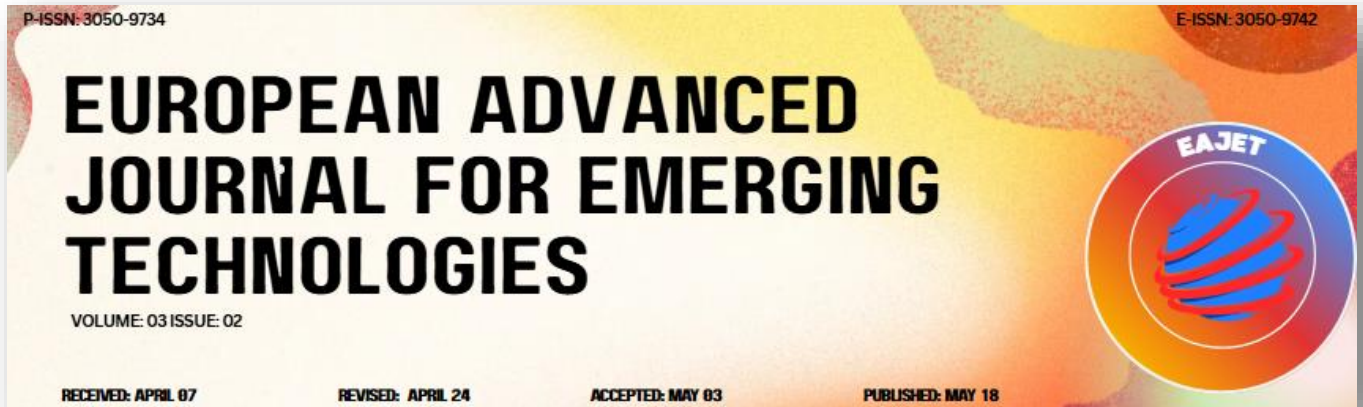




Trust-Aware Access Control and Secure Delivery

Dhanaraj Sathiri

Independent Researcher
dhanrajsathiri@gmail.com

Abstract

We present a Trust-Centric Cloud Intelligence Framework for autonomous access governance and secure enterprise software delivery, aimed at achieving deep governance of cloud services through intelligent, autonomous operations. While artificial intelligence (AI) and automation create unprecedented opportunities for enterprises, cybersecurity remains a persistent and critical challenge. Despite cloud providers' assurances of robust security measures, numerous high-profile breaches have demonstrated the limitations of these claims. We argue that trust serves as a foundational construct enabling security managers to establish sufficient cyber-resilience. Furthermore, the vast volume of data generated across cloud services offers a valuable source of intelligence for continuously monitoring and enforcing governance policies. By quantifying trustworthiness as an indicator of the risk associated with cloud service usage, our framework establishes the foundation for an intelligent access-governance model—one that integrates privilege management, identity administration, role assignment, and automated policy enforcement.

Keywords—Trust, cloud intelligence, autonomous governance, access governance, privilege management, identities, roles, policy enforcement, secure software delivery, enterprise security .

1. INTRODUCTION

The Governance of Cloud Services in an Ecosystem of Trust

Cloud adoption indeed addresses many organizational requirements and enables organizations to focus on their core business areas while letting cloud providers manage the underlying infrastructure. During the process, corporate data becomes the most valuable asset in the cloud ecosystem, and organizational governance aims to protect it from unauthorized access. With challenges in protecting sensitive data in public cloud services, cloud usage becoming ubiquitous over multi-cloud and hybrid environments, and edge computing making sensitive data traversing and residing in many cloud services, trust is now the key to enabling enterprise cloud ecosystems while fulfilling security requirements. A trust-centric cloud intelligence framework for autonomous access governance helps enterprises move towards the vision of providing secure, autonomous access to cloud resources, eliminating the burden of maintaining security posture through continuous manual intervention. Access policies are indicated as being verified through certified telemetry and audit trails, enabling autonomous granting of access or defining conditions to be approved by an approver pool. Foundations of cloud trust intelligence define risk and assurance signals, formulating rules of what constitutes compliant, non-compliant, or within-risk access.

The continuous provisioning of risk-adaptive access leverages external providers' risk context to dynamically zero-in-time provisioning of access. The intended system will provide organizations with always-compliant working environments, reducing the organization's audit effort. Trust is continuously measured since a risk-adaptive trust is known to fluctuate and affect access provisioning. These aspects, combined with secured software delivery, ensure corporate data remains confidential. Security validation of operating systems and applications through attestation and assurance of expected behavior through secure telemetry maintain data integrity and confidentiality—enabling secure enterprise software delivery on multi-cloud infrastructures.

A. Core Trust Constructs for Autonomous Governance

Six core trust constructs—credibility, reliability, accountability, transparency, and resilience—enable autonomous, trustworthy access governance and guide enterprise software delivery across the software supply chain. Credibility determines whether a signaller can be trusted. Reliability measures whether a signaller is trustworthy over time. Accountability quantifies if trust violated incurs a repair cost. Transparency gauges the extent of available signal evidence. Resilience describes the capacity to withstand failures without significant impact.

Signals for measuring these trust constructs, their interaction with autonomous enforcement, and the underlying evidence pipelines from source to signaller are described. Risk and assurance assessment of each trust construct, together with a supporting evidence proxy, forms the basis for effective wide-area enterprise security through autonomous, trusted access governance, enabling the drawing together of cloud services, edges, and multi-cloud infrastructures.

Trust derivation is commonly a central function of the governance of access decisions. The above trust constructs not only enable access governance decision-making, but also facilitate building cloud intelligence layers for tracking, monitoring, and managing trusted access governance for cloud and edge services on a larger scale of operation through automation and autonomy.

Figure 1 — Layered Reference Architecture

Visual rendering of the perception–decision–actuation–supervision architecture described in Section 3, with a continuous supervision feedback loop across all layers.

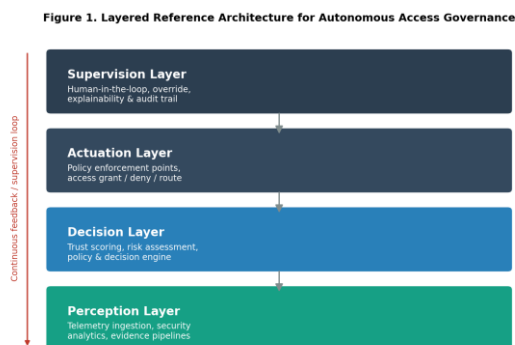


Figure 1. Layered reference architecture for autonomous access governance.

Figure 2 — Illustrative Trust-Construct Profile

A radar chart showing an illustrative, normalized (0–1) score for each of the five trust constructs for a single cloud-service signaller, as would be produced by the trust-scoring function in Equation 1.

Figure 2. Illustrative Trust-Construct Profile of a Cloud Service Signaller

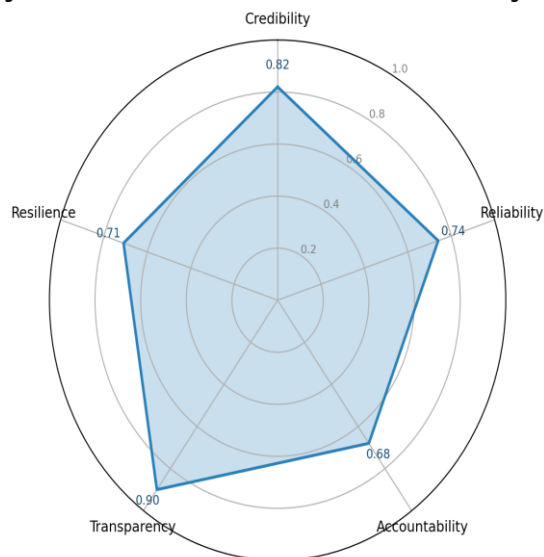


Figure 2. Example trust-construct profile (illustrative values, not paper data).

Figure 3 — Risk-Adaptive Access Decision Flow

Flow from evidence signals through trust scoring, risk adjustment, and the threshold-based decision described in Section 4 (autonomous grant vs. routing to an approver pool).

Figure 3. Risk-Adaptive Access Decision Flow



2. Foundational Principles of Trust-Centric Cloud Intelligence

Trust-centric cloud intelligence addresses autonomous governance and decision-making. Central to the approach are data assurance and policy-driven, auditable automation.

Definitions and Scope

Trust-centric cloud intelligence applies to cloud services (virtual machines and containers) and systems-of-systems (multi-clouds with edge or on-premise components), accomplished through additional cloud intelligence and autonomous governance layers. The intelligence layer can be implicit, via explicit validation signals, or explicit, via an integrated knowledge engine leveraging data from the governance layer, the broader context, and pre-existing knowledge. In both cases, governance is policy-driven and automation auditable, enabling user wish to Verify, and Correct, through Transparency, Awareness, and Knowledge.

Architectural Framework

The reference architecture for trust-centric cloud intelligence and autonomous access governance comprises perception, decision, actuation, and supervision layers. Perception captures telemetry for analytics; decision and actuation support autonomous access governance; and supervision provides assurance via a knowledge engine capable of imprinting on external-edge Cloud Service Providers and verifying own Cloud Services partners using audit trails and supporting Knowledge Evidence Points and Pipelines.

A. Definitions and Scope

Cloud services and their associated components hosted within multicloud or edgedeployed environments deliver the required applications, compute, storage, and infrastructure resources. The delivery scheme adopts the service-oriented architecture model where service consumers interact with service providers for resource provisioning. However, trust is a critical enabler for the cloud adoption of businesses. Trust is primarily rooted in the well-defined and enforced security, risk, governance, and compliance controls of the cloud services. Therefore, cloud service consumers and providers require new independent methods for continuous assurance of the trustworthiness of all the cloud components involved.

Existing studies primarily focus on trust between cloud service consumers and providers. This framework expands the definition to all the involved cloud components, providing a multidimensional view of trust. Furthermore, cloud components require a higher degree of autonomy driven by artificial intelligence and engaging machine learning. An architecture for cloud components capable of autonomous decision-making has been proposed, incorporating new layers that allow interactions, decision-making, and perception based on the combination of different datasets. The focus of the architecture is autonomous access governance in a cloud environment, complemented by an intelligence layer capable of providing an additional degree of mission assurance.

Mathematical Formulas:

$$T_i = \sum_k w_k \cdot S_{k,i}, \quad \sum_k w_k = 1 \quad (1)$$

Where $S_{k,i} \in [0,1]$ is the normalized evidence score for trust construct k (credibility, reliability, accountability, transparency, resilience) of signaller i , and w_k is its governance-assigned weight.

Risk-Adjusted Access Score

$$A_i = T_i \cdot (I - R_i) \quad (2)$$

Where $R_i \in [0,1]$ is the real-time, external risk-context signal for signaller i , combining trust with continuously updated risk to support risk-adaptive access control (RADAC).

Threshold-Based Access Decision

Grant access if $A_i \geq \theta$; otherwise route to approver pool (3)

Where θ is a policy-defined trust/risk threshold. This encodes the paper's description of autonomous granting versus conditions approved by an approver pool.

Reliability Decay Between Evidence Updates

$$T_i(t) = T_i(t_0) \cdot e^{-\lambda \Delta t} \quad (4)$$

A simple exponential-decay term reflecting that risk-adaptive trust is continuously measured and known to fluctuate over time, where λ is a decay-rate parameter and Δt is elapsed time since the last evidence update.

3. Architectural Framework

A layered architecture for autonomous access governance is proposed, comprising perception, decision-making, actuation, and supervision layers. Horizontal components provide telemetry, analytics, and policy enforcement. The architecture specifies internal and external interfaces, delineates data flow and governance boundaries, and identifies components in the context of multi-cloud and edge ecosystems. Interoperability and vendor-agnostic considerations are emphasized.

The architecture for autonomous governance of access in cloud services is presented in Figure 1. Cloud services span multiple infrastructure stacks, supported by a vast network of infrastructure and edge services. Governance for such a wide perimeter requires a level of autonomy to enable real-time decision-making while remaining, at every moment, supervised by sensitive humans that may trigger overrides of decisions they consider not aligned with the expected and required behavior. Autonomy is created by a layered architecture where perception, telemetry, decision-making, actuation, and supervision are separated. Such layers prevent overloaded information in the supervision layer, which deals only with exceptions, changes in strategy, or new threats. Telemetry and analytics provide the organizational governance with the information needed to create the strategy to align the environment risks, impacts on strategic assets, and trustworthiness.

Table 1 — Core Trust Constructs

Construct	Definition (per paper)	Example Evidence Signal
Credibility	Whether a signaller can be trusted at all	Certificate/attestation validity, provenance
Reliability	Whether a signaller is trustworthy over time	Historical uptime, consistency of telemetry
Accountability	Whether a trust violation incurs a repair cost	SLA penalties, incident remediation records
Transparency	Extent of available signal evidence	Audit-log completeness, telemetry coverage
Resilience	Capacity to withstand failures without significant impact	Failover success rate, recovery time

Table 2 — Layered Reference Architecture

Layer	Primary Function	Representative Components
Perception	Captures telemetry for analytics	Telemetry sources, security-analytics engines
Decision	Autonomous access governance decision-making	Trust/risk scoring, policy & decision engine
Actuation	Executes access governance decisions	Policy enforcement points
Supervision	Provides assurance and human oversight	Knowledge engine, human-in-the-loop, override

A. Reference Architecture for Autonomous Access Governance

Intelligent Automation for Autonomous Access Governance

Figure 1 presents a layered reference architecture for autonomous access governance, encompassing perception, decision-making, actuation, and supervision layers. Fundamental components consist of telemetry that feeds security analytics capabilities and policy enforcement points integrated with cloud services. The critical governance aspect is centered on telemetry sources forwarding evidence to security analytics engines, which analyze the received data flow, build related indicators, and generate telemetry analytics reports. These reports are then scrutinized against defined trust policies to identify and assess risks. Identified risks are relayed to corresponding policy enforcement points for resolution or compensatory decision-making.

The architecture is designed to promote open industry standards for interoperability while remaining vendor-agnostic. Autonomous access governance serves as a control layer for accessing cloud resources and capabilities by enterprise users and the corresponding access-eligible cloud service users. An access governance model encapsulating identities, roles, and privilege management, formed from core trust constructs, defines the access decisions involved. Continuous compliance ensures that continuous monitoring of defined risk-assurance indicators contribute to the decision-making executed by control mechanisms and policy enforcement points.

4. Access Governance Model

Access Governance Model

Access governance governs access provisioning, enforcement, and infrastructure for cloud-based applications and services. Identity, Role, and Privilege Management I. Identity Management defines identity types and their users, supported authentication methods, and federation across

federated identity management. Role Management defines roles and role-based access control (RBAC). Entitlement Definition and Management supports attribute-based access control (ABAC) and risk-adaptive access control (RAdAC). Privilege Management defines and implements privileged identity management (PIM), least-privilege entitlement provisioning, entitlement lifecycle management, entitlement separation of duties (SoD) enforcement, and entitlement revocation. Continuous compliance, including monitoring, logging, reporting, auditing, and explainability, is also defined.

Policy Definition and Enforcement defines policy framework and decision engines for all access governance functions. Policy-driven decision-making is fundamental to Trust-Centric Cloud Intelligence. A Policy and Decision Management Component in the Cloud Intelligence Decision Layer ensures that access governance decisions comply with enterprise policy and risk appetite. Basic Cloud Identity, Access, Role, and Privilege Governance Functions ensure consistent policy-based decision-making. The corresponding processes provide around-the-clock continuous compliance for that governance domain. Available backup and override mechanisms allow human administrators to override continuous compliance decisions, while the decision- and audit-trail logs provide full explainability of the new decisions. Human-in-the-loop functions provide for security-critical situations requiring human intervention to make the decision.

Table 3 — Identity, Authentication, and Federation Building Blocks

Category	Types / Methods Described in Paper
Identity types	End-user, device, application, service
Authentication methods	Passwords, Public Key Infrastructure (PKI), biometric techniques
Federation mechanisms	SAML, OAuth2, W3C Web Authentication

Table 4 — Access Control Model Comparison

Model	Basis for Decision	Adaptivity
RBAC (Role-Based)	Predefined roles assigned to identities	Static
ABAC (Attribute-Based)	Attributes of subject, resource, and environment	Moderate
RAdAC (Risk-Adaptive)	Real-time trust and risk signals	Dynamic / continuous

A. Identities, Roles, and Privilege Management

Identity Management, Authentication, and Federation

Identity types (end-user, device, application, service), authentication methods (passwords, Public Key

Infrastructure/PKI, biometric techniques), and federation mechanisms (security assertion markup language, OAuth2, W3C Web Authentication) are foundational to access governance. Role-based access control (RBAC), attribute-based access control (ABAC), and risk-adaptive access controls are implementations that satisfy the business objectives and risk appetite of the cloud and edge service providers and their customers.

Identity–Role–Attribute Relationships and Privilege Provisioning

Identity management enables the provisioning of all user types in a governance ecosystem, including those from third parties with goodwill; life-cycle management; binding of users, devices, applications, and services to multiple roles; and constant least-privilege reinforcement. Testing of separation of duties reduces operational security risks. Revocation lists, monitoring of user activities, and workflows for triggering additional logging and auditing help to ensure compliance with policies while respecting legitimate business needs.

5. Conclusion

The proposed architecture and model constitute a Trust-Centric Cloud Intelligence Framework for Autonomous Access Governance and Secure Enterprise Software Delivery. The design aims for the automation of trust-centric access governance, for cloud services deployed in multi-cloud and/or edge environments, with a focus on the cloud and edge components that govern access and authorisation. A layered, control-understanding architecture is proposed for autonomous access governance, comprising perception, decision, actuation, and supervision layers. Within the decision layer, a model for identities, roles, and privilege management is detailed. This incorporates identity federation, risk-adaptive access control, continuous compliance assurance, and a policy framework for management and monitoring. Decision automation is governed through explainability, auditing, human-in-the-loop, and override provisions. The model advances risk-adaptive privilege management within a continuous compliance framework for complex enterprise software delivery scenarios, mitigating top enterprise risks identified by CIS.

The framework investigates the need for intelligence-assisted, autonomous approach and therefore brings cloud governance challenges from the supporting literature. The Trust-Centric Cloud Intelligence Framework for Autonomous Access Governance and Secure Enterprise Software Delivery is deeply analysed and key findings are presented in the current section. Addressing the evident causes of trust misalignments is the focal area as these impact overall security of cloud services. Management of cloud trust must therefore move beyond a validation phase and shift to support for the continuous dynamic trust mechanism, based on the Security Council. With Internet-oriented service methodology adopted by cloud, trust decisions must therefore be place in the hands of dynamic trusted authority to continuously assess the behaviour of Cloud Providers and Cloud Services. Such trust decisions therefore must take

place in a decentralized manner through distributed cloud ledger technology for Cloud Services.

REFERENCES

1. Chandramouli, R., Butcher, Z., & Chetal, A. (2021). Attribute-based access control for microservices-based applications using a service mesh. National Institute of Standards and Technology.
2. Duan, R., Alrawi, O., Kasturi, R. P., Elder, R., Saltaformaggio, B., & Lee, W. (2021). Towards measuring supply chain attacks on package managers for interpreted languages. *Proceedings of the Network and Distributed System Security Symposium*.
3. Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Journal of Safety and Security Engineering*, 11(5), 537–545.
4. Mattaparthi, R. (2024). Transformer-Based Fault Diagnosis for Large-Scale Standby Power Generators: Partial Discharge Pattern Recognition at Hyperscale Data Center Installations. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 8781–8799.
5. Afzali, H., Kuppusamy, T. K., Torres-Arias, S., Curtmola, R., & Cappos, J. (2021). Towards secure software supply chains: A survey of current practices and emerging approaches. *IEEE Security & Privacy*.
6. Shree, S., & Kumar, S. (2021). Zero trust security architecture for cloud computing environments. *International Journal of Computer Networks and Applications*, 8(6), 671–682.
7. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2021). Zero trust architecture: Concepts and deployment considerations. National Institute of Standards and Technology.
8. NIST. (2021). Security measures for “EO critical software” use under Executive Order 14028. National Institute of Standards and Technology.
9. Venkateswara Rao Movva. (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. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5827>
10. NIST. (2021). Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities. National Institute of Standards and Technology.
11. Syed, N. F., Shah, S. W. H., Shaghagh, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access*, 10, 57143–57179.
12. 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. Retrieved from <https://jneonatsurg.com/index.php/jns/article/view/10577>
13. Okafor, C., Schorlemmer, T. R., Torres-Arias, S., & Davis, J. C. (2022). SoK: Analysis of software supply chain security by establishing secure design properties. In *Proceedings of the 2022 Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses* (pp. 15–24).
14. Jiang, W., Synovic, N., Sethi, R., Indrapu, A., Hyatt, M., Schorlemmer, T. R., Thiruvathukal, G. K., & Davis, J. C. (2022). An empirical study of artifacts and security risks in the pre-trained model supply chain. In *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses* (pp. 105–114).
15. Pranitha Potturi. (2024). AI-Augmented Analytics Architecture for Intelligent Enterprise Reporting and Predictive Business Decision-Making. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(05), 3830–3841. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5797>
16. 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, 102625.
17. Sun, Q., Liang, G., Wu, Y., Wu, B., Tian, C., & Wang, W. (2022). Data-driven open source software supply chain maintenance risk analysis method. *Journal of East China Normal University (Natural Science)*, 2022(5), 90–99.
18. 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.

19. Research on risk analysis and governance measures of open-source components of information system in transportation industry. (2022). *Procedia Computer Science*, 208, 106–110.
20. Melara, M. S., & Bowman, M. (2022). What is software supply chain security? arXiv.
21. Kolla, S. H., & Peddi, R. K. (2024). Designing Governance-Aligned GenAI Pipelines Using Small Language Models for Enterprise Workflow Intelligence. *International Journal of Science, Research and Technology*, 7(6), 13256-13268.
22. National Institute of Standards and Technology. (2022). Cybersecurity supply chain risk management practices for systems and organizations. National Institute of Standards and Technology.
23. National Institute of Standards and Technology. (2022). Blockchain for access control systems. National Institute of Standards and Technology.
24. Sasidhar Reddy Mondeddula. (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. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5813>
25. Duan, R., Alrawi, O., Kasturi, R. P., Elder, R., Saltaformaggio, B., & Lee, W. (2023). On the prevalence of software supply chain attacks: Empirical study and investigative framework. *Forensic Science International: Digital Investigation*, 44, 301508.
26. Amusuo, P. C., Robinson, K. A., Singla, T., Peng, H., Machiry, A., Torres-Arias, S., Simon, L., & Davis, J. C. (2023). ZTDJava: Mitigating software supply chain vulnerabilities via zero-trust dependencies.
27. Hu, V. C. (2023). Overview and considerations of access control based on attribute encryption. National Institute of Standards and Technology.
28. Rajesh Reddy Ellenki. (2024). Deep Learning-Based Demand Intelligence for Dynamic Merchandise Planning and Allocation. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 7796–7802. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5832>
29. Saxena, U. R., & Alam, T. (2023). Provisioning trust-oriented role-based access control for maintaining data integrity in cloud. *Indian Journal of Science and Technology*, 14(6), 1–10.
30. Research on zero trust evaluation method for network security. (2023). In *Proceedings of the 3rd International Conference on Frontiers of Electronics, Information and Computation Technologies*.
31. Tang, B., et al. (2023). Blockchain-based zero-trust access control for Internet of Things environments. IEEE-related research on decentralized trust and access control.
32. Chandramouli, R., & Butcher, Z. (2023). A zero trust architecture model for access control in cloud-native applications in multilocation environments. National Institute of Standards and Technology.
33. Torres-Arias, S., Afzali, H., Kuppusamy, T. K., Curtmola, R., & Cappos, J. (2023). Software supply-chain security: Issues and countermeasures. *Computer*, 56(7), 54–66.
34. Zhou, X., et al. (2024). A blockchain-based and microservices-architected software composition analysis system. *Journal of Software: Evolution and Process*.
35. Reddy, V. A. R. (2024). Generative Intelligence for Healthcare Claims Processing and Personalized Benefits Management. *International Journal of Advanced Engineering Science and Information Technology (IJAESIT)*, 7(3), 14099.
36. 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.
37. Chandramouli, R., Kautz, F., & Torres-Arias, S. (2024). Strategies for the integration of software supply chain security in DevSecOps CI/CD pipelines. National Institute of Standards and Technology.
38. Boyens, J. (2024). Appendix F: Software security in supply chains. National Institute of Standards and Technology.
39. Okafor, C., Schorlemmer, T. R., Torres-Arias, S., & Davis, J. C. (2024). SoK: Analysis of software supply chain security by establishing secure design properties. *Proceedings of the 2024 software supply-chain security research community*.
40. ZTSA: Zero trust security architecture—A comprehensive survey. (2024). In *Proceedings of the 2024 International Conference on Communication, Computer Sciences and Engineering*.
41. Ding, Y., Wu, Z., Miao, Y., & Ding, M. (2024). SharAcc: Enhancing scalability and security in attribute-based access control with sharding-based blockchain and full decentralization. *Computer Networks*.
42. Strategy for implementing of zero trust architecture. (2024). *IEEE Transactions on Reliability*, 73(1), 93–100.
43. IEEE Computer Society. (2024). IEEE Standard for blockchain-based zero-trust framework for the Internet of Things (IEEE Standard 3219-2023). IEEE Standards Association.
44. Anasuri, S., & Rusum, G. P. (2024). Software supply chain security: Policy, tooling, and real-world incidents. *International Journal of Emerging Trends in Computer Science and Information Technology*, 5(3), 79–88.