

Original Article

A Dynamic, Attribute-Based Access Control (ABAC) Model for Microservices and Cloud-Native Applications Integrated with Traditional IGA

Sunnykumar Kamani

Lead Software Developer - SailPoint, United States

Received Date: 02 July 2025

Revised Date: 22 August 2025

Accepted Date: 17 September 2025

Abstract: The rapid cloud-native adoption architecture defined by loosely coupled components (microservices) has fundamentally changed the enterprise IT landscapes. These dynamic, distributed systems require an equally dynamic and granular access control mechanism that cannot be provided traditionally. Though traditional Identity Governance and Administration (IGA) systems are very good at managing static roles, they do not relate to the contextual, real-time decisions needed in modern applications. This paper will present an architectural model that unifies IGA with Attribute-Based Access Control (ABAC) by redefining the IGA system as a central Policy Administration Point (PAP) of a federated enterprise-wide ABAC system. The IGA platform is thus repositioned in this model as a source of authority with responsibility for defining, managing, and disseminating all attribute-based policies to distributed Policy Decision Points (PDPs) within cloud environments. This framework overcomes the disadvantages of Role-Based Access Control (RBAC) such as "role explosion" and reduces the administrative burden of ABAC by eliminating "policy sprawl." The proposed model allows for continuous authorization, making compliance easy while offering a scalable, resilient security posture for hybrid, cloud-native application environments that align directly with modern security paradigms like Zero Trust.

Keywords: ABAC, Policy Administration Point (PAP), microservices security, cloud-native security, hybrid policy models, continuous authorization, Identity Governance and Administration (IGA), Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP).

I. INTRODUCTION

Attribute based access control is an authorization methodology that establishes and implements rules according to attributes like manager, department, location, and time of day. ABAC uses conditional statements to define the user, request, resource, and action in order to generate access rules. ABAC provides more[1].

A. Motivation and Problem Statement

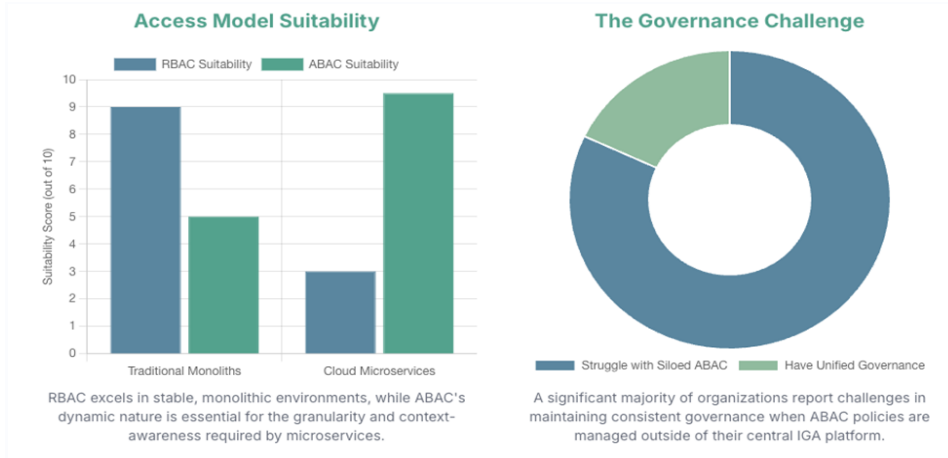
The move to cloud-native architectures with dynamic microservices means a major security concern for access control in the traditional model. Legacy paradigms, such as Role-Based Access Control (RBAC), prove to be extremely inflexible because of the phenomenon known as role explosion-collecting an unmanageable number of necessary roles within an organization-all required for this modern environment[2,5]. Just like IGA systems are very important in managing identities and ensuring compliance, they do not work holistically and dynamically with real-time access decisions that are necessary in the cloud[3].

This paper suggests a consolidated architectural model. It also puts forward that the IGA system can be architected to work as the main Policy Administration Point in an enterprise-distributed Attribute-Based Access Control setup. This unification takes advantage of both centralized, auditable governance offered by IGA and the dynamic fine-grained control presented by ABAC in delivering scalable yet compliant security postures appropriate for contemporary hybrid environments.

B. The Modernization Governance Gap

As enterprises move to dynamic cloud-native architectures, traditional access control models struggle to keep pace. Role-Based Access Control (RBAC) is too static for microservices, while Attribute-Based Access Control (ABAC) is often managed in silos, creating visibility gaps and policy





II. BACKGROUND AND FOUNDATIONAL CONCEPTS

A. The Evolution of Access Control Models

Traditional access control models began with simple Discretionary Access Control (DAC) and Mandatory Access Control (MAC). They have now moved to the most popular version, Role-Based Access Control (RBAC) RBAC facilitates management by granting access based on the role of a user within an organization[4]. Since it is static in nature, if the situation requires dynamism and context-based scenarios, then this will not be suitable. This leads to multiple roles which cause "role explosion"[2,4].

Access-Based Attribute Control (ABAC) surfaced as a solution. ABAC evaluates the attributes of four major entities to an access decision: the subject (user), object (resource), action (operation), and some environmental/contextual data such as time or place[1]. It allows for very fine-grained dynamic and contextual decisions that match the complexity of today's modern cloud and hybrid infrastructures[5].

B. Core Components of the ABAC Architecture

The normal ABAC system has separation of decision and enforcement by four major components:

- Policy Enforcement Point (PEP): Catches all access requests and forwards them to the PDP for evaluation. It is the component which enforces or blocks access based on a decision made by the PDP[6,7].
- Policy Decision Point (PDP): This forms the "brain" of an ABAC system. It takes requests and attributes from PEP, evaluates them against defined policies, and returns a decision (permit/deny)[6,7].
- Policy Information Point (PIP): Serves as a data-gathering mechanism, providing the PDP with up-to-date attribute values that it collects from all potential sources (for example, HR databases or device management tools)[6,7].
- Policy Administration Point (PAP): The admin interface for policy definition, management, and storage. The PDP interrogates the PAP to fetch the requisite policies for evaluation[6,7].

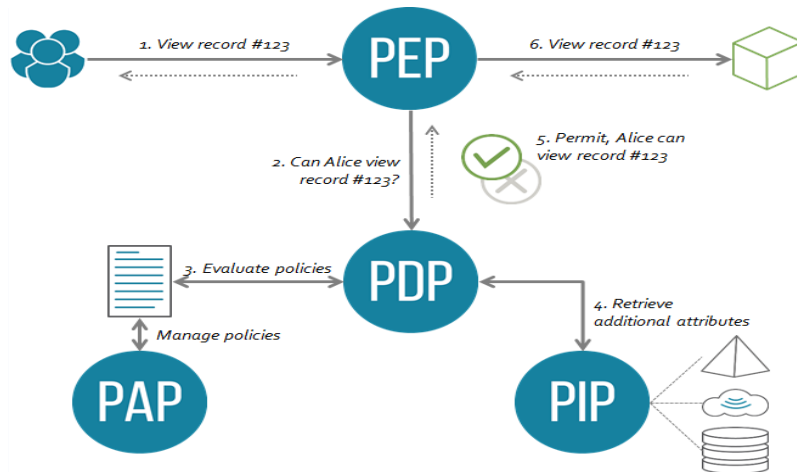


Figure 1: ABAC in the Microservice Architecture Flow

ABAC flow, where Policy Enforcement Point (PEP) sits between the user and the resource, it passes attributes to Policy Decision Point (PDP), which is the brain of ABAC, PDP evaluates the request against policies and makes decisions.

C. Identity Governance and Administration (IGA)

Identity Governance and Administration (IGA) is the framework that manages digital identities and their entitlements over their lifecycle. IGA has traditionally been very strong at providing a centralized, auditable record of who has access to what. Built for regulatory compliance, in most modern enterprises, its legacy architecture exists as a somewhat isolated function competing against the dynamic needs of cloud-native access control[8]. Because it will serve as the system of record for identity and attribute data, the IGA platform is logically positioned to become the PAP for any ABAC implementation.

To put the architectural value of this proposed model into perspective, Table 1 draws a comparison between these access control paradigms.

Table 1: Comparative Analysis of Access Control Models

Characteristic	RBAC (Traditional)	Traditional IGA	ABAC	Unified IGA-ABAC (Proposed)
Granularity	Low (based on roles)	Low-Medium	High (based on attributes)	High (fine-grained and governed)
Scalability	Limited ("role explosion")	High (for identity lifecycle)	Very High	Very High
Context-Awareness	Low (static roles)	Low	High (real-time attributes)	Very High (context-aware and continuously governed)
Administrative Overhead	Low-Medium	Medium-High	High (policy complexity)	Low-Medium (centralized management)
Primary Use Case	On-premises, monolithic systems	Identity lifecycle, compliance	Dynamic, distributed systems	Hybrid, cloud-native governance
Compliance/Auditability	Difficult to trace	Excellent (centralized)	Challenging (distributed)	Excellent (centralized source of truth)

III. THE UNIFIED IGA-ABAC GOVERNANCE MODEL: AN ARCHITECTURAL PROPOSAL

A. Redefining the IGA Platform as a Central PAP

The core hypothesis of this paper is that the gap between identity governance and dynamic access control, both architectural and operational, can be bridged by uplifting the traditional IGA platform to become the central Policy Administration Point (PAP) for an enterprise-wide ABAC framework. In this model being proposed, the IGA platform does not remain just a user role and entitlement management system but rather becomes the authoritative source for defining, managing, and distributing all attribute-based policies.

The IGA platform forms, by its very nature, the 'single source of truth for identity and attribute data[8].' It perpetually consumes internal sources of data such as HR and ERP systems for managing the user identity lifecycle-hire, any change in user's role or responsibility, and termination[8]. This is exactly what is required to overcome one of the biggest hurdles in ABAC implementation: Attribute governance. By making the IGA the PAP, just by design and operation of the system, this problem is addressed.

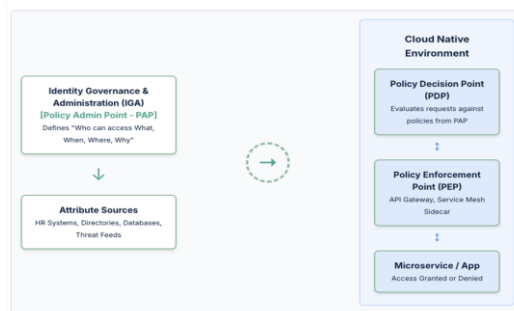


Figure 2: Integrated Policy Architecture

This model elevates the IGA system to a unified Policy Administration Point (PAP). It authors, manages, and distributes fine-grained ABAC policies directly to Policy Decision Points (PDPs) co-located with cloud-native applications.

B. The Continuous Policy Lifecycle

The IGA-as-PAP model enables the uninterrupted, fully-automated policy lifecycle that fundamentally evolves access management. This is a dynamic feedback loop ensuring security posture alignment with the state of business operations. An administrator initiates orchestration by defining a new policy within IGA/PAP using attributes from any trusted source—typically HR systems[4]. As soon as the policy gets approved and activated, it leads to further steps of orchestration where distribution to all relevant distributed PDPs—which are located wherever needed across the cloud-native environment—is carried out[6,7]. When a user or service tries to access some resource, local PEP intercepts invocation and submits it to colocation PDP for decision-making in real-time based on policies received from IGA/PAP and attributes obtained from PIP[6,7]. Such a continuous lifecycle practically brings about Continuous Authorization.

IV. TECHNICAL IMPLEMENTATION AND ANALYSIS

The architectural success of the unified IGA-ABAC model depends on a secure, scalable, and low-latency policy distribution mechanism. The best fit is a hybrid model where the centralized IGA/PAP acts as an event-driven publisher of policies while distributed PDPs act as subscribers[9]. Such architecture is realizable via asynchronous messaging leveraging a message queue. The major benefits of using this pattern are decoupling and fault tolerance added with scalability[10].

The split of PAP and PDP is an architectural decision that answers the performance concern[6,7]. The PAP is an administrative function, while the PDP needs to perform a real-time low-latency decision for every access request. By implementing PDPs as local components, there would be a co-located decision with microservices hence reducing network latency[6,7]. Therefore, with such architectural separation, the centralized nature of policy governance does not bring about system performance degradation.

The model is designed to work in hybrid and multi-cloud. As an element of the grand IGA/PAP architecture, it offers a single interface for policy management that can cover on-premises data centers, private clouds, and public cloud providers in unison[11]. The architectural premise logically supports what is being marketed as one of the "core" capabilities in CNAPPs – Centralized Compliance and Permissions Management.

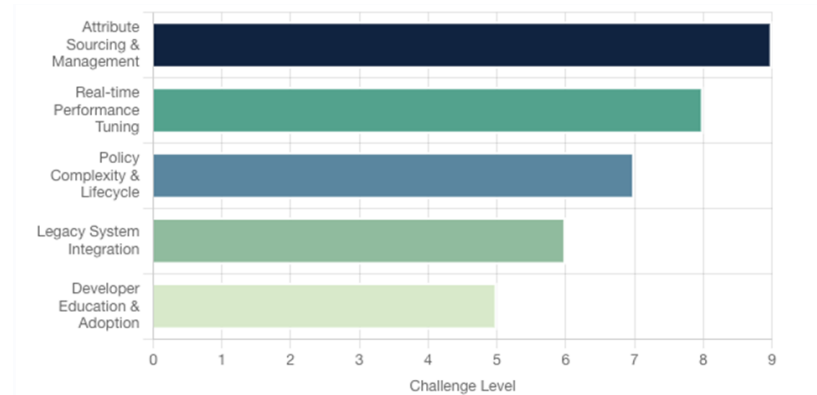


Figure 3: Implementation Considerations

While powerful, this model requires careful planning. Success depends on robust attribute management, performant policy evaluation, and clear policy lifecycle governance

V. DISCUSSION AND IMPLICATIONS

A. Benefits of the Unified Governance Model

The unified governance model seamlessly merges IGA and ABAC delivering several key advantages for security, compliance, and operational streamlining. Security is optimized by diminishing the attack surface while ensuring the best practice of applying the principle of least privilege via detailed policy-based access decisions that are contextually aware[10]. Therefore, there is a simplified means for attaining and maintaining compliance since a single, auditable source exists for all access policies removing manual, error-prone spreadsheets so readily available to show that an organization is in conformance with regulatory standards such as GDPR and HIPAA.

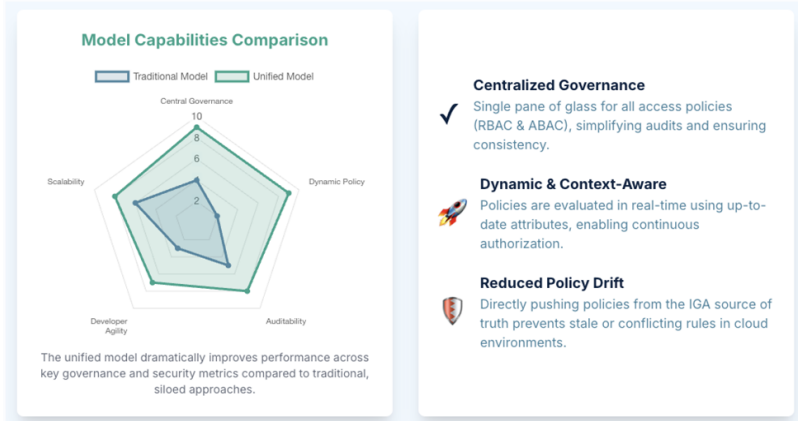


Figure 4: Key Benefits of a Unified Model

B. Alignment with Modern Security Paradigms

This proposed unified IGA-ABAC model is, therefore, not just an architectural framework that would align with the most advanced security paradigms but also serves as an enabler[10]. It verifies access dynamically based on a set of attributes thereby transforming the "never trust always verify" principle into a practical architecture[12]. In addition, this model happens to be one of the foundational pieces for the continuous authorization that validates user access rights constantly and consistently within an active session[10].

Table 2 explicitly maps how each of the components in the proposed model directly tackles known security challenges within modern, distributed environments.

Table 2 : Mapping Model Components to Security Challenges

Identified Challenge	How the Proposed Model Addresses It
Siloed systems	IGA-as-PAP: Centralizes identity and policy management into a single, unified platform, eliminating disparate, manual processes and providing a single source of truth for governance across the entire enterprise.
Policy sprawl	Centralized IGA/PAP: Provides a singular, enterprise-wide location for creating, storing, and managing all attribute-based policies, preventing the creation of overlapping or conflicting rules across different teams and applications.
Lack of visibility	Centralized Audit Trail: The IGA platform provides comprehensive logs of all identity and access-related activities, offering a top-down view of security posture and providing data for risk assessment and forensic analysis.
Manual errors	Policy-based Automation: The model automates access reviews, provisioning, and deprovisioning based on predefined policies, reducing the risk of mistakes caused by manual processes such as overprovisioning or undetected orphaned accounts.

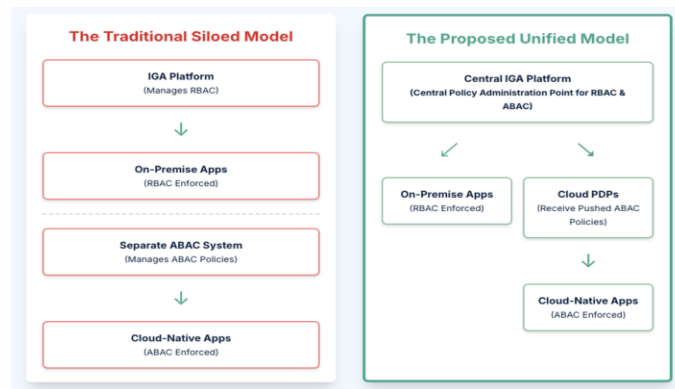


Figure 5; From Siloed Operations to Unified Governance

VI. CONCLUSION

This paper has detailed a new architectural model that brings together Unified Identity Governance and Administration (IGA) with Attribute-Based Access Control (ABAC), which combines into a dynamic and comprehensive security framework for microservices and cloud-native applications. The main principle presented as part of this model is redefining the IGA platform to now function as PAP - Policy Administration Point so that there is one central mechanism serving as the authoritative source for defining and distributing all attribute-based policies. This architectural integration simultaneously solves the historic problem of siloed systems by leveraging IGA's natural strengths in centralized identity lifecycle management, compliance, and auditing to lay down a strong governance foundation for a distributed ABAC framework. The framework yields an approach to access control that is much more secure, compliant, and operationally efficient than what traditional models have provided. This model ties directly into modern security frameworks—think Zero Trust, think continuous authorization—taking them from high-level ideas and making them into a real, usable architecture.

Future work in this regard should prioritize the creation of a formal standardized policy language that can easily be used to communicate between an IGA/PAP of governance orientation and a distributed technical ABAC system. This should be followed by a proof-of-concept implementation accompanied by an extensive performance analysis to validate the current model's claimed performance metrics. The injection of artificial intelligence and machine learning into such unified IGA/PAPs may become transformative, enabled by such centralized venues for anomaly detection that recommend risk-based enhancements to policies and automate compliance activities.

VII. REFERENCES

- [1] V. C. Hu et al., “Guide to Attribute-Based Access Control (ABAC) Definition and Considerations,” NIST Special Publication 800-162, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2019. doi: 10.6028/NIST.SP.800-162.
- [2] F. Vaz and J. Ferreira, “RBAC and ABAC Models: A Comparative Analysis for Security in IoT Environments,” in 2020 IEEE International Conference on Cyber Security and Resilience (CSR), 2020, pp. 37-42.
- [3] A. J. Yawn and T. Hicks, “Identity Governance and Administration Powered by Risk Context: Taking Access Control to the Next Level,” SANS Institute, SANS Whitepaper, Oct. 2023. [Online]. Available: <https://www.sans.org/whitepapers/identity-governance-and-administration-powered-by-risk-context/>
- [4] N. Farhadighalati, L. A. Estrada-Jimenez, S. Nikghadam-Hojjati, and J. Barata, “A Systematic Review of Access Control Models: Background, Existing Research, and Challenges,” IEEE Access, vol. 13, pp. 101–115, 2025.
- [5] I. Al-Sarayeh, A. Yasin, M. Tawalbeh, and S. Awwad, “A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues,” Sensors, vol. 20, no. 14, p. 3918, 2020, doi: 10.3390/s20143918.
- [6] R. Singh et al., “Decentralized Policy Information Points for Multi-Domain Environments,” arXiv, 2021. [Online]. Available: <https://info.arxiv.org/help/submit/index.html>.
- [7] N. Farhadighalati, L. A. Estrada-Jimenez, S. Nikghadam-Hojjati, and J. Barata, “A Systematic Review of Access Control Models: Background, Existing Research, and Challenges,” IEEE Access, vol. 13, pp. 101–115, 2025.
- [8] M. M. A. Hasan, M. A. H. Abedin, and K. M. T. T. Al-Muztaba, “A Survey of Access Control Models and Their Applications in Cloud Computing,” J. Comput. Sci. Technol., vol. 39, no. 5, pp. 1010–1025, 2024.
- [9] T. Reese, “Your Guide to Identity Governance and Administration (IGA),” Netwrix Blog, Aug. 20, 2024. [Online]. Available: <https://blog.netwrix.com/what-is-identity-governance-and-administration>
- [10] D. Cahill, “A Modern Approach to Identity Governance and Administration,” Enterprise Strategy Group, Research Insights Paper, Apr. 2021. [Online]. Available: <https://omadaidentity.com/wp-content/uploads/2021/05/ESG-Research-Insights-Paper-Omada-Modern-IGA-Apr-2021.pdf>
- [11] K. Bowman, “The Interplay of IGA, IAM and GRC for Comprehensive Protection in Cloud Transitions,” ISACA, Industry News, July 2023. [Online]. Available: <https://www.isaca.org/resources/news-and-trends/industry-news/2023/the-interplay-of-iga-iam-and-grc-for-comprehensive-protection-in-cloud-transitions>
- [12] Z. A. Abualkibash, B. H. Z. Abualkibash, and M. M. S. Al-Enezi, “Zero Trust Cybersecurity: Procedures and Considerations in Context,” *Applied Sciences*, vol. 14, no. 12, p. 4811, 2024, doi: 10.3390/app14124811.