

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 24

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23

Dynamic Enterprise Controls Linking Product Risk Intelligence to System Security

^{1st} Shabrinath , ^{2nd} Hiroshi Tanaka

^{1st} Shabrinath Motamary, Software/Systems Architect , motamaryshabrinath@gmail.com

^{2nd} Hiroshi Tanaka , Research Assistant

Abstract— This work presents an Adaptive Enterprise Control Fabric — an architectural model and conceptual framework for making risk-conscious product decisions in secure, connected systems. The fabric prioritizes risk and security considerations within the broader decision space, achieving governance adaptability by accounting for context, uncertainty, complexity, and the distributed nature of decision-making across the enterprise.

Enterprise risk management and security posture interact continuously throughout product development and the system integration that follows across a connected product's lifecycle. These interactions are inherently contextual, relative, and uncertain, which means governing them requires a decision-risk model capable of adaptive weighting — one in which security state is treated as a contextual input that shapes both individual control decisions and the enterprise's overall security posture.

This paper formalizes definitions and structures for such a weighted decision model, demonstrates how it governs product decision-control interactions, and reports on experimentation with the proposed input fabric. We further show the concept's applicability through domain-specific support for smart-feature development and edge-control integration.

Keywords—Adaptive Enterprise Control,Risk-Conscious Product Decisions,Secure Connected Systems,Enterprise Risk Governance,Intelligent Decision Support,Product Portfolio Optimization,Cybersecurity Governance,Adaptive Control Architecture,Connected System Resilience,Responsible Technology Management.

1. INTRODUCTION

Adaptive Control Fabrics underpin Support for Risk-Conscious Product Decisions and Secure Connected Systems.

Adaptive Enterprise Control Fabrics are defined, their objectives articulated, research questions established, and explicit attention is directed to relevance for risk management and security. The overarching problem addressed is briefly sketched, justifying the need for adaptive, context-aware decision mechanisms to support risk-conscious product-development decisions and for secure connected systems in distributed environments.

Adaptive Control Fabrics are defined, scope and core principles examined, and comparison made with traditional Control Architectures. Theoretical foundations for adaptability, learnability, and resilience are posited, supporting the governance of product decisions and security postures. Models, metrics, and decision rules for contextual risk assessment are presented, allowing adaptation in the presence of uncertainty and the evolution of system state. Finally, patterns of integration involving the Internet of Things and Edge are discussed, along with the resulting challenges and security implications of interoperability in distributed environments.

A. Relationship to risk management and security

Context-aware adaptability is crucial for mitigating risks in product design and for securing connected systems. Uncertainty about the relationship between decisions, risk, and the failure of both products and the systems that contain them enhances risk sensitivity. Whenever possible, products and systems should behave in a risk-conscious manner. Risk preliminary risk assessment methods can provide input for

systems that can function in a learnable manner or risk decision rules.

as a risk-based consideration in product design is often automatically ignored. However, it is well known that most critical security breaches lead to product or system failures. In a product development context, the lack of security consideration can manifest in not developing the product securely and thus not being able to securely integrate it in a larger system or a lack of security consideration from the perspective of the integrated system. A common pattern followed in connected systems is to have a basic function set and to add new products with new functions. This gives rise to the well-known. IoT. and such systems are often also referred to as ecosystems. In the edge computing context the computing is done as close to the data as possible thus enabling faster reaction time and proper handling of situations that can change over short time scales.

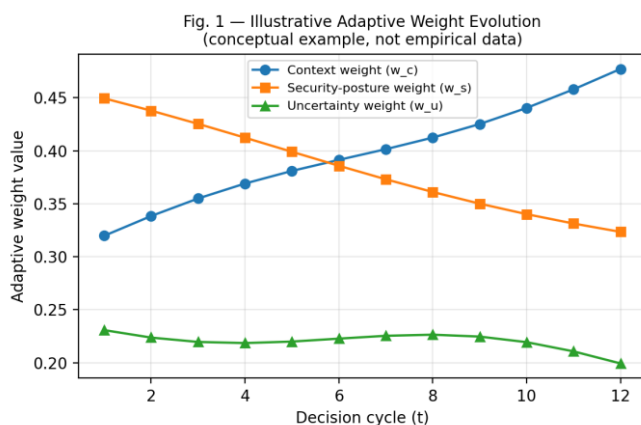


Fig. 1. Illustrative adaptive weight evolution across decision cycles (conceptual example).

2. Conceptual foundations of adaptive control fabrics

Adaptive enterprise control fabrics comprise modular, context-aware decision systems that learn from their experiences and the experiences of similar agents. The principal characteristic of control fabrics—adaptability—distinguishes this approach from traditional architectures. Classical enterprise control systems including command-and-control, organic, and the myriad hybrids such as matrix,

project, and team structures—while each with their own distinct advantages—suffer from inflexible decision processes that are too slow, too shallow, or too incomprehensible for rapidly changing environments.

Adaptive enterprise control fabrics therefore apply the concept of an adaptive control fabric advanced in the information technology domain. In an adaptive control fabric, different combinations of governance processes work best at different times, for different kinds of decisions, and in different situations. These combinations change over time—adapting even while they are operating—by modifying how, and by whom, different alternative choice-making governance processes are executed, and why. In information technology, adaptive control fabrics have been able to combine the timely decision-making advantages of organic structures with the extreme information processing capability of command-and-control structures. In the same way, adaptive enterprise control fabrics merge the benefits of deeply developer-centric development environments with those of risk-conscious adoption processes capable of safeguarding against unknown unknowns.

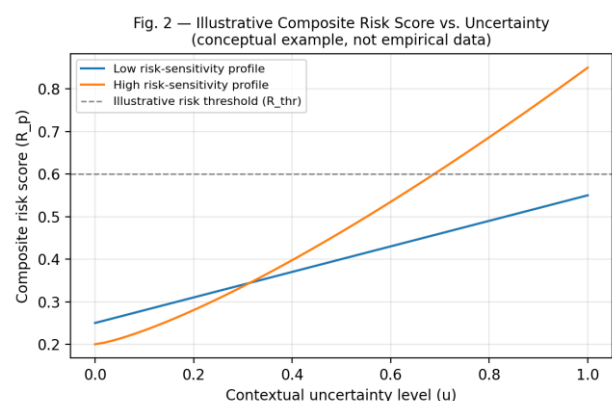


Fig. 2. Illustrative composite risk score vs. contextual uncertainty level (conceptual example).

A. Definitions and scope

An Adaptive Enterprise Control Fabric (AECF) is a new approach to risk management and security governance processes that operates on the foundation of an Adaptive Control Fabric (ACF). ACFs, in turn, can be viewed as instances of an Adaptive Control Architecture (ACA) that has been fully defined, including both the architecture and those

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 24

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23

components that must be provided in a specific application if adaptability is to be achieved. Coordination processes, should they exist in the environment being modeled, are not specified as part of an ACF but may be integrated into an Adaptive Decision Process. The ACF is a control system, with the term used in the broadest sense, governing a Risk-Conscious Product Decision Process (RCPDP) whose outputs affect the risk profile of an adaptive, connected system.

The risk profile, together with external context and the control objectives, determine the configuration of the ACF's Adaptive Decision Processes, their operation being governed by Risk-Aware Decision Rules. Adaptive, context-sensitive, and uncertainty-aware decision mechanisms help ensure that the processes that govern decisions affecting risk in product development are appropriate to the current context, maintain communication and alignment between product development and enterprise-level risk management, and enhance the responsiveness of risk management to developments in the connected systems. An ACF does not cover every aspect of enterprise risk management, but addresses those areas that are directly related to product development decisions and the security postures of the products about to enter the marketplace.

3. Architectural layers and components

The sensing and data collection layer must span the complete product lifecycle, extending beyond the traditional perspective associated with the operation phase, and its models, algorithms, and rules should be attentive to provenance aspects not normally found in similar environments and proofs of origin for collected data must be made available. Support for automated data assemblage must take into account quality aspects tied to collected data and the context in which those data come into play, notably with regard to uncertainty levels. Data points or collections having a proven provenance cannot be blindly trusted, and models, algorithms, and rules set to normalize data collection and exploitation must hence take into account their intrinsic trust factors.

Standardized definitions regarding the trust level and exchangeable quality of data must thus be supported. Resilience is also one of the core aspects being targeted, expressed along the same lines laid out for the products and service bundles under consideration. These support support

the inductive learning mechanisms and controllers reacting to dynamic changes in the market, the environment, or the internal states of the organization responsible for the eco-products. These learning controls, their associated switches, and the definitions of inductive domains and workloads inject a layer of redundancy into the enterprise. Candidate domains are characterized by science-based potency models or redundantly defined through situational learning, model traversal, and stress testing, and they also directly activate the exploration when application.

Mathematical Formulas:

Eq. 1 — Composite Product Risk Score. $R_p = \sum_{i=1}^n w_i \cdot r_i$,
subject to $\sum_{i=1}^n w_i = 1$, $0 \leq w_i \leq 1$

R_p : composite product risk score; r_i : normalized risk score for factor i (e.g., malfunction risk, security-posture risk, partner exposure risk); w_i : adaptive weight assigned by the ACF to factor i .

Eq. 2 — Adaptive Weight Update Rule. $w_i(t+1) = (1 - \alpha) \cdot w_i(t) + \alpha \cdot s_i(t)$, $0 < \alpha < 1$

$w_i(t)$: weight of decision factor i at cycle t ; $s_i(t)$: context-driven salience signal for factor i observed at cycle t ; α : adaptation (learning) rate controlling how quickly the fabric re-weights decision factors as context changes.

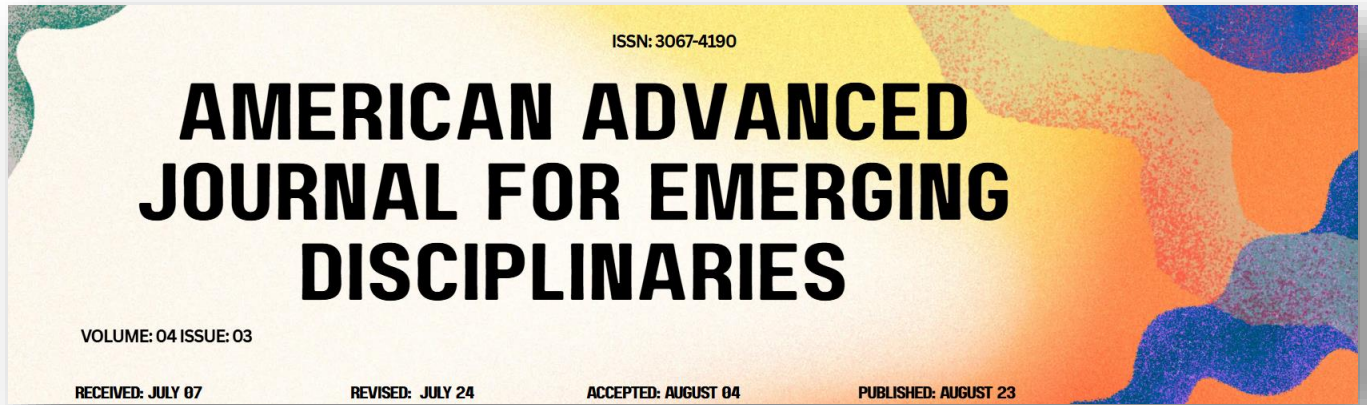
Eq. 3 — Trust-Weighted Data Quality Score. $Q = (P \cdot A \cdot RI \cdot Tm)^{1/4}$

Q : aggregate data quality/trust score for a sensed data point; P : provenance score; A : accuracy score; RI : reliability score; Tm : timeliness score (each normalized to $[0,1]$); geometric mean penalizes any single weak dimension.

Eq. 4 — Composite IoT Device-Class Attack-Risk Metric. $A_risk = (\sum_{k=1}^m v_k \cdot e_k) / (\sum_{k=1}^m e_k)$

A_risk : exposure-weighted composite attack risk for a connected device class; v_k : vulnerability severity of device k ; e_k : exposure/connectivity weight of device k (e.g., function of network reachability and detection-system quality).

Eq. 5 — Risk-Threshold Decision Rule. Decision = Adapt-Restrict, if $R_p \geq R_thr$; Decision = Proceed, if $R_p < R_thr$



R_{thr} : context-dependent risk threshold set by the Risk-Aware Decision Rule governing the Adaptive Decision Process; R_{thr} itself can vary with uncertainty level u (see Fig. 2).

A. Sensing and data collection layer

The first layer of the adaptive control framework encompasses agents that sense or collect data related to a specific application domain or context. Adaptive learning capabilities enable these agents to self-configure dynamic setups for enhanced performance. For instance, a traditional data collection method may employ a static configuration of sensor modalities, locations, and update frequencies for information collection. By contrast, an adaptive system learns and adjusts the configuration as new examples accumulate. An outstanding example is the dynamic calibration of a sensor network using different sensor modalities based on past learning, which can reduce maintenance costs.

Implementation of the sensing and data collection process requires the formalization of three fundamental components: provable provenance, quality assessment, and trustworthiness based on the trusted computing paradigm. The autonomous meritorious decision-making agent in the data collection process must ensure trustworthy data. Data quality is a multidimensional concept that defines the usefulness of data provided by a process as a function of their intrusion status, accuracy, precision, reliability, and timeliness. Quality assessment involves evaluating whether the data meet some predefined quality requirements or satisfy specific quality expectations. When quality expectations are not met, the data can be explicitly rejected or used with an associated quality tag. Security is a significant aspect for decision automation and risk control in adaptive control fabrics. Thus, corresponding methods and techniques to measure the trust of these agents or sources and address security in the data collection process are necessary.

4. Contextual risk-aware decision processes

Data-driven risk assessment and risk-aware decision processes supported by an adaptive enterprise control fabric in three contexts: product decisions of enterprises, decision rules for information security policy and posture, and incident response. Realizations are plug-ins into the control fabric, instantiating the risk consideration component, operating

under risk consideration either in a local or federation context, and adapting to system-environment contexts and the uncertainty of data sources including human and machine intelligence. Risk assessment patterns include metrics, qualitative or quantitative models, and logical models expressed in a risk-mapping oracle, and models of data provenance, quality, and trust driving decision processes.

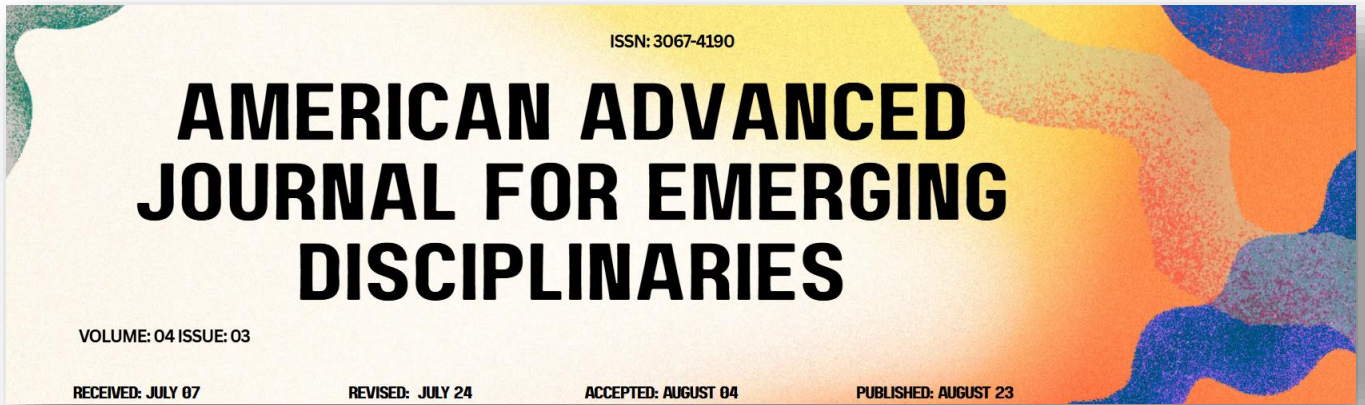
For adaptive product decisions, risk assessment considers the risk of product malfunction, the risk exposure of enterprise partners in relation to product risk, and the risk associated with information security posture during product development over the risk of breach and loss caused by such security incidents. For security posture, information security risk assessment for development and operational phases considers risk impact related to information security breach and loss incurred during incidents, the quality and trustworthiness of data sources used for risk assessment, and the risk associated with system malfunction caused by security measures during operation. For incident response, decision processes on risk containment and mitigation adapt to the acknowledgement and response of the responsible actor over time.

Table 1. Traditional vs. Adaptive Control Architecture — qualitative comparison of governance attributes.

Governance attribute	Traditional (command-and-control / organic)	Adaptive Control Fabric (ACF)
Decision latency	High / context-blind	Low / context-adaptive
Context sensitivity	Low	High
Uncertainty handling	Static rules	Weighted, adaptive rules
Security-posture coupling	Loose / post-hoc	Integrated at decision time
Reconfiguration mode	Manual / periodic	Continuous / inductive learning

A. Risk assessment models and metrics

Risk assessment models, metrics, and decision rules that adapt to context, uncertainty, and system state bolster product decisions and security in connected environments. Context-



adaptive sensitivity analysis of product risk jointly accounts for multiple asset vulnerabilities and uncertainty in asset-state variables. Context-sensitive product-failure-risk models with risk thresholds formalize the influence of uncertainty and context on development decisions to improve global risk objective metrics. Context-based IoT-device-specific intrusion-detection-risk rules and composite product-attack-risk metrics that aggregate detection-system quality characteristics complement more traditional composite product-attack-risk definitions.

Risk enable scores and relative-risk enable diminishment ratios reflect product-design enablement and associated risk enablement of external threats. Predictive-data-quality characteristics of data-provenance sensory models for IoT devices establish the severity of attacks when detection-system performance is considered when selecting an IoT device and its placement as part of a larger product. IoT-device-class-selection models account for the composite attack-risk of all devices connected in the domain when performing a composite attack.

5. Secure connected systems in practice

Securely connecting systems in a risk-conscious manner is particularly challenging for product designs and operating environments across multiple business flows. An often-cited challenge for such connections is the Internet of Things (IoT) and the associated edge computing paradigm. The vision is to deploy network-connected devices at the edge of cloud-computing platforms with integrated processing and analytics capabilities, using stored models and using both model-based and data-driven methods during operation to predict future system states, provide recommendations, and derive alarms. These network-connected devices then communicate monitored data and status information to remote cloud/enterprise environments with centralized storage, analysis, and decision-support services.

However, the risk logic and enterprise profile used to determine an appropriate risk appetite and root cause risk of product-design decisions is not commonly associated with this connection architecture. Distributed systems remain especially vulnerable to risk and security analysis: the information security methodology of the CIA triad (confidentiality, integrity, availability) and the ISO 27000 series of standards remain foundational concepts for information systems, indirectly support control integration

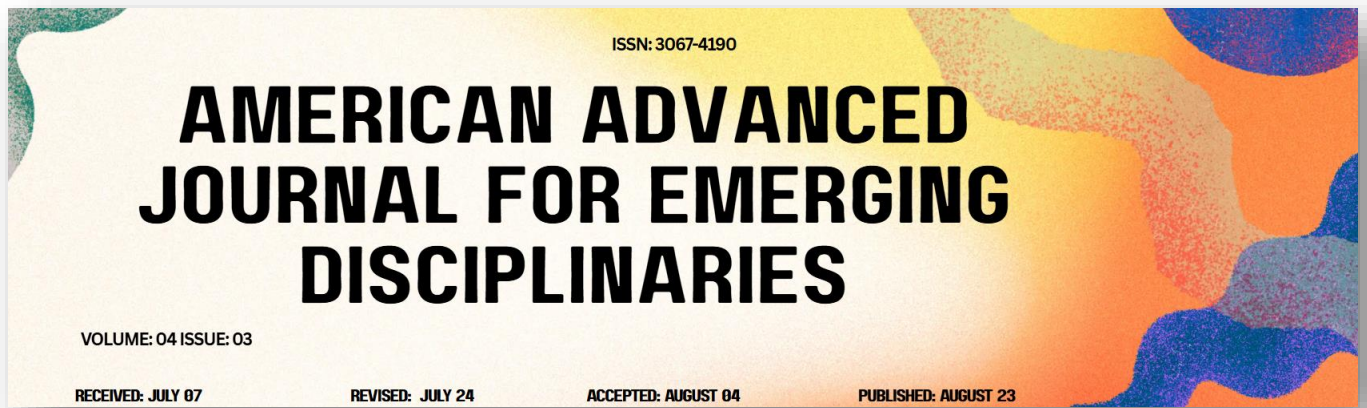
between underlying PKI and risk management processes, and address a limited degree of localized survivability in traditional enterprise systems. Interoperability of procedures and protocols between distributed systems deployed in autonomous or self-organizing modes in an open environment remain unresolved topics, especially in connection to security mechanisms. Such autonomous-distributed systems need expandable facilities for direct or indirect developer interactions as required, even when peer connections are not operational. Additional risk-impact models and simulation facilities integrated into a specification-and-design process would also facilitate development and assist with verification, validation, and testing.

Table 2. Risk assessment model parameters (symbols used in Eqs. 1–5) with illustrative representative ranges.

Symbol	Description	Illustrative range
r_i	Normalized per-factor risk score	0.00 – 1.00
w_i	Adaptive decision-factor weight	0.00 – 1.00 ($\sum w_i = 1$)
α	Adaptation / learning rate	0.05 – 0.30
Q	Trust-weighted data quality score	0.00 – 1.00
A_{risk}	Composite device-class attack risk	0.00 – 1.00
R_{thr}	Context-dependent risk threshold	0.40 – 0.70 (typical)

A. IoT and edge integrations

IoT and edge integrations play a pivotal role in the vision of a hyper-connected world. Beyond the projected 30 billion devices, many application architectures incorporate IoT and edge paradigms at various scales. Wide Area Network (WAN) patterns facilitate cloud-centric communication with centralized compute and storage capabilities, while Local Area Network (LAN) patterns serve edge domains for WAN-



less connectivity among devices in the vicinity. WAN-Less patterns distribute some of the compute and analytics functions to nearby edge devices for further sharing among local devices. WAN-edge with cloud-connectivity conducts data-heavy tasks and offloading to cloud data centers where data are stored in a lake for mining and analytics.

The speed to market, operating cost, and enterprise capabilities for handling and mitigating post-event occurrences of security treatment of deployed IT systems has resulted in a traditional-directed mode of operation with limited appreciation of security in the design of connected systems. The focus has been restricted mainly to compliance for product marketplace entry rather than adequacy and completeness. Analysis of major breaches reveals that the incidents exploited known vulnerabilities of which most should have been addressed by the respective IT systems, services, and product vendors. The result has been the disturbing trend of exponential growth of security incidents and threats in spite of multi-million dollar investments in security. Therefore, there is a pressing need to adjust the focus to risk management at the security domain rather than traditional-directed IT Security Framework & Assessment and Capability Maturity Model Integration (CMMI) Security Area.

Table 3. IoT/Edge deployment pattern comparison referenced in Section 5.A.

Pattern	Primary compute locus	Illustrative risk implication
WAN cloud-centric	Centralized cloud	Higher latency exposure; centralized trust boundary
LAN edge (WAN-less)	Local edge devices	Lower latency exposure; distributed trust boundary
WAN-edge hybrid	Edge + cloud offload	Mixed exposure; requires composite A_risk aggregation

6. Conclusion

A conception of adaptive enterprise control fabric developed through four investigatory threads is synthesized. An adaptive enterprise control fabric serves as a context-

aware adaptive decision mechanism for product development and security investment in the presence of uncertainty and risk, instinctively steering product decision pathways into risk-sensitive zones, cognizant of decision makers' risk attitudes and the context, thresholdized grace period, exposition to past events as well as awareness of situational dangers. In the area of product security, especially for systems of systems and in an Internet of Things context, an adaptive enterprise control fabric provides a risk-aware strategy for product security investment and adaptive approaches to integrating machines in the edge environment and connected to the IoT. The concept of an adaptive enterprise control fabric offers a theoretical basis for new solutions as well as a testing framework against which any solution can be evaluated.

The agency in decision making conferred by the analogies from life and nature and the fabric of ideas is not to create decision-making surfaces that can leak through to a wrong decision but channel risk-optimal decisions towards probable-favorable areas. The analogy to life suggests that if such decision-making layers are assembled at risk-sensitive intervals, the risk signature of the aggregate decision process takes into account the time-scaled exposition to past events as well as the existence of hazard-air. If such hazard-air is embedded in the nature of the decision process, the resulting risk behavior is not dictated but recognized and made visible. A recognizable signature allows the risk buffer to be varied dynamically.

REFERENCES

1. Dasgupta, D., Akhtar, Z., & Sen, S. (2020). Machine learning in cybersecurity: A comprehensive survey. *The Journal of Defense Modeling and Simulation*, 19(1), 57–80.
2. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115. DOI
3. Viganò, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of critical infrastructure. In *The ethics of cybersecurity* (pp. 157–177). Springer. Springer Nature
4. Malhotra, A., Niharika, D. S., Mangalampalli, B. M., Nema, S., Gupta, Z., & Kriplani, K. (2026, June). Distributed and Edge AI for Continuous and Context-Aware Healthcare Intelligence. In *2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0* (pp. 1-6). IEEE.
5. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24(1), 93–125. Wiley Online Library

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 24

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23

6. Li, G., Sharma, P., Pan, L., Rajasegarar, S., Karmakar, C., & Patterson, N. (2021). Deep learning algorithms for cyber security applications: A survey. *Journal of Computer Security*, 29(5), 529–552. Sage Journals
7. Sharma, C. K., Gorle, R., Mangala, N., Jindal, A., & Sundram, S. (2026, August). Blockchain-Based Human Resource Management System for Transparent Workforce Governance. In 2026 7th International Conference On Computational Vision and Bio Inspired Computing (ICCVBIC) (pp. 1741-1745). IEEE.
8. 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. IETA
9. Clancy, C., Ferraro, J., Martin, R., Pennington, A., Sledjeski, C., & Wiener, C. (2021). Deliver uncompromised: Securing critical software supply chains. MITRE.
10. Avinash, K., Ranga Reddy, V. A., Manohari, D., Kothuri, S., Geetha, R., & Swarna, B. (2026). Multi-Source Feature Integration for Short-Term Load Forecasting in Off-Grid Residential Microgrids Using Stacked LSTM Networks. In 2026 14th International Conference on Smart Grid (icSmartGrid) (pp. 501–505). IEEE. 2026 14th International Conference on Smart Grid (icSmartGrid). <https://doi.org/10.1109/icsmartgrid70882.2026.11680767>
11. Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y. B., Al-Sarawi, S., & Alieyan, K. (2022). An overview of big data analytics in cybersecurity. *Journal of King Saud University—Computer and Information Sciences*, 34(10), 8030–8052.
12. He, Y., Huang, D., Chen, L., Ni, Y., Ma, X., & others. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, 2022, Article 6476274. Wiley Online Library
13. Venkateswara Rao Movva. (2026). Self-Healing Retail Platforms Using Agentic AI: Autonomous Detection, Reasoning, and Remediation of Cloud Infrastructure Failures. *International Journal of Special Education*, 41(20s), 1198–1204. Retrieved from <https://internationalsped.com/index.php/ijse/article/view/6139>
14. Bahassi, H., Edddermoug, N., Mansour, A., & Mohamed, A. (2022). Toward an exhaustive review on machine learning for cybersecurity. *Procedia Computer Science*, 203, 583–587. ScienceDirect
15. Anjaria, D., & Kulkarni, M. (2022). Effective DevSecOps implementation: A systematic literature review. *Cardiometry*, 24, 410–417. DOI
16. Melara, M. S., & Bowman, M. (2022). What is software supply chain security? arXiv. arXiv
17. Anand, V., A. S. K., Vemulapalli, N., Loganathan, R., Guntupalli, A., & Ahammed, S. R. (2026). Federated Deep Learning for Decentralized Cybersecurity in Smart Grid Communication Networks. In 2026 14th International Conference on Smart Grid (icSmartGrid) (pp. 475–481). IEEE. 2026 14th International Conference on Smart Grid (icSmartGrid). <https://doi.org/10.1109/icsmartgrid70882.2026.11680752>
18. Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2023). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences*, 13(1), Article 395. MDPI
19. Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet*, 15(10), Article 324. MDPI
20. Potturi, P. (2026). Agentic Business Intelligence Architecture for Autonomous Data Exploration, Insight Generation, and Strategic Decision Orchestration. *International Journal of Computer Information Systems and Industrial Management Applications*, 18(22s), 536-542.
21. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, Article 101804. DOI
22. Gokkaya, B., Aniello, L., & Halak, B. (2023). Software supply chain: Review of attacks, risk assessment strategies and security controls. arXiv.
23. Penaka, B. (2026). AUTONOMOUS MULTI-AGENT AI FRAMEWORK FOR END-TO-END CLINICAL DECISION SUPPORT AND CARE COORDINATION. *Genetics and Molecular Research*.
24. Ruiz, R., & others. (2023). On the prevalence of software supply chain attacks: Empirical study and investigative framework. *Forensic Science International: Digital Investigation*, 44, Article 301508. ScienceDirect
25. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, Article 101804. DOI
26. Seenu, A., Kolla, S. H., Aitha, A. R., Amistapuram, K., Abhireddy, N., & Yandamuri, U. S. (2026, June). Agentic Enterprise Intelligence: A Unified Architecture for Secure RAG-Enabled LLM Automation in Insurance Risk and Fraud Ecosystems. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-5). IEEE.
27. Software supply-chain security: Issues and countermeasures. (2023). *Computer*, 56(7), 54–66. IEEE Xplore
28. Assessing the threat level of software supply chains with the log model. (2023). In 2023 IEEE International Conference on Big Data (BigData). IEEE. IEEE Xplore
29. Quinn, S., Pillitteri, V., Barrett, M., Smith, G., & Witte, G. (2024). NIST cybersecurity framework 2.0: Enterprise risk management quick-start guide. National Institute of Standards and Technology. NIST
30. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST cybersecurity framework (CSF) 2.0. National Institute of Standards and Technology. NIST
31. Singh, K. U., Gupta, S. K., Dubey, Y., & Mangalampalli, B. M. (2026, June). Enhancing Healthcare Cyber Defense with Machine Learning-Based Attack Prediction and Prevention. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-6). IEEE.
32. Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. (2024). NIST cybersecurity framework 2.0: Resource and overview guide. National Institute of Standards and Technology. NIST
33. Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. (2024). *Journal of Systems and Software*, 214, Article 112063. ScienceDirect
34. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. (2024). *Internet of Things*, 27, Article 101227. ScienceDirect
35. Suprith, M., Davuluri, P. N., Paramasamy, S., Yandamuri, U. S., & Motamary, S. (2026, June). AI-Enabled Business Process Reengineering for Agile and Data-Driven Organizations. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-6). IEEE.
36. Vakkalagadda, T., & Pareek, P. K. (2026). Self-Learning Artificial Intelligence Platforms for Autonomous Financial Risk Management. *International Journal of Special Education*, 41(15s), 238-254.
37. Supply chain risk analysis via SBOM data enrichment. (2025). In 2025 IEEE International Systems Conference (SysCon). IEEE. IEEE Xplore

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 24

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23

38. Swetha, T., Kumaran, U., Meena, V. P., & Hameed, I. A. (2025). Leveraging AI for enhanced cybersecurity: A comprehensive review. *Discover Applied Sciences*, 7, Article 584. Springer Nature
39. Hamid, I., & Rahman, M. M. H. (2025). AI, machine learning and deep learning in cyber risk management. *Discover Sustainability*, 6, Article 389. Springer Nature
40. Mahadevan, S. (2026). Governed Serverless Automation Ecosystem for AI-Driven Enterprise Integration and Sustainable Cloud Operations. *International Journal of Computer Information Systems and Industrial Management Applications*, 18(16s), 1561-1570.
41. Yan Azura, Y. T., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology*, 9, 85–104. Springer Nature
42. Gambo, M. L., & Almulhem, A. (2025). Zero trust architecture: A systematic literature review. *Journal of Network and Systems Management*. DOI
43. Arunakumari, M., Mattaparthi, R., Kothuri, S., Prakash, V. D., & Prasad, E. S. (2026, July). Data-Driven Framework for Real-Time Carbon Accounting and Sustainability Monitoring in Off-Grid Urban Residential Microgrids. In *2026 14th International Conference on Smart Grid (icSmartGrid)* (pp. 493-500). IEEE.
44. Zhang, J., Bu, H., Wen, H., Liu, Y., Fei, H., Xi, R., Li, L., Yang, Y., Zhu, H., & Meng, D. (2025). When LLMs meet cybersecurity: A systematic literature review. *Cybersecurity*, 8, Article 55. Springer Nature
45. Xu, D., Gondal, I., Yi, X., Susnjak, T., Watters, P., & McIntosh, T. R. (2025). The erosion of cybersecurity zero-trust principles through generative AI: A survey on the challenges and future directions. *Journal of Cybersecurity and Privacy*, 5(4), Article 87. DOI
46. Lezzi, M., Montefusco, P., Lazoi, M., & Corallo, A. (2025). AI-based cybersecurity for a sustainable digital industry: Systematic literature review and future research directions. *Journal of Industrial Information Integration*, 48, Article 100980. DOI
47. Nemani, R., Singuluri, I., Ramani, V. S., Guntupalli, A., Mopathi, U., & Madineni, A. V. S. (2026, July). A Machine Learning-Augmented Penalty Difference Approach for Transportation Cost Optimization. In *2026 14th International Conference on Smart Grid (icSmartGrid)* (pp. 511-516). IEEE.
48. Poirrier, A., Cailleux, L., & Clausen, T. H. (2025). Is trust misplaced? A zero-trust survey. *Proceedings of the IEEE*, 113(1), 5–39. researchgate.net
49. Ellenki, R. R., & Venkatesh, P. (2026). Collaborative AI Agent Architecture for Autonomous Retail Inventory and Allocation Management. *International Journal of Computer Information Systems and Industrial Management Applications*, 18(23s), 933-940.
50. Slapničar, S., Axelsen, M., & Eulerich, M. (2025). Cyber risk management: An illusion of a risk-based approach. *Journal of Management Control*.