freedom for users. The reasoning behind a policy containing more protection not necessarily being a better policy is that the policy needs to be suited to the organization and the priorities. This means that the choice of policy needs to be individually selected for each organization.

On the other hand, a mechanism is a low-level software and hardware function that is configured to implement different policies. The use of mechanisms supports confidentiality, integrity, and availability.

2.4.2 Access matrix

The access matrix dictates the rights of all subjects and objects [20]. It does so by using a reference monitor and separates authentication and authorization. For large systems, the access matrix will be very large in size with most of the cells being empty due to restricted access, therefore the matrix is often presented using different tools, such as access control lists, and capability lists.

Access control list (ACL)

Access control list (ACL) is a popular implementation of an access matrix [20]. Each object has its ACL which shows the access rights for each subject in the system. ACLs make it easy to study the access rights to all objects, which includes the ability to remove all accesses to a selected object in a fast manner. This, however, makes it harder to get an overview of all accesses tied to a user. Additionally, to decrease the size needed for the ACL and make it more manageable compared to access matrices, group names are allowed in ACLs in addition to individual names. Using group names aims to ease the implementation of ACLs and can thus be argued as superior to regular access matrices.

Capability list

A capability list introduces a list for each subject containing detailed permissions to objects in the system [20]. In contrast to ACLs, using capability lists makes it easy to get an overview of all accesses for a specific subject, but more complicated to get an overview for an object.

2.4.3 Access control policies

When it comes to access control policies there are three common types of policies; discretionary, mandatory, and role-based policies [20]. The policies are independent of the different access control models and organizations they can be implemented for. However, these policies are not exclusive and can be combined to produce more suitable protection for the system.

Discretionary policies

Discretionary policies handle access based on authorizations for users connected to specific objects, where access is either granted if the rules are followed or denied otherwise [20]. Discretionary policies are flexible and are therefore widely used. The drawback of discretionary policies is, however, that the flow of information can not be assured as it is easy to evade the stated authorizations [20].

Mandatory policies

Mandatory policies, as opposed to discretionary policies, handle accesses based on security classifications of subjects and objects [20]. Two main principles are required to hold; read down and write up, to control the flow of information. Read down means that a subject must have a higher security level than the object to be able to read the object and write up means an object must have a higher security level than the subject to be able to write. Additionally, categories can be introduced to all subjects and objects to ensure that both the subject and the object have what is needed to allow access. Categories can be based on an area e.g. either physical or of expertise that the user operates in, and therefore should be granted access to.

Role-based policies

Role-based policies, on the other hand, handle accesses for users through the basis of the activities the users execute and require the identification of roles in the system [20]. The role-based policies have advantages in the form of easier authorization management, clear hierarchy among roles, least privilege, and SoD are supported, and object classes are introduced by classification of all user activities.

2.5 Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) can be seen as a policy-neutral access control model, but depending on the configuration, it can vary between mandatory or discretionary access depending on the policy used [19]. RBAC introduces the ability to connect roles to other roles, permissions, and users. Permissions tied to a role can be defined before the role is tied to a user, which simplifies the process of connecting users to permissions and often requires less technical skill from the administrators than assigning permissions to roles. Further, RBAC supports least privilege and SoD, as well as data abstraction meaning the possibility to grant permissions for credit and debit actions to extend permissions for the more traditional actions read, write and execute.

Different versions of RBAC exist and are often referred to as dimensions [19]. However, the base model with the minimum requirement includes four entities: users, roles, permissions, and sessions. Users can be employees or machine users and roles are job functions. Permissions, as mentioned in 2.1, are access to objects within the system, where an object can be a file, data, or other resources. Permission can be granted in several different ways, for example, access granted to a complete subnetwork or access granted to a subsection (e.g. a folder) of a subnetwork. The objects and operations for a specific implementation of an access control model need to be case-sensitive as it depends on the characteristics of the system for the implementation itself. Permissions can be granted for objects individually as well as grouped. Lastly, sessions are periods when users activate different roles or sets of roles. During these individual sessions, multiple permissions assigned to a single user can be activated at once.

Further, RBAC includes user assignment and permission assignment [19]. User assignment focuses on the users tied to a role, where a user can have multiple roles and a role can have multiple users. In the same sense, for permission assignment, a role can have several permissions and permission can be granted to several roles. For system administrators managing the roles and permissions can be a large task, these tasks are usually performed by a small group for security reasons.

Apart from the minimum requirements, the models can include role hierarchies, constraints, or both combined [19]. Role hierarchies are natural ways of structuring roles within organizations in terms of authority and responsibility, where generally more senior roles are granted larger permissions than subordinates. Moreover, the constraint is a method of implementing organizational-specific policies, which can state what permission cannot be combined. Further, in some cases negative permissions are discussed, meaning that permission is denied for specific resources, rather than granted.

During the years several developments of RBAC have been finalized and a few of these will be described below.

2.6 Temporal Role-Based Access Control (TRBAC)

A known limitation with traditional RBAC is that some roles may need to be granted to users only during periods [2]. This means that there is a dynamic aspect to manage with temporal dependencies. This can be done with Temporal Role-Based Access Control (TRBAC) that extends RBAC with support for periodic handling of roles and temporal dependencies, namely role triggers.

When a role only should be able to have access during specific times, e.g. for part-time staff, a temporal dimension to roles is needed [2]. Therefore, TRBAC introduces two concepts, role enabling and role disabling. Role enabling is the transition from disabled to enabled access and role disabling is the opposite. Both enabling and disabling can be handled through role triggers which are rules that are automatically performed. The backside of the influence from TRBAC to roles is that situations, where it is undecided what roles are enabled, might occur [2].

As with traditional RBAC, TRBAC also has known limitations such as only addressing the role enabling constraint and no other temporal aspect. Further, another known limitation is a lack of security analyses that identifies potential security breaches. These limitations have influenced the researchers to further develop the model, resulting in ATRBAC and GTRBAC, which are described below.

2.7 Administrative Temporal Role-Based Access Control (ATRBAC)

Apart from addressing the temporal dimension of RBAC that is done in TRBAC, Administrative Temporal Role-Based Access Control (ATRBAC) focuses on the administrative aspect of an access control model which can be performed according to the temporal aspects of TRBAC [28].

In the traditional RBAC model, the administration is performed by users who are granted administrative privileges [28]. In ATRBAC, on the other hand, policies control the assignment and revocation of roles. Policies within these systems are generally represented by rules that permit administrative users to perform operations that are limited by the policies.

ATRBAC, however, does not cover all aspects of role hierarchy and throughout its development a static environment has been assumed, meaning that no changes to the environment were introduced during testing [28].

2.8 Generalized Temporal Role-Based Access Control (GTRBAC)

Generalized Temporal Role-Based Access Control (GTRBAC) is an access control model that builds on TRBAC that only addresses the issue of role enabling constraints, to address more temporal constraints, namely duration and periodic constraints on roles and user-role as well as role-permissions assignments [10]. GTRBAC also provides both events and triggers developed from those in TRBAC. Further, GTRBAC allows for role hierarchies and SoD combined with a temporal aspect.

GTRBAC separates the differences between role enabling, and role activation [10]. Role enabling means that a role has permission to access, while role activation means that a role is being activated in the system and accessing objects. This is tied to the three states of a role: enabled, disabled, and active. The role enabling and activation can be specified for both user-role and role-permission assignments.

2.9 Priority Attribute Role-Based Access Control (PARBAC)

Priority Attribute Role-Based Access Control (PARBAC) is developed for Azure IoT cloud [25], where the priority of users and objects are taken into account for authentication and authorization. PARBAC extends both the model of RBAC and ABAC by maintaining the flexibility of ABAC and the administration, permission review, and policy analysis from RBAC while combining it with simplified authentication and authorization.

PARBAC introduces decisions taken by priority-based conditions, as well as managing authentication and authorization according to specific permission and privilege tied to priority attributes instead of personal identities [25]. The priority of the user is important within PARBAC regarding what information about user role and permission assignment is deemed relevant. PARBAC is also known to lower the costs for computation, communication, storage, as well as time [25].

2.10 Dynamic Role-Based Access Control (DRBAC)

Dynamic Role-Based Access Control (DRBAC) extends the traditional RBAC model by improving the policies using machine learning based on reinforcement learning and Bayesian belief networks [6]. Reinforcement learning means sequential decision-making policy, combined with machine learning in the form of deep learning which enables the ability to learn a system without human supervision. Bayesian belief networks use historic behavioral profiles to build a trust scheme of users to enhance the security of the system. The model is trained offline to assure the security of the system.

DRBAC was developed to avoid several issues known to traditional RBAC, e.g. if credentials are lost, insider threats, and misconfigured policies, which would allow unauthorized personnel to access sensitive resources [6].

2.11 Resource and Role hierarchy Based Access Control (RRBAC)

Resource and Role hierarchy Based Access Control (RRBAC) builds on the RBAC model by introducing resource hierarchy, meaning the natural hierarchy of objects, which allows for redundant access assignments to be eliminated [23]. The main aim of RRBAC is to improve policies, as well as the convenience and efficiency of permission management found in the RBAC model.

With resource hierarchy, the problem of permission validation is more complex than for traditional RBAC [23]. With RRBAC a resource tree-based permission assignment and validation mechanism are used, meaning permissions will be granted and inherited down to children's resources. The resource tree will ease the task of permission assignment, by eliminating the need to assign all permissions individually and therefore decreasing the amount of administrative work required. However, this will mean that performance of permission validation will not improve, especially for large organizations.

2.12 Attribute-Based Access Control (ABAC)

Attribute-Based Access Control (ABAC) is a flexible access control model that functions by denying or granting user requests based on the attributes of the user and environmental conditions in relation to relevant policies of the company [9]. An attribute can manifest in different ways depending on the environment and needs of the company, for example, an attribute could be a role in the company or which department or team the user belongs to. The environmental attributes may include the date, time, and location, and are defined by situational factors as well as the relationship between the subject and object [29]. The policies determine if access to an object will be granted depending on the attributes of the user, object, and environmental factors.

ABAC has in recent years been described as the latest milestone within the evolution of access control models, some of the reasons for this being its high flexibility, fine granularity, and customizability [31]. In ABAC both users and objects have attributes, in objects, this might take the form of sensitivity level or file type [4].

There are some security threats to ABAC such as attribute forgery or permission counterfeiting, which can have devastating outcomes for businesses [31]. Further, there are policy errors that can become crucial in conflict prevention in the system [29]. Some of the more notable policy errors are:

- **Rule-Redundancy** means two sets of rules are equivalent and requests of operations are equivalent, thus one set of rules becomes redundant and the set that is not a subset of the other should be removed.
- **Rules-Discrepancy** can create a critical security issue and malfunction if the decision of two sets of rules is not identical. This can happen e.g. if a set of attributes have been reconstructed but are not the same everywhere, either because they have not been synced or possibly on account of attribute forgery.

- **Rules-Inadequacy** develops if the rules are not adequate to decide if permission can be granted or not, based on the attribute values and policy set.
- **Conflict-Decision-Positive-Negative** occurs if a request is denied by one set of rules and allowed by another.
- **Conflict-Demand** is if the demand rises for a particular resource and can be solved by priority scheduling.

2.13 Capability-Based Access control (CapBAC)

Capability-Based Access Control (CapBAC) is a kind of access control model where a capability token is assigned to users instead of roles or attributes [8]. The tokens uniquely identify what permissions the user has on different objects, i.e. what the user is capable of doing with different objects. Beyond the permissions, other aspects can be included in the token such as the place or time when the object can be accessed. CapBAC can be considered more scalable and lighter than RBAC and ABAC models, particularly in IoT networks [22].

Compared to ACLs where the object would check if the user has the correct criterion to be allowed access, in CapBAC that information lies within the user instead, who then presents their capability and credibility to the service provider [8].

Some advantages CapBAC has over other access control models are that it supports the principle of least authority, fine-grained access control, and does not need to manage the complexity of handling subject's identities [8]. This means that identity management is not a critical part of CapBAC, which in turn aids in cross-domain access control management.

2.14 Function-Based Access Control (FBAC)

Function-Based Access Control (FBAC) is an access control model which utilizes function-permission rather than a role or attribute assignment to determine what the user may or may not do with the object [5]. In other words, in FBAC objects such as files or images are data blocks and the policy determines if the user has permission to perform functions e.g. read, write, copy, or search. This makes FBAC an object-dependent approach.

The advantage of FBAC lies within the level of precision in the access control as it handles smaller data segments rather than entire objects [5]. This can be utilized in different manners e.g. the ability to search for topics in documents without being permitted reading access to the file or to aid in the user's work by also copying the source by modifying the copy/paste function. The level of modification of functions by FBAC can also be used for security purposes, for example, if a user would attach a file with sensitive information, then said information file can be hidden as it's attached to the email as part of the email function.

2.15 Policy-Based Access Control (PBAC)

Policy-Based Access Control (PBAC) uses several policy enforcement endpoints that work together to load user policies, making PBAC an extensible and flexible access control model [30]. In PBAC the process to get access to a file might look like this: a session request is sent and notified by the Policy Decision Point (PDP) which checks the policies assigned to the session, target, and user and then makes the decision regarding access to the file [30]. There might also be a Policy Enforcement Point (PEP) to act as a gatekeeper between the request and the PDP, as well as a Policy Information Point (PIP) that the PDP can gather policy information and data from [32].

In PBAC there are four main attributes: subject, resource, action, and context [32]. The subject is the information regarding the user, the resource contains information regarding the request, the action is what action the user requests to perform on the resource, and the context represents different environmental factors that may be relevant in the decision-making process. The attributes work together with the policies to determine access rights making it not quite as linear of a process as RBAC. However, it gives greater flexibility and the ability to have a multi-policy supporting system [30].

2.16 Topic-Based Access Control (TBAC)

Topic-Based Access Control (TBAC) is a fine-grained access control model that can be used as an extension to ABAC, it can be used to achieve paragraph-level access control [14]. TBAC includes two kinds of sub-access control models: file-driven TBAC (FD-TBAC) and purpose-driven TBAC (PD-TBAC). The main difference between the two access control models is that PD-TBAC is based on the purpose of the user and FD-TBAC is based on the topics of the file.

PD-TBAC functions by first looking at the user's access request (the purpose) and the access rights to determine which paragraphs may be viewed by the user by utilizing the request (subject-to-object) [14]. FD-TBAC operates similarly to PD-TBAC but in reverse as it starts with looking at the topics of the file and then it looks at all users and suggests different access rights to different users as a result of that process (object-to-subject). FD-TBAC uses a multi-level permission structure to grant users permissions on both file and paragraph levels. FD-TBAC can also work well as a complement to PD-TBAC, for instance, if the user is not able to explain the purpose relating to their role other than needing to see a specific file, in which case FD-TBAC would work better. This means that there are three options of how to use TBAC, namely PD-TBAC, FD-TBAC, and a combination of PD-TBAC and FD-TBAC.

3 Related Work

The research and development within the topic of access control models commonly center around four topics: the development of new access control models, the adaption of access control models to new areas of use, security analysis of access control models, and comparisons between different access control models.

A large part of the conducted research either focuses on the development of a new access control model based on earlier models, such as the previously mentioned PARBAC in Chapter 2 that is a combination of RBAC and ABAC. Long and Yan [13] developed a hybrid of RBAC and ABAC, called RBAC and ABAC Combining Access Control (RACAC). RACAC takes the advantages and disadvantages of both models into account and combines the two models into one. The authors performed a case study that showed that RACAC lowers the complexity and improves flexibility, as well as handles limitations from RBAC and ABAC.

Le et al. [12] present another example of an access control model development by introducing an enhanced RBAC model that includes constraints, entities, attributes, and more. The enhanced access control model further adapts the access control model to fit information management in team collaboration and workflows. The model was applied to a project which showed that it could be used for the intended purposes more effectively than traditional RBAC.

Additionally, Nazerian, Motameni, and Nematzadeh [16] also introduce a developed model called Emergency Role-Based Access Control (E-RBAC) which builds on RBAC and aims to improve flexibility in crisis situations. The authors present how access rights may need to be altered temporarily during an emergency, which traditional RBAC does not achieve as the model is more frigid. The study also includes an administrative model to manage a large E-RBAC system.

Other research conducted on the topic focuses on the security aspect of a chosen model and performs a security analysis, but often time this is done for one model at a time. For instance, Shahen, Niu, and Tripunitara [21] studied the safety of the ATRBAC model and addresses new challenges to security introduced by the development of the traditional RBAC model. The study also analyses the finding combined with prior studies within the same area and concludes that the safety tool used provides the same result as other tools available.

Vijayalakshmi and Jayalakshmi [29] have identified and analyzed anomalies and conflicts within policies in ABAC, which could lead to security vulnerabilities. The authors determine that previous research within the area fail to address five major policy errors, namely Rules-redundancy, Rules-Discrepancy, Rules-Inadequacy, Conflict-Decision-Positive-Negative, and Conflict-Demand.

Furthermore, current research also focuses on adapting access control models to different areas of use. Talegaon and Krishnan [24] analyzed recent works on using RBAC for Android systems and discovered that some key aspects of RBAC, such as sessions, are not being utilized. Therefore, the authors further studied the implementation of RBAC and propose several new models for RBAC in Android to cultivate all benefits of RBAC. The presented models address both flexibility and user permission management.

Similarly, Cui, Lan, and Bai [3] researched how a traditional RBAC model can be adapted to suit a smart home system. The authors develop a model, called ET-RBAC, that exhibits dynamic authorization and role assignment. Also, the study includes descriptions of how ET-RBAC can best be implemented for the use case.

Another aspect of the research conducted is the analysis and comparison between different existing models. Kunz et al. [11] analyze both role-based identity and access management based on 22 quality criteria and techniques used. Attribute-based approaches are also presented in the article giving a sense of role-based models vs other models. Some criteria presented in the article are: reducing the number of roles, decreasing role similarities, and increasing role coverage. The purpose and achieved goal of the criteria are to help improve the quality of role-mining techniques.

Aftab et al. [27] compare RBAC and ABAC using 10 parameters to present the different pros and cons of the models. Some examples of aspects of the comparison are: manageability, flexibility, and easiness. These are used to come up with the conclusion that RBAC is the more trustworthy access control model but ABAC is more flexible and dynamic to its' environment than RBAC.

Further, Aftab et al. [26] presented a survey of both traditional and hybrid access control models to provide more substantial documentation about the models, discuss limitations, and highlight advantages. The main conclusions include that limitations to traditional models mean that hybrid models are more efficient, flexible, scalable, and secure, and can be used in different types of organizations.

Additionally, Parkinson and Khan [17] perform a security-focused systematic literature review aimed at the real-world analyses and challenges of access control models. In the article, Parkinson and Khan primarily focuses on RBAC, ABAC, and DAC, and reviews how these models are evaluated and whether the analyses are related to real-world tasks and challenges.

This differentiates from this thesis in the sense that it aims to provide an aid for organizations both objectively and scenario-specific to choose the access control models best fitted according to their needs and priorities. Compared to this thesis, much of the related work centers around the development of new access control models or security analysis of access control models. This type of research acts as the basis for the literature study part of the thesis. Moreover, the research that focuses on adaptation to new areas of use is mainly looked at as background to the topic. Also, the research containing comparisons between different access control models is used as both bases for the literature study and the model evaluation.

Lastly, the study by Aftab et al. [26], which to some extent has a similar aim to our thesis, acts both as the basis for different models as well as insight for the evaluation. The main difference is that the results of this thesis aim to be adaptable for organizations.

4 Evaluation Roadmap

In this chapter, the methodology of the study is presented in three parts: the literature study, the model evaluation parameters, and the scenario-based evaluation. The literature study is described as well as the categorization, the model evaluation presents the parameters used to analyze the access control models, and the scenario-based evaluation describes the detailed scenarios.

4.1 Literature study

The first step of the process was to identify and select appropriate access control models. This was done through a literature study, starting with RBAC and ABAC and branching out to find access control models suitable for the case presented in this thesis. Aspects of access control models that would deem them unsuitable and thus will not be included in the literature review includes: device-to-device focus, relationship-based access control models, and unfitting conditions e.g. emergencies. To achieve a more diverse mixture of access control models both recent and more historical models were chosen. Another important factor that was examined was whether the access control model could be suitable for a development-focused organization on account of mainly flexibility and security.

4.1.1 Model categorization

The second step of the process was to sort the access control models into categories in a matter that made the models more logical to compare and evaluate. The most intuitive way to do this was to create two main categories: role-based models and other models, see Table 4.1.

Table 4.1: Categorization of access control models

Category	**Access control models**
RBAC models	RBAC, TRBAC, ATRBAC, GTRBAC, PARBAC, DRBAC, RRBAC
Other models	ABAC, CapBAC, FBAC, PBAC, TBAC

4.2 Model evaluation parameters

The third step of the method was to evaluate the different access control models. For the evaluation, different parameters of importance for organizations needed to be defined. To find parameters of significance for the evaluation research was conducted combined with consultations with experts. These parameters are described in Table 4.2.

Table 4.2: Descriptions of parameters for Model Evaluation.

	Parameter	**Description**
Attribute Definition	Minimize Redundancy	Minimize redundancy is the notion that there should be a clear distinction between different roles or attributes so that there is no overlap that can cause confusion, bugs or security breaches. Further, by minimizing the redundancy the structure of roles becomes clearer.
	Attributes	Attributes, as seen in Section 2.12, are factors that represent who the user is and what actions the user is allowed to perform. These factors can take shape as e.g. roles or environmental factors such as location or department.
Economy	Cost of Implementation	Cost can partly be the financial impact, but the more important aspects of costs for this analysis is the impact of time of implementation, the complexity of the model, psychological impact and amount of research, see Table 4.3 for a detailed description.
	Similarity	The similarity of the already implemented model and the other models is another important factor as it impacts the ability of an enterprise to change the access control model used.
Control Authorities	Workload	The workload on the administrative-like roles in the company, which also encompasses to some extent the simplicity level of the access control model both if the system is relatively easy to work in and with. This aspect focuses on the amount of work needed to be executed by administrators and the difficulty.
	Flexibility	Flexibility represents the amount of freedom for the organization available under the policy, as well as how adaptable the access control model is. This is important as the access control model needs to adjust to each specific organization.
Organization	Recertification	Recertification manages the events where a user retrieves a new role or loses an old role. The important aspect to focus on is how easily the access granted to a user can be changed and how straightforward the process to apply for updated access rights is.
	Reorganization	Reorganization captures how the access control models work under a reorganization, meaning when an organization is changing its structure. It addresses the difficulty of maintaining access control during changes in an organization.
Security	Least Privilege	As described in Section 2.2, least privilege allows users to operate using the lowest privilege needed for the specific task. It is an important factor in access control models to prevent safety breaches, as it prevents possible intruders and users from making unintended errors.
	Separation of Duty	As described in Section 2.3, a user should not be permitted to be able to misuse the system as it can become a security risk whether it be on purpose or not.
	Granular Permission	Granular Permission includes the possibility to grant and use limited permission so that not all employees are given access to all resources. It also supports the ability to target permission using precision permission.

As described in Table 4.2, the parameter cost of implementation depends on four different factors; time of implementation, the complexity of the model, psychological impact, and amount of research. These factors are further described in detail in Table 4.3.

Table 4.3: Descriptions of sub-parameters for Cost of Implementation.

	Sub-parameter	Description
Cost of Implementation	Time of Implementation	Time of implementation is intended to show how demanding the process to change access control model will be in terms of time needed. This is tied to how similar the model is compared to the currently used model.
	Complexity of the Model	The complexity of the model is studied to highlight the amount of knowledge needed to implement the model. Models that are similar to the currently used model will score higher since the enterprise is familiar with it.
	Psychological Impact	Psychological impact includes the impact on personnel by getting introduced to a new system, new accesses, and a new way of working. Usually, personnel is more comfortable with the system that is more similar to the current setup. This aspect is important to study as the attitude and adjustment of employees can be critical to the changes.
	Amount of Research	As there are a lot of different access control models to study, the amount of research that can be found regarding a model can drastically impact the cost of the implementation as well as the number of services and help that are available.

With these parameters in mind, the selected access control models were further researched and graded according to the literature on a scale of 1-4, 1 being the worst and 4 the best. The scale of 1-4 was chosen to give a wide enough spectrum, while at the same time not being too broad so that the literature provides enough information for a grade to be set. The results from the calculations are then presented in tables, which also show averages calculated to give a sense of the overall grade for each model. The averages for the main categories, as well as the average for cost of implementation are rounded to the nearest integer to maintain the clarity of the tables.

The last part of the model evaluation included a compatibility analysis, which centered around RBAC and ABAC. Compatibility with other access control models is important for making a hybrid that would perform even better within the organization. The results were entered into a table showing the compatibility for RBAC and ABAC.

4.3 Scenario-based evaluation

The fourth step of the method was to create scenarios in which the parameters were analyzed. This was done by weighing the parameters mentioned above, to suit the needs or priorities of each scenario, by giving each main parameter a weight from 1-3 with 1 representing a less important parameter for the scenario and 3 representing a very important parameter for the scenario. After weighing the parameters, a weighted average was calculated for all models in the different scenarios. The calculations of the weighted average include multiplying the grades of the parameters with the weight, before establishing the new average.

There are three scenarios used in this report representing differently-sized organizations: small organizations, large organizations, and growing organizations. The scenarios were determined to represent different stages of an organization and are possible to relay to parts of an organization as needed. The different scenarios produced more tailored results through the weighted parameters that can be used to create recommendations of suggested access control models for the different scenarios.

5 Literature-based Model Evaluation

In this chapter, the result of the analysis of the selected access control models is presented, using the roadmap developed in Chapter 4. The parameters used in the analysis are described in Section 4.2. The results are largely presented in tables to highlight similarities and differences between the different models. The results in the tables are based on the literature study conducted and presented above, see Chapters 2 and 3.

To fully understand the analysis it is important to note the basis that is assumed, which is described in Section 1.3, namely that the current access control model used by the company is RBAC.

5.1 Cost of Implementation

The cost of implementation represents the effort in different aspects that it will take to implement the access control models. The aspects deemed of most importance in this situation, as described in Table 4.3, are; time of implementation, complexity of the model, psychological impact, and amount of research, see Table 5.1.

Table 5.1: Comparison of Cost of Implementation

	RBAC-based							**Other**				
	RBAC	**TRBAC**	**ATRBAC**	**GTRBAC**	**PARBAC**	**DRBAC**	**RRBAC**	**ABAC**	**CapBAC**	**FBAC**	**PBAC**	**TBAC**
Time of Implementation	4	3	3	3	2	2	3	2	2	3	2	1
Complexity of the Model	4	4	3	3	2	2	2	3	1	3	3	2
Psychological Impact	4	3	3	3	3	2	4	4	2	2	4	3
Amount of Research	4	3	2	2	2	1	1	4	3	1	2	1
Average Score (to nearest integer)	4	3	3	3	2	2	3	3	2	2	3	2

As described earlier, the assumption used as a basis for this analysis is a company that is using RBAC as its access control model. This means that, as seen in Table 5.1, there is no time to take into account regarding change of access control model and no substantial psychological impact, and therefore RBAC scores high for those aspects. In regards to complexity and research, these aspects also scored high due to the model being present for many years which can be of help during the implementation and use of the model.

For the remaining models, with regards to time of implementation, TBAC is the worst graded because RBAC and TBAC are largely different models. Further, the similarity to RBAC is visible for TRBAC, ATRBAC, GTRBAC, and RRBAC, which score close to the grade of RBAC. However, PARBAC and DRBAC do not follow this pattern, even though these models are also RBAC-based. As for the other models, apart from FBAC, larger differences can be seen compared to RBAC, which means they are graded lower.

Regarding the complexity of the model, CapBAC is the most complex model analyzed and TRBAC is the least complex model since it is similar to RBAC. Further, the other models are less complex which results in better grades for the parameter complexity of the model.

Moreover, for psychological impact a high grade, such as RRBAC, ABAC, and PBAC, means that the models are easy for personnel to operate and that the changes to daily work are relatively small compared to the current model RBAC. In general, the largest impact of access control models is usually more noticeable for administrators, hence no models score very low in this regard. Interestingly, DRBAC scores low for psychological impact, even though it uses machine learning which should imply easier handling by personnel. The main reason behind this is that due to the improved automation, DRBAC differs largely from RBAC and can hence significantly impact the personnel.

The grades for amount of research differ a lot for the different models. Some models, such as RBAC and ABAC, are largely researched over the last two decades and have been developed over time. For other models, like DRBAC, RRBAC, FBAC, and TBAC, research is far more sparse. For both DRBAC and RRBAC it is challenging to find the amount of research available as both abbreviations exist for several different models. However, for both DRBAC and RRBAC, there is quite sparse research.

Lastly, the average score rounded to the nearest integer is calculated for each of the models. The average score shows how the access control models are graded in terms of cost of implementation, meaning how expensive the different models are. This average score is used later in the overall grade of the models, see Section 5.2.

5.2 Overall Model Evaluation

The overall model evaluation represents the average score of each of the access control models analyzed. The average score contains decimals to distinguish the results and is based on five main categories, namely; attribute definition, economy, control authorities, organization, and security, see Table 5.2.

Table 5.2: Overall Model Evaluation of Access Control Models

	RBAC-based							**Other**				
	RBAC	**TRBAC**	**ATRBAC**	**GTRBAC**	**PARBAC**	**DRBAC**	**RRBAC**	**ABAC**	**CapBAC**	**FBAC**	**PBAC**	**TBAC**
Attribute Definition	2	2	2	2	2	2	3	4	3	2	2	3
Minimize Redundancy	1	2	2	2	1	1	4	3	3	1	1	2
Attributes	2	2	2	2	3	2	2	4	3	2	2	3
Economy	4	3	3	3	2	2	2	2	2	2	3	2
Cost of Implementation	4	3	3	3	2	2	3	3	2	2	3	2
Similarity	4	3	3	3	2	2	1	1	2	1	2	2
Control Authorities	2	2	3	3	3	4	3	3	2	2	3	3
Workload	1	1	3	2	1	4	3	3	1	2	3	2
Flexibility	3	3	3	3	4	3	2	3	3	2	3	3
Organization	3	3	3	4	3	3	2	4	3	2	3	3
Recertification	2	3	3	3	3	3	2	4	3	2	3	3
Reorganization	3	3	3	4	3	3	2	3	3	2	3	3
Security	3	3	3	3	3	3	3	3	4	3	3	4
Least Privilege	4	4	4	4	4	4	4	3	4	4	4	4
Separation of Duty	3	3	3	3	3	3	3	4	4	1	3	3
Granular Permission	2	2	2	2	3	2	3	3	3	4	2	4
Average Score	2.80	2.60	2.80	3.00	2.60	2.80	2.60	3.20	2.80	2.20	2.80	3.00

As seen in Table 5.2, attribute definition is an average of minimize redundancy and attributes, where only RRBAC achieve the highest grade for minimize redundancy, while five different models score the lowest. Further, for attributes, no model scores a 1, but the majority of models score a 2. Also, only ABAC is graded a four on the scale regarding attributes due to a clear distinction of who the user is and what actions the user can perform.

Continuing, economy is an average of both cost of implementation, which is further presented in Table 5.1, and similarity. RBAC scores high in both aspects since the basis for the analysis is an enterprise using RBAC, which then implicates a low general cost of implementation, as well as high similarity to the currently used model. Moreover, regarding the similarity, the models scored according to how different the models are from RBAC. This means that RRBAC, ABAC, and FBAC are the models that differ the most from RBAC and therefore the similarity for these models score low. It is interesting that some of the models that are based on RBAC score lower for similarity. For PARBAC and DRBAC, which score a 2, the reason is that the line of thought is quite different from RBAC while introducing priorities and machine learning respectively. Also, for RRBAC, which scores a 1, the reason is the introduction of tree-based permissions and hierarchies which are not present for RBAC. For similarity, it is also interesting that three of the models that are not based on RBAC, namely CapBAC, PBAC, and TBAC, score higher than RRBAC. This is due to similar control of access, even though the process of granting access to users differs slightly.

Control authorities is an average of workload and flexibility. For workload, the different models are graded very varyingly, where RBAC, TRBAC, PARBAC, and CapBAC are deemed to have a heavy workload on administrators. On the contrary, DRBAC scored the highest with a lower workload for administrators since it uses machine learning and can learn the system. As for flexibility, no models score a 1 on the scale, which means that they all handle flexibility to some extent. Also, PARBAC is graded highest and deemed most adaptable.

Further, organization is an average of recertification and reorganization, where no models are graded as 1 on the scale. ABAC scored the highest for recertification and GTRBAC scored the highest for reorganization. RBAC, RRBAC, and FBAC, however, scored lowest for recertification and RRBAC and FBAC scored lowest for reorganization. This means that RRBAC and

FBAC receive the lowest average and is therefore the model that adapts the worst according to changes both of the user and of the organization.

Security is the average of least privilege, separation of duty, and granular permission. All models are graded high for least privilege, except for ABAC which is graded slightly lower. For separation of duty, the majority of models scored a 3 on the scale, but ABAC and CapBAC scored the highest and FBAC scored the lowest. Lastly, for granular permission, no model was graded a 1, although FBAC and TBAC are graded the highest.

The total average score is calculated using the above presented main categories, but not rounded to show the result in higher detail. The average score shows that many of the models score alike, apart from FBAC which clearly scores lower, and ABAC which scores the highest.

5.3 Compatibility

The compatibility of access control models displays which models are noted to be able to be utilized together or as an extension of each other. In past research, combinations of access control models have been used to improve and develop both new and hybrid models, as described in Chapter 3. Therefore, in Table 5.3, the compatibility between the access control models is presented. More precisely, the compatibility between the 12 access control models and RBAC and ABAC are compared. RBAC and ABAC were chosen as parameters based on the literature study in Section 2, which also is described as a delimitation in Section 1.3. This, however, does not imply that other models are not compatible.

Table 5.3: Compatibility comparison of access control models

	RBAC-based							**Other**				
	RBAC	**TRBAC**	**ATRBAC**	**GTRBAC**	**PARBAC**	**DRBAC**	**RRBAC**	**ABAC**	**CapBAC**	**FBAC**	**PBAC**	**TBAC**
RBAC	I	◐	◐	◐	◐	◐	◐	●	●	○	▨	○
ABAC	●	○	○	○	◐	○	○	I	○	○	◐	●

●= Compatible, ◐= Based on, ○= No information,
▨= Compatible under circumstances, I = Itself

From the comparison in Table 5.3 it can be deducted, that the models in the RBAC-based category are based on RBAC. Interestingly it also indicates that PBAC is compatible with RBAC due to the similarities in the basic structure of the models. Both ABAC and CapBAC are compatible with RBAC. Further, ABAC shows compatibility with TBAC, which can function as an extension of ABAC. It also shows that PARBAC and PBAC are based on ABAC as established previously. Also, there are multiple models for which there is no information about compatibility. But as mentioned above this does not imply that the models are not compatible.

6 Organization-based Evaluation

In this chapter the organizational scenarios: small organization, large organization, and growing organization are presented. The most important parameters are then evaluated for each scenario which is displayed in the form of weights. Lastly, for each scenario, a new average score for each access control model based on the weights is presented, as well as how many points the access control models increased or decreased.

6.1 Scenario identification

To be able to construct the different scenarios described below, experts within the area were leveraged using interviews. The main purpose of the interviews was to gather as much expertise as possible from people working in the area, both regarding different organizations as well as about important aspects to focus on in the evaluation. The interviews had a qualitative focus, rather than quantitative, as the aim was to better understand the topic from the expert and to collect information.

6.2 Organization descriptions

Organizations at large contain several components with different tasks and purposes and can be of different sizes, in this case, either small or large. Other organizations are in the process of a transition stage going from small to large. These different kinds of organizations are described more in detail below.

6.2.1 Small organization

A small organization in this case is defined as one that is ranging in the hundreds of employees. The small organization frequently works with other organizations to collaborate or provide support. As a result of their work, the employees usually have a basic level of access as well as some additional access to aid in the work as a single employee might handle several different tasks.

Small organizations can experience difficulties to define roles that last over time as employees change and the assignment of the roles changes. Therefore, employees are granted more access rights than necessary to not hinder their work. The role assignment of the system entails manual work, which shows the need for automation. Further, for small organizations, the simplicity of the system and the stress of the change are of high importance to keep the cost down.

6.2.2 Large organization

A large organization is defined as a larger business ranging in the thousands of employees or more. The large organization mainly collaborates with other large organizations with the purpose to deliver a joint finished product. This also means that employees of large organizations can only read resources from other organizations and vice versa. Further, the access of employees in large organizations often focuses on positions and roles.

For large organizations, the biggest problem is manual work tied to granting and removing access within the system, which entails a large amount of work in day-to-day operations, showing a need for automation. Further regarding administration, the simplicity of the access management system is important to maintain efficiency. Due to the large size of the organization and the read-rights to and from other large organizations, the roles, and access rights are important to minimize and monitor.

6.2.3 Growing organization

A growing organization is a small organization that is becoming more important and has the prospect of a larger market share, hence the organization is expected to grow into a large organization. A growing organization might experience growing pains e.g. how the organization operates might have to change as more people are involved and as the organization's priorities change.

Further, as the organization grows it is important to focus on having efficient roles and role-assignment, as well as focus on the security aspect regarding accesses tied to roles. Most importantly, a growing organization needs to be flexible and be able to address and handle the changes presented by the growth.

The growing organization differs from a small and large organization mainly regarding the importance of adaptability during organizational change. This is also impacted by how well the access control model handles changes in existing accesses of users in the system. Further, another difference is that management of resources is of even higher importance to keep the profitability of the business during the growing process.

6.3 Scenarios

In this section, the parameter weights as well as the new results will be presented, which can be used by different kinds of organizations to find a model that fits them. The new results will be presented in the form of tables including the new weighted score and the difference from the previous unweighted score. Both factors can be used as indicators to show whether or not the access control model is suitable for the scenario.

6.3.1 Small organization

From the small organization described above, the key parameters identified are economy, control authorities, and organization. The most important is economy, as the small organization might not have the same amount of resources as a larger organization thus making it a more precious parameter to consider. Further, control authorities are an important factor as the administration is a key problem with the potential to improve using automation. Lastly, organization is an important factor in any such organization as if done poorly, can become a viable security risk.

This results in the parameter weights ranging from 1 to 3 as seen in Table 6.1, with 1 being the less important factor to 3 being the most important factor.

Table 6.1: Parameter weights for small organizations

Parameter	Weight
Attribute definition	1
Economy	3
Control authorities	2
Organization	2
Security	1

The table reflects the most important parameters for a small organization, with economy being given the highest grade of importance and control authorities as well as organization being marked as important parameters. The weights are then used in Table 5.2 to provide the new weighted results as seen in Table 6.2.

Table 6.2: Weighted comparison for small organizations

	RBAC-based							Other				
	RBAC	TRBAC	ATRBAC	GTRBAC	PARBAC	DRBAC	RRBAC	ABAC	CapBAC	FBAC	PBAC	TBAC
Weighted average score	3.00	2.67	2.89	3.11	2.56	2.78	2.44	3.00	2.56	2.11	2.89	2.78
Diff from overall	0.20	0.07	0.09	0.11	-0.04	-0.02	-0.16	-0.20	-0.24	-0.09	0.09	-0.22

From the new weighted average, it is shown that the best scoring option at a score of 3.11 is GTRBAC which went up 0.11 points. The lowest scoring and thus less fitting model for a small organization is FBAC which scored 2.11 which is a third of a point behind the second lowest scorer RRBAC. The highest increase is at +0.20 points by RBAC and the biggest decrease is at -0.24 by CapBAC.

6.3.2 Large organization

As a result of the large organization described above, the most significant parameters are control authorities and security. Control authorities are of high importance as a large organization has more employees and thus an ill-suited system can increase the workload thus the flexibility to the organization becomes more important as well, which can create a bottleneck effect. Because of this, it is placed as a higher priority than in a smaller organization. Security becomes a high priority parameter as well as there can be more to protect with more people possibly taking part in the information. Another aspect of importance is attribute definition as it impacts the constraint of different roles. The organization parameter, in a similar matter to the security parameter, as there are more employees in the system and more people that would be affected by a reorganization. However, although being weighted the same as for small organizations it is for a different reason, namely, that is more focused on recertification and to some degree reorganization within the organization rather than the reorganization tied to possible future growth. These factors result in Table 6.3.

Table 6.3: Parameter weights for large organizations

Parameter	Weight
Attribute definition	2
Economy	1
Control authorities	3
Organization	2
Security	3

The table shows the results from the scenario in form of weights where control authorities and security got 3s or placed as high-importance parameters and attribute definition and organization got 2s or placed as parameters with importance. The weights are used to present a new average score better suited to large organizations, shown in Table 6.4.

Table 6.4: Weighted comparison for large organizations

	RBAC-based							Other				
	RBAC	TRBAC	ATRBAC	GTRBAC	PARBAC	DRBAC	RRBAC	ABAC	CapBAC	FBAC	PBAC	TBAC
Weighted average score	2.64	2.55	2.82	3.00	2.73	3.00	2.73	3.27	2.91	2.27	2.82	3.18
Diff from overall	-0.16	-0.05	0.02	0.00	0.13	0.20	0.13	0.07	0.11	0.07	0.02	0.18

The weighted comparison table shows that ABAC got the highest score at 3.27 thus representing the most suitable option and FBAC got the lowest score at 2.27 thus representing the least suitable option. The biggest increase post-weighing is DRBAC at +0.20 points and the largest decrease is RBAC at -0.16.

6.3.3 Growing organization

For the growing organization as described in the results above the two parameters of highest importance are control authorities and organization, as the organization is gaining more and more employees. Thus the workload could increase depending on the access control model and the flexibility of the access control model becomes more important as the organization is changing and the organization is going through a form of reorganization as it grows. Another important parameter is attribute definition as there are a larger amount of roles to fit into the organization's structure. Further, security is an important parameter when the organization is growing, as more employees are coming in thus there are a larger amount of people that can take part in information.

This results in the following weights seen in Table 6.5.

Table 6.5: Parameter weights for growing organizations

Parameter	Weight
Attribute definition	2
Economy	1
Control authorities	3
Organization	3
Security	2

As reflected from the scenario the table shows that control authorities and organization got 3s, being of the highest importance for the growing organization. Attribute definition and security got 2s reflecting their importance for a growing organization. The weights are then used in Table 5.2 to get a new average for the growing organization, which can be seen in Table 6.6.

Table 6.6: Weighted comparison for growing organizations

	RBAC-based							Other				
	RBAC	TRBAC	ATRBAC	GTRBAC	PARBAC	DRBAC	RRBAC	ABAC	CapBAC	FBAC	PBAC	TBAC
Weighted average score	2.64	2.55	2.82	3.09	2.73	3.00	2.64	3.36	2.82	2.18	2.82	3.09
Diff from overall	-0.16	-0.05	0.02	0.09	0.13	0.20	0.04	0.16	0.02	-0.02	0.02	0.09

The table shows that the best suited access control model for a growing organization is ABAC at a score of 3.36 and the least suitable access control model is FBAC at a score of 2.18. The biggest increase is done by DRBAC at +0.20 points and the largest decrease is done by RBAC at -0.16 points.

7 Discussion

In this chapter, the results are discussed and recommendations for each scenario are presented. This chapter also presents a method discussion where the methods used in the report are examined and discussed. Lastly, the societal and ethical aspects are discussed.

7.1 Results

The access control models are evaluated based on the five main categories displayed in Table 4.2. These parameters are attribute definition, economy, control authorities, organization, and security, whose scores are presented for each access control model in Table 5.2 as well as an average score. The scores of the parameters are displayed for each model in Figure 7.1. The main purpose of the figure is to display the strengths and weaknesses of the 12 access control models. This can then aid in strengthening access control models by balancing out the models with another model that performs better where the chosen model is weaker.

In Figure 7.1, it is shown that some of the access control models are more well-rounded than others. Among other examples, FBAC and GTRBAC are good examples of this as FBAC scores relatively low and thus is not as well rounded as GTRBAC which scores close to maximum. It is also prevalent from the figure that GTRBAC might be generally well-rounded but does not score well in attribute definition, it could in theory then be combined with a model which performs better at that.

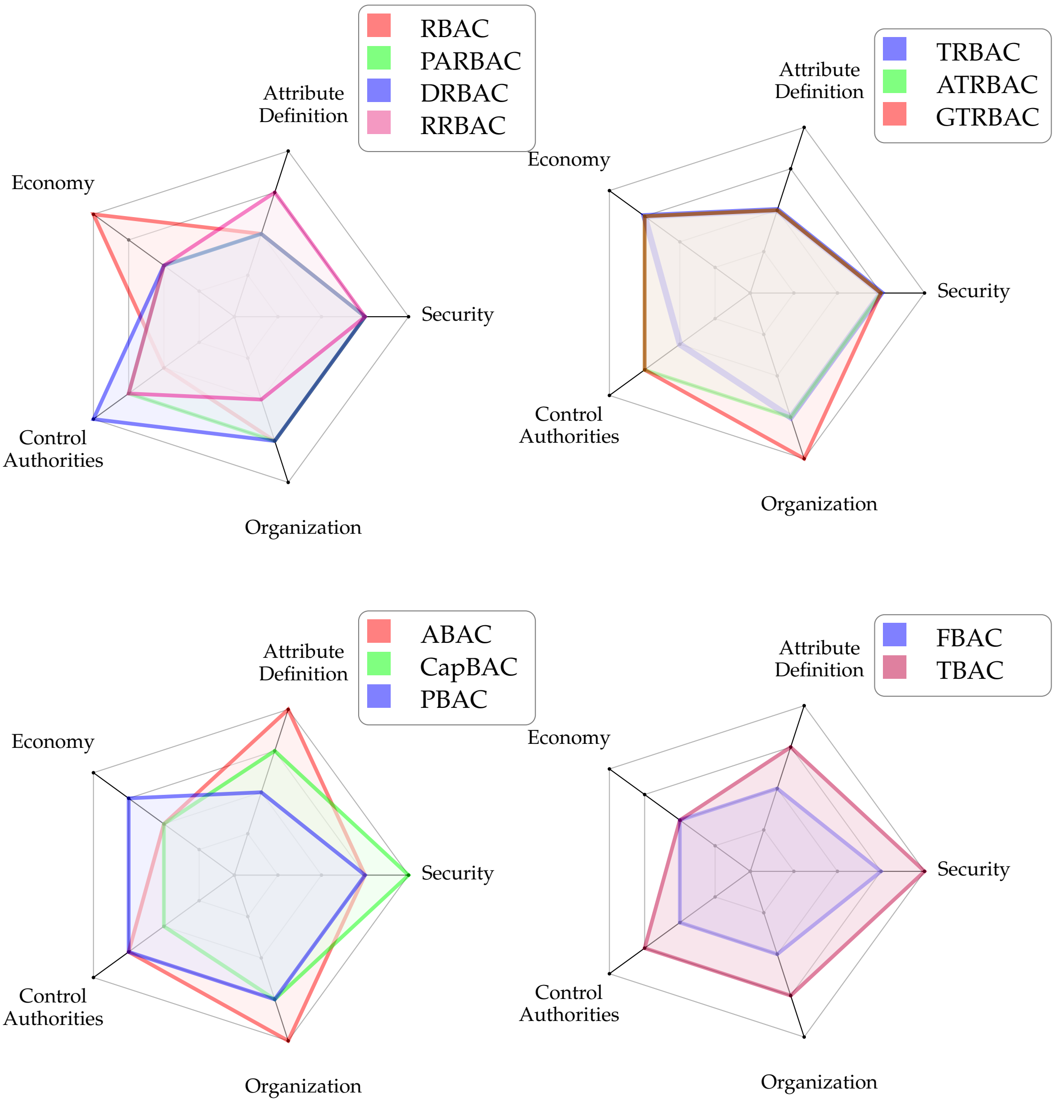

Figure 7.1: Spider charts presenting the results from Table 5.2

From the spider charts in Figure 7.1 clear structural similarities between access control models can be seen. These similarities results in clusters of models with similar structure, see Figure 7.2. In general, the models combined in clusters score similarly for the different parameters, although some distinctions do appear which results in different unweighted averages. Important to note is that this does not mean that the models in the clusters are equivalent, therefore details about the models still need to be examined.

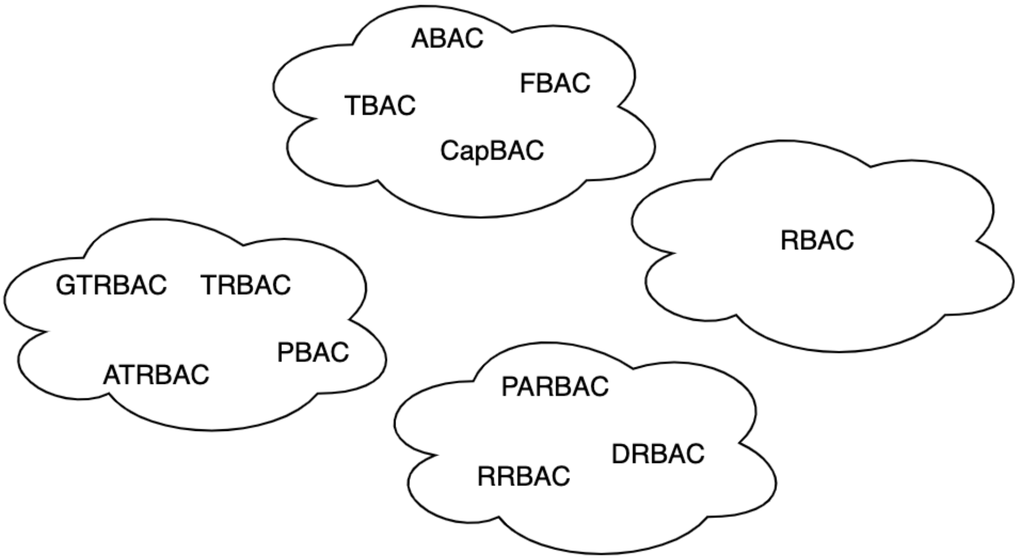

Figure 7.2: Structural similarity between the access control models

Based on Figure 7.2, the spider charts in Figure 7.1 can be modified into new spider charts with one diagram for each cluster, see Figure 7.3. The main aim of the modification of the spider charts is to show the similarities within the clusters at the same time as highlighting minor differences that can be of importance to discuss.

The first cluster in Figure 7.3 includes ABAC, TBAC, CapBAC, and FBAC, all of which belong in the other models' category, as described in Section 4.1.1. All these models score according to the same pattern, where they score lower for economy, control authorities, and organization, compared to higher scores for attribute definition and security. However, ABAC differs from these patterns in regard to attribute definition and organization. Further, it can be seen that although FBAC follows the same pattern, it scores distinctly lower compared to the other models in the cluster. This cluster could be considered in a scenario where the security of the system is priorities as well as if the attribute definition is important for roles.

The second cluster, see Figure 7.3, includes TRBAC, GTRBAC, ATRBAC, and PBAC, where TRBAC, GTRBAC, and ATRBAC belong to the RBAC-based category and PBAC belongs to the other models' category. Generally, these models score well for economy, control authorities, organization, and security, whilst the scores for attribute definition are low. PBAC and ATRBAC score exactly identically, which is interesting as the two models do not belong to the same category. Further, TRBAC scores lower due to control authorities, and GTRBAC scores higher due to organization. Scenarios, where this cluster could be considered, are when the ability to handle changes to the organization is important combined with a relatively low strain in regard to economy.

In Figure 7.3, the third cluster includes PARBAC, RRBAC, and DRBAC, which all belong to the RBAC-based category. These models do in general score well for control authorities, organization, security, and attribute definition, they all also score low for economy. It is worth noting that RRBAC scores higher in attribute definition but lower for organizations and DRBAC scores higher for control authorities. To some extent, it could be argued that PARBAC is a middle ground between RRBAC and DRBAC. If simplicity for control authorities is of the highest priority then this cluster could be considered.

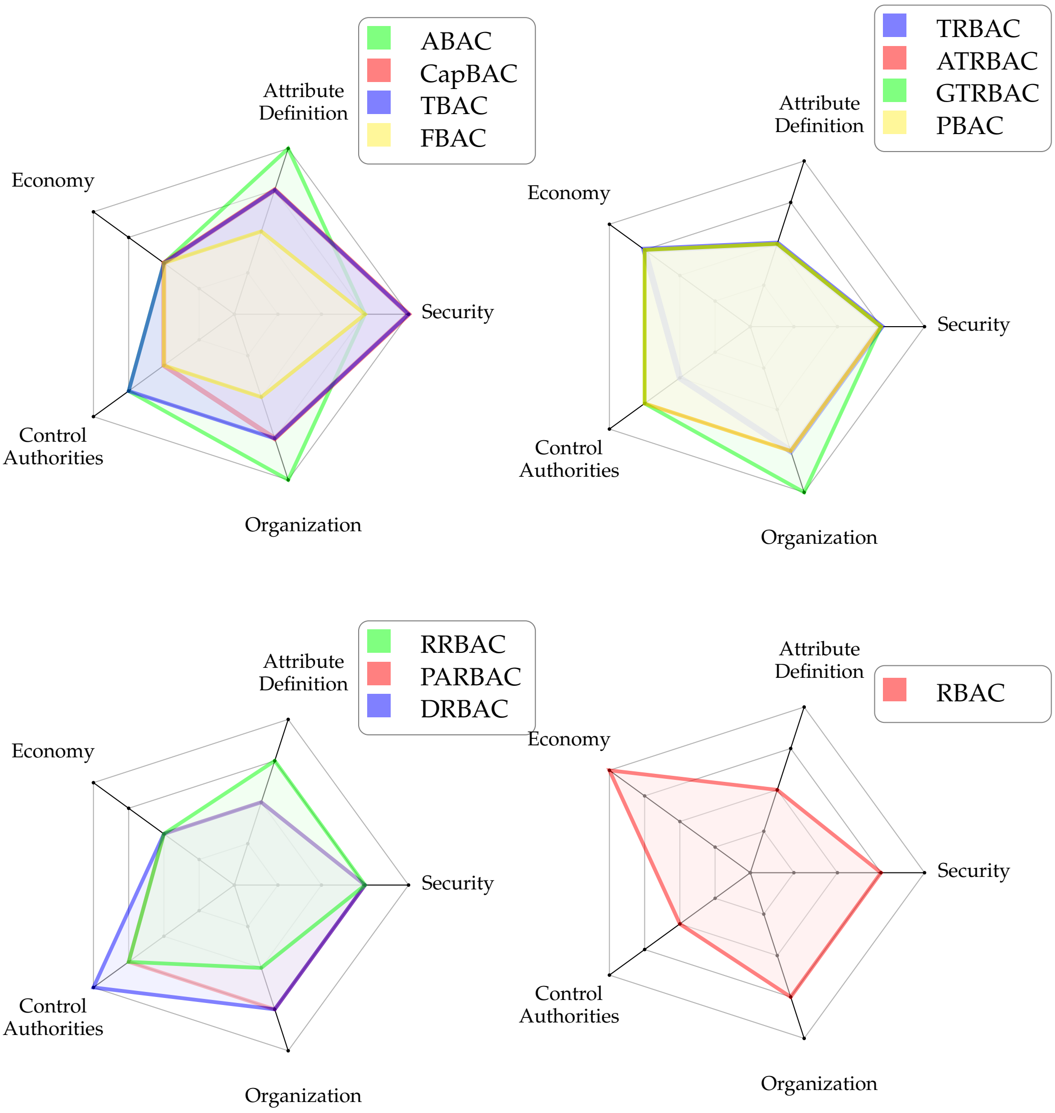

Figure 7.3: Spider charts presenting the clusters in Figure 7.2

Lastly, in Figure 7.3, the fourth cluster only includes RBAC, which is the model that is assumed as the basis for this thesis. There are multiple reasons for leaving RBAC in a separate cluster, mainly that RBAC differs from the other models' scores and that RBAC is the basis for the evaluation. This is interesting as RBAC is the foundation of all models in the RBAC-based category but still does not fit into any other cluster. RBAC scores low in general for all parameters, except for economy where it has an outstanding score as a result of it being the basis of the evaluation. RBAC could be considered in a lot of different scenarios, but mainly when economy is the most important parameter as the choice of RBAC as an access control model would mean that no change needs to be executed and therefore economy would not be impacted.

Overall, the clusters help to show which models are similar and therefore might be valuable to consider when choosing the suitable access control model for a specific scenario. If the results from the scenario shown, e.g. ABAC, then the organization should also consider the models in the same cluster because, depending on the priorities of the organization, any of those models might be the best fitted.

Another interesting aspect that the clusters introduce is the visualization of models that could be combined. The best combination would be of models that belong to different clusters as they will complement each other the most. Although, it is important to remember that not all models in a cluster score identically, hence different combinations might also be of value.

7.2 Weighted results

A summary of the weighted averages for the different scenarios from Chapter 6 is presented in Table 7.1, alongside the result from Chapter 5. The results are presented in an average, where in each row the best score is marked in green and the worst score is marked in red.

Table 7.1: Results of comparisons of access control models

	RBAC							Other				
	RBAC	**TRBAC**	**ATRBAC**	**GTRBAC**	**PARBAC**	**DRBAC**	**RRBAC**	**ABAC**	**CapBAC**	**FBAC**	**PBAC**	**TBAC**
Overall average	2.80	2.60	2.80	3.00	2.60	2.80	2.60	3.20	2.80	2.20	2.80	3.00
Small organizations	3.00	2.67	2.89	3.11	2.56	2.78	2.44	3.00	2.56	2.11	2.89	2.78
Large organizations	2.64	2.55	2.82	3.00	2.73	3.00	2.73	3.27	2.91	2.27	2.82	3.18
Growing organizations	2.64	2.55	2.82	3.09	2.73	3.00	2.64	3.36	2.82	2.18	2.82	3.09

From Table 7.1 some general remarks will be discussed before each scenario and in more detail. The weighted results will be compared to the unweighted results to show the impacts of the weights as well as if the scenarios impact the recommendations for the different organizations.

7.2.1 General remarks

From the theory, ABAC can be argued as an improvement of RBAC, which could mean that ABAC would be a better choice than RBAC for all organizations that use RBAC today. This also aligns with the results for all cases seen in Table 7.1, with the exception of small organizations for which RBAC and ABAC scores alike. This would mean that if the organization can afford the change of model and is prepared for a more complex model, then ABAC would be the clear choice over RBAC.

As described above, RBAC is assumed as the access control model used by the organization as a start. Therefore, this mainly impacts the economy parameter, and for the cases where economy is weighted, this impacts the results drastically. Important to note is that all other parameters can be chosen to achieve the best score possible when combining multiple access control models. For economy, on the other hand, the lowest number needs to be kept in mind as the factor overall is meant to show the impact of change. It might also be argued that economy shows a score even lower than the lowest score of the models that are being combined. However, it is surprising that even though RBAC score highly for economy, overall for the different scenario, RBAC do not score as high as expected despite it being the presumably most widely used model. This means that RBAC has simplicity as well as a lot of research which leads to widespread use, even though other models in practice are better for all organizations. The use of RBAC is therefore most likely tied to the wide adaptation possibilities to receive a model that works well enough and does not need to be customized to the organization.

Another interesting remark is that throughout the results, both unweighted and weighted, FBAC scores the lowest by far. FBAC struggles to fulfill decent scores for all categories but security, within which it scores higher due to the support of least privilege and the ability to use granular permission. However, FBAC still scores low for separation of duty. Therefore, the functional approach, rather than roles or attributes might not be adapted to these types of organizations, even though the clear focus on security and restricted access might be something a lot of organizations desire. If an organization would want to implement the functional approach of FBAC in regard to the security of objects, the best approach would be to use it in combination together with another model.

7.2.2 Small organizations

For small organizations, the impression given solely by the literature study of the models is that TRBAC or one of its expansions, namely ATRBAC or GTRBAC, would be the best fit because of the temporal aspect and the ability to handle expiration of accesses easier. The temporal aspect would help small organizations in the sense that accesses can be assigned using time intervals which both helps the assignment of accesses as well as the administrators. This, as described earlier, is important for small organizations as a lot of users have several different roles with different permissions to maintain at once, which also applies to administrators.

As seen in the results in Table 7.1, GTRBAC is the best suited model for small organizations according to the weighting, which is in line with the theory. This might be because, as described in Section 6.3, for small organizations economy, control authorities and organization are important parameters for model selections. GTRBAC has the advantage of the temporal aspect, as mentioned above which eases both the administrative factor of control authorities and the possibility to handle changes for the organization. Further, as GTRBAC is based on traditional RBAC, the economical aspect can be seen as fairly well.

Interestingly though, RBAC and ABAC scored a shared second place, even though they are drastically different models. The score of ABAC decreased by 0.20 points compared to the unweighted results, which can be explained as a result of the high weight for economy while ABAC unweighted scores only 2 for that same parameter mainly due to the large difference of implementation compared to RBAC. Although, since ABAC scored a shared second place, it can be assumed that ABAC would also be a good fit for a small organization. Apart from the low-scoring parameter economy, ABAC provides good potential for control authorities as it is flexible due to the attributes which also is positive for the administration. Further, also as a result of the use of attributes, ABAC handles changes in the organization well. Therefore, if a small organization can handle the cost of implementation and a drastically different model compared to RBAC, ABAC can be a good choice for an access control model. Also, as ABAC is the best suited model for both large and growing organizations, according to the weighted results, it might be a good choice of access control model to prepare for potential growth in the future.

Moreover, RBAC increased the most by 0.20 points, which indicates that RBAC contains a lot of the parameters identified as important for small organizations. This is the result of the good score for RBAC in regard to economy, as RBAC is assumed to be the model already implemented by the organization, which means that no additional implementation is needed. Further, RBAC also handles changes in the organization well but falls short of control authorities compared to other models both in flexibility and administration. Therefore, just like ABAC, RBAC can be a good fit for access control models for small organizations if the organizations are willing to compromise in regard to control authorities, which might be realistic since the administration will not be as demanding as for larger organizations.

7.2.3 Large organizations

For large organizations, the weighted results in Table 7.1 show that ABAC would be the best suited model, the same result as for the unweighted result. This is because the important factors for large organizations described in Section 6.3, are control authorities, organizations, attribute definition, and security, and ABAC scores well for control authorities, organization, and attribute definition as a result of the wide use of attributes which makes the model flexible. Also, in terms of security, ABAC scores well as the use of attributes helps monitor the access both for separation of duty and granular permission. Therefore, ABAC would be a good fit for large organizations if the economy aspect can be handled in terms of a higher impact on personnel and a more expensive change of model.

However, the impression given by the theory is that TBAC would be the best fit, as TBAC introduces a good notion of control for granular permission. TBAC is the second-best scoring model due to the exceptionally good score for security as the model provides good opportunities to handle granular permissions. Further, TBAC also scores 3s for all other weighted parameters, making economy the lowest scoring parameter for the model due to the drastic differences to RBAC. This would make TBAC a good fit for large organizations if a high impact on economy can be handled as the change of access control model is performed.

The difference between ABAC and TBAC is that ABAC handles attribute definition and organization slightly better, while TBAC handles security slightly better. This means that a large organization can use both of the models depending on the priority, either the priority of role definitions and management during changes or the priority of security to prohibit vulnerabilities. Further, both ABAC and TBAC put the same stress on the system during a change in terms of economy. Both models also score the same for control authorities, which means that they have the same support for administrators. This means that if an organization prioritizes both economy and control authorities both models can be chosen.

Another interesting aspect of the weighted results for large organizations is that the majority of the models see an increase in the results, which might be because there are a larger amount of weights implemented compared to the weighting for a small organization. Also, many of the access control models score relatively high for control authorities and security, which are of the highest importance for large organizations. This stands from the overall good support for least privilege and separation of duty seen among the models. These two parameters are basic concepts of access control models, which often is the aim of implementing access control overall. However, different models fulfill the parameters differently, which could be seen in the unweighted results.

The only two models that do not increase for large organizations are RBAC and TRBAC as they have a low score for administrative workload and hence get a low score for control authorities overall. This would mean a lot of continued manual work for administrators, which is one of the problems that the change of access control model aims to solve for large organizations. Further, GTRBAC sees no changes because its best score is for organization as the model handles changes well, mainly because the organization parameter is not weighted the highest in this scenario.

The model with the biggest increase is DRBAC, resulting in a shared third for the best suited model. This might be because of its outstanding good score for control authorities as the model is dynamic and operates using machine learning. However, DRBAC scores low for attribute definition, meaning that roles and attributes might not be used to their full potential. This would be for an organization where overlap in roles might exist and where the division of users into roles experience some difficulties since users' attributes will not be recognized to the same extent. Also, for organization and security, DRBAC could score better to be able to handle changes and protect the system from misusage or vulnerabilities tied to over-authorization. Therefore, even though DRBAC increased the most from the weights, DRBAC might not be a good fit for large organizations. However, as DRBAC scores well for some of the important parameters it can still be argued that it should be considered for combinations with other access control models to achieve the outstanding administration tied to machine learning.

7.2.4 Growing organizations

From the theory, the impression is that PARBAC would be the best fit for a growing organization as it utilizes the flexibility of ABAC and the administration of RBAC, which is needed as the organization is changing. Another important aspect for growing organizations is the ability to handle changes, for which GTRBAC might be a better choice than PARBAC because of the ability to work with the temporal aspect found in GTRBAC. Although, both GTRBAC and PARBAC scores are relatively low for attribute definition, which might be a problem when applied to growing organizations as clear roles and the use of attributes to divide users into roles can the change from small to large organizations easier. This might also be the reason why neither GTRBAC nor PARBAC scored the highest for the weighted results for growing organizations, as attribute definition is one of the weighted parameters.

Overall, the model needed for a growing organization needs to be flexible to adapt to the organization as it is changing, but at the same time fit for the organization when it is at its largest. Therefore, many of the important aspects are alike to those of large organizations, meaning also that the results for a large organization and a growing organization might be quite similar.

The weighted results in Table 7.1 for a growing organization show that ABAC is the best fitted model. As discussed both for small and large organizations, ABAC scored well for the important parameters for a growing organization, see Section 6.3, as a result of the use of attributes and the flexibility they imply. Overall, the argument for both small and large organizations using ABAC can be implemented for growing organizations as well. Also, because of the large difference in points to the second-best scoring models, ABAC has clear advantages when an organization grows.

The model with the largest increase is DRBAC, just as for large organizations, which again shows how similar the scenarios for large and growing organizations are. The increase can yet again be explained by the exceptionally good score for control authorities and the good score for both organization and security. As discussed above, DRBAC might not be a good fit for implementation by itself, but rather that it should be combined with another model to be able to be used to its fullest.

RBAC, however, is the model with the largest decrease, also the same as for large organizations. The reasoning behind the decrease follows the line as described for large organizations. Mainly due to the weights determined and the similarities seen between the cases of large and growing organizations, where both scenarios have a 2 for attribute definition and a 3 for control authorities, followed by some importance also for organization and security. Therefore, the only reason for continued use of RBAC would be to avoid having to make the change of access control model, but the use of another model, e.g. ABAC, would be considerably better for the growing organization.

As shared second best models, GTRBAC and TBAC score. The differences between GTRBAC and TBAC are that GTRBAC utilizes a temporal aspect that allows for a special type of control of accesses and TBAC controls accesses through topics in terms of granular permission. Even though both GTRBAC and TBAC score a shared second, they score 0.27 points lower than the best scoring model ABAC, due to the outstanding score for attribute definition and organization for ABAC. Further, the large gap can also be because the high scores for control authorities for DRBAC and security for TBAC are offset by a lower number for other parameters while ABAC still scores quite high.

7.3 Model combinations

In Section 6.3 the scenario-based weights are presented and used on the overall grade to create new scores to better represent the needs of the differently sized organizations. The total scores and differences from the unweighted average are presented in the weighted comparison tables in Section 6.3. This will be used in this section to present the top 3 access control models from each scenario based on the highest total score and the largest increase in score separately. This is done because an access control model might score a high amount of points and could be deemed best as a result of that but a large increase in points might also indicate that that access control model is a good fit for the scenario.

While considering the scores and increases of the models for each scenario, different combinations of models will be suggested. A combination of models intends to create a hybrid model containing valuable aspects from different models to achieve a more tailored access control model that corresponds to the importance of the parameters. There is no guideline to combining models, since the main focus is to find individually suited models for organizations, meaning that organizations can select parts of interest for them to include in the combination. Although, all combinations of models may not result in a better performing model, as a large quantity of models can cause confusion rather than improving the access control.

7.3.1 Small organizations

The highest scoring access control models and the largest increase of score for the small organization scenario are presented in Table 7.2.

Placement	Total score	Access model
First	3.11	GTRBAC
Second	3.00	RBAC & ABAC
Third	2.89	ATRBAC & PBAC

(a) Highest scores

Placement	Increase	Access model
First	0.20	RBAC
Second	0.11	GTRBAC
Third	0.09	ATRBAC & PBAC

(b) Largest increases

Table 7.2: Highest scoring and largest increases of access control models for small organizations

For small organizations, the highest scoring access control models are at first place position GTRBAC which scored 3.11 points, with ABAC and RBAC following behind scoring 3.00 in second place, and in third place, there are ATRBAC and PBAC at 2.89 points. The largest increase in placements seems different from that of the highest scoring as RBAC is in first place having had an increase of 0.20 points followed by GTRBAC in second place which increased by 0.11 points. The third largest increase is shared by ATRBAC and PBAC at a 0.09 point increase.

It might be wise to choose RBAC which had the largest increase for small organizations and placed a shared second overall in the highest score as well. Another option would be to go for GTRBAC which scored the highest score overall and placed second but did an increase of about half of the increase that RBAC did. Another option is to combine ABAC which scored the second highest score and combines it with PBAC which had the third largest increase. As seen in Figure 7.1 they could be a good fit to balance each other out in terms of economy and attribute definition.

Another way to proceed could be to take regards the weighted parameters as displayed in Table 6.1, where it is shown that the most important parameter is economy but control authorities and organization might be worth being taken into consideration as well, especially if the organization is expected to grow later on. As displayed in Figure 7.1 it is shown that the economy parameter does not dismiss any of the top-scoring access control models except for ABAC as the remaining access control models all score 3 or better. This could point out that for a small organization using RBAC might still be a well-suited option. However, if RBAC is not desired the organization could turn to the second most important parameter. In regards to organization, GTRBAC which is the highest scorer and had the second largest increase could be a good option as it has good scores in organization and control authorities as well. Another option could be to extend RBAC with PBAC to score a bit better in the two aforementioned parameters.

7.3.2 Large organizations

For the large organization scenario, the highest scoring access control models and the largest increase in points of the access control models are presented in Table 7.3.

Placement	Total score	Access model
First	3.27	ABAC
Second	3.18	TBAC
Third	3.00	GTRBAC & DRBAC

(a) Highest scores

Placement	Increase	Access model
First	0.20	DRBAC
Second	0.18	TBAC
Third	0.13	RRBAC & PARBAC

(b) Largest increases

Table 7.3: Highest scoring and increasing access control models for large organizations

When it comes to the highest score for large organizations ABAC comes in first place with 3.27 points, followed by second place TBAC at 3.18 points, and a shared third place is GTRBAC and DRBAC at 3.00 points. It can be noted that the top scores for large organizations are a bit higher than those of small organizations indicating that the model is slightly better suited for larger organizations. When it comes to the largest increase DRBAC places first with a 0.20 point increase followed by TBAC in second at a 0.18 point increase and RRBAC and PARBAC in a shared third place at a 0.13 point increase.

In this case, the large organization has a lot of options to consider when picking an access control model. One option would be to pick ABAC as it has the highest score or DRBAC with the largest increase of points. However, it could be another option to combine ABAC or DRBAC with PBAC or GTRBAC which scored the third highest score and could act as a complement and give them a larger reach.

Security and control authorities are deemed to be the most important parameters for large organizations as per Table 6.3. Thus some other access control models to consider more closely could be TBAC or DRBAC, as TBAC is the top-scoring access control model for large organizations in security and DRBAC is the only access control model that has gotten the highest grade in control authorities. DRBAC and TBAC combined could in theory fit the large organization in regard to the parameters that would be most important. This combination would however not take into consideration the second most important parameters and score below par in attribute definition and organization. Thus another option could be to use ABAC in combination with TBAC to achieve a model suited for the purpose. Regardless of the high increase of RRBAC and PARBAC, they might not be suitable alternatives as their reach might be too small to be used on their own or to be used as a complement in this scenario.

7.3.3 Growing organizations

The top placing access control models for growing organizations can be viewed in Table 7.4 below.

Placement	Total score	Access model
First	3.36	ABAC
Second	3.09	GTRBAC & TBAC
Third	3.00	DRBAC

(a) Highest scores

Placement	Increase	Access model
First	0.20	DRBAC
Second	0.16	ABAC
Third	0.13	PARBAC

(b) Largest increases

Table 7.4: Highest scoring and increasing access control models for growing organizations

As displayed in the tables, ABAC places first in regards to highest score at 3.36 points followed by GTRBAC and TBAC in second place both scoring 3.09 points, and lastly DRBAC in third place having scored 3.00 points. The parameters for growing organizations score better overall than the top scorers for small organizations as well indicating again that the method might be better suited for larger organizations. When it comes to the largest increase DRBAC comes in first at a 0.20 point increase followed by ABAC at a 0.16 point increase and PARBAC at a 0.13 point increase.

From these placements, there is no lack of choices for making a decision of which access control model to choose. From Table 6.5 it can be concluded that the most important factors for a growing organization are control authorities and organization, and the second most important parameters are attribute definition and security. It could then be a logical conclusion to choose an access control model or two that excels in those parameters. DRBAC for example has the highest increase of points and is the only access control model to score a 4 in the control authorities parameter, and could therefore be a contender. On the other hand, GTRBAC and ABAC score full marks in the organization parameter. Therefore in theory a solution could be to combine DRBAC and GTRBAC to get a better reach in the higher-importance parameters. Whilst that combination would score well in the security parameter it would score sub-par in the attribute definition parameter. Therefore, it could be a preferable approach to include ABAC or TBAC in the chosen method.

7.4 Recommendations

To answer the question of which access control model is best suited for the differently sized organizations in the scenario cases a recommendation needs to be given to each one individually.

For the small organization scenario, it is agreeable to keep RBAC as the access control model of choice, which as seen in Table 7.2, performs quite well in this scenario. Additionally, as the economy parameter is the most important parameter for small organizations it might be the best choice to choose a single access control model and not combine them as it might be a bit excessive for the organization. If there is a need for the organization to improve the access control model either DRBAC or GTRBAC could be used instead of RBAC to improve the expressed prioritized parameters: control authorities and organization. As previously discussed DRBAC could add relief to the workload of the administrator as it performs well in the control authorities parameter. It does however not perform as well as either RBAC or GTRBAC in the most important parameter for small organizations, economy. GTRBAC on the other hand performs better in the economy parameter and well in the other two parameters of importance and still aids in the over-authorization problem by utilizing a temporal aspect as mentioned in the literature study. Therefore, for small organizations, it is worth considering whether it is worth keeping RBAC because of the economical aspect or if it is worth more to downgrade economy a step and upgrade the other important parameters.

For larger organizations as described in the scenario, it could be beneficial to change from RBAC to ABAC as it is the highest scorer and has a relatively large margin to the next access control model, as seen in Table 7.3. It could also be beneficial for a large organization to include aspects of TBAC or DRBAC to get an overall better-performing access control model relative to the parameters of importance for the scenario. Namely, control authorities and security, mentioned in Table 6.3 as the most important parameters for large organizations. Depending on the focus of the individual organization TBAC would offer a better security score whilst DRBAC would offer a better score for control authorities. Another reason ABAC might be the best core access control model for large organizations is that it scores the maximum amount of points in both of the second most important parameters and 3s in the most important parameters which makes it a good foundation to build upon. Therefore, as previously mentioned, a combination of ABAC and either TBAC or DRBAC depending on the priorities of the organization might be a wise choice for the access control model combination. A more complex option could be to create a new access control model based on ABAC, TBAC, and DRBAC, although that might be a bit excessive depending on the needs of the organization.

Lastly, growing organizations as depicted in the scenario might also benefit the most from the use of ABAC as shown by the high scores in Table 7.4. Growing organizations might also benefit from the use of TBAC as an extension of ABAC similar to large organizations. However, it might also be a favorable option to consider a combination of GTRBAC and DRBAC, which might be more similar to the access control model of choice for a small organization. Accordingly, for growing organizations, it is important to consider if the resemblance of a small or a large organization would be best fitted, as it is in the process of growing. However, based on the most important parameters for growing organizations the ABAC and TBAC combination would be better for the security aspect and the GTRBAC and DRBAC combination would be best for the control authorities aspect. Another recommendation, for organizations that knows that the growth will be delayed or for organizations that want to remain smaller, is to postpone the cost of the change of access control model to a later stage.

7.5 Method

In this section, the steps of the method are discussed ranging from the literature study to the final evaluation.

7.5.1 Literature study

During the literature study, several different aspects that could be improved were identified. Firstly, while searching for access control models to study it was realized that multiple different models existed using the same abbreviation, for example, DRBAC. This meant that it was hard to find relevant sources for some of the models.

On the same topic, while searching sources for the literature study, the varying amount of research available for the different models was recognized, which made it more difficult to get an equal view of all models. Further, the sources that were studied were quite theoretical, meaning there are not many cases of application discussed, and a few models are aimed at different use cases. This can have an impact on the results and judgment of suitability.

Another aspect of the literature study that could be improved is the process used while choosing relevant models to study. The process involved studying RBAC and ABAC and branching out to find models to study further. This, however, might have impacted what models were found and later studied. Meaning that there might be models which have not been identified and therefore not studied. Also, the models that were part of the start phase but later were removed as they were not deemed suitable are not mentioned at all, which means that the reader will not know about them.

7.5.2 Unweighted calculations

Continuing on the topic of literature study, the examples and cases presented in the literature might imply a bias for models presented in the results, this also means that the grades in Table 5.2 and Table 5.1 could be argued.

Further, the parameters that the models are evaluated based on are factors that are thought to be important for organizations. This means that there might be parameters that are not identified in this thesis that can be of importance. This could have been improved by consulting experts to make sure the parameters are relevant.

Also, as a basis for the analysis, an organization using RBAC is assumed, which impacts some of the parameters discussed, mainly the cost of implementation and similarity. This needs to be kept in mind while analyzing the economy category and will impact the combinations of models, as economy combines to the lower score rather than the highest score as for the other parameters. The basis was needed to be able to determine the impact the change of access control model will have in terms of economy. The use of RBAC specifically as a basis means that models based on RBAC will score relatively well, which would not have been the case if another model, from the category of other models, would have been chosen as the basis.

7.5.3 Scenarios

To further build the basis for the organizations and scenarios, additional consultations with experts in the area could have been of use. This could impact the construction of the scenarios as different experts might introduce different knowledge when it comes to organizational aspects and important parameters to study.

On the same note, it is hard to use experts from different enterprises within the area without discussing too much of a topic that is deemed to be an enterprise secret. This is important as enterprises need to maintain their security, but for the sake of the study as much information as possible to gather is helpful to better construct the scenarios.

7.5.4 Final evaluation

Another result from the literature study is that there is little evidence of the compatibility of different models presented. Therefore, the compatibility is hard to research and it might have impacted the recommendations made for organizations. The biggest impact would be if some models are not compatible but research on this was not discovered.

As seen in the discussion, different recommendations can provide just as good of model suggestions. As the choice of access control model for each organization depends on a lot of different parameters and important aspects, some of which might be needed to keep secret for security reasons, it is hard to find one single recommendation. This means that organizations will have to consider the different recommendations presented with their priorities in mind to be able to determine what access control model they should choose.

7.6 The work in a wider context

Whilst there are no major ethical or societal aspects related to the content of this report directly there are some aspects under the security umbrella of access control models that are relevant to the aforementioned aspects. One example of this is that access control can raise ethical question marks as the openness level of the system can open doors for ethical misconduct. Ma, Yang, and Xiang [15] raised examples of employees of big enterprises as well as government agencies releasing information on users and company secrets and even going as far as spying on underage users. Rath and Colin [18] raises the concern of location tracking as if the location of a person is stored and the system is compromised this can lead to a situation where a user or employee could get in physical danger.

Further, if a lot of clients' information were leaked due to an access control model where over-authorization was a reality this could have a larger societal effect as more people would be affected. Rath and Colin [18] mention the legal aspect in the form of general data protection regulation (GDPR). Thus in a worst-case scenario, a massive information leak could be extended to new legal requirements e.g. for all EU countries due to an over-authorization in one enterprise.

8 Conclusion

From the study, using the different methods, namely the literature study, the model evaluation, and the scenario-based evaluation, different conclusions can be made to answer the research questions. Overall, it can be concluded that the choice of access control model for a specific organization depends on several different factors, which means that there is no singular recommendation that can be trusted blindly in all cases.

According to the literature study in Chapter 2, 12 access control models have been identified as suitable for organizations within the technology industry. The main common factor of the models is good adaptability during change, high flexibility, and high security in terms of least privilege and separation of duty. Overall, the desired aspects that were sought when identifying models were well-developed models with good explanations of implementations and clear uniqueness that differentiates the models. Although, as seen in the results, not all models score that well in terms of the overall model evaluation. For example, FBAC was clearly deemed not relevant as it scored low for almost all important parameters, and therefore should not be named a suitable access control model for organizations within the technology industry.

For organizations, the first step towards choosing an access control model is to identify different characteristics and highlight aspects of importance. This could be, for example, wide collaborations, a high need for granular permissions, or issues regarding administration. An organization could proceed to choose the best suited access control model by using the evaluation presented in Table 5.2 and weight the parameters of greatest importance as shown in Chapter 6. This will result in one or more models that are best suited for the particular organization. However, as seen in Chapter 7, multiple different choices or combinations can be the answer for what works best for each organization depending on the priorities and abilities of the organization.

This thesis recommends the following choices of access control model for each scenario based on Section 7.4. For small organizations, it is recommended to keep RBAC or upgrade to DRBAC or GTRBAC depending on the needs and future planning of the organization. For large organizations, ABAC in combination with TBAC or DRBAC is suggested and can be formed to the organization's needs. Lastly, for growing organizations, a combination of either ABAC and TBAC or GTRBAC and DRBAC is suggested although the choice of which depends on the needs and goals of the organization.

8.1 Future work

In the future, it would be interesting to implement a recommended access control model combination such as ABAC and TBAC or GTRBAC and DRBAC. This could bring forward a new access control model as several other models have been created through the combination of existing ones.

Another continuation that would be interesting would be to create a more generalized method of access control model recommendation by utilizing a larger organization based both on the interviews but also scenario differentiation.

Bibliography

[1] Muhammad Umar Aftab, Zhiguang Qin, Negalign Wake Hundera, Oluwasanmi Ariyo, Ngo Tung Son, and Tran Van Dinh. "Permission-based separation of duty in dynamic role-based access control model". In: *Symmetry* 11.5 (2019), p. 669. DOI: 10.3390/sym11050669.

[2] Elisa Bertino, Piero Andrea Bonatti, and Elena Ferrari. "TRBAC: A Temporal Role-Based Access Control Model". In: *ACM Trans. Inf. Syst. Secur.* 4.3 (2001), pp. 191–233. DOI: 10.1145/501978.501979.

[3] Bo Cui, Zhikun Lan, and Xiangyu Bai. "Research on Role-based Access Control in IPv6 Smart Home". In: *Proceedings of the IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*. 2019, pp. 205–208. DOI: 10.1109/ICEIEC.2019.8784596.

[4] Saptarshi Das, Shamik Sural, Jaideep Vaidya, and Vijayalakshmi Atluri. "Policy Adaptation in Hierarchical Attribute-Based Access Control Systems". In: *ACM Trans. Internet Technol.* 19.3 (Aug. 2019). DOI: 10.1145/3323233.

[5] Yvo Desmedt and Arash Shaghaghi. "Function-Based Access Control (FBAC) From Access Control Matrix to Access Control Tensor". In: *Proceedings of the ACM CCS International Workshop on Managing Insider Security Threats*. 2016, pp. 89–92. DOI: 10.1145/2995959.2995974.

[6] Georgios Fragkos, Jay Johnson, and Eirini Eleni Tsiropoulou. "Dynamic Role-Based Access Control Policy for Smart Grid Applications: An Offline Deep Reinforcement Learning Approach". In: *IEEE Transactions on Human-Machine Systems* (2022), pp. 761–773. DOI: 10.1109/THMS.2022.3163185.

[7] Virginia Franqueira and Roel Wieringa. "Role-based access control in retrospect". In: *Computer* 45.6 (2012), pp. 81–88.

[8] Sergio Gusmeroli, Salvatore Piccione, and Domenico Rotondi. "A capability-based security approach to manage access control in the internet of things". In: *Mathematical and Computer Modelling* 58.5-6 (2013), pp. 1189–1205. DOI: 10.1016/j.mcm.2013.02.006.

[9] Vincent C. Hu, D. Richard Kuhn, David F. Ferraiolo, and Jeffrey Voas. "Attribute-Based Access Control". In: *Computer* 48.2 (2015), pp. 85–88. DOI: 10.1109/MC.2015.33.

[10] J.B.D. Joshi, E. Bertino, U. Latif, and A. Ghafoor. “A generalized temporal role-based access control model”. In: *IEEE Transactions on Knowledge and Data Engineering* 17.1 (2005), pp. 4–23. DOI: `10.1109/TKDE.2005.1`.

[11] Michael Kunz, Ludwig Fuchs, Michael Netter, and Günther Pernul. “Analyzing quality criteria in role-based identity and access management”. In: *Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP)*. IEEE. 2015, pp. 1–9. DOI: `10.5283/epub.31342`.

[12] Xuan Hung Le, Terry Doll, Monica Barbosu, Amneris Luque, and Dongwen Wang. “An enhancement of the Role-Based Access Control model to facilitate information access management in context of team collaboration and workflow”. In: *Journal of Biomedical Informatics* (2012), pp. 1084–1107. DOI: `https://doi.org/10.1016/j.jbi.2012.06.001`.

[13] Sun Long and Li Yan. “RACAC: An Approach toward RBAC and ABAC Combining Access Control”. In: *Proceedings of the IEEE International Conference on Computer and Communications (ICCC)*. 2019, pp. 1609–1616. DOI: `10.1109/ICCC47050.2019.9064301`.

[14] Ke Ma and Geng Yang. “TBAC: A Fine-Grained Topic-Based Access Control Model for Text Data”. In: *IEEE Transactions on Services Computing* (2022), pp. 1–14. DOI: `10.1109/TSC.2022.3190385`.

[15] Ke Ma, Geng Yang, and Yang Xiang. “RCBAC: A risk-aware content-based access control model for large-scale text data”. In: *Journal of Network and Computer Applications* 167 (2020), p. 102733. DOI: `10.1016/j.jnca.2020.102733`.

[16] Fatemeh Nazerian, Homayun Motameni, and Hossein Nematzadeh. “Emergency role-based access control (E-RBAC) and analysis of model specifications with alloy”. In: *Journal of Information Security and Applications* (2019), pp. 131–142. DOI: `https://doi.org/10.1016/j.jisa.2019.01.008`.

[17] Simon Parkinson and Saad Khan. “A Survey on Empirical Security Analysis of Access-Control Systems: A Real-World Perspective”. In: *ACM Comput. Surv.* 55.6 (Dec. 2022). ISSN: 0360-0300. DOI: `10.1145/3533703`. URL: `https://doi.org/10.1145/3533703`.

[18] Thavymony Annanda Rath and Jean-Noël Colin. “Adaptive risk-aware access control model for internet of things”. In: *Proceedings of the International Workshop on Secure Internet of Things (SIoT)*. IEEE. 2017, pp. 40–49. DOI: `10.1109/SIoT.2017.00010`.

[19] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. “Role-based access control models”. In: *Computer* 29.2 (1996), pp. 38–47. DOI: `10.1109/2.485845`.

[20] R.S. Sandhu and P. Samarati. “Access control: principle and practice”. In: *IEEE Communications Magazine* (1994), pp. 40–48. DOI: `10.1109/35.312842`.

[21] Jonathan Shahen, Jianwei Niu, and Mahesh Tripunitara. “Cree: A Performant Tool for Safety Analysis of Administrative Temporal Role-Based Access Control (ATRBAC) Policies”. In: *IEEE Transactions on Dependable and Secure Computing* (2021), pp. 2349–2364. DOI: `10.1109/TDSC.2019.2949410`.

[22] N Sivaselvan, Waqar Asif, Bhat K Vivekananda, and Muttukrishnan Rajarajan. “Authentication and Capability-based Access Control: An Integrated Approach for IoT Environment”. In: *Proceedings of the International Conference on Communication Software and Networks (ICCSN)*. 2020, pp. 110–117. DOI: `10.1109/ICCSN49894.2020.9139051`.

[23] Nidhiben Solanki, Yongtao Huang, I-Ling Yen, Farokh Bastani, and Yuqun Zhang. “Resource and Role Hierarchy Based Access Control for Resourceful Systems”. In: *Proceedings of IEEE Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 02. 2018, pp. 480–486. DOI: `10.1109/COMPSAC.2018.10280`.

[24] Samir Talegaon and Ram Krishnan. "Role-Based Access Control Models for Android". In: *Proceedings of the IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. 2020, pp. 179–188. DOI: 10.1109/TPS-ISA50397.2020.00033.

[25] Abhijeet Thakare, Euijong Lee, Ajay Kumar, Valmik B. Nikam, and Young-Gab Kim. "PARBAC: Priority-Attribute-Based RBAC Model for Azure IoT Cloud". In: *IEEE Internet of Things Journal* 7.4 (2020), pp. 2890–2900. DOI: 10.1109/JIOT.2019.2963794.

[26] Muhammad Umar Aftab, Ali Hamza, Ariyo Oluwasanmi, Xuyun Nie, Muhammad Shahzad Sarfraz, Danish Shehzad, Zhiguang Qin, and Ammar Rafiq. "Traditional and Hybrid Access Control Models: A Detailed Survey." In: *Security and Communication Networks* 2022 (2022). ISSN: 1939-0122. DOI: 10.1155/2022/1560885.

[27] Muhammad Umar Aftab, Zhiguang Qin, Safeer Ali, Jalaluddin Khan, et al. "The evaluation and comparative analysis of role based access control and attribute based access control model". In: *Proceedings International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*. IEEE. 2018, pp. 35–39. DOI: 10.1109/ICCWAMTIP.2018.8632578.

[28] Emre Uzun, Vijayalakshmi Atluri, Shamik Sural, Jaideep Vaidya, Gennaro Parlato, Anna Lisa Ferrara, and Madhusudan Parthasarathy. "Analyzing Temporal Role Based Access Control Models". In: *Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT)*. 2012, pp. 177–186. DOI: 10.1145/2295136.2295169.

[29] K. Vijayalakshmi and V. Jayalakshmi. "Identifying Considerable Anomalies and Conflicts in ABAC Security Policies". In: *Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS)*. 2021, pp. 1273–1280. DOI: 10.1109/ICICCS51141.2021.9432162.

[30] Lin Zhi, Wang Jing, Chen Xiao-su, and Jia Lian-xing. "Research on Policy-based Access Control Model". In: *Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing*. Vol. 2. 2009, pp. 164–167. DOI: 10.1109/NSWCTC.2009.313.

[31] Yan Zhu, Ruyun Yu, Di Ma, and William Cheng-Chung Chu. "Cryptographic Attribute-Based Access Control (ABAC) for Secure Decision Making of Dynamic Policy With Multiauthority Attribute Tokens". In: *IEEE Transactions on Reliability* 68.4 (2019), pp. 1330–1346. DOI: 10.1109/TR.2019.2948713.

[32] Yi Zong, Yao Guo, and Xiangqun Chen. "Policy-Based Access Control for Robotic Applications". In: *Proceedings of the IEEE International Conference on Service-Oriented System Engineering (SOSE)*. 2019, pp. 368–3685. DOI: 10.1109/SOSE.2019.00062.