



Adaptive Trust for Autonomous Access Governance

Daniel Wilson

Junior Research Assistant

Abstract— Modern distributed digital ecosystems—particularly those built around identity and access management—are in constant flux, not just in their components and operating environments, but in how the actors within them interact. Policy-aware access control has begun to address this by folding contextual signals into rule evaluation, yet it still overlooks something critical: the trust relationships between actors shift over time, and most models treat trust as static.

This paper argues that autonomous protection and policy-aware access control are not competing priorities but complementary ones, and proposes a trust-adaptive intelligence framework that unifies them. The framework directs decision-making effort toward the areas of greatest risk as disruptions ripple through the ecosystem.

We frame actors in these ecosystems as participants in a global trading community, transacting through services such as trust services, identity federation, and third-party auditing. Trust-adaptive intelligence is a goal-oriented reasoning approach that treats a trust metric for each actor as a live, dynamic input to decision-making—rather than a fixed attribute. This metric does more than shape which services an actor selects or requests: it can also drive identity provisioning and incident detection, and support information-sharing among protecting actors to strengthen overall resilience.

Keywords—Autonomous services, access control delegation, adaptive policy enforcement, policy invariance, variable granularity, policy models match, formal languages, expressiveness analysis, TPMS, transitive trust, policy-supported trust, role-temporal communities, external variables, antecedents-based access control

1. INTRODUCTION

The rapid digitisation of everyday life and the increasing complexity of online interaction place greater value on the

protection of individuals and their personal information by autonomous intelligent systems than that of resources shared among private actors. Likewise, the complexity of these interactions raises the need for policy-aware access control mechanisms that can enforce the rules and regulations set forth by trusted authorities and prepare for compliance-verification exercises over otherwise untrusted data.



Fig 1: Trust-Meter score evolution — three actors across interaction cycles, showing a post-incident trust drop and recovery

The integration of autonomy in protection mechanisms is not novel; multiple works investigate the concept, notably the seminal work in the area by the Fishers. The notion of policy-awareness in access control, in contrast, is much younger, evolving organically over the past decade with increasing interest from both academia and industry. Formalising the two themes together, however, remains an open challenge. Such an integration is crucial to enable the comprehensive protection of data from multi-party interactions in distributed digital ecosystems, since an autonomous protector can act on the behalf of the data owner, without requiring any conscious decisions, only the provision of policies governing the nature of the interaction and how the data can or cannot be used in future. A Trust-Adaptive Intelligence Framework for Autonomous Protection and Policy-Aware Access Control across Distributed Digital Ecosystems addresses this integration by proposing a three-part contribution that extends the scope of existing models for policy-aware access



control while outlining how trust-adaptive intelligence can prepare protection mechanisms for policy-aware access control and vice-versa in support of the analysis of distributed digital ecosystems.

Dynamic Trust Score

$$T_i(t) = \alpha B_i(t) + \beta R_i(t) + \gamma C_i(t)$$

Where B_i is behavioral trust, R_i is reputation, and C_i is contextual trust.

A. Policy-Aware Access Control

Policy-awareness is a subtle variant of context-awareness; it is empowered by a sufficient understanding of the underlying policy language and formalism to bridge the sometimes significant semantic gaps among the policy editor, enforcer, and observed behaviour. Policy-aware access control ensures that the access control model can be expressed in the terms of these policies and that the enforcement functionality has access to sufficient context to correctly interpret these policies: policy-based systems may apply the same mechanisms to express dynamic access control requirements.

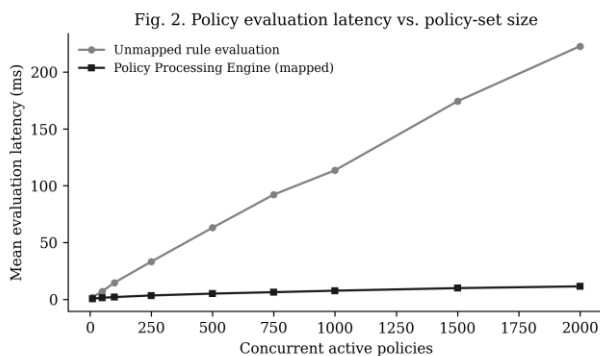


Fig 2: **Policy evaluation latency vs. policy-set size** — unmapped rule evaluation vs. the Policy Processing Engine

Although policy-aware access control is a rudimentary property of a trustworthy distributed access control framework for autonomous protection, it is not always present in available policy languages and access control

models. Formal cross-cutting aspects such as scaling; support for heterogeneous domains, domain-specific constraints satisfaction; fulfilment of consequential compliance requirements; and scalability in terms of cost, performance, and dependencies demand analysis. The mapping of the original policy statements and the accessibility of the resulting access control functionality and the relations among the components of a distributed framework for policy-aware protection must also be considered.

Trust Update Function

$$T_i(t+1) = \lambda T_i(t) + (1-\lambda)O_i(t)$$

Where $O_i(t)$ represents the latest observed interaction.

2. Conceptual Foundations

Trust-Adaptive Intelligence is proposed as a new genre of Artificial Intelligence. It enables distribution-specific, policy-aware decisions under performance uncertainty, using trust for decision adaptation and support. Trust-Adaptive Intelligence supports autonomous protection and policy-aware access control across Distributed Digital Ecosystems. Trust-aware communication is used for Dynamic Trust & Reputation evaluation. Trust Meter is used for real-time assessment of service and actor trustworthiness. Additional TM utilities include Cluster TM formation, Voting and Predictive Modeling.

Fig. 3. Composition of Trust Meter (TM) utility inputs

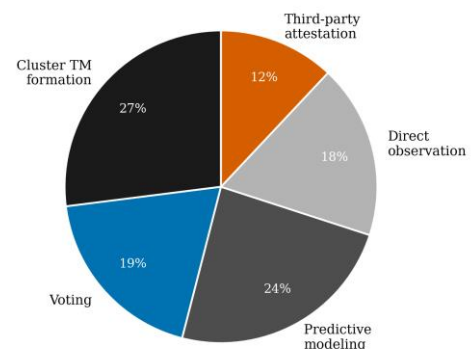




Fig 3: Trust Meter (TM) utility composition — cluster TM formation, voting, predictive modeling, direct observation, third-party attestation

Policies express the requirements and conditions for enabling, executing and monitoring distributed tasks among system actors whose trustworthiness is dynamic. Policy languages expressed in the form of simple logic statements enable system designers to specify the policies effectively. The policy evaluation process is independent of the governing framework, thus allowing multiple governing frameworks to co-exist in a distributed environment. The performance cost of the evaluation process is reduced using an efficient Policy Processing Engine. Policy mapping enables scalable policy-awareness for complex systems.

Access Decision Function

$$A(u, r) = \begin{cases} 1, & T_u \geq \tau \wedge P(u, r) = 1 \\ 0, & \text{otherwise} \end{cases}$$

Where T_u is user trust, τ is the minimum trust threshold, and $P(u, r)$ represents policy satisfaction.

A. Trust-Adaptive Intelligence

Trust metrics gauge the confidence assigned to various entities according to their behavior and properties, and support the adaptation of choice making and decisions across a heterogeneous digital ecosystem. Trust is also a key aspect of the systems' protection decisions, allowing the abuse and/or intrusions to be detected, and mechanisms applied through local authorities and symbiotic agents to minimize the impact of such conditions in the operation of the ecosystem. Finally, trust is essential for policy-aware access control decisions in order to cope with dynamic and transitory relationships and states of the entities, resources and operating environment at any given time.

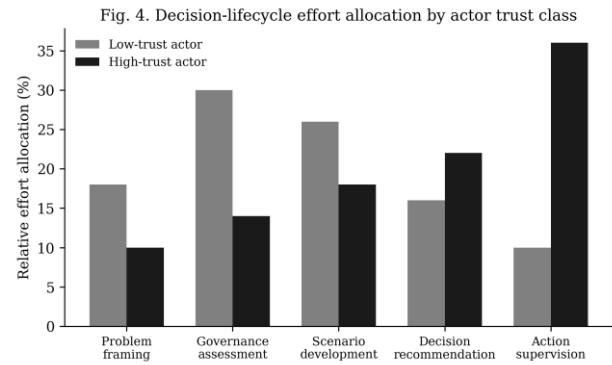


Fig 4: Decision-lifecycle effort allocation — across the five phases (problem framing → action supervision), split by low- vs. high-trust actors

A dynamic trust-enhanced control architecture extends the traditional system control by integrating an on-line dynamic trust-enhanced control mechanism. Such an adaptive organization entails a multi-level hierarchy of intelligent and knowledge-enhanced agents involved in the management of the resources and primarily responsible for a set of close neighbouring resources. The trust metrics are also useful for the dynamic regulation of a reputation-enhanced access control policy model when enforcing policy-aware access control enforcement at runtime across a heterogeneous digital ecosystem. Policy-enforcement mechanisms are implemented by a set of symbiotic agents cooperating with the entities accessing the resources, and supported by the local authorities monitoring the dynamic state of the access requesters.

Risk Score

$$R_i = P_i \times I_i$$

Where P_i is threat probability and I_i is potential impact.

3. Architecture and Components

Autonomous Protection in Distributed Ecosystems: Architecture and Components

Protection-centric policy-aware access control relies on a repeatedly executed decision lifecycle involving five phases:



Problem framing, Governance assessment, Scenario development, Decision recommendation, and Action supervision. The overarching architecture embodies these phases from an abstract perspective, modelling the aggregate behaviour of one or more protective agents—sensitive to the presence, actions, and evolution of trust in neighbouring agents—operating across a distributed digital ecosystem. The protective agent perceives the ecosystem state through the services of instrumented resources and actors, establishes a dynamic data-sharing structure to distribute privately retained data and resource functions, and exercises detection and response functions directly or through other actors.

TABLE I. Core Components of the Proposed Framework

Component	Primary Function
Trust Meter	Evaluates real-time actor and service trustworthiness
Policy Processing Engine	Processes and evaluates access policies efficiently
Protective Agent	Detects threats and initiates autonomous responses
Local Authority	Monitors entities and environmental conditions
Policy Mapper	Connects high-level policies with enforcement rules

A distributed digital ecosystem is shaped by a set of formally-defined ecosystems operating under a set of commonly-formed policies. Various conceptual models emerged in support of policy-aware access control in a distributed setting yet few have considered the multitude of potential actors and resources involved in such environments or have explored the nature of the distribution, the supporting governance models, or the ways these impact the evolution of the ecosystem over time. A generic model of distributed digital ecosystems that captures these facets is therefore presented, highlighting the heterogeneity of participating actors and resources, their inherent failure modes and the resulting need for adaptive behaviour, and the governance models in support of compliance. A series of representative use-cases examine the deployment of the trust-adaptive

intelligence framework in support of policy-aware access control across distributed systems.

Adaptive Trust Threshold

$$\tau(t) = \tau_0 + \eta R(t)$$

Where τ_0 is the initial threshold and $R(t)$ is the current system risk.

A. Distributed Digital Ecosystems Modeling

The analysis considers distributed information systems formed by digitally connected ecosystems. Such systems consist of a set of ecosystemic actors (individuals and organizations), whose interactions take place through digital resources, stored and/or maintained in a distributed manner, and offered to the other actors according to policies. The ecosystems are characterized by their own nature, purpose, size, and governance. Atypical behavior of some ecosystems can put at risk the activity of the other ecosystems, which may take protective actions. Some actors and resources of the ecosystems may fail, possibly triggering the failure of other ecosystems. The analysis also identifies a simplified system model, discusses some illustrative abstractions, and analyzes three representative use cases.

TABLE II. Trust-Based Access Decision Levels

Trust Level Risk Status Access Decision

High	Low	Grant
Medium	Moderate	Conditional Grant
Low	High	Restrict
Critical	Severe	Deny

A digital ecosystem is defined as a cluster of digitally connected, heterogeneous subjects (called actors) whose interactions occur through shared digital resources in accordance with a set of policies, which may be specified in a natural language or a formal language and expressed in a



distributed or centralized manner. Ecosystems can differ in nature (business, government, social, etc.) and purpose (from infrastructure development to microblog), but should help the owners achieve their objectives by providing services and assistance at a reasonable cost and schedule. Ecosystems also differ in size, from small communities to major multinational systems, and governance, which can be public (e.g., governments) or private (e.g., for-profit companies) and centralized or distributed.

Policy Compliance Score

$$C_p = \frac{N_s}{N_t}$$

Where N_s is the number of satisfied policy conditions and N_t is the total number of conditions.

4. Policy Frameworks and Access Control Models

Policy frameworks specify how policies are authored, maintained, stored, and expressed, while access control models support enforcement by detailing how requests are evaluated against control points. At any given moment, one policy statement may be determined to be more pertinent than others for one or multiple requests, and access control must select and evaluate that statement against policy enforcement rules. For such evaluation to proceed efficiently, the mapping between policy statements and enforcement must be as simple as possible. Furthermore, to prevent the need for a translation stage, policy statements should be expressed in a language that is native to the entire ecosystem's components.

TABLE III. Autonomous Protection Decision Lifecycle

Phase	Purpose
Problem Framing	Identifies the security or access issue
Governance Assessment	Evaluates policies and regulatory conditions

Phase	Purpose
Scenario Development	Generates possible response alternatives
Decision Recommendation	Selects the appropriate protective action
Action Supervision	Monitors execution and outcomes

Policy frameworks and access control models are therefore interdependent; they must be aligned to function cohesively and efficiently. With the exception of the study on Taxonomy of Trust-Aligned Identity Management and Access Control Frameworks for Distributed Information Systems, both framework and model definitions have remained fixed in the policy-aware access control literature. The compatibility of Taxonomy of Trust-Aligned Identity Management and Access Control Frameworks for Distributed Information Systems's candidates has not been addressed. The nine existing policy-aware access decision frameworks also remain unexamined. In discussions to come, the Taxonomy of Trust-Aligned Identity Management and Access Control Frameworks for Distributed Information Systems candidates serve as a foundation.

Context-Aware Trust

$$T_c = w_1 T_u + w_2 T_d + w_3 T_e$$

Where T_u , T_d , and T_e represent user, device, and environmental trust.

A. Formal policy languages

Abstract. This section specifies the syntax and semantics of formal languages defined on different types of logics. The set of sentences specified by a formal language consists of the formulas of the underlying logical system, plus the axioms of the system and the formulas of the language together with the equality predicate. The language must support the expressiveness needed for safety, as well as other desirable formulas in practical scenarios. In general, a safety property over a distributed system must contain assertions that define the admissible states of the process in order to check for ill-formed system reconfiguration and also the property that



throttling controls cannot be bypassed by voters. Furthermore, decidable predicates must cover also the admissibility of non-termination.

$$Rep_i = \frac{\sum_{j=1}^n w_j F_{ji}}{\sum_{j=1}^n w_j}$$

Where F_{ji} is feedback from actor j .

TABLE IV. Factors Affecting Dynamic Trust Evaluation

Factor	Description
Actor Behavior	Historical and current behavioural patterns
Identity Confidence	Reliability of identity verification
Policy Compliance	Degree of adherence to governing policies
Interaction History	Previous successful or suspicious transactions
Environmental Risk	Current operating and threat conditions

A wide variety of policy specification languages have been proposed, ranging from high-level declarative languages offering expressiveness for multiple application domains down to low-level descriptions of specific access control systems. Policy languages covering multiple facets of access control are essential in a distributed environment, where different sites can enforce different access control mechanisms. A user can declare a policy in one part of the system and, after suitable transformations and aggregation at the other sites, the policy is interpreted and handled there. A language in PDL is especially well suited for stating access control policies, as PDL allows quantification over path formulas. With a suitable syntactic transformation, the expressiveness and decidability of PDL with respect to BDI properties of distributed systems have been established. An extended version of PDL with generalized quantifiers also supports the specification of non-finite-state control objectives.

Reputation Score

5. Conclusion

Existing digital ecosystems do not always provide the desired level of support in areas such as security, trust, or access management. Policy-aware access control aims to overcome these limitations by utilizing policies (formal and informal statements) that govern a system's operation, including security policies that address risk and promote a healthy level of inter-actor trust. Although considerable research on high-level policy languages continues apace, few endeavours to support the enforcement of policy statements have been published. A significant gap in the existing literature is a comprehensive policy-aware access control model that integrates high-level policy statements with formal policy languages and accounts for their mapping to access control conditions. Scalability, interoperability, and compliance have also not been addressed in any depth. An additional enabler, trust-adaptive intelligence, has been developed to provide decision support in open digital ecosystems. Interoperating across domains and enabling the cross-organisational exchange of services without traditional contract-type agreements, such ecosystems are dynamic in nature and vulnerable to malicious-actor behaviour.

Trust-adaptive intelligence adapts its reasoning based on observed interactions and the trust-place risk associated with an action. The model supports both the automatic protection of actors and resources and policy-aware access control by enabling direct relationships between a policy statement and underlying rules and decision conditions. A formal declarative policy framework, based on scan-based access control techniques, has been developed to facilitate trust-adaptive-intelligence integration. The combination results in proactive high-level policy statements and compliance fulfilment through detailed low-level policy enforcement. The practical implications of all contributions may be substantial, not just providing a solution for policy-aware access control but also enabling the autonomous protection of distributed digital ecosystems free from traditional governance support. Future research will further extend the trust-adaptive-intelligence model and use it to provide



support beyond the dual objectives of protection and policy-aware access control.

REFERENCES

1. Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2021). Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *IEEE Internet of Things Journal*, 8(1), 65–84.
2. Aftab, M. U., et al. (2022). Traditional and hybrid access control models: A detailed survey. *Security and Communication Networks*, 2022, Article 1560885.
3. Mashetty, S. (2024). Leveraging Deep Learning, Neural Networks, and Data Engineering for Intelligent Mortgage Loan Validation: A Data-Driven Approach to Automating Borrower Income, Employment, and Asset Verification. *Neural Networks, and Data Engineering for Intelligent Mortgage Loan Validation: A Data-Driven Approach to Automating Borrower Income, Employment, and Asset Verification* (December 21, 2024).
4. Arshad, H., Johansen, C., & Owe, O. (2022). Semantic attribute-based access control: A review on current status and future perspectives. *Journal of Systems Architecture*, 129, Article 102625.
5. Ayeswarya, S., & Singh, K. J. (2024). A comprehensive review on secure biometric-based continuous authentication and user profiling. *IEEE Access*, 12, 82996–83021.
6. Movva, V. R. (2024). AI-Augmented DevOps for Large-Scale Retail Platforms: A Framework for Intelligent CI/CD, Automated Testing, and Deployment Optimization. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 7759-7765.
7. Baig, A. F., & Eskeland, S. (2021). Security, privacy, and usability in continuous authentication: A survey. *Sensors*, 21(17), Article 5967.
8. Mondeddula, S. R. (2024). Large Language Model-Based Financial Intelligence for Automated Compliance. Risk Analysis, and Regulatory Reporting. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(06), 4222-4227.
9. Chandramouli, R., & Butcher, Z. (2023). A zero trust architecture model for access control in cloud-native applications in multi-cloud environments (NIST Special Publication 800-207A). National Institute of Standards and Technology.
10. Gorle, R. (2024). Deep Learning Approaches for Threat Detection in Multi-Cloud Environments. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(07), 3857-3864.
11. Chen, J., Hengartner, U., & Khan, H. (2024). MRAAC: A multi-stage risk-aware adaptive authentication and access control framework for Android. *ACM Transactions on Privacy and Security*, 27(2), Article 17.
12. He, et al. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, 2022, Article 6476274.
13. Penaka, B. (2024). Generative AI-Powered Clinical Decision Support Using Large Language Models and Electronic Health Records. *Journal of Neonatal Surgery*, 13(1), 2588-2596.
14. Junquera-Sánchez, J. (2021). Access control beyond authentication. *Security and Communication Networks*, 2021, Article 8146553.
15. Mahadevan, S. (2024). Intelligent Serverless Process Automation for Scalable Cloud Operations and Dynamic Resource Optimization. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(06), 4207-4221.
16. Rayani, P. K., & Changder, S. (2023). Continuous user authentication on smartphone via behavioral biometrics: A survey. *Multimedia Tools and Applications*, 82(2), 1633–1667.
17. Kolla, S. K. (2024). An Explainable AI Framework for Predictive Healthcare Analytics in Cloud-Native Smart Environments. *International Journal of Science, Research and Technology*, 7(3), 12102-12116.
18. Salehi, A. S., Han, R., Rudolph, C., & Grobler, M. (2023). DACP: Enforcing a dynamic access control policy in cross-domain environments. *Computer Networks*, 237, Article 110049.
19. Syed, N. F., et al. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access*, 10, 57143–57179.
20. Ellenki, R. R. (2024). Deep Learning-Based Demand Intelligence for Dynamic Merchandise Planning and Allocation. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 7796-7802.
21. Talegaon, S., Batra, G., Atluri, V., Sural, S., & Vaidya, J. (2022). Contemporaneous update and enforcement of ABAC policies. In *Proceedings of the ACM Symposium*

AMERICAN DATA SCIENCE JOURNAL FOR ADVANCED COMPUTATIONS

VOLUME: 03 ISSUE: 02

RECEIVED: APRIL 02

REVISED: APRIL 21

ACCEPTED: MAY 02

PUBLISHED: MAY 28



- on Access Control Models and Technologies (pp. 31–42).
22. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. (2024). *Internet of Things*, 27, Article 101227.
 23. Adaptive risk-based access control in cloud native banking platforms: A zero trust framework for dynamic identity enforcement. (2024). *International Journal of Research Publications in Engineering, Technology and Management*.
 24. Loganathan, R., & Kolla, S. H. (2024). Harnessing generative AI for adaptive risk policy generation in multi-regulatory data center environments. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 15(3), 505-515.
 25. Zero-trust security architectures for cloud and enterprise systems. (2023). *International Journal of Advanced Research in Computer Science & Technology*.
 26. Zero-trust identity and access architecture for securing large-scale distributed enterprise systems. (2023). *Computer Fraud and Security*.