

Beyond the Perimeter: The Impact of Zero Trust Security on Cybersecurity Resilience in U.S. Organizations

Author Name & Affiliations

Ethan Wexford

School of Computer and
Information Sciences

University of the Cumberland

wexford@ucumberland.edu

Article Processing History:

Received: 16 June 2026

Revised: 22 July 2026

Published: 10 Aug 2026

Index Terms :

Zero Trust Architecture; cybersecurity resilience; NIST SP 800-207; network security; identity and access management; critical infrastructure protection; U.S. cybersecurity policy.

Abstract

The evolution of cloud computing, remote working, and Internet of Things (IoT) deployments has made the traditional perimeter-based security model more outdated than ever, and led to a paradigm shift towards Zero Trust Architecture (ZTA) in the United States public and private sectors. This review brings together existing literature from peer-reviewed and institutional origin to assess the impact of Zero Trust security on the cybersecurity resilience of organizations. The review builds on guidance provided by the National Institute of Standards and Technology (NIST) and federal policy documents, including Executive Order 14028 and OMB Memorandum M-22-09, and a body of IEEE, Elsevier, and MDPI indexed studies to highlight the concept's foundations, architecture, models, and empirical results of Zero Trust adoption. The analysis shows that ZTA provides a tangible benefit in reducing lateral effort, it has the potential to limit the breach blast radius, increase detection and response, and offers certain constraints in multi-cloud and industrial environments, including legacy infrastructure, identity governance complexity, workforce readiness, and interoperability. The review ends with recommendations for critical success factors and future research areas such as developing standardized maturity metrics, AI-enabled continuous authentication, and quantifiable resilience indicators for U.S. organizations.

INTRODUCTION

The United States has long had an approach to enterprise cybersecurity that was based on a castle and moat structure where a hardened external network perimeter protects a trusted internal network domain. This is no longer true with the rise of cloud adoption, remote and hybrid working, BYOD policies and increasingly sophisticated adversaries that can move laterally once they have a foothold [1]. Major breaches using stolen credentials and supply-chain attacks proved that allowing any user, device, or network segment to access a system is an inherent vulnerability, not a safe bet [2].

Zero Trust Architecture (ZTA) is a rethinking of security that extends to the entirety of access requests, including those from outside the network, and applies the “never trust, always verify” model, meaning there is constant authentication and authorization required for every access [1]. The U.S. federal government officially endorsed this paradigm in Executive Order 14028, “Improving the Nation's Cybersecurity,” which mandates that federal civilian agencies have Zero Trust implementation plans [2], and in OMB Memorandum M-22-09, which sets out clear milestones and goals for Zero Trust across four distinct dimensions: identity, device, network, application, and data [3]. These requirements, bolstered by the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model [4] have spurred ZT uptake across the private sector, including defense contractors, financial institutions and critical infrastructure operators.

The questions this review aims to answer are: (1) What are the architectural and policy concepts that define Zero Trust in the U.S. context; (2) What are the empirical and analytical evidence of the impact of Zero Trust on organizational cybersecurity resilience; (3) What are the current barriers to the adoption of Zero Trust; and (4) What are the gaps to consider for future research. The review draws from NIST publications, U.S. federal policy documents, and IEEE-IACCP indexed papers and studies from IEEE Access, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Security, and other venues.

FROM PERIMETER DEFENSE TO ZERO TRUST: A CONCEPTUAL EVOLUTION

Perimeter-centric security architectures rely on the assumption that most security threats will come from outside the network and that once someone has been authenticated at the perimeter of the network, internal traffic should be implicitly trusted. Wherever the endpoints are mobile, there are third-party integrations, and the cloud workloads are spread across the distributed cloud, this assumption is invalidated [1], [8]. However, flat internal network designs allow attackers to move more freely across the organization to the high value assets, which is something Zero Trust is specifically targeting [8].

The concept of Zero Trust has been around for years; NIST Special Publication 800-207 is a collection of early concepts that eventually merged into a coherent architectural model of a Zero Trust – a set of evolving paradigms, shifting the focus from static, network-based perimeters to users, assets, and resources [1]. Later, systematic literature reviews document the evolution of this model from a conceptual model to an actual deployment pattern in enterprise [6], cloud-native [9] and industrial settings.

ZERO TRUST ARCHITECTURE: CORE PRINCIPLES AND COMPONENTS

FOUNDATIONAL TENETS

NIST SP 800-207 defines tenets of ZTA: all data sources and computing services are viewed as resources; all communications are secured in any location; access is granted on a per-session basis; access is determined dynamically by policy that incorporates identity, device posture, behavioral attributes, environmental attributes; and the organization continuously monitors and measures the security posture of all owned and associated assets [1]. Syed et al. combine these tenets into a reference model that includes a policy engine, a policy administrator, and policy enforcement points which intervene in each access decision [6].

ARCHITECTURAL COMPONENTS

Implementing Zero Trust involves the coordination of identity and access management, device trust and posture assessment, micro-segmentation, encrypted communication, and continuous monitoring and analytics. Phiayura and Teerakanok suggest a complete migration model that progresses these elements in deployable steps and note that, in most cases, identity governance is the most feasible and impactful initial step for organizations moving from legacy architectures. In a cloud-native and multi-cloud world, additional needs exist for workload identity and service-to-service authentication, as outlined in NIST SP 800-207A—Access Control Patterns for Containerized and API-Mediated Architectures by NIST [5].

The “never trust, always verify” approach is also implemented at the session level through continuous authentication mechanisms. Hong et al. introduce a near real-time, fine-grained, continuously evaluated access policy enforcement mechanism, SysFlow, at the system-call level, which detects and contains abnormal access behavior [15]. Likewise, Meng et al. and related continuous-authentication protocols limit the time window, given to an adversary using stolen credentials, for a static, session-initiation-only trust decision.

SEGMENTATION AND NETWORK-LAYER CONTROLS

Micro-segmentation is able to limit the reach of a breach by breaking networks into small segments, with their own policies that can be enforced separately. In hybrid on-premises and cloud environments, where legacy flat network topologies remain, the attack surface for lateral movement can be significantly decreased by implementing network segmentation combined with Zero Trust policy enforcement, as shown by Simpson and Foltz [17].

Network segmentation

is a security practice that divides a network into smaller, isolated segments to enhance security and performance.

There are **four primary types** of Network Segmentations.



Firewall Segmentation

- i** Uses firewalls to create internal zones within a network.
- +** Complex to configure and expensive.
- Can lead to service interruptions if misconfigured.

Network Segmentation with VLANs and Subnets

- i** Divides networks using VLANs or subnets.
- +** Improves network performance and security.
- Requires frequent infrastructure changes and complex ACL management.

Micro-Segmentation

- i** Uses host-based firewalls to segment workloads.
- +** Provides granular control down to the process level.
- Requires workload telemetry and may require new skills for administrators.

Segmentation with SDN

- i** Uses software-defined networking to create virtual networks.
- +** Provides granular control and easier administration.
- +** Assumes all devices are untrusted by default.
- Can be complex to implement for large-scale environments.

Fig 1: Network Segmentation

U.S. POLICY AND REGULATORY DRIVERS

The top-down pressure on organizations to implement Zero Trust has noticeably spurred its adoption in the United States, as opposed to organic demand. In May 2021, Executive Order 14028, following a series of high-impact cyberattacks on public and private infrastructure, mandated federal agencies to create a plan to implement ZTA and eliminate implicit trust on networks as a top priority [2]. OMB Memorandum M-22-09 was translated into a five-pillar plan: identity, devices, networks, applications and workloads, and data, which will include technical requirements including phishing-resistant multi-factor authentication and end-to-end encryption, by the end of fiscal year 2024 [3].

CISA's Zero Trust Maturity Model supports these mandates by providing agencies (and by extension, private-sector organizations that follow federal guidance) with a continuum of maturity from traditional to optimal on the same five pillars, providing them the ability to compare and contrast their level of maturity and prioritize investment accordingly [4]. The practical impact of the Zero Trust policy extends beyond federal civilian agencies, as many U.S. organizations are federal contractors or part of regulated critical-infrastructure sectors, and these federal requirements have spread into the private sector through procurement and compliance requirements, such as the Department of Defense's Cybersecurity Maturity Model Certification ecosystem.

IMPACT OF ZERO TRUST ON CYBERSECURITY RESILIENCE

BREACH CONTAINMENT AND ATTACK-SURFACE REDUCTION

Although this is not always the case, a common theme in the reviewed literature is that Zero Trust helps to enhance resilience by containing, not just preventing, compromise. A successful initial intrusion is not likely to lead to widespread network compromise as access is continually evaluated and limited to the lowest common denominator of required resource [6, 8]. In industrial IoT infrastructures, Zanasi et al. show how a flexible Zero Trust architecture reduces the spread of polluted traffic from operational technology across flat industrial networks [11].

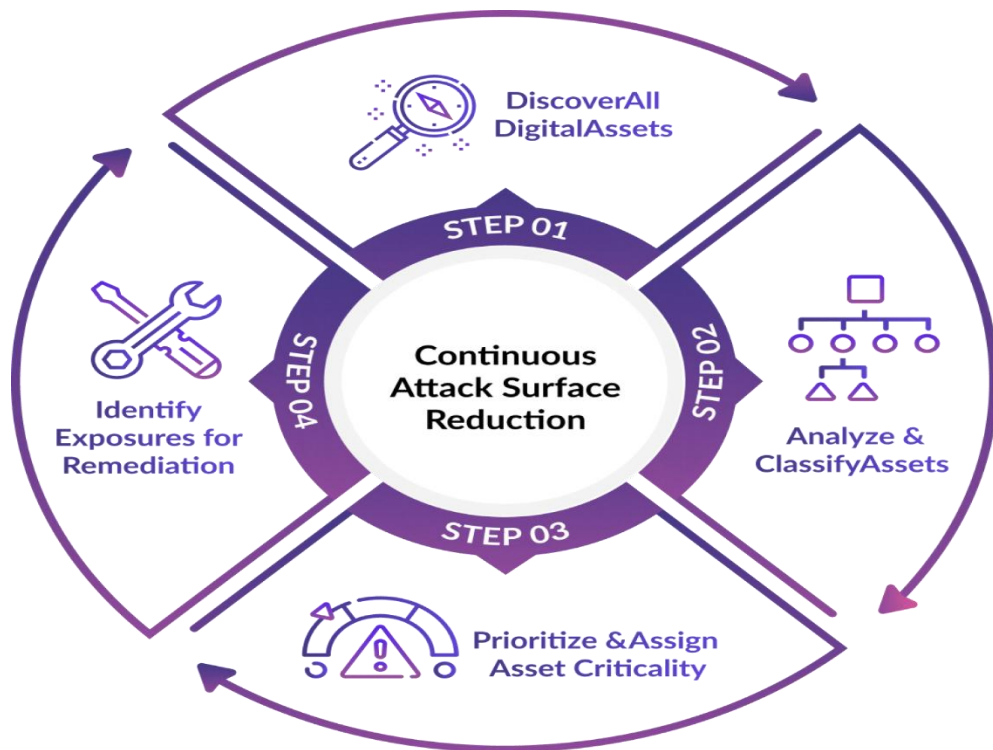


Fig 2: Breach Containment & Attack-Surface Reduction

IDENTITY-CENTRIC RESILIENCE IN CLOUD AND MULTI-CLOUD ENVIRONMENTS

The identity is the de facto control plane for resilience, as more and more organizational assets are being placed outside any one network boundary. In this work, the authors, Dhanapala et al., demonstrate that performance-aware, trust-based access-control models maintain security guarantees in distributed systems of edge-cloud continuums without significant performance impact, which is a recurring issue against Zero Trust controls affecting operational performance [19]. The attack surface of heterogeneous IoT and edge devices, which have historically been hard to secure under perimeter models, is also greatly reduced by the use of identity- and context-aware verification, as found by Azad et al. [12].

ORGANIZATIONAL AND MATURITY-BASED DETERMINANTS OF RESILIENCE OUTCOMES

It's important to note that adopting Zero Trust terminology or point products is not an automatic gain in resilience, but depends on the maturity of the organization. In this regard Yeoh et al. share with us critical success factors that separate

organizations that experience measurable gains in resilience from others who have a partial or superficial uptake of the changes, among which executive sponsorship, cross-functional governance, and phased implementation roadmaps stand out, and suggest a maturity assessment framework to measure that difference [14]. This is in line with He et al., which refer to the journey of Zero Trust as an incremental process, rather than a discrete technology deployment, and that the benefits of resilience are realized over time as the controls of the identity, device and data layers evolve in parallel [13].

AUTOMATION, ORCHESTRATION, AND RESPONSE VELOCITY

Manual policy administration is impractical at scale, as Zero Trust policy decisions need to be made on an ongoing basis. Cao et al. examine a range of automation and orchestration techniques that incorporate policy engines with security information and event management (SIEM) and extended detection and response (XDR) tooling, and argue that automated policy orchestration is a necessary precondition for delivering real measurable gains in speed of detection and response, one of the primary considerations of operational resilience, when based on Zero Trust principles [16].

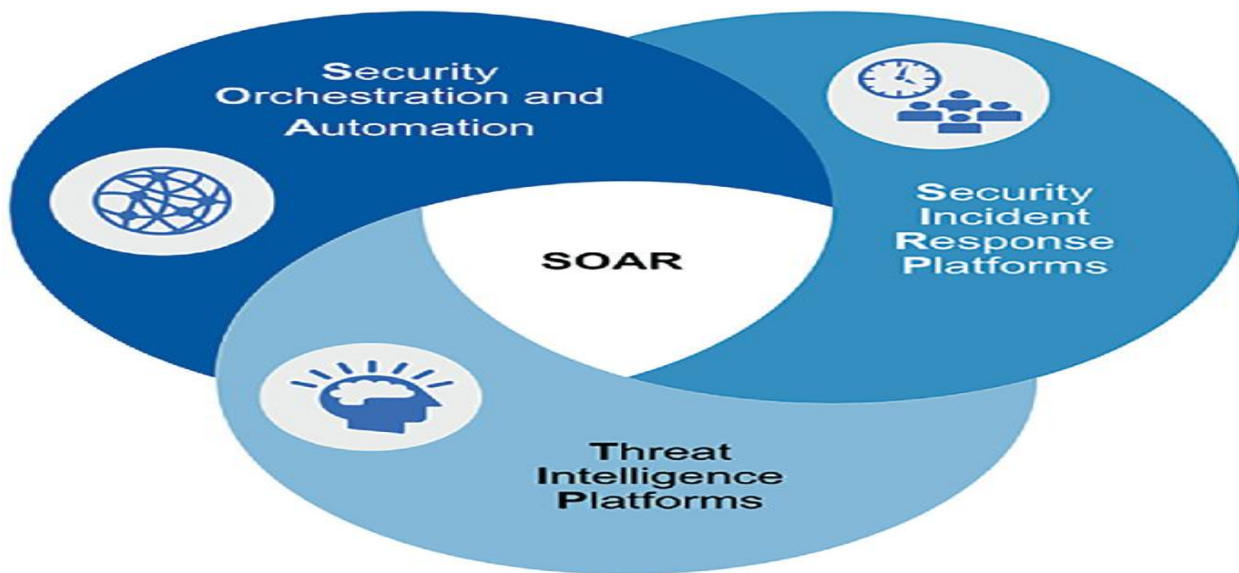


Fig 3: Automation, Orchestration & Response Velocity

Structured Zero Trust validation exercises by organizations found in empirical validation research by Bobbert and Scheerder, show that a significant number of these organizations discover much more policy gaps than those who only rely on self-reported maturity assessments, which reinforces the need that the Zero Trust program is always verified, not only of its users and devices but also the program itself [18].

SECTOR APPLICATIONS AND IMPLEMENTATION CONTEXTS

There are some distinct differences in the approach to implementing Zero Trust, by sector. Phishing-resistant identity controls [2, 3] are a key focus with implementation in federal and defense-adjacent environments required by compliance deadlines in EO 14028 and M-22-09. Zero Trust in industrial and critical-infrastructure environments must also support legacy operational-technology protocols and safety requirements that will not allow the rapid network changes that can be

made in pure information-technology environments, which is being met with flexible, phased segmentation architectures [11]. However, in a cloud-native enterprise context, Zero Trust is more than just about humans; it's also about workload and service identities, which is particularly enabling in this case, and this is best expressed in formal models like those described by SPIFFE in the NIST SP 800-207A [5]. A number of comparative studies, such as those by Dhiman et al. and Fernandez and Brazhuk, have found that there is no universal reference architecture for Zero Trust; that is, the principles it represents can be implemented in multiple ways to suit the risk appetite, legacy constraints, and regulatory environment of an organization [10, 20].

IMPLEMENTATION CHALLENGES AND CRITICAL SUCCESS FACTORS

However, there are ongoing challenges in the U.S. for organizations to adopt Zero Trust, despite the known benefits for resilience. Many legacy systems and monolithic applications are generally not constructed with granular authentication hooks that enable policy enforcement per session, which leaves organizations trapped in a time-consuming and costly modernization process before they can effectively implement Zero Trust controls [7], [9]. As organizations roll out Zero Trust to machine and service identities, as well as workloads, identity-governance complexity grows significantly, which many early implementations underestimate [5], [12]. Fernandez and Brazhuk provide a critical examination and warn that in some instances, vendor marketing has surpassed architectural rigor, such as the “Zero Trust” label being used on products that do not actually provide the ongoing, policy-driven verification that the model demands, rendering the true level of maturity difficult to assess [10].

Workforce readiness and organizational governance is another obstacle: Yeoh et al. conclude that where cross-functional ownership of security, network, and application teams is lacking, it's one of the strongest indicators of unsuccessful or superficial Zero Trust initiatives [25]. Multi-cloud and hybrid scenarios present another challenge for interoperability, as no common policy-exchange format exists for policy engines from various vendors and platforms as mentioned in a number of surveys reviewed [23, 24, 19]. Combining these results, key U.S. organizations that have been successful in deploying Zero Trust point-to-point have included: Exec. Sponsorship and dedicated governance structures, phased and identity-first implementation roadmaps, automated policy orchestration to sustain enforcement at scale, and continuous, evidence-based validation of Zero Trust controls as opposed to point-in-time compliance attestations [14, 16, 18].

FUTURE RESEARCH DIRECTIONS

There are still a number of gaps requiring further research. One, there are no uniform, measurable metrics for cybersecurity resilience associated with Zero Trust controls specifically, rather than with subsequent investments in other security initiatives, as such measurements would bolster causal statements currently made, through architectural analysis and case description, in part. Second, the promise of AI and machine learning in continuous authentication and anomaly detection is still a work in progress, and there is considerable potential for empirical evaluation with real-world, enterprise-level systems like programmable enforcement frameworks (Pef) such as SysFlow [15]. Third, the applicability of Zero Trust principles to resource constrained environments for IoT and operational-tech applications while avoiding prohibitive latency and

availability risk is not fully solved [11, 12]. Lastly, comparative policy studies on differences and similarities in the patterns of federal implementation and private-sector adoption could help to better understand how far the federal Zero Trust policies go to achieve national security resilience and to what degree, as they pass their original FY targets [2] [3] [4].

CONCLUSION

Zero Trust Architecture is a radical shift from perimeter oriented security, based on the fundamental concept that “never trust, always verify.” The evidence reviewed shows that U.S. organizations that deploy Zero Trust – and those with more advanced identity governance, automated policy orchestration and cross-functional ownership – see measurable benefits in breach containment, attack surface reduction and response speed. Executive Order 14028, OMB Memorandum M-22-09, and CISA's Zero Trust Maturity Model are important enablers for adoption, both in the public and private sectors. However, the pace and consistency of implementation remains constrained by legacy infrastructure, identity-governance complexity and the lack of common metrics for resilience. There is a need for further empirical study, particularly longitudinal and metric studies, to better quantify the relationship between Zero Trust maturity and the organization's cybersecurity resilience.

REFERENCES

- [1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2020, doi: 10.6028/NIST.SP.800-207.
- [2] Executive Office of the President, “Executive Order 14028: Improving the Nation’s Cybersecurity,” Federal Register, Washington, DC, USA, May 12, 2021.
- [3] Office of Management and Budget, “M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” Memorandum for Heads of Executive Departments and Agencies, Washington, DC, USA, Jan. 26, 2022.
- [4] Cybersecurity and Infrastructure Security Agency, “Zero Trust Maturity Model, Version 2.0,” U.S. Department of Homeland Security, Washington, DC, USA, 2022.
- [5] S. T. Hasan, “Predictive modeling for labor law risk detection in Medicaid funded home care programs in New York: Forecasting overtime exposure, payroll errors, and workforce compliance gaps,” *Int. J. Bus. Integrity Technol. Advancements*, vol. 1, no. 1, pp. 1–10, 2025.
- [6] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, “Zero Trust Architecture (ZTA): A comprehensive survey,” *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.
- [7] P. Phiayura and S. Teerakanok, “A comprehensive framework for migrating to zero trust architecture,” *IEEE Access*, vol. 11, pp. 19487–19511, 2023, doi: 10.1109/ACCESS.2023.3248622.
- [8] E. Bertino, “Zero trust architecture: Does it help?,” *IEEE Security & Privacy*, vol. 19, no. 5, pp. 95–96, Sep./Oct. 2021, doi: 10.1109/MSEC.2021.3091195.
- [9] I. Kate, “Marketing innovation in the US e-commerce sector: Strategies for success in the evolving digital environment,” *Int. J. Bus. Integrity Technol. Advancements*, vol. 1, no. 2, pp. 1–7, 2025.

- [10] U. Imtiaz, B. Ahmad, M. H. Sajid, Q. Abbas, M. A. Qureshi, S. Rasheed, and A. Khan, “An integrated machine learning framework for structural health monitoring of bridges: A case study on Soan Bridge,” *The Asian Bulletin of Big Data Management*, vol. 5, no. 2, pp. 194–207, 2025.
- [11] U. Imtiaz and H. Elbedour, “Cybersecurity risk management in the digital era: The strategic value of ethical hacking,” *Spectrum of Engineering Sciences*, pp. 1076–1086, 2025.
- [12] S. M. H. Shah, F. Amin, and A. Khan, “Cyber-resilient mobile edge computing: A deep neural approach for secure and efficient task offloading,” *The Asian Bulletin of Big Data Management*, vol. 5, no. 1, pp. 200–215, 2025.
- [13] M. Z. Islam, I. Ahmed, R. Parveen, S. T. H. Rimon, and J. I. Janjua, “Revolutionizing healthcare for critical diseases with AI and enhancing security via low-latency edge intelligence,” in *Proc. 2025 Int. Conf. AI-Driven STEM Education and Learning Technologies (AISTEMEDU)*, Piscataway, NJ, USA: IEEE, Dec. 2025, pp. 1–6.
- [14] A. Khan, U. Imtiaz, and F. Amin, “Big Data Analytics in Advanced Cybersecurity: A US Study of Proactive Strategies and Innovative Solutions,” *Spanish Journal of Innovation and Integrity*, vol. 54, pp. 163–180, 2026.
- [15] R. Bhattacharya, J. Mukherjee, S. Roy, M. T. Rana, and R. Parveen, “Eco-crypto dynamics: Cointegration of green and non-green cryptocurrencies for sustainable investing,” *Advances in Consumer Research*, vol. 2, no. 3, 2025.
- [16] I. A. Badhan, M. N. Hasnain, and M. H. Rahman, “Advancing operational efficiency: An in-depth study of machine learning applications in industrial automation,” *Policy Research Journal*, vol. 1, no. 2, pp. 21–41, 2023.
- [17] U. Iqbal and Y. Bhutto, “Digital transformation through artificial intelligence and advance business analytic in American operational management,” *Journal of Theoretical and Applied Econometrics*, vol. 3, no. 1, pp. 37–50, 2026.
- [18] M. R. Islam, I. A. Badhan, M. H. Rahman, and M. N. Hasnain, “The economics of global renewable energy supply chains: Opportunities and vulnerabilities for the U.S.,” *International Journal of AI, Engineering and Management Studies (IJAIEMS)*, vol. 1, no. 1, pp. 108–136, 2026.
- [19] U. Iqbal, S. Bekmez, and F. A. Qurashi, “Operational risk management through machine learning and business intelligence in U.S. businesses,” *Spanish Journal of Innovation and Integrity*, vol. 54, pp. 239–253, 2026.
- [20] I. Alim, R. N. Meghla, T. F. Matin, and T. M. M. H. Prodhan, “A semantic and behavioral AI framework for detecting invoice fraud in automated accounts payable,” *International Journal of Science and Research Archive*, vol. 19, no. 2, pp. 1356–1380, 2026.
- [21] S. T. Hasan, “Predictive modeling for labor law risk detection in Medicaid funded home care programs in New York: Forecasting overtime exposure, payroll errors, and workforce compliance gaps,” *Int. J. Bus. Integrity Technol. Advancements*, vol. 1, no. 1, pp. 1–10, 2025.
- [22] A. Kumar, “The role of banking credit access in healthcare analytics-driven practice growth: Implications for regional economic development in the US,” *J. Comput. Syst. Eng. Insights*, vol. 2, no. 2, pp. 15–28, 2024.

- [23] M. Chaudhari, “Hydrophilic Nanofiber Barrier Coatings for Aluminum: Waterborne Crosslinking, Microstructure–Property Links, and EIS-Based Protection,” *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3017, Jul. 27, 2026, doi: 10.4238/rhd2k915.
- [24] M. Chaudhari, “R2R Plasma-Textured Polymer Films: Nanostructured AR/Hydrophobic Surfaces and EB Cured Varnish Proxies for Scalable Coatings,” *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3018, Jul. 27, 2026, doi: 10.4238/e5d1rq05.
- [25] M. S. Islam, F. Ahmed, W. Ishtiaq, et al., “Advanced explainable ensemble models for multi-class intrusion detection in heterogeneous drone and industrial networks,” *J. Inf. Secur.*, vol. 14, 2026, doi: 10.1186/s13635-026-00234-w.