IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46SP/2025/4636525/
Vol. 2025 (37), Article ID 4636525

Beyond Roles: The Shift to Attribute-Based and Risk-Aware Access Control*

Piotr KONTOWICZ and Mateusz BARSKI

Poznan University of Technology, Faculty of Computing and Telecommunications,

Piotrowo 3, 60-965 Poznan, Poland

Correspondence should be addressed to: Piotr KONTOWICZ, piotr.kontowicz@put.poznan.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

The increasing complexity of distributed and cloud-based systems has revealed the limitations of traditional access control mechanisms and highlighted the need for adaptive models capable of operating in dynamic environments. This study analyzes the progression of access control from classical models, such as Discretionary Access Control and Mandatory Access Control, to more recent approaches, including Role-Based Access Control and Attribute-Based Access Control. The primary objective is to evaluate the suitability of these models for contemporary system architectures, including cloud computing and the Internet of Things. While previous research has typically examined these models in isolation, there remains a gap in comprehensive comparisons that address scalability, administrative effort, and adaptability to evolving contexts.

This research employs a systematic comparative analysis using operational, administrative, and security criteria. Each model is assessed based on its capacity to fulfill confidentiality, integrity, and availability requirements under varying conditions. The findings indicate that Discretionary and Mandatory Access Control represent contrasting paradigms, emphasizing either flexibility or control. Role-Based Access Control offers enhanced scalability and administrative simplicity, though it may encounter challenges related to role proliferation. Attribute-Based Access Control enables dynamic, context-aware policies that align with the Zero Trust model and deliver the greatest adaptability in complex environments.

The results confirm that no single access control model is universally applicable. Nevertheless, Attribute-Based Access Control demonstrates the greatest potential for securing modern IoT and cloud ecosystems, provided that robust policy and attribute management mechanisms are in place.

Keywords: Access Control, DAC, MAC, RBAC, ABAC

Introduction

In modern systems, access control is a fundamental security mechanism. Its purpose is to enforce policies that define who can gain access to system resources and to what extent. The access control process consists of three elements: identification, authentication, and authorization, and their role is to ensure the key security principles of integrity, confidentiality, and availability [1].

The evolution of access control models is closely linked to the development of application architectures and the expansion of organizational needs. Initially, models such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC) were characterized by rigid rules. Due to advances in systems, these models became too

Cite this Article as: Piotr KONTOWICZ and Mateusz BARSKI, Vol. 2025 (37) "Beyond Roles: The Shift to Attribute-Based and Risk-Aware Access Control " Communications of International Proceedings, Vol. 2025 (37), Article ID 4636525, https://doi.org/10.5171/2025.4636525

restrictive, leading to the development of a new model – Role-Based Access Control (RBAC). This model significantly simplified permission management in large organizations. A new challenge for access control models has emerged with the development of cloud services and the Internet of Things (IoT), where the static nature of RBAC proved insufficient. The solution to the arising problems became Attribute-Based Access Control (ABAC). This paper analyzes and evaluates access control models, identifying their strengths and weaknesses and assessing their applicability to current and emerging system challenges.

Overview of Discretionary Access Control (DAC)

Discretionary Access Control (DAC) was the initial access control model, implemented in early academic and commercial systems that did not require stringent protection. In this model, user identity is central, and the security policy is determined by the resource owner [2]. The model relies on two primary elements:

1. resource ownership: in most cases, the creator of an object becomes its owner, having full control over it and being able to decide who can access it and under what conditions.
2. access control list (ACL): the rules imposed by the owner are enforced using an acl, a list associated with each object that defines which users and groups have permissions to perform specific operations.

This model is flexible and performs well in small environments. Resource owners can manage access themselves, which facilitates collaboration within teams. However, in some environments, ownership can also introduce additional risks associated with:

1. propagation of privileges: a user with legitimate access to a resource may pass those permissions to another user. The issue is that this can happen without the resource owner's knowledge.
2. malware: all processes launched by a user inherit that user's privileges. as a result, if a user runs malicious software, it gains full access to all of the user's resources.
3. decisions: due to user errors, particularly from the resource owner, incorrect permission assignments may occur, increasing the risk of information leakage.

Mandatory Access Control (MAC) was developed as a more restrictive model to address the limitations identified in DAC.

Principles and Limitations of Mandatory Access Control (MAC)

One of the first and most rigorous authorization models, designed to provide a high level of security [2]. This model is centrally defined by the system administrator and enforced by the operating system, without the possibility of modification by users. Even if a user is the creator of a resource, they cannot independently grant access to other entities. The concept of Mandatory Access Control (MAC) is based on security labels assigned to all objects in the system. Object labels represent classifications, while user labels (including those of processes and services) are defined as credentials. Access decisions are made by comparing labels according to global rules. The greatest advantage of MAC is its high level of security and confidentiality. Centralized management eliminates the risk of user error or malicious changes. However, the model offers no flexibility, which makes it unsuitable for dynamic commercial environments.

Efficient Access Management Through Roles - RBAC

The limitations of early access control models prevented their widespread adoption in large corporate environments. Role-Based Access Control (RBAC) was developed to address these shortcomings [3].

The main idea behind this model is the separation of user permissions from their identities through the introduction of roles. The model assumes that permissions are assigned to specific roles, and users gain access to resources by being assigned the appropriate roles. This approach to permission management greatly facilitates administration, especially in large corporate environments, where managing permissions for each individual user is too complex and error-prone. According to the NIST standard [4], the architecture consists of:

1. core elements: users, roles, and operations
2. relationships: assigning users to roles and assigning permissions to roles

The standard also defines model levels:

1. flat: users are assigned to roles, and permissions are assigned to roles. Users obtain permissions through their membership in appropriate roles. It's important to note that these are many-to-many relationships a user can be assigned to multiple roles, and a single role can have multiple users.

1. hierarchical: allows for permission inheritance, which simplifies management.
2. constrained: allows for defining constraints and separation of duties. Its goal is to distribute responsibilities and permissions related to specific tasks, significantly limiting the possibility of abuse, as execution requires more than one person.
3. symmetric: introduces the requirement of being able to review the permissions assigned to each role.

This approach supports the principle of least privilege and separation of duties, significantly reducing administrative overhead. The model offers good scalability in large environments and is relatively easy to audit.

The main issue associated with RBAC is the tendency for the number of roles to grow excessively. This is especially noticeable in large environments that require a high level of permission granularity. The need to handle exceptions may lead to a proliferation of roles, which ultimately makes effective management more difficult.

ABAC Model: Enabling Zero Trust and Adaptive Security

Attribute-Based Access Control (ABAC) was developed to address limitations inherent in RBAC. ABAC is effective in large, dynamic corporate environments. Access decisions are made dynamically according to policies that evaluate resource attributes [5]. The system updates context in real time and grants or denies access based on current conditions.

The ability to perform a requested operation is determined based on the attributes assigned to the requester, the object, environmental conditions, and the defined policies. Attributes are characteristics that describe a resource, a subject, or environmental conditions. A subject may be either a human or non-human user (e.g., a device). Each subject is assigned at least one attribute. An object is a system resource to which access is controlled. A policy is a set of rules describing specific operations (read, write, edit, delete, copy, execute) that determine whether access should be granted based on the attribute values.

This approach enables ABAC to deliver flexible and fine-grained access control. The model is scalable in large, distributed environments because generalized policies accommodate new users and resources through attribute assignment, without requiring policy modification.

ABAC is also used in the Zero Trust approach [6], which assumes continuous verification of every access request [7].

Key challenges in implementing ABAC include complex policy management, particularly in large organizations, and attribute management, which necessitates integration with data sources such as human resources systems or asset databases. Effective administration requires close collaboration between the security team and the broader organization. Developing effective policies depends on a thorough understanding of business processes and data flows, resulting in security policies that reflect operational procedures.

From DAC to ABAC: Evaluating Access Control Strategies for Modern Systems

The characteristics of each access control model demonstrate that selecting an appropriate solution requires balancing security, control granularity, and administrative flexibility.
The DAC and MAC models represent opposing philosophies. DAC, based on access control lists and resource ownership, offers flexibility to the user. In contrast, MAC is a centrally managed model where the end user cannot make any modifications. It provides a higher level of security but does not allow for any flexibility. A certain compromise is offered by the RBAC model, which is significantly more secure than DAC and more flexible than MAC. The main advantage of this model is ease of administration, but over time, organizational requirements can lead to excessive growth in the number of required roles, making administration more difficult.
ABAC, by introducing dynamic policies that evaluate attributes in real time, responds to the challenges associated with maintaining roles in the RBAC model. Table 1 contains a comparison of the key features of the discussed models.

As shown in Table 1, each of the presented access control methods has its strengths and weaknesses. Choosing one of them should depend on the system architecture, its scale, and the type of data stored and processed in the system. DAC, due to its focus on the resource owner, is suitable for home systems and small organizations.

However, because access rights are managed by all users, the risk of incorrect permission management may increase as the system scales.

As mentioned earlier, the MAC model follows a different philosophy and is ideal for systems that store data with a clearly defined hierarchy of confidentiality. However, this lack of flexibility makes it unsuitable for dynamic systems and those where access rights do not follow a simple hierarchy.

The RBAC model, by assigning permissions to roles, performs well even in large environments. However, if too many roles are created or a high level of access detail is required, permission management becomes challenging. The ABAC model is effective in large, dynamic environments and those requiring fine-grained control. However, it necessitates comprehensive policy management and a thorough understanding of organizational processes and existing policies. Table 1 demonstrates that no single model is universally applicable; selection should be based on specific system requirements.

Table 1. Comparison of Access Control Models

	DAC	MAC	RBAC	ABAC
Main Feature	Access rights defined by resource owners	Access rights defined by the system administrator using appropriate labels	Access rights based on roles with assigned permissions to resources	Access rights dynamically defined by the system based on attributes and policies
Granularity	High	Low	Medium	High
Scalability	Low	High	Medium	High
Advantages	Simplicity in small environments, flexibility	High level of security, resilience to user errors	Simplified administration, auditability	Contextual flexibility, Zero Trust support
Disadvantages	Security depends on users	Low flexibility	Large number of roles complicates administration	As scale increases, policy management becomes more difficult

Future of Access Control Models: Adaptive Security for IoT and Cloud Systems

Access control methods continue to evolve in response to emerging technologies and challenges related to security and scalability. This evolution is particularly evident in Internet of Things (IoT) and cloud-based systems [8], where environments are highly variable and widely distributed. Risk-Based Access Control (RiBAC) [9] has been proposed as a solution, relying on the estimation of security incident risk associated with granting access to specific resources.

Based on the estimated risk value and the predefined access policy for the resource, the model dynamically makes decisions to grant or deny access. When assessing risk, this model may take into account factors such as:

1. The confidentiality of the resource
2. The relevance of the resource to the subject's responsibilities
3. Information about the current state of the environment
4. The impact of performing the requested operation on the organization's data security
5. The history of access grant and denial decisions for the given subject

This model is suitable for managing dynamically changing environments by utilizing real-time contextual information. The effectiveness of Risk-Based Access Control depends on implementing a balanced and realistic risk assessment methodology.

Conclusions

The analysis confirms that access control models have been developed in response to ongoing changes in system architectures. The early classical models form the foundation, presenting contrasting approaches, with DAC offering high flexibility and MAC providing strong security but lacking flexibility.

Due to the limitations of these models, RBAC was introduced and became a standard by offering a compromise between security and manageability. The key factor behind its popularity was the simplification of administration through the introduction of roles. However, in large and complex environments, this element may lead to excessive growth in the number of roles and complicate the administrative process.

ABAC was developed to enable access decisions based on attributes and defined policies. This model inherently supports the Zero Trust approach, which is increasingly adopted in modern security frameworks.
The selection of an access control model should be guided by organizational requirements, available administrative resources, and the desired level of security.

Acknowledgements

This research was funded by the Polish Ministry of Science and Higher Education under Grant 0313/SBAD/1311.

Bibliography

- William Stallings, Lawrie Brown. Computer Security: Principles and Practice, 4th Edition. Pearson Education. 2018.
- Trusted Computer System Evaluation Criteria. Department of Defence. 1983.
- Ravi Sandhu, David Ferraiolo, Richard Kuhn. The NIST Model for Role-Based Access Control: Towards a Unified Standard. 2000.
- SANDHU, Ravi, et al. The NIST model for role-based access control: towards a unified standard. In: *ACM workshop on Role-based access control*. 2000.
- Vincent C. Hu, D. Richard Kuhn, David F. Ferraiolo, Jeffrey Voas. Attribute-Based Access Control. Computer. 2015.
- Dhiman P, Saini N, Gulzar Y, Turaev S, Kaur A, Nisa KU, Hamid Y. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors*. 2024; 24(4):1328. https://doi.org/10.3390/s24041328
- Meha James, Thomas Newe, Donna O'Shea, George D. O'Mahony. Authentication and Authorization in Zero Trust IoT: A Survey. 35th Irish Signals and Systems Conference (ISSC). 2024.
- Fangbo Cai, Nafei Zhu, Jingsha He, Pengyu Mu, Wenxin Li, Yi Yu. Survey of access control models and technologies for cloud computing. Cluster Computing, 22. 2018.
- Atlam HF, Azad MA, Alassafi MO, Alshdadi AA, Alenezi A. Risk-Based Access Control Model: A Systematic Literature Review. Future Internet. 2020.