



Trust-Driven Governance for Secure Enterprise Delivery

1st Shabrinath , 2nd Luca Romano

Shabrinath Motamary, Software/Systems Architect , motamaryshabrinath@gmail.com
Luca Romano , Graduate Research Assistant

Abstract— Delivering corporate-sensitive, data-rich information and seamless access to enterprise software for employees, business partners, and external contractors through cloud environments offers firms substantial potential benefits. These advantages, however, have also given rise to black swan events—unexpected, highly damaging incidents rooted in thin or even non-existent risk management processes and procedures. This situation demands a rethinking of legacy information governance concepts and solutions originally designed for traditional, perimeter-protected corporate environments. A fundamental digital transformation is therefore becoming essential, one that must drive both technical and managerial change grounded in agility, scalability, flexibility, robust business continuity planning, and regulatory compliance. As a result, concerns over corporate information security and trust have intensified sharply in recent years. Addressing both dimensions together calls for a thorough examination of how governance processes and procedures can be supported through a trust-centric cloud intelligence management model.

This paper presents a conceptual framework that supports an autonomous access governance solution. Grounded in a trust-centric cloud intelligence approach, the proposed framework aims to narrow the gap between internal and third-party management and business functions during software deployment and use. Cloud-based services are frequently requested and adopted without IT function approval, thereby violating existing corporate digital governance frameworks—frameworks specifically designed to ensure business continuity and legal compliance.

Keywords—Cloud Computing, Cloud Intelligence, Administrative and Access Governance, Trust Management,

Trust-Centricity, Cooperative and Autonomous agents, Software as a Service, Software Supply Chain, Enterprise Software Security.

1. INTRODUCTION

Cloud computing has opened a plethora of new possibilities for Information Technology (IT) and enterprises. Cloud services enable organisations, ranging from small, single-location businesses to multinational conglomerates, to easily use a broad range of services. These include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Security as a Service (SECaaS), Database as a Service (DBaaS), and many others. The cloud service provisioning model, however, introduces new complexities with respect to data and service governance. Autonomous Access Governance (AAG) is introduced as a set of functions and facilities for governing access to cloud-based resources without any direct human involvement throughout the governance lifecycle — from defining the access policies to performing the actual access request and granting operations.

Existing approaches and solutions that relate to AAG examine individual parts of the access governance lifecycle, and they are often deployed in isolation. A lack of integration among them inhibits realising the full potential and value of AAG. A more economical, reliable, and scalable solution can be achieved by addressing the autonomous access governance lifecycle collectively and systematically. A Trust-Centric Cloud Intelligence Framework (TCCIF) enables such a coherent approach. It uses cloud intelligence to collect and analyse evidence from multiple trustworthy sources, including other cloud services, users, and their devices, to continuously establish and maintain a trust model

for supplier-consumer pairs. The trust model is then queried to autonomously govern access to the supplier’s resources for the consumer’s requests.

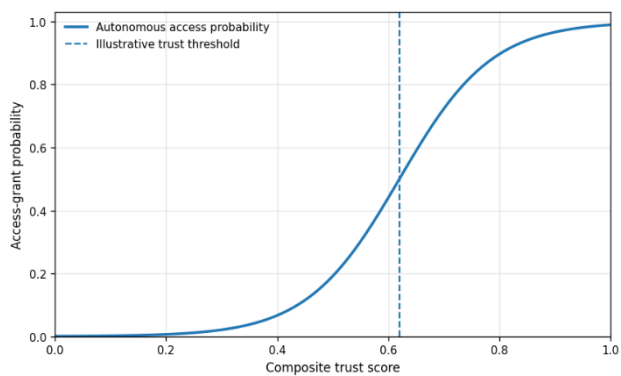


Fig. 1 — trust score trajectory for stable vs. erratic behavior against the autonomy threshold

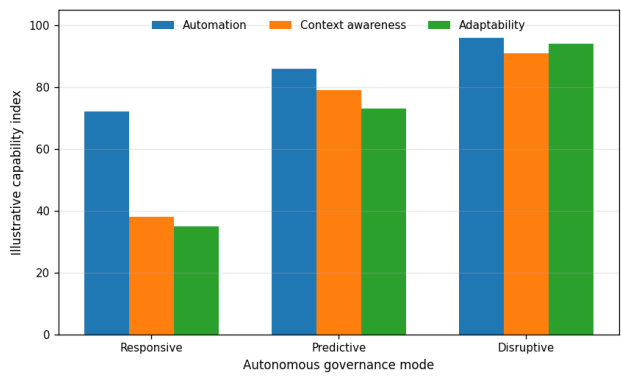


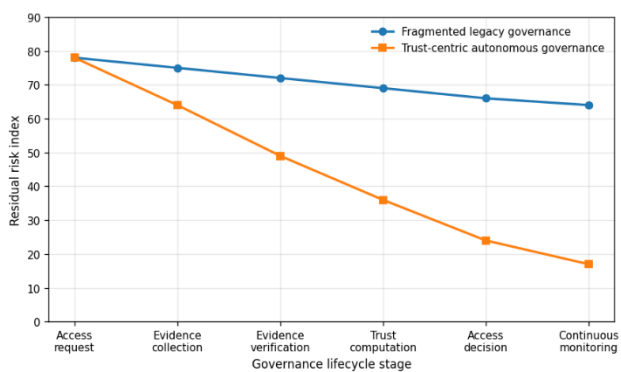
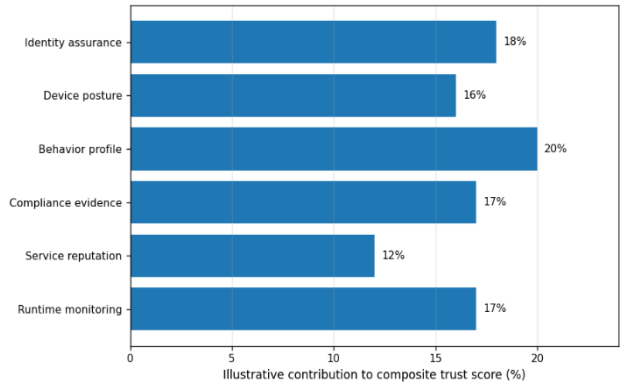
Fig. 2 — indicative weighting of evidence dimensions feeding the trust score

A. Autonomous Access Governance: Definitions and Scope

Autonomous access governance is understood conceptually, parametrically, and operationally. Conceptually, it refers to the removal of human effort from the management and operation of access governance processes, be they physical, conceptual, or logical. Such processes liaise between systems, services employing these systems, and the individuals who operate such services and systems. It pertains to the autonomous, self-service provisioning, deprovisioning, and/or management of access in other forms, such as identity, authentication, or authorisation. It encompasses three types of process automation: responsive, predictive, and disruptive.

In terms of taxonomy, it is an apex concept supported by two subcategories. For autonomous access governance to be achieved in practice, true, automated, intelligent, and contextual fulfilment of access requests is paramount. Such fulfilments of access requests must rely on a risk posture, associated with a unified and configurable organisation-wide risk management strategy. This subordinate category forms responsive autonomous access governance. This remains contextually blind to the fulfilment process. Predictive

fulfilment of access requests addresses such context, by leveraging historical patterns and trends in access behaviour.



2. Conceptual Foundations

The framework is grounded in a trust-centric perspective, converging cloud computing, multi-agent systems, and intelligent agents, specifically: (i) the suite of security requirements underscoring the provision of trustworthy services in the cloud; (ii) the decentralised provision and management of services while enabling information sharing and collaboration among enterprises; and (iii) the cloud intelligence application areas that require autonomous agents able to operate within particular IoT ecosystems.

The alliance of these perspectives produces a trust-centric cloud intelligence architecture enabling the autonomous governance of access permissions and the shielded, trustworthy delivery of enterprise software in the cloud. Its self-governed operation manages and verifies the trust information required by its agents to act and make decisions autonomously, thus facilitating both the adoption of cloud computing services with the appropriate trust characteristics and enterprise cooperation.

Table I — Core Architectural Components and Interfaces

Component	Acronym	Primary Role
Trust Evidence User	TEU	Requests generation of trust evidence for a target cloud service (e.g., service desk, EMM solution)

Component	Acronym	Primary Role
Trust Evidence Provider	TEP	Produces and supplies trust evidence based on monitored attributes (compliance, reputation, SLA history)
Autonomous Decision Maker	ADM	Consumes trust evidence to independently deploy software and govern security-sensitive access decisions
Cloud Service Monitor	CSM	Observes monitored cloud operations and reliably reports on their execution
Service Provider (Trusted Third Party)	SP	Validates supplier trustworthiness using a threshold scheme and mediates SLA-based risk sharing

Table II — Autonomous Access Governance: Automation Types

Automation Type	Contextual Awareness	Governing Basis
Responsive	Context-blind	Unified, configurable organisation-wide risk posture
Predictive	Context-aware	Historical patterns and trends in access behaviour
Disruptive	Context-transformative	Emergent trust signals prompting policy re-evaluation

A. Trust-Centricity in Cloud Intelligence

A central aspect of Artificial Intelligence (AI) in the Cloud is the form of Cloud Intelligence (CI), i.e., the AI operating as a service provided within the Cloud model. This central aspect of CI must be influence able, trustworthy, and understandable. Influenceable – because, despite the data on which the AI was trained are with the owner of the data, the outcome of the trained AI could be influenced by malicious third parties – for example Cloud providers against their customers or by government agencies influencing the CI algorithms. Trustworthy – because everything is in the Cloud and therefore trust in its correctness is more than crucial. Understandable – because the CI Owner must validate the automatic AI actions and also generate the data for the AI to learn.

This becomes relevant when more than one expert in a Field is absent for a long time, and different AIs in the same Field start making decisions without them being verified. Therefore, governing the AIs becomes of extreme importance before the worst happens. Input from the owner of the data and from experts could fulfill these requirements. The desired properties would be fulfilled by two parties: the CI Owner and an Expert Group influenced by but not dependent on the CI. This thesis proposes a conceptual framework that addresses and ensures influenceability, trustworthiness, and understandability as seal of trust without impairing the autonomous operation of CI.

3. Architectural Overview

An overview of the proposed trust-centric cloud-intelligence architecture is provided initially. The architecture includes three core components: software suppliers, enterprise users, and relying party services. These are integrated in a symmetric manner to establish trust-based communication paths for securely deploying enterprise software services. The functions of the various components are then summarised, as well as the connections between them.

The provision of enterprise software-as-a-service from untrusted sources is inherently risky. A trust-centric cloud-intelligence architecture is proposed for supporting autonomous access-governance processes that operate without user intervention. A threshold scheme is used to define trust levels, and a service provider acts as a trusted third party to validate the trustworthiness of suppliers offering enterprise software solutions. Trust evidence is analysed and stored in a decentralised manner, while trust-hierarchy information is obtained from socially linked data. A service-level agreement framework addresses different aspects of risk-sharing among involved parties.

Table III — Trust Evidence Sources and Verification Techniques

Evidence Source	Verification Technique	Example Indicator
Behavioural profile	Machine-learning anomaly detection	Deviation from stable access pattern
Compliance record	Deterministic rule/test validation	Adherence to privacy regulation
Reputation / SLA history	Statistical evaluation of service use	Historical SLA violation rate
Monitoring report (CSM)	Heuristic assessment	Reliability of reported execution
Forensic alert	Deterministic / rule-based flag	Detected misconduct or crime alert

A. Core Components and Interfaces

The architecture comprises five interrelated components that cooperate according to a set of principles and adopt open interfaces to facilitate collaboration with external trust and cloud intelligence services. Trust evidence users (TEU) request the generation of trust evidence related to certain cloud services from trust evidence providers (TEP) to support trust-based access governance policies considered by autonomous decision makers (ADM). In turn, ADMs independently deploy the software offered by the monitored cloud services and automatically govern all security-sensitive decisions about the usage of such services. Cloud services offering sensible operations to be monitored are observed by cloud service monitors (CSM), which assure that a proper execution of such operations is reliably reported. When needed, the ADMs and the CSMs cooperate for cloud service monitoring by sharing dedicated trust evidence with the monitoring reports about the detected execution.

Mathematical Formulas:

Eq. (1) — Composite Trust Score

$$T(s,c) = \sum w_i \cdot e_i(s,c), \text{ for } i = 1 \dots n, \sum w_i = 1$$

where $T(s,c)$ is the composite trust score for a supplier–consumer pair (s,c) , e_i is the normalised evidence value from source i ($0 \leq e_i \leq 100$), and w_i is its relative weight.

Eq. (2) — Autonomy / Access Decision Rule

Decision (s,c) = Grant, if $T(s,c) \geq \tau$; Restrict, if $\tau_r \leq T(s,c) < \tau$; Deny, if $T(s,c) < \tau_r$

where τ is the autonomy threshold above which access is fully granted without human intervention, and τ_r is a lower restriction threshold below which access is denied.

Eq. (3) — Trust Score Decay Over Time

$$T(t) = T(t-1) \cdot (1 - \lambda) + \Delta e(t)$$

where λ is a decay (forgetting) factor applied to prior trust, and $\Delta e(t)$ is the net evidence contribution observed at epoch t , capturing how erratic behaviour more rapidly erodes accumulated trust than stable behaviour reinforces it.

Eq. (4) — Risk-Adjusted Trust Threshold

$$\tau = \tau_0 + \beta \cdot R(s)$$

where τ_0 is the baseline organisational threshold, $R(s)$ is the risk posture associated with supplier s , and β scales the threshold upward for higher-risk suppliers.

4. Trust Model and Assurance Mechanisms

Trust is a condition that is real in its consequences but inescapably subjective. In a computing context, it enables a user to make decisions concerning an entity and rely on the services provided without fear of any potential risk. As with any model, this trust model requires two major aspects to be discovered and controlled: Trust Evidence, which expresses the participants' perspectives through a trust value in a trustworthiness dimension, and Verification Techniques, which assess this trustworthiness dimension based on the defined evidence. The user could therefore decide and act based on a given trust level, whether to continue with a

restricted set of services or applications until the level of trust increased and allowed sufficient autonomy, or to terminate the use of the service, application, or entity altogether.

Trust evidence reflects the assurance level established upon a thorough assurance process. Assurance can be considered a system performed to ensure the trustworthiness of a product or service regarding a specific trust dimension, based on a set of criteria, metrics, and evidence. The trust model encompasses a collection of assurance mechanisms requiring evidence support. The key to a successful assurance process is not only to define the set of criteria that must be fulfilled but also to decide which kind of evidence must be provided to ensure compliance with these criteria. These compliance evidences can come from many origins, such as deterministic validation through a set of tests, statistical evaluation based on service utilization, or heuristic assessment based on other users' trust decisions.

A. Trust Evidence and Verification Techniques

"Trust evidence" refers to configurations or behaviours that serve as indicators of trustworthiness. A user who exhibits stable or predictable behaviour is expected to be less suspicious than one with a largely erratic pattern of operation. Similarly, a user who accesses a limited or predictable range of resources is regarded as being less suspicious in connection with access to resources outside that pattern. Behaviour models and behavioural profiling are two well-established forms of modelling for detecting anomalies. Patterns can be identical (e.g. rule-based systems) or generated through machine learning processes.

Verification techniques function in tandem with evidence sources to support the trust model. Such techniques enable the service cloud to quantify the risk associated with a trust request and thus interpret the validity of the trust evidence from a business-compliance perspective. For example, if a forensic verification technique identifies a serious crime alert in connection with user access, it thus indicates misconduct. Detection techniques rely on robust definitions of "normal" behaviour, behaviour profiles, and/or behaviour models, typically built by machine learning methods and techniques.

5. Conclusion

The proposed Trust-Centric Cloud Intelligence framework supports enabling autonomous access governance in enterprise cloud federations, mitigating temporal risks associated with security breaches or artificial accidents. It equally accommodates secure enterprise software delivery by exploiting the underlying trust model. An alternative external usage is also considered, where the framework acts as a privacy-preserving, covert communication channel for distributed peer-to-peer environments.

The present contribution draws on several disciplines and is positioned along a complexity spectrum between pure theory and exploratory design. An explicit architecture with precisely defined module responsibilities creates a reliable foundation to support subsequent implementation work and substantiate the framework's practicality by experimental

validation. Trust and privacy are only two of the many perspectives or requirements that such a framework could fulfil; a future objective is to create an integrated service ambience that is indeed holistic.

REFERENCES

- Cao, Y., Pokhrel, S. R., Zhu, Y., & Doss, R. (2024). Automation and orchestration of zero trust architecture: Potential solutions and challenges. *Machine Intelligence Research*, 21, 294–317.
- Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of zero trust architecture (ZTA). *Computer Standards & Interfaces*, 89, Article 103832.
- He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, 2022, Article 6476274.
- 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).
- Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y., et al. (2024). Dissecting zero trust: Research landscape and its implementation in IoT. *Cybersecurity*, 7, Article 20.
- Nahar, N., Andersson, K., Schelén, O., & Saguna, S. (2024). A survey on zero trust architecture: Applications and challenges of 6G networks. *IEEE Access*, 12, 94753–94764.
- Mahadevan, S. (2024). Empowering Manufacturing: Generative AI Revolutionizes ERP Application. *Int. J. Innov. Sci. Res.*, 9, 593-595.
- Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. *Information and Software Technology*, 141, Article 106700.
- Reichert, B. M., & Obelheiro, R. R. (2024). Software supply chain security: A systematic literature review. *International Journal of Computers and Applications*, 46(10), 853–867.
- Manukonda, K. R. R. (2024). Chapter-5 Enhancing Test Automation Efficiency Through AI-driven Reporting: An Empirical Study on Defect Detection and Resolution Time. *ADVANCES IN*, 119, 107.
- Syed, N. F., Shah, S. W., Shaghghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access*, 10, 57143–57179.
- Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. (2024). *Journal of Systems and Software*, 214, Article 112063.
- Alshaikh, M. (2021). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, Article 102003.
- Sreenivasulu Naidu Yalakaturi. (2024). AI-Assisted Reference Data Harmonization Across Global Data Center Systems. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 9576–9587. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5790>
- World Economic Forum. (2023). *Global cybersecurity outlook 2023*. World Economic Forum.
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint*.
- Burch, G. F., Burch, J., & McGarry, M. (2024). Cybersecurity risk management governance: An agency theory perspective. *ISACA Journal*.
- KOLLA, S. K. (2024). DEEP LEARNING AND CLINICAL NLP FRAMEWORK FOR AUTOMATED KNOWLEDGE EXTRACTION FROM MULTIMODAL HEALTH . TPM – Testing, Psychometrics, Methodology in Applied Psychology, 31(S2), 134–140. Retrieved from <https://tpmap.org/submission/index.php/tpm/article/view/4748>
- Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2021). *DevOps*. *IEEE Software*, 38(3), 7–15.
- Shah, S. W., Syed, N. F., Shaghghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture: A comprehensive survey. *IEEE Access*, 10, 57143–57179.
- Movva, V. R. (2024). Cloud-Native Platform Engineering for High-Scale Retail Systems: Designing Resilient Microservices and Intelligent Infrastructure. Available at SSRN 7449480.
- NIST. (2024). The NIST cybersecurity framework (CSF) 2.0. National Institute of Standards and Technology.
- NIST. (2022). Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities (Special Publication 800-218). National Institute of Standards and Technology.
- Rohit Gorle. (2024). Deep Learning Approaches for Threat Detection in Multi-Cloud Environments. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(07), 3857–3864. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5879>
- NIST. (2022). Guidelines for minimum standards for developer verification of software (Special Publication 800-218A). National Institute of Standards and Technology.
- NIST. (2021). Security and privacy controls for information systems and organizations (Special Publication 800-53, Revision 5). National Institute of Standards and Technology.
- Yandamuri, U. S. (2024). AI-Driven Decision Support Systems for Operational Optimization in Hospitality Technology. *Metallurgical and Materials Engineering*.
- NIST. (2021). Cybersecurity supply chain risk management practices for systems and organizations (Special Publication 800-161, Revision 1). National Institute of Standards and Technology.
- NIST. (2023). Zero trust architecture model for access control in cloud-native applications in multi-cloud environments (Special Publication 800-207A). National Institute of Standards and Technology.
- Mangalampalli, B. M. Generative AI Applications In Healthcare Data Mart Design And Optimization.
- European Union Agency for Cybersecurity. (2021). ENISA threat landscape 2021. Publications Office of the European Union.
- European Union Agency for Cybersecurity. (2022). ENISA threat landscape 2022. Publications Office of the European Union.
- European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. Publications Office of the European Union.
- Manukonda, K. R. R., Swamy, H., Sankar, R., & CM, C. (2024, August). Application of Explicit Group Sparse Projection in Optimizing 5G Network Resource Allocation and Topology Design. In *2024 4th Asian Conference on Innovation in Technology (ASIANCON)* (pp. 1-6). IEEE.
- European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. Publications Office of the European Union.
- Cybersecurity and Infrastructure Security Agency. (2023). Shifting the balance of cybersecurity risk: Principles and approaches for security-by-design and -default. U.S. Department of Homeland Security.
- Cybersecurity and Infrastructure Security Agency. (2023). Secure by design. U.S. Department of Homeland Security.
- Cybersecurity and Infrastructure Security Agency. (2024). The open source software security roadmap. U.S. Department of Homeland Security.
- Mahadevan, S., Desani, N. R., Yadav, P. S., Joseph, T., & Malcom, A. (2024). *FutureTech Innovations*. Cari Journals USA LLC.
- National Institute of Standards and Technology. (2021). A zero trust architecture for the federal government. National Institute of Standards and Technology.
- National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). National Institute of Standards and Technology.
- National Institute of Standards and Technology. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). National Institute of Standards and Technology.
- Mangalampalli, B. M. Intelligent Data Profiling for Healthcare Data Lakes Using AI-Enhanced Analytics.
- World Economic Forum. (2022). *Global cybersecurity outlook 2022*. World Economic Forum.
- International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC 27001:2022). ISO.
- International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection—Information security controls (ISO/IEC 27002:2022). ISO.
- Yandamuri, U. S. (2022). Cloud-Based Data Integration Architectures for Scalable Enterprise Analytics. *International Journal of Intelligent Systems and Applications in Engineering*, 10, 472-483.
- World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum.