INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume10 Issue11, November -2025, pg. 66-75

Published Date: - 30-11-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

A Comprehensive Theoretical Framework for Zero-Trust Migration and Adaptive Defense in Multi-Tenant Cloud Environments: Mitigating Lateral Movement, DDoS, and Identity-Based Threats

Dr. Mariana López

Department of Computer Science, Universidad Internacional del Pacífico

Abstract: This article presents a comprehensive, publication-ready theoretical synthesis and framework addressing the security challenges of migrating to and operating within multi-tenant cloud environments under the paradigm of Zero Trust Architecture (ZTA). The study integrates interdisciplinary perspectives — cloud migration security, identity and access management (IAM), lateral movement detection and mitigation, distributed denial of service (DDoS) defense, load balancing optimization, deception and resilience strategies, and the application of artificial intelligence to behavioral analytics — to construct a cohesive research agenda and prescriptive architecture for practitioners and researchers. Drawing on a curated set of contemporary doctoral dissertations, peer-reviewed surveys, domain white papers, industry blogs, and governmental guidance, the framework articulates the theoretical rationale for adopting ZTA in cloud migrations, details identity-centric controls and AI-augmented IAM mechanisms, explicates lateral movement attack vectors and evidence-reasoning detection models suitable for edge-to-cloud topologies, examines DDoS defensive architectures and their interplay with multi-tenant load balancing, and proposes layered deception and resilience techniques to harden tenant isolation and minimize blast radius. The methodology is conceptual and analytical; it synthesizes existing empirical and theoretical findings to generate testable propositions, design patterns, and operational guidance for secure cloud transformations. The article concludes with a detailed discussion of implementation trade-offs, limitations of current research, regulatory and operational considerations, and a roadmap for future empirical validation. This contribution aims to bridge the gap between high-level ZTA advocacy and the implementable defensive mechanisms required for complex, shared cloud ecosystems.

Keywords: Zero Trust Architecture, cloud migration security, lateral movement detection, identity and access management, DDoS defense, deception, multi-tenant cloud

INTRODUCTION

Cloud computing has become the de facto model for enterprise digital transformation; organizations migrate applications, data, and business processes to public, private, or hybrid cloud platforms to obtain elasticity, cost efficiency, and operational agility (Shitta-Bey & Adewole, 2023). However, this migration substantially alters the attack surface and threat dynamics confronting organizations. Cloud migration introduces new security concerns: tenant co-residency risks, expanded identity surfaces, network segmentation complexities, and novel lateral movement opportunities for advanced adversaries (Shitta-Bey & Adewole, 2023; FORTRA Terranova Security, 2023). The literature increasingly recognizes that legacy perimeter-centric models are insufficient for cloud deployments, especially within multi-tenant contexts where tenants share infrastructure resources and rely on provider-managed controls (Rose, 2022; House, 2021). Against this backdrop, Zero Trust Architecture (ZTA) — which rejects implicit trust based on network location and instead enforces continuous, context-aware verification of every access request — has emerged as a leading paradigm for redesigning cybersecurity in cloud environments (Rose, 2022; Phiayura & Teerakanok, 2023).

Despite strong theoretical endorsement and federal guidance for ZTA (House, 2021; Rose, 2022; CISA), the operationalization of ZTA in multi-tenant clouds is fraught with unresolved technical and organizational challenges. These include the scalability of continuous authentication and authorization, the integration of Identity and Access Management (IAM) systems with AI-assisted behavioral analytics, detection of lateral movement in horizontally distributed cloud-edge topologies, and preserving performance and availability during DDoS mitigation and load balancing (Singh, Thakkar & Warraich, 2023; Olabanji et al., 2024; Tian et al., 2019; Agrawal & Tapaswi, 2019). Moreover, recent critical analyses have pointed out gaps and ambiguities in the ZTA concept as currently published, highlighting the need for rigorous, prescriptive frameworks that translate ZTA principles into implementable controls for cloud service providers and tenants (Fernandez & Brazhuk, 2024).

This article responds to that need by synthesizing and elaborating the state of knowledge on cloud migration security and ZTA, integrating cross-domain defensive constructs (e.g., deception, AI-enabled IAM, meta-heuristic load balancing) and proposing a conceptual architecture tailored to multi-tenant cloud environments. The problem statement addressed here is: How can organizations migrating to multi-tenant clouds adopt a Zero Trust posture while effectively mitigating lateral movement, DDoS attacks, and IAM weaknesses without sacrificing operational efficiency? The literature gap is twofold: first, a scarcity of integrated frameworks that reconcile identity, detection, mitigation, and performance concerns under ZTA for multi-tenant clouds; second, a lack of analytic synthesis linking research on lateral movement detection, AI for IAM, DDoS defense, and load balancing into coherent design patterns and evaluative hypotheses. This work fills those gaps by offering a theoretically grounded, richly detailed framework, articulating testable propositions and detailed design considerations for future empirical study.

METHODOLOGY

The methodology employed is conceptual synthesis and analytic framework development applied to the provided corpus of contemporary scholarly and practitioner references. This is not an empirical experiment; rather, the method is a structured integrative review augmented by design science reasoning. The approach comprises four interrelated steps:

1. Systematic thematic extraction. Each reference was parsed to extract key constructs, mechanisms, and empirical claims relevant to cloud migration security, ZTA, IAM, lateral movement, DDoS defense, load balancing, deception, and AI-enabled detection. For example, doctoral-level analyses of cloud migration security illuminated business transformation risks and organizational implications (Shitta-Bey & Adewole, 2023), while survey literature on DDoS defenses provided taxonomy and identified research gaps in mitigation strategies (Agrawal & Tapaswi, 2019). Evidence-reasoning models for lateral movement were identified in industrial and academic work (Tian et al., 2019; WIZ, 2023), and meta-heuristic approaches to load balancing were sourced from computational operations research literature (Milan et al., 2019).
2. Cross-domain mapping. Extracted themes were mapped to one another to identify interaction points, conflicts, and synergies. For instance, the demands of continuous authentication under ZTA map directly to IAM scalability concerns and the potential for AI to augment authentication decisions (Singh et al., 2023; Olabanji et al., 2024). Similarly, DDoS defense techniques interact with load balancing algorithms and may be at odds with tenant isolation goals unless carefully designed (Agrawal & Tapaswi, 2019; Milan et al., 2019).
3. Framework construction. A layered, identity-centric ZTA framework was designed to integrate detection, control, and resilience mechanisms. The design is guided by ZTA planning guides and federal recommendations (Rose, 2022; House, 2021), incorporates critical analyses of ZTA limitations (Fernandez & Brazhuk, 2024), and embeds state-of-the-art lateral movement detection (Tian et al., 2019), AI for IAM (Olabanji et al., 2024; Martín et al., 2021), deception and cyber resilient education constructs (Steingartner, Galinec & Kozina, 2021), and practical considerations for cloud storage security (FORTRA Terranova Security, 2023).
4. Propositional elaboration and operational guidance. From the constructed framework, a set of design patterns, principles, and testable propositions for future empirical evaluation were derived. This includes prescriptive recommendations for IAM instrumentation, telemetry aggregation for evidence-reasoning networks, DDoS mitigation patterns that preserve tenant QoS, and the controlled introduction of deception for blast radius reduction.

Throughout, claims and design choices were cross-referenced to the supplied literature to ensure traceability and to ground propositions in extant research. The method emphasizes thorough textual explanation rather than mathematical formalism, reflecting the practitioner and policy orientation of the article and respecting the constraint against including mathematical notation or tables.

RESULTS

The results present the synthesized theoretical constructs, the proposed integrated Zero Trust framework for multi-tenant clouds, and a set of analytical findings that emerge from the cross-domain mapping. The presentation is descriptive and detailed to facilitate conceptual replication and future empirical operationalization.

A. The Identity-First Posture

The synthesis underscores that identity is the fulcrum of effective cloud security. Identity and Access Management (IAM) systems are not merely authentication repositories; they are dynamic policy engines that must interoperate with telemetry, behavioral analytics, and enforcement points across cloud control planes (Singh, Thakkar & Warraich, 2023; Olabanji et al., 2024). The move to ZTA requires IAM to evolve from static role mappings to probabilistic, context-aware decision making that ingests device posture, network context, user behavior, and historical risk signals (Rose, 2022; Phiayura & Teerakanok, 2023). The result is a policy fabric where access is continuously re-evaluated rather than granted once per session. This continuous evaluation model amplifies the need for high-fidelity telemetry and low-latency decision loops; it implies architectural proximity between telemetry collectors and policy decision points to avoid performance penalties and to provide timely mitigation against active threats (Shitta-Bey & Adewole, 2023; Fernandez & Brazhuk, 2024).

B. AI-Augmented IAM and User Behavior Analytics

Machine learning and AI enhance IAM by enabling user behavior analysis (UBA), anomaly detection, and adaptive authentication. Surveys and empirical studies show that behavioral biometrics, time-series analysis of authentication events, and supervised classification techniques can distinguish legitimate deviations from malicious anomalies when trained on representative datasets (Martín et al., 2021; Olabanji et al., 2024). The integration of AI into IAM must be carefully designed: models require explainability for auditability and must be robust to adversarial manipulation. The literature cautions against overreliance on opaque models without rigorous validation because attackers can attempt to poison telemetry or craft mimicry behaviors (Martín et al., 2021; Olabanji et al., 2024). Consequently, AI components should operate in hybrid modes where model recommendations influence but do not unilaterally decide high-impact actions — for example, AI can raise risk scores that prompt step-up authentication or session isolation rather than fully blocking access without human oversight (Singh et al., 2023; Olabanji et al., 2024).

C. Evidence-Reasoning Networks for Lateral Movement Detection

Lateral movement — the stage where attackers traverse from a breached entry point to high-value assets — presents severe challenges in distributed cloud and edge systems. Evidence-reasoning networks (ERNs) have been proposed as a means to correlate heterogeneous telemetry streams (system logs, network flow metadata, process creation events) and reason about causal chains that indicate lateral progression (Tian et al., 2019). ERNs encode evidential rules and abductive reasoning to assess the likelihood that a sequence of events represents malicious lateral movement rather than benign administrative activity. In cloud settings, ERNs must be extended to incorporate multi-tenant telemetry provenance, tenant identifiers, resource tagging, and provider metadata to avoid false positives resulting from legitimate cross-tenant orchestration (Tian et al., 2019; WIZ, 2023). ERN effectiveness depends on quality labeling of event patterns and robust correlation of temporally dispersed signals; thus, instrumenting consistent, high-granularity telemetry pipelines is a prerequisite (Tian et al., 2019).

D. DDoS Defense in Multi-Tenant Clouds and its Interaction with Load Balancing

DDoS attacks threaten availability and can be especially disruptive in shared infrastructures where mitigation must avoid collateral damage to uninvolved tenants. Surveys of DDoS defense identify layered mitigations: edge filtering, scrubbing centers, rate limiting, and application-level hardening (Agrawal & Tapaswi, 2019). In multi-tenant clouds, load balancing is both a performance enabler and a potential leverage point for selective DDoS mitigation; advanced load balancing strategies can redistribute load to mitigate volumetric bursts, but naive load redistribution can exacerbate cross-tenant interference if tenant isolation is not preserved (Milan et al., 2019; Agrawal & Tapaswi, 2019). Meta-heuristic algorithms (e.g., particle swarm optimization, genetic algorithms) provide promising approaches for adaptive load balancing under adversarial conditions by dynamically optimizing resource allocation with multiple objectives (latency, fairness, cost) while responding to evolving attack patterns (Milan et al., 2019). The literature suggests that integrating DDoS detection signals with load balancing orchestration — while maintaining per-tenant QoS policies — yields better outcomes than static, one-size-fits-all mitigation (Agrawal & Tapaswi, 2019; Milan et al., 2019).

E. Deception and Cyber Resilience

Deceptive defenses, including honeypots, honeytokens, and active misdirection, form an additional layer in the proposed framework. Deception increases adversary uncertainty and provides high-value forensic data that can be used to refine detection models (Steingartner, Galinec & Kozina, 2021). When used strategically within ZTA, deception can be employed to direct suspicious activity into controlled conduits where evidence-reasoning mechanisms operate with elevated surveillance. However, deception must be applied judiciously in multi-tenant clouds to avoid entanglement with legitimate tenant traffic and to prevent legal or compliance issues (Steingartner et al., 2021). Effective deception requires close integration with IAM (to validate actor identities), telemetry pipelines (to route and collect deceptive engagement data), and incident response playbooks (to extract intelligence) (Steingartner et al., 2021).

F. Critical Appraisal of Zero Trust Adoption Challenges

Critical analyses of ZTA highlight conceptual ambiguities and implementation challenges that must be addressed in practice (Fernandez & Brazhuk, 2024). Key issues include the limitless surface of identity that requires governance, the operational cost of continuous verification, and the potential for degraded usability if step-up authentication is poorly tuned. Federal planning guides emphasize the phased adoption of ZTA, prioritizing high-value applications and leveraging existing IAM investments (Rose, 2022; House, 2021). Empirical reports from vendor studies claim high returns on investment for ZTA initiatives, but independent evaluations are limited, and vendor claims must be weighed against operational realities (Jakkal, 2023). The synthesis concludes that ZTA is a necessary conceptual shift for cloud security but requires precise operational blueprints — particularly in multi-tenant environments where provider and tenant responsibilities must be carefully delineated (Fernandez & Brazhuk, 2024; Rose, 2022).

G. Operational Patterns and Design Principles

From the integration work, the article derives a set of operational design principles:

1. Identity prioritization with telemetry fusion: Centralize identity signals while aggregating device and network telemetry at the enforcement edge to minimize latency for continuous evaluation (Singh et al., 2023; Rose, 2022).

2. Hybrid AI governance: Use AI for risk scoring and anomaly detection, but preserve human-in-the-loop controls for high-impact actions and auditability requirements (Martín et al., 2021; Olabanji et al., 2024).
3. Multi-layered DDoS and load balancing coordination: Couple detection with adaptive meta-heuristic load balancing strategies while preserving tenant isolation (Agrawal & Tapaswi, 2019; Milan et al., 2019).
4. Evidence-reasoning for lateral movement: Deploy ERN-based correlation engines that incorporate cloud metadata and tenant context to reduce false positives (Tian et al., 2019; WIZ, 2023).
5. Controlled deception: Introduce deception in designated zones with strict tenant tagging and legal review to enrich detection intelligence (Steingartner et al., 2021).
6. Governance and phased deployment: Follow phased ZTA adoption plans focused on critical assets and iteratively expand controls informed by measured operational impact (Rose, 2022; Phiayura & Teerakanok, 2023).

These principles translate into design patterns, such as proximate policy decision points co-located with telemetry collectors, identity-anchored microsegmentation, AI-driven risk score pipelines with explainability layers, and load balancing controllers that accept risk signals to prioritize critical tenant traffic during mitigations.

DISCUSSION

This section interprets the synthesized findings, explores theoretical implications, discusses limitations, and outlines avenues for future research.

A. Theoretical Interpretation and Contributions

The principal theoretical contribution is the articulation of an identity-anchored, evidence-centric ZTA framework that reconciles disparate literatures into a coherent architecture suitable for multi-tenant clouds. The framework advances three conceptual points:

1. Identity as control plane. While identity has been recognized as critical, this framework elevates identity to the primary control plane for both authentication and dynamic access policy enforcement across provider and tenant boundaries (Singh et al., 2023; Rose, 2022). This reconceptualization requires rethinking telemetry, placing identity context at the core of network, compute, and storage authorization decisions.
2. Evidence-reasoning as analytic glue. The ERN paradigm provides a robust, explainable approach to linking disparate signals into coherent narratives of adversary behavior — particularly lateral movement — which is essential in environments where attackers exploit distributed services (Tian et al., 2019). The explanatory power of ERNs helps bridge explainability requirements in AI-augmented IAM.
3. Operationalized ZTA for shared infrastructures. The framework shows how ZTA principles can be operationalized with concrete mechanisms — AI-assisted IAM, meta-heuristic load balancing integration, deception zones, and ERN pipelines — all within the constraints of multi-tenant performance and compliance needs (Fernandez & Brazhuk, 2024; Milan et al., 2019; Steingartner et al., 2021).

These contributions respond to the literature gap by moving beyond high-level prescriptions and delivering a prescriptive set of patterns and hypotheses suitable for empirical instrumentation and validation.

B. Practical Implications for Cloud Providers and Tenants

The proposed framework implies concrete roles for both cloud providers and tenants. Providers should expose rich, tenant-scoped telemetry APIs, implement proximate policy decision points (possibly as managed services), and support tenant isolation semantics that integrate with deception and ERN pipelines (Shitta-Bey & Adewole, 2023; Tian et al., 2019). Tenants, in turn, must invest in IAM maturity, accept hybrid AI governance models for continuous access evaluation, and design application architectures that are amenable to microsegmentation and identity-aware routing (Singh et al., 2023; Olabanji et al., 2024). The shared responsibility model must be finely specified in service contracts to avoid ambiguity about who is responsible for telemetry retention, analysis, and incident response, particularly when deception mechanisms are employed.

C. Limitations and Areas of Uncertainty

Several limitations constrain the generalizability of the framework:

1. Evidence base composition. The synthesis primarily utilizes the provided corpus, which — while contemporary and diverse — is not exhaustive. Some assertions draw on practitioner blogs and vendor reports (FORTRA Terranova Security, WIZ, Microsoft Security Blog), which provide useful operational perspective but may present biased or promotional views (FORTRA Terranova Security, 2023; Jakkal, 2023).
2. Operational complexity and performance trade-offs. Continuous evaluation imposes latency and compute costs; the framework suggests architectural proximity of telemetry and decision points to mitigate latency but empirical quantification of overheads is required (Rose, 2022; Fernandez & Brazhuk, 2024).
3. AI robustness and adversarial resilience. AI-augmented IAM introduces risks of model poisoning and adversarial examples. While hybrid governance mitigates these risks, the optimal balance between automation and human oversight remains an empirical question (Martín et al., 2021; Olabanji et al., 2024).
4. Legal and compliance constraints on deception. Deceptive defenses raise complex legal questions about entrapment, privacy, and cross-jurisdictional data handling when deployed at scale in cloud environments; these aspects require domain-specific legal review and policy frameworks (Steingartner et al., 2021).

D. Future Research Directions

To move the framework from prescriptive theory to empirically validated practice, several research projects are recommended:

1. Controlled experiments measuring ZTA decision latency. Instrument prototypes that co-locate telemetry collectors and policy decision points to measure round-trip latency, authorization throughput, and user experience under varying loads and attack scenarios.
2. ERN validation across cloud-edge telemetry. Implement ERN pipelines that ingest simulated and production datasets to evaluate detection accuracy, false positive rates, and robustness to evasive tactics.

Published Date: - 30-11-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

3. AI governance models for IAM. Compare different hybrid governance strategies (e.g., AI advisory vs. AI enforcement) across operational metrics, adversarial robustness, and compliance outcomes.
4. Cooperative DDoS mitigation strategies. Design and evaluate meta-heuristic load balancing controllers that accept DDoS risk signals and measure cross-tenant fairness and availability preservation.

5. Deception effectiveness studies. Quantify the intelligence yield from deception zones and assess the legal, privacy, and operational costs of integrating deception at cloud scale.
6. Economic modeling of ZTA adoption. Build cost-benefit models that incorporate operational overheads, reduced breach costs, and potential ROI claims to guide executive decision making (Jakkal, 2023).

E. Ethical and Governance Considerations

Adoption of the proposed framework requires careful governance structures that address privacy, transparency, and accountability. Continuous monitoring and behavioral analytics risk creating privacy intrusion if not bounded by clear policies and consent mechanisms. Explainability of AI models must be prioritized to meet regulatory demands and to enable meaningful audit trails for access decisions (Martín et al., 2021). Deception techniques must be constrained by legal counsel to avoid regulatory violations and to maintain trust among tenant populations. Finally, the shared responsibility model should be codified in service level agreements to make explicit who is accountable for telemetry retention, analysis, and response actions (Shitta-Bey & Adewole, 2023).

CONCLUSION

This article synthesizes contemporary research and practitioner knowledge to propose an integrated, identity-centric Zero Trust framework for multi-tenant cloud environments that addresses lateral movement, DDoS, IAM scalability, and resilience through deception and AI-assisted analytics. The framework advances the state of knowledge by translating ZTA principles into concrete operational patterns — identity-anchored policy control planes, evidence-reasoning networks for lateral movement detection, AI-augmented IAM under hybrid governance, and coordinated DDoS/load balancing strategies guided by meta-heuristics. While the framework is theoretically grounded, empirical research is required to validate performance trade-offs, AI robustness, and legal constraints. The article offers a research roadmap including experimental measures of latency and throughput for continuous evaluation, ERN validation, AI governance studies, DDoS/load balancing coordination experiments, and deception effectiveness assessment. In an era where cloud migration is a strategic imperative, a rigorous, implementable approach to Zero Trust that carefully balances security, usability, and performance is essential. The proposed framework and its derived design principles provide a scaffold for practitioners and researchers striving to make ZTA operational in complex, shared cloud ecosystems.

REFERENCES

1. M. Shitta-Bey and M. Adewole, "Security Concerns of Cloud Migration and Its Implications on Cloud-Enabled Business Transformation," Doctoral dissertation, 2023.

Published Date: - 30-11-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

2. N. Agrawal and S. Tapaswi, "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3769-3795, 2019.
3. FORTRA Terranova Security, "How Secure is Cloud Storage? Here are the Important Risks to Know," 29 December 2023. Available: https://terranovasecurity.com/blog/how-secure-is-cloudstorage/
4. S. T. Milan, L. Rajabion, H. Ranjbar and N. J. Navimipour, "Nature inspired meta-heuristic algorithms for solving the load-balancing problem in cloud environments," Computers & Operations Research, vol. 110, pp. 159-187, 2019.
5. Singh, R. Thakkar and J. Warraich, "IAM identity Access Management—importance in maintaining security systems within organizations," European Journal of Engineering and Technology Research, pp. 30-38, 2023.
6. W. Steingartner, D. Galinec and A. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model," Symmetry, p. 597, 2021.
7. Z. Tian, W. Shi, Y. Wang, C. Zhu, X. Du, S. Su and N. Guizani, "Real-time lateral movement detection based on evidence reasoning network for edge computing environment," IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4285-4294, 2019.
8. WIZ, "Lateral Movement Explained," 10 August 2023. Available: https://www.wiz.io/academy/what-is-lateral-movement
9. E. B. Fernandez and A. Brazhuk, "A critical analysis of Zero Trust Architecture (ZTA)," Computer Standards & Interfaces, p. 103832, 2024.
10. G. Martín, A. Fernández-Isabel, I. Martín de Diego and M. Beltrán, "A survey for user behavior analysis based on machine learning techniques: current models and applications," Applied Intelligence, pp. 6029-6055, 2021.
11. S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye and T. O. Oladoyinbo, "AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems," Asian Journal of Research in Computer Science, pp. 38-56, 2024.
12. Phiayura, P., & Teerakanok, S., "A comprehensive framework for migrating to zero trust architecture," IEEE Access, vol. 11, pp. 19487-19511, 2023.
13. Moore, C., "A Zero Trust Approach to Fundamentally Redesign Network Architecture within Federal Agencies," Doctoral dissertation, Capella University, 2022.
14. Hariharan, R., "Zero trust security in multi-tenant cloud environments," Journal of Information Systems Engineering and Management, 10, 2025.
15. D'Silva, D., & Ambawade, D. D., "Building a zero-trust architecture using kubernetes," in 2021 6th International Conference for Convergence in Technology (i2ct), pp. 1-8, IEEE, 2021.
16. House, W., "Executive Order on Improving the Nation's Cybersecurity," The White House, 12 May 2021. https://www.whitehouse.gov/briefingroom/presidential-actions/2021/05/12/executiveorder-on-improving-the-nations-cybersecurity/

Published Date: - 30-11-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

17. Defense Information Systems for Security (DISS). Defense Information Systems Agency. www.dcsa.mil/is/diss/

18. "CISA Insights: Zero Trust Architectures." Cybersecurity and Infrastructure Security Agency. www.cisa.gov/cyber-insights/cisa-insights-zero-trustarchitectures

19. Jakkal, V., "Microsoft Zero Trust solutions deliver 92 percent return on investment, says a new Forrester study," Microsoft Security Blog, 16 May 2023. https://www.microsoft.com/en-us/security/blog/2022/01/12/microsoft-zero-trustsolutions-deliver-92-percent-return-on-investmentsays-new-forrester-study/

20. Rose, S., "Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators," 2022 NIST Cybersecurity White Paper, NIST CSWP 20.