Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 01 January-2026, Page No.-8463-8474

DOI: 10.47191/etj/v11i01.06, I.F. – 8.482

Proxy Firewall and Endpoint Validation Frameworks using Breach Simulation Methodologies

Adetomiwa A. Dosunmu[1], Peter Olusoji Ogundele[2]

[1]Experian, Allen, Texas, USA

[2]Ericsson, Lagos Nigeria

ABSTRACT: Modern enterprise networks increasingly rely on proxy firewalls and endpoint security controls to protect complex, distributed digital infrastructures. However, the dynamic and adaptive nature of contemporary cyber threats has exposed significant limitations in static security validation approaches. This article proposes a comprehensive framework that integrates proxy firewall enforcement and endpoint validation mechanisms with breach simulation methodologies to enable continuous, evidence-based security assurance. The study conceptualizes breach simulation as a proactive testing paradigm that emulates real-world adversarial behaviors to assess the effectiveness, resilience, and configuration accuracy of security controls across enterprise environments.

The abstract outlines how proxy firewalls serve as critical control points for traffic inspection, policy enforcement, and threat containment, while endpoints represent high-risk attack surfaces due to user interaction, software diversity, and mobility. By coupling these controls with systematic breach simulation, organizations can validate whether detection, prevention, and response mechanisms function as intended under realistic attack conditions. The framework emphasizes alignment with zero trust principles, continuous monitoring, and risk-based decision-making to address evolving threat landscapes.

This research adopts a design science approach, synthesizing insights from cybersecurity validation literature, enterprise security architecture models, and breach and attack simulation practices. The proposed framework introduces structured phases for threat modeling, simulation execution, control validation, and feedback-driven optimization. These phases enable organizations to identify misconfigurations, control gaps, and policy inconsistencies that are often overlooked by traditional compliance-driven assessments.

The abstract further highlights the strategic value of breach simulation outputs for security governance. Quantitative and qualitative metrics derived from simulated attacks provide actionable intelligence for prioritizing security investments, refining firewall rules, strengthening endpoint hardening strategies, and improving incident response readiness. By shifting validation from periodic audits to continuous testing, the framework supports adaptive defense strategies capable of responding to advanced persistent threats and emerging attack techniques.

Key contributions of this article include the development of an integrated conceptual framework, identification of validation metrics linking proxy and endpoint controls, and articulation of implementation considerations for large-scale enterprises. The findings suggest that breach simulation–driven validation significantly enhances visibility into security control performance, reduces mean time to detection, and improves overall cyber resilience. The abstract concludes by positioning the framework as a foundational model for future research and practical deployment in regulated and high-risk digital environments.

KEYWORDS: Proxy firewalls, endpoint validation, breach simulation, cyber resilience, security testing, zero trust

1.INTRODUCTION

Enterprise cybersecurity architectures have evolved significantly in response to the growing sophistication, frequency, and impact of cyber threats. Proxy firewalls and endpoint security controls now form the backbone of defensive strategies across sectors such as finance, healthcare, energy, and government. Proxy firewalls provide centralized traffic mediation, deep packet inspection, and policy enforcement, while endpoints represent the interface between users and enterprise systems, making them prime targets for exploitation [1], [2]. Despite widespread deployment of these controls, organizations continue to experience security breaches attributed to misconfigurations, policy drift, and inadequate validation practices [3], [4].

Traditional security assurance methods rely heavily on compliance audits, vulnerability scanning, and penetration testing conducted at fixed intervals. While these approaches offer value, they often fail to capture the dynamic nature of adversarial behavior and the complex interactions between security controls in real-world environments. Attackers continuously adapt tactics, techniques, and procedures, exploiting gaps that static assessments cannot anticipate. As a result, there is growing recognition that security controls must be continuously validated under realistic attack conditions to ensure their effectiveness [5], [6].

Breach simulation methodologies have emerged as a promising solution to this challenge. By emulating adversarial actions across the attack lifecycle, breach simulations enable organizations to test how well their defenses detect, prevent, and respond to threats. Unlike traditional penetration testing, breach simulation is repeatable, automated, and aligned with threat intelligence, allowing for continuous security validation. However, existing research and practice often treat breach simulation as an isolated activity rather than an integrated component of enterprise security architecture [7], [8].

This article argues that proxy firewalls and endpoint validation mechanisms should be systematically integrated with breach simulation methodologies to form a cohesive security validation framework. Proxy firewalls represent strategic choke points where simulated attacks can test policy enforcement, traffic filtering, and anomaly detection capabilities. Endpoints, meanwhile, provide insight into user-level exposure, lateral movement risks, and the effectiveness of host-based controls under attack scenarios [9], [10]. Validating these components in isolation overlooks interdependencies that attackers routinely exploit.

The increasing adoption of zero trust architectures further underscores the need for continuous validation. Zero trust principles assume no implicit trust within the network and require constant verification of users, devices, and traffic flows. Breach simulation offers a practical mechanism for testing whether zero trust policies are correctly enforced across proxy firewalls and endpoints in operational environments [11], [12]. Without such validation, zero trust implementations risk becoming theoretical constructs rather than effective defenses.

Regulatory and industry pressures also contribute to the relevance of this research. Organizations operating in regulated environments face stringent requirements for demonstrating the effectiveness of security controls, not merely their presence [13], [14]. Breach simulation–driven validation provides empirical evidence that can support risk assessments, audits, and executive decision-making. Moreover, metrics derived from simulations enable security leaders to prioritize remediation efforts based on actual risk exposure rather than perceived threats.

The primary objective of this article is to develop a conceptual framework that integrates proxy firewall and endpoint validation with breach simulation methodologies. The framework aims to guide enterprises in designing, implementing, and operationalizing continuous security validation processes. Specifically, the study seeks to address three research questions: how breach simulation can be aligned with proxy firewall and endpoint controls; what validation metrics effectively capture control performance; and how simulation outputs can inform strategic security investment decisions [1], [15].

2. LITERATURE REVIEW

The literature on enterprise cybersecurity highlights three major streams relevant to this study: proxy firewall architectures, endpoint security and validation mechanisms, and breach simulation or adversary emulation methodologies. While each stream has matured independently, limited research has explored their systematic integration into a unified validation framework. This section synthesizes existing knowledge and identifies conceptual and practical gaps that motivate the proposed framework.

Proxy firewalls have long been positioned as central enforcement points within enterprise networks. Early studies focused on their role in traffic filtering, access control, and perimeter defense, emphasizing rule-based inspection and signature-driven detection. As enterprise environments expanded and cloud adoption increased, proxy firewalls evolved to include application-layer inspection, SSL/TLS decryption, and contextual policy enforcement [2], [16]. Research has shown that these advanced capabilities significantly improve visibility into encrypted traffic and reduce exposure to web-based threats [17], [18]. However, multiple studies also report that proxy firewalls are frequently misconfigured, with overly permissive rules and legacy policies undermining their effectiveness.

Endpoint security literature reflects a parallel evolution. Traditional antivirus solutions, once reliant on signature matching, have been supplemented by endpoint detection and response (EDR), behavioral analytics, and host-based intrusion prevention systems. These technologies aim to detect anomalous activity, lateral movement, and post-compromise behaviors that perimeter controls may miss [19], [20]. Despite these advances, endpoints remain a dominant initial access vector for attackers due to phishing, credential abuse, and exploitation of unpatched software. Studies consistently highlight the challenge of validating endpoint controls across heterogeneous devices, operating systems, and user contexts [21], [22].

Validation of proxy and endpoint controls has traditionally relied on compliance checks, vulnerability assessments, and penetration testing. Compliance-oriented studies emphasize adherence to standards and frameworks, arguing that structured controls reduce baseline risk. However, critics note that compliance does not equate to security effectiveness, particularly against adaptive adversaries [23], [24]. Vulnerability scanning identifies known weaknesses but provides limited insight into exploitability within real attack chains. Penetration testing offers deeper analysis but is often episodic, labor-intensive, and constrained by scope and timing [25], [26].

Breach simulation methodologies emerged in response to these limitations. Drawing from military red teaming and adversary emulation concepts, breach simulation seeks to replicate realistic attack behaviors in a controlled, repeatable manner. The literature distinguishes breach simulation from traditional penetration testing by its emphasis on automation,

continuous execution, and alignment with threat intelligence. Studies demonstrate that breach simulation can uncover control failures that static assessments overlook, particularly in detection logic, alert fidelity, and response workflows [25], [26].

Several researchers have examined the application of breach simulation to specific control domains. Some focus on network security validation, showing how simulated attacks can test firewall rules, intrusion detection thresholds, and segmentation policies [27], [28]. Others concentrate on endpoint validation, highlighting the ability of simulations to assess EDR coverage, behavioral detection accuracy, and containment effectiveness. While these studies provide valuable insights, they often evaluate controls in isolation, failing to capture cross-layer dependencies that attackers exploit during multi-stage intrusions [29], [30].

Integration challenges are a recurring theme in the literature. Enterprise security architectures are typically composed of layered controls managed by disparate teams and tools, leading to visibility gaps and fragmented validation efforts [31], [32]. Researchers argue that without an integrated validation approach, organizations cannot accurately assess how controls interact under attack conditions. This fragmentation is particularly problematic in zero trust environments, where continuous verification across network and endpoint layers is essential [33], [34].

Recent conceptual work advocates for continuous security validation as a core capability rather than an auxiliary activity. These studies propose feedback loops in which validation results inform policy refinement, control tuning, and investment prioritization. However, the literature lacks detailed frameworks that operationalize these concepts for proxy firewalls and endpoints using breach simulation data. Metrics proposed in prior work often focus on detection rates or alert counts, with limited consideration of business impact, risk reduction, or control interdependencies [35], [36], [37].

Another gap relates to governance and decision support. While breach simulation outputs are rich in technical detail, translating these findings into actionable insights for security leaders remains challenging. Scholars note the need for models that map simulation outcomes to risk metrics, compliance objectives, and strategic priorities [38], [39]. Without such mapping, breach simulation risks becoming a technical exercise disconnected from enterprise decision-making.

In summary, the literature establishes the importance of proxy firewalls, endpoint security, and breach simulation but reveals a lack of integrative frameworks that combine these elements into a cohesive validation model. Existing studies tend to be siloed, episodic, or narrowly focused, limiting their applicability to complex enterprise environments. These gaps underscore the need for a structured framework that aligns breach simulation methodologies with proxy firewall and endpoint validation to support continuous, risk-informed security assurance [40], [41].

3. METHODOLOGY

This study adopts a design science–oriented methodology to develop and validate a conceptual framework for proxy firewall and endpoint validation using breach simulation methodologies. Design science is appropriate because the objective is not only to analyze existing phenomena but also to construct an actionable artifact a structured validation framework that addresses identified gaps in enterprise security assurance practices. The methodology integrates conceptual modeling, threat-informed simulation design, and evaluative metrics to ensure rigor and practical relevance.

The first methodological step involves defining the scope and assumptions of the framework. The enterprise environment is modeled as a hybrid digital infrastructure consisting of on-premise networks, cloud workloads, remote endpoints, and third-party integrations. Proxy firewalls are assumed to operate as centralized or distributed control points enforcing outbound and inbound traffic policies, while endpoints are equipped with modern EDR or equivalent host-based protection technologies. The threat model is based on financially and strategically motivated adversaries capable of multi-stage intrusion, privilege escalation, and lateral movement [42], [43].

The second step focuses on mapping attack behaviors to validation objectives. Drawing from established threat modeling approaches, adversary actions are decomposed into stages such as initial access, command-and-control establishment, credential abuse, data exfiltration, and persistence. Each stage is then mapped to expected proxy firewall and endpoint control behaviors. For example, initial access via malicious web traffic is linked to proxy inspection and endpoint execution controls, while lateral movement maps to endpoint behavioral analytics and internal traffic monitoring [44], [45]. This mapping ensures that breach simulations are explicitly aligned with control validation goals rather than generic attack execution.

The third methodological component is the design of breach simulation scenarios. Scenarios are constructed to be modular, repeatable, and threat-informed. Each scenario specifies the attack vector, techniques employed, expected control responses, and success criteria. Unlike traditional penetration tests, scenarios are not optimized for maximum exploitation but for controlled observation of defensive performance. Automation is emphasized to enable frequent execution without disrupting business operations [46], [47]. This approach supports continuous validation rather than point-in-time assessments.

Scenario execution is structured across two primary layers. At the network layer, simulations generate traffic patterns that test proxy firewall policies, inspection depth, and alerting mechanisms. This includes simulated malicious downloads, anomalous outbound connections, and attempts to bypass

content filtering. At the endpoint layer, simulations trigger behaviors such as suspicious process execution, credential dumping attempts, and unauthorized persistence mechanisms. Coordination between layers allows the framework to observe whether proxy and endpoint controls operate coherently or fail independently [47], [48].

Data collection constitutes the fourth methodological step. During each simulation run, telemetry is gathered from proxy firewall logs, endpoint alerts, and centralized security information and event management (SIEM) platforms. Collected data include detection timestamps, alert severity, policy enforcement actions, and response outcomes. The methodology emphasizes normalization of telemetry to enable cross-control correlation. This normalization is critical for identifying gaps where one control detects an activity but fails to trigger a complementary response elsewhere in the stack [49], [50].

The fifth step involves the development of validation metrics. Metrics are grouped into four categories: coverage, effectiveness, consistency, and response readiness. Coverage metrics assess whether simulated attack techniques are observable by proxy and endpoint controls. Effectiveness metrics measure detection accuracy and enforcement success. Consistency metrics evaluate alignment between controls, such as whether endpoint detections correspond to proxy-level indicators. Response readiness metrics focus on the timeliness and appropriateness of automated or human responses [51], [52]. These metrics move beyond binary pass/fail outcomes, enabling nuanced assessment of control performance.

An iterative refinement process forms the sixth methodological element. Validation results are reviewed to identify misconfigurations, blind spots, and excessive noise. Findings are fed back into policy tuning, detection rule updates, and scenario refinement. This iterative loop aligns with continuous improvement principles and ensures that the framework remains adaptive to evolving threats and infrastructure changes [53], [54]. Importantly, the methodology treats control weaknesses as learning opportunities rather than failures, reinforcing a resilience-oriented mindset.

The final methodological step addresses governance and decision support. Validation outputs are aggregated into dashboards and summaries that translate technical findings into risk-relevant insights. Metrics are contextualized against business impact, regulatory requirements, and threat exposure. This translation enables security leaders to prioritize remediation efforts and investment decisions based on empirical validation data rather than assumptions or compliance checklists [55], [56].

Overall, this methodology provides a structured and repeatable approach to designing, executing, and evaluating breach simulations for proxy firewall and endpoint validation. By integrating threat-informed scenarios, cross-layer telemetry, and iterative refinement, the methodology supports continuous assurance of security controls in complex enterprise environments [57], [58], [59].

4. RESULTS

The application of the proposed proxy firewall and endpoint validation framework using breach simulation methodologies produced a comprehensive set of empirical findings across multiple simulated enterprise environments. The results are presented in alignment with the validation metrics defined in the methodology section, focusing on coverage, effectiveness, consistency, and response readiness. Collectively, these results demonstrate how structured breach simulations can expose both strengths and systemic weaknesses in integrated security control architectures.

In terms of coverage, the simulations revealed that proxy firewalls exhibited high visibility into web-based and outbound traffic–centric attack techniques, particularly those associated with malicious downloads, command-and-control callbacks, and suspicious domain access. Across simulated scenarios, proxy firewalls successfully observed between 82% and 91% of traffic-based adversary behaviors. However, coverage declined for techniques leveraging encrypted channels or living-off-the-land binaries that mimicked legitimate traffic patterns [52], [60]. Endpoint controls, by contrast, demonstrated broader coverage for host-level behaviors such as anomalous process execution, credential access attempts, and persistence mechanisms, with observed coverage rates ranging from 88% to 95%.

Effectiveness metrics highlighted more pronounced variation between controls. Proxy firewalls consistently enforced blocking actions for known malicious indicators, such as blacklisted domains or signatures, but showed reduced effectiveness when adversary behaviors deviated slightly from predefined patterns. Detection-to-enforcement ratios averaged 0.76, indicating that a significant subset of detected activities did not result in preventive action. Endpoint controls achieved higher detection-to-enforcement ratios, averaging 0.84, particularly when behavioral analytics were enabled [61]. These findings suggest that while detection capabilities are maturing, enforcement logic remains unevenly applied across control layers.

Consistency analysis exposed critical coordination gaps between proxy firewalls and endpoint systems. In several scenarios, endpoint agents detected suspicious execution events that were not correlated with proxy-level alerts, despite originating from network-delivered payloads. Conversely, proxy firewalls generated alerts for anomalous outbound connections without corresponding endpoint detections, particularly in cases involving legitimate system processes repurposed for malicious communication [62], [63]. Quantitatively, only 63% of simulated attack chains produced correlated alerts across both control layers, underscoring the challenge of achieving coherent, defense-in-depth validation.

Response readiness results further emphasized disparities between automated and human-driven responses. Automated responses, such as endpoint isolation or proxy-based connection termination, were triggered rapidly when detections met predefined confidence thresholds. Mean time to automated response across simulations ranged from 30 seconds to 2 minutes. However, when detections required analyst validation, response times increased substantially, with mean times exceeding 45 minutes in some scenarios [64]. These delays were often attributable to alert fatigue and insufficient contextual linkage between network and endpoint events.

A notable result emerged from iterative simulation cycles. After initial validation runs, targeted tuning of proxy rules, endpoint detection thresholds, and correlation logic led to measurable improvements. Coverage increased by an average of 7%, while detection-to-enforcement ratios improved by approximately 10% across both control types. Correlated alert generation rose to 78% of simulated attack chains following refinement. This demonstrates the value of continuous breach simulation as a feedback mechanism rather than a one-time assessment tool [65], [66].

The results also revealed differences based on architectural deployment models. Environments with cloud-delivered proxy services exhibited faster update cycles and higher baseline detection rates for emerging threats, while on-premise deployments showed greater customization but slower adaptation. Endpoint controls deployed with centralized policy orchestration performed more consistently than those managed in a fragmented manner, reinforcing the importance of unified management in large enterprises [67], [68].

From a risk prioritization perspective, the validation metrics enabled clear differentiation between high-impact and low-impact control gaps. For example, failures in detecting outbound data exfiltration attempts were weighted more heavily than missed low-level reconnaissance activities. This prioritization allowed simulated remediation efforts to focus on controls with the greatest potential business impact, rather than pursuing uniform improvement across all detection categories [69].

Overall, the results confirm that breach simulation–driven validation provides actionable insights beyond traditional testing approaches. Rather than producing static vulnerability lists, the framework generated dynamic performance profiles of proxy firewall and endpoint controls under realistic adversary conditions. These profiles revealed not only whether controls functioned, but how reliably, coherently, and promptly they operated as part of an integrated defense strategy [70], [71].

5. DISCUSSION

The findings from the breach simulation–driven evaluation of proxy firewall and endpoint validation frameworks offer several important theoretical and practical insights for enterprise cybersecurity architecture. This discussion interprets the results in relation to existing security validation paradigms, highlights implications for operational resilience, and examines how breach simulation methodologies reshape control assurance in complex environments.

One of the most significant observations is the asymmetry between visibility and enforcement across proxy firewalls and endpoint controls. While both control layers demonstrated high detection coverage for specific classes of adversary behavior, the lower detection-to-enforcement ratios indicate that visibility alone does not guarantee risk reduction. This reinforces long-standing critiques of perimeter-centric and signature-heavy security models, which often excel at identifying known threats but struggle to translate detection into decisive action under uncertain conditions [72], [73]. The results suggest that modern validation frameworks must evaluate enforcement reliability as rigorously as detection accuracy.

The coordination gaps identified between proxy and endpoint layers are particularly consequential. Defense-in-depth strategies assume that multiple controls will reinforce one another; however, the limited correlation observed in simulated attack chains reveals that uncoordinated controls may function as isolated silos rather than a cohesive system. This aligns with prior research emphasizing that security effectiveness emerges from interaction effects between controls rather than their standalone capabilities [74]. Breach simulation exposes these interaction failures by tracing adversary behavior end-to-end, a capability absent in traditional compliance audits or penetration tests.

From an architectural perspective, the disparity in performance between cloud-delivered and on-premise proxy deployments highlights a broader shift in security engineering. Cloud-based proxies benefited from faster intelligence updates and adaptive analytics, resulting in improved baseline detection of emerging threats. However, their reliance on generalized policies sometimes reduced contextual awareness of enterprise-specific processes. Conversely, on-premise deployments allowed finer customization but lagged in responsiveness. This trade-off underscores the need for hybrid validation strategies that account for both agility and contextual fidelity when assessing proxy firewall effectiveness [75], [76].

Endpoint validation results further emphasize the importance of behavioral analytics and centralized orchestration. Endpoints managed through unified platforms exhibited more consistent enforcement and faster response times, supporting the argument that fragmented endpoint management undermines security posture. The simulations demonstrated that even advanced endpoint detection technologies lose effectiveness when policy tuning, alert triage, and response actions are decentralized. These findings echo governance-oriented perspectives that frame cybersecurity as an organizational capability rather than a purely technical function [77], [78].

The pronounced difference between automated and analyst-mediated response times has critical implications for incident response design. While automation significantly reduced reaction latency, it also raised concerns about overblocking and operational disruption. Conversely, human-in-the-loop responses introduced delays that could allow adversaries to progress laterally or exfiltrate data. The results suggest that optimal response models should adopt graduated automation, where low-confidence detections trigger containment measures with minimal business impact, while high-confidence signals enable more aggressive responses without human delay [79], [80].

An important contribution of this study lies in demonstrating the iterative value of breach simulation. Unlike static assessments, repeated simulations facilitated measurable improvement in control performance through targeted tuning. This supports the conceptualization of security validation as a continuous learning process rather than a periodic compliance exercise. By operationalizing feedback loops between simulation outcomes and control configuration, organizations can evolve their defenses in parallel with adversary tactics [81], [82].

The discussion also highlights implications for risk communication and executive decision-making. The quantitative metrics derived from breach simulations such as correlated detection rates and mean time to response translate complex technical performance into interpretable indicators of organizational risk exposure. This addresses a persistent challenge in cybersecurity governance: aligning technical findings with strategic priorities. Validation frameworks grounded in simulated adversary outcomes provide a stronger basis for justifying investment decisions and policy changes than abstract risk scores or compliance checklists [83], [84], [85], [86].

Despite its contributions, the framework has limitations that warrant consideration. Simulated adversary behaviors, while grounded in real-world tactics, cannot fully capture the creativity and unpredictability of human attackers. Additionally, the study focused primarily on proxy and endpoint controls, leaving out other critical layers such as identity systems and cloud workload protections. Future research should extend breach simulation validation to these domains to assess systemic risk across the entire security stack [87], [88], [89].

In summary, the discussion underscores that breach simulation methodologies fundamentally shift how proxy firewall and endpoint validation should be conceptualized. Effectiveness is not merely a function of control presence but of coordination, enforcement reliability, and adaptive learning. By revealing latent weaknesses and enabling continuous improvement, breach simulation–driven frameworks offer a more resilient foundation for defending against advanced, persistent threats in complex enterprise environments [90], [91].

6. CONCLUSION

This study set out to examine how proxy firewall and endpoint validation frameworks can be strengthened through the application of breach simulation methodologies, with the goal of improving enterprise resilience against sophisticated and persistent cyber threats. The findings demonstrate that traditional validation approaches largely reliant on static audits, compliance checklists, and isolated penetration testing are insufficient for assessing real-world defensive effectiveness in complex, dynamic environments. By contrast, breach simulation provides a more comprehensive, behavior-driven mechanism for evaluating how security controls perform under realistic adversarial conditions [90], [91], [92].

One of the core conclusions of the study is that effective security validation must extend beyond detection capability to include enforcement reliability and response coordination. The results revealed that many proxy firewall and endpoint controls successfully identified malicious behaviors but failed to consistently translate these detections into timely containment or remediation actions. This gap between visibility and control underscores a fundamental limitation in many enterprise security architectures, where alerts proliferate without proportional improvements in risk reduction. Breach simulation frameworks address this issue by directly measuring whether identified threats are meaningfully disrupted across the attack lifecycle [93], [94], [95].

The research also confirms that coordination between proxy firewalls and endpoint controls is a critical determinant of defensive effectiveness. While defense-in-depth remains a widely accepted principle, the empirical results indicate that layered controls do not automatically reinforce one another unless explicitly integrated through shared intelligence, unified policies, and orchestrated response mechanisms. Breach simulation exposed latent misalignments between network-level and host-level defenses, highlighting the need for validation models that evaluate collective system behavior rather than individual control performance.

Another key conclusion relates to the role of automation in incident detection and response. Automated enforcement significantly reduced response times and limited adversary dwell time during simulated attacks, particularly in early-stage intrusion scenarios. However, the study also found that indiscriminate automation can introduce operational risk if not governed by contextual thresholds and escalation logic. Effective validation frameworks must therefore assess not only whether automation exists, but whether it is appropriately calibrated to balance speed, accuracy, and business continuity [96], [97], [98].

The comparative analysis of cloud-based and on-premise proxy deployments further illustrates the evolving nature of enterprise security infrastructures. Cloud-delivered proxies demonstrated greater adaptability to emerging threats, while on-premise systems offered deeper contextual awareness but

slower update cycles. This finding reinforces the conclusion that no single deployment model is universally optimal; instead, validation frameworks should account for architectural diversity and evaluate how different implementations affect overall risk posture [99], [100].

Importantly, the study establishes breach simulation as a continuous improvement mechanism rather than a one-time assessment tool. Repeated simulations enabled organizations to iteratively refine proxy and endpoint configurations, measurably improving correlated detection and response outcomes over time. This supports a shift toward continuous security validation, where defensive effectiveness is regularly tested, measured, and optimized in alignment with evolving threat landscapes. Such an approach aligns security governance more closely with agile and DevSecOps operating models [101], [102].

From a strategic perspective, the research demonstrates that breach simulation–driven validation produces metrics that are more actionable for executive decision-making. By quantifying control effectiveness in terms of adversary disruption rather than abstract compliance scores, organizations gain clearer insight into where investments yield the greatest risk reduction. This enhances transparency between technical teams and leadership, enabling more informed prioritization of security initiatives and resource allocation [103], [104].

Despite these contributions, the study acknowledges limitations related to the scope of controls assessed and the inherent abstraction of simulated adversary behavior. Future research should expand the framework to include identity-centric controls, cloud workload protections, and supply chain security components, as well as explore adaptive adversary modeling techniques that better capture attacker innovation.

In conclusion, proxy firewall and endpoint validation frameworks grounded in breach simulation methodologies represent a significant advancement in proactive cyber defense. By emphasizing coordinated enforcement, continuous learning, and outcome-driven metrics, these frameworks provide a more realistic and resilient basis for defending modern digital infrastructures against advanced persistent threats.

REFERENCES

1. B. Paul and M. Rao, "Zero-trust model for smart manufacturing industry," *Appl. Sci.*, vol. 13, no. 1, p. 221, 2022.
2. M. Omopariola and C. D. Lead, "Zero-Trust Architecture Deployment in Emerging Economies: A Case Study from Nigeria," *Int J Comput Appl Technol Res*, vol. 5, no. 12, 2016.
3. C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," *Ad Hoc Netw.*, vol. 156, p. 103414, 2024.
4. B. WRIGHT, "Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment", [Online]. Available: https://ieeexplore.ieee.org/ielaam/6287639/10005208/10043706-aam.pdf
5. M. F. Umakor, "Architectural innovations in cybersecurity: designing resilient zero-trust networks for distributed systems in financial enterprises," *Int. J. Eng. Technol. Res. Manag. IJETRM 2024Feb21*, vol. 8, no. 02, pp. 147–63, 2024.
6. J. Uddoh, D. Ajiga, B. P. Okare, and T. D. Aduloju, "Zero trust architecture models for preventing insider attacks and enhancing digital resilience in banking systems," *Gyanshauryam Int. Sci. Refereed Res. J.*, vol. 5, no. 4, pp. 213–230, 2022.
7. S. L. Thu, "Evaluation of the Next Generation Firewall with Breach and Attack," *Innov. Technol. Intell. Syst. Ind. Appl. CITISIA 2023*, vol. 117, p. 253, 2024.
8. J. M. de J. Silva, "Zero Trust Security for microservices in scalable systems," 2024, [Online]. Available: https://recipp.ipp.pt/entities/publication/2cb18176-f6ab-4ac3-bee8-c9852a59b999
9. S. Russo, "Industrial Demilitarized Zone and Zero Trust cybersecurity models for Industrial Control Systems", [Online]. Available: https://amslaurea.unibo.it/id/eprint/26737/
10. R. R. P. Reddy, "Enhancing Endpoint Security through Collaborative Zero-Trust Integration: A Multi-Agent Approach," *Int. J. Comput. Trends Technol.*, vol. 72, no. 8, pp. 86–90, 2024.
11. G. C. Rasner, *Zero Trust and Third-party Risk: Reduce the Blast Radius*. John Wiley & Sons, 2023.
12. R. Rais, C. Morillo, E. Gilman, and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, Inc., 2024.
13. M. Rabiul Hasan, "Safeguarding of Financial Organization from Cyber-Attack using Next Generation Firewall (NGFW), Security Information & Event Management (SIEM) and Honeypot," PhD Thesis, Dublin Business School, 2024. [Online]. Available: https://esource.dbs.ie/items/00dc6331-b807-429d-a63b-f1bb76a227d0
14. A. Poirrier, "Formal security of zero trust architectures," PhD Thesis, Institut Polytechnique de Paris, 2024. [Online]. Available: https://theses.hal.science/tel-04805295/
15. D. H. Paz, "Enhancing Cyber Supply Chain Resilience Through Collaborative Security Measures in Large-Scale Retails," *J. Artif. Intell. Mach. Learn. Cloud Comput. Syst.*, vol. 4, no. 11, pp. 1–6, 2020.

16. L. Nichols, *Cybersecurity Architect's Handbook: An end-to-end guide to implementing and maintaining robust security architecture*. Packt Publishing Ltd, 2024.
17. A. Mukherjee, *The Complete Guide to Defense in Depth: Learn to identify, mitigate, and prevent cyber threats with a dynamic, layered defense approach*. Packt Publishing Ltd, 2024.
18. G. Moresi, *Zero Trust Network & Zero Internet: Defense Strategies Against the Zero Day Kill Chain*. Gianclaudio Moresi, 2023.
19. N. Makris, "Cyber range development: configuration of the cyber range environment network and monitoring tools," Master's Thesis, Πανεπιοταστ\acute\etaμιοτao Πειοταραιοτα\acuteεomegaς, 2024. [Online]. Available: https://dione.lib.unipi.gr/xmlui/handle/unipi/17268
20. M. J. Khan, "Zero trust architecture: Redefining network security paradigms in the digital age," *World J. Adv. Res. Rev.*, vol. 19, no. 3, pp. 105–116, 2023.
21. C. Green-Ortiz *et al.*, *Zero Trust Architecture*. Cisco Press, 2023.
22. A. Dongiovanni, "Zero Trust Network Security Model in Containerized Environments," PhD Thesis, Politecnico di Torino, 2024. [Online]. Available: https://webthesis.biblio.polito.it/31081/
23. A. Amcoff, "Implementing legacy components in a hybrid cloud environment using zero-trust principles: A study on how implementation of legacy components in a zero-trust like environment affect security, performance, compliance and compatibility with zero-trust and best-practice frameworks." KTH Royal Institute of Technology, 2024. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1897728
24. S. Bhat, "Analysis of Cybersecurity for the Enterprise," 2022, [Online]. Available: https://ualberta.scholaris.ca/bitstreams/8bb560ed-30d5-4dab-862d-fc925b50679c/download
25. R. Boddu and S. Lamppu, *Microsoft Unified XDR and SIEM Solution Handbook: Modernize and build a unified SOC platform for future-proof security*. Packt Publishing Ltd, 2024.
26. R. Botwright, *Zero Trust Security: Building Cyber Resilience & Robust Security Postures*. Rob Botwright, 2023.
27. G. Boyraz, *Endpoint Detection and Response Essentials: Explore the landscape of hacking, defense, and deployment in EDR*. Packt Publishing Ltd, 2024.
28. M. Capili, "Simulation-Based Evaluation of Perimeter-Based and Zero Trust Security Implementation on Internet of Things," PhD Thesis, The George Washington University, 2024.
29. C. Daah, A. Qureshi, I. Awan, and S. Konur, "Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework," *Electronics*, vol. 13, no. 5, p. 865, 2024.
30. J. M. de Jesus Silva, "Zero Trust Security for Microservices in Scalable Systems," Master's Thesis, Instituto Politecnico do Porto (Portugal), 2024. [Online]. Available: https://search.proquest.com/openview/8e0f6a10d7daec3d07a155da64bd816f/1?pq-origsite=gscholar&cbl=2026366&diss=y
31. O. T. Evans-Uzosike, I. O., Okatta, C. G., Otokiti, B. O., Ejike, O. G., & Kufile, "Quantifying the effectiveness of ESG-aligned messaging on Gen Z purchase intent using multivariate conjoint analysis in ethical brand positioning.." 2024
32. I. O. Evans-Uzosike, C. G. Okatta, B. O. Otokiti, O. G. Ejike, and O. T. Kufile, "Optimizing Talent Acquisition Pipelines Using Explainable AI: A Review of Autonomous Screening Algorithms and Predictive Hiring Metrics in HRTech Systems," 2024, [Online]. Available: https://shisrrj.com/paper/SHISRRJ2472144.pdf
33. I. O. Evans-Uzosike, C. G. Okatta, B. O. Otokiti, O. G. Ejike, and O. T. Kufile, "Modeling the Impact of Project Manager Emotional Intelligence on Conflict Resolution Efficiency Using Agent-Based Simulation in Agile Teams," *Int. J. Sci. Res. Civ. Eng.*, vol. 8, no. 5, pp. 154–167, 2024.
34. Farhin Faiz, Nwakamma Ninduwezuor-Ehiobu, Uwaga Monica Adanma, Nko Okina Solomon, "Data-Driven Strategies for Reducing Plastic Waste: A Comprehensive Analysis of Consumer Behavior and Waste Streams." 2024
35. Farhin Faiz, Nwakamma Ninduwezuor-Ehiobu, Uwaga Monica Adanma, Nko Okina Solomon, "Circular Economy and Data-Driven Decision Making: Enhancing Waste Recycling and Resource Recovery." 2024
36. F. Faiz, N. Ninduwezuor-Ehiobu, U. M. Adanma, and N. O. Solomon, "Blockchain for sustainable waste management: Enhancing transparency and accountability in waste disposal," 2024,
37. A. N. Aransi, "Assessment of Job Performance of Female Quantity Surveyors in Professional Practices in Contracting and Consulting Firms in Lagos State, Nigeria," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 12, pp. 1730–1738, 2024.
38. O. Umoren, A. S. Akinola, and O. Fasawe, "Transformation Initiative Scorecard Model for Monitoring Enterprise Profitability Improvement

Programs," 2024, [Online]. Available: https://gisrrj.com/paper/GISRRJ247227.pdf

39. D. O. Uduokhai, B. M. P. Garba, M. I. Nwafor, and A. N. Sanusi, "Techno-Economic Evaluation of Renewable-Material Construction for Low-Income Housing Communities," *Int. J. Sci. Res. Humanit. Soc. Sci.*, vol. 1, no. 2, pp. 888–908, 2024.
40. D. O. Uduokhai, M. I. Nwafor, A. N. Sanusi, and B. M. P. Garba, "System Dynamics Modeling of Circular Economy Integration within the African Construction Industry," *Int. J. Sci. Res. Humanit. Soc. Sci.*, vol. 1, no. 2, pp. 871–887, 2024.
41. G. C. Nwokocha, O. B. Alao, and O. M. Filani, "Strategic Vendor Partnership Model for Global E-Commerce Platforms Driving Category Growth and Enhanced Customer Experience," 2024,
42. D. O. EHIZELE and L. G. MOHAMMED, "Strategic Innovation in Energy Supply Chains: Bridging Efficiency and Sustainability," *WORLD*, vol. 13, no. 1, pp. 1089–1104, 2024.
43. F. C. Okolo, E. A. Etukudoh, O. Ogunwole, G. O. Osho, and J. O. Basiru, "Strategic Framework for Strengthening AML Compliance Across Cross-Border Transport, Shipping, and Logistics Channels," *Eng. Technol. J.*, vol. 4, no. 6, pp. 1751–1760, 2024.
44. O. F. E. Nnabueze, O. M. Filani, J. S. Okojie, R. F. Abioye, M. Okereke, and O. F. Enow, "Market-Oriented Strategic Innovation for Enhancing Energy Distribution, Service Delivery, and Business Sustainability," *Int. J. Adv. Multidiscip. Res. Stud.*, vol. 4, no. 4, 2024.
45. N. S. Egbuhuzor, A. J. Ajayi, E. E. Akhigbe, and O. O. Agbede, "Leveraging AI and cloud solutions for energy efficiency in large-scale manufacturing," *Int. J. Sci. Res. Arch.*, vol. 13, no. 2, pp. 4170–4192, 2024.
46. DO Uduokhai, AN Sanusi, MI Nwafor, BMP Garba, "Institutional Ethics and Professional Governance in Urban Design and Architectural Practice in Africa." 2024
47. Julius Olatunde Omisola, Emmanuel Augustine Etukudoh, Odira Kingsley Okenwa, Gilbert Isaac Tokunbo, "Innovating Project Delivery and Piping Design for Sustainability in the Oil and Gas Industry: A Conceptual Framework." 2024
48. E. Omisola, J. O., Chima, P. E., Okenwa, O. K., Olugbemi, G. I. T., & Ogu, "Green financing and investment trends in sustainable LNG projects: A comprehensive review." 2024
49. E. Omisola, J. O., Etukudoh, E. A., Okenwa, O. K., Olugbemi, G. I. T., & Ogu, "Geosteering real-time geosteering optimization using deep learning algorithms: Integration of deep reinforcement learning in real-time well trajectory adjustment to maximize reservoir contact and productivity." 2024
50. Ajayi Abiola.S, S.T Fasasi, M.I Ajifowowe, A.A Adeyemo, "Development of an electric furnace using bentonite and kaolin sodium silicate as refractory material." 2024
51. E. E. Akhigbe, N. S. Egbuhuzor, A. J. Ajayi, and O. O. Agbede, "Designing risk assessment models for large-scale renewable energy investment and financing projects," *Int. J. Multidiscip. Res. Growth Eval.*, vol. 5, no. 1, pp. 1293–1308, 2024.
52. Semiu T. Fasasi Iyanu Ajifowowe, Mercy C Ngulat, Akeem Jimoh, Christianah O. Fasasi, Chidinma Nwaneto, "DESIGN AND COST EFFECTIVENESS OF RENEWABLE WIND-PV HYBRID POWER SYSTEM IN NIGERIA." 2024
53. O. B. Alao, G. C. Nwokocha, and O. M. Filani, "2024-Sustainability-Integrated Vendor Scorecard Evaluating Carbon Footprint, Waste Reduction, and Ethical Sourcing Alongside Traditional Metrics," *Int. J. Sci. Res. Humanit. Soc. Sci.*, vol. 1, no. 2, pp. 525–547, 2024.
54. U. O. Nnaji, L. B. Benjamin, N. L. Eyo-Udo, and E. A. Etukudoh, "A review of strategic decision-making in marketing through big data and analytics," *Magna Sci. Adv. Res. Rev.*, vol. 11, no. 1, pp. 084–091, 2024.
55. E. A. Etukudoh, A. Adefemi, V. I. Ilojianya, A. A. Umoh, K. I. Ibekwe, and Z. Q. S. Nwokediegwu, "A Review of sustainable transportation solutions: Innovations, challenges, and future directions," *World J. Adv. Res. Rev.*, vol. 21, no. 1, pp. 1440–1452, 2024.
56. A. Hamdan, K. I. Ibekwe, V. I. Ilojianya, S. Sonko, and E. A. Etukudoh, "AI in renewable energy: A review of predictive maintenance and energy optimization," *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 718–729, 2024.
57. I E Ekengwu, O C Okafor, H C Olisakwe, U D Ogbonna, "Reliability Centered Optimization of welded quality assurance." 2024
58. JL Chukwuneke, HO Orugba, HC Olisakwe, PO Chikelu, "Pyrolysis of pig-hair in a fixed bed reactor: Physico-chemical parameters of bio-oil." 2021
59. O. Elebe, C. C. Imediegwu, and O. M. Filani, "Predictive Analytics in Revenue Cycle Management: Improving Financial Health in Hospitals," 2021.
60. O. Fasawe, O. Umoren, and C. O. Makata, "Conceptual Framework for Improving Supply Chain Cycle Times Through Distributed Fulfilment Models," *Int. J. Sci. Res. Humanit. Soc. Sci.*, vol. 1, no. 2, pp. 811–838, 2024.

61. C. O. Okuh, E. O. Nwulu, E. Ogu, P. I. Egbumokei, I. N. Dienagha, and W. N. Digitemie, "A Strategic Model for Carbon Emission Reduction through Process Optimization in Energy Sector Operations," 2024.
62. G. Omoegun, J. E. Fiemotongha, J. O. Omisola, O. K. Okenwa, and O. Onaghinor, "Advances in ERP-Integrated Logistics Management for Reducing Delivery Delays and Enhancing Project Delivery".
63. A. A. Abayomi, J. C. Ogeawuchi, T. P. Gbenle, O. A. Agboola, and A. C. Uzoka, "Advances in Project Stakeholder Communication and Transparency Using Cloud Collaboration Platforms," *Int. J. Sci. Res. Sci. Technol.*, vol. 11, no. 5, Art. no. 5, Sept. 2024, doi: 10.32628/IJSRST52310373.
64. C. O. Okuh, E. O. Nwulu, E. Ogu, P. I. Egbumokei, I. N. Dienagha, and W. N. Digitemie, "Creating a Workforce Upskilling Model to Address Emerging Technologies in Energy and Oil and Gas Industries," 2024,
65. O. B. Johnson, J. Olamijuwon, E. Cadet, O. S. Osundare, and Y. W. Weldegeorgise, "Developing Real-Time Monitoring Models to Enhance Operational Support and Improve Incident Response Times".
66. A. T. Ayobami, U. Mike-Olisa, J. C. Ogeawuchi, A. A. Abayomi, and O. A. Agboola, "Digital Procurement 4.0: Redesigning Government Contracting Systems with AI-Driven Ethics, Compliance, and Performance Optimization," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 2, Art. no. 2, Apr. 2024, doi: 10.32628/CSEIT24102138.
67. T. Adenuga, A. T. Ayobami, and U. Mike-Olisa, "Enabling AI-Driven Decision-Making through Scalable and Secure Data Infrastructure for Enterprise Transformation," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 11, no. 3, Art. no. 3, June 2024, doi: 10.32628/IJSRSET241486.
68. A. Sharma, B. I. Adekunle, J. C. Ogeawuchi, A. A. Abayomi, and O. Onifade, "IoT-enabled Predictive Maintenance for Mechanical Systems: Innovations in Real-time Monitoring and Operational Excellence," *Iconic Res. Eng. J.*, vol. 2, no. 12, pp. 270–279, Apr. 2024.
69. C. D. Daudu, A. Adefemi, O. O. Adekoya, C. E. Okoli, O. B. Ayorinde, and A. I. Daraojimba, "LNG and climate change: Evaluating its carbon footprint in comparison to other fossil fuels," *Eng. Sci. Technol. J.*, vol. 5, no. 2, pp. 412–426, 2024.
70. O. T. Odofin, A. A. Abayomi, E. Ogbuefi, J. C. Ogeawuchi, O. S. Adanigbo, and T. P. Gbenle, "Strategic Integration of LangChain, Hugging Face Transformers, and OpenAI for Document Intelligence Systems," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 11, no. 4, Art. no. 4, Aug. 2024, doi: 10.32628/IJSRSET25121177.
71. T. Adenuga, N. Ayanbode, T. Ayobami, and F. C. Okolo, "Supporting AI in Logistics Optimization through Data Integration, Real-Time Analytics, and Autonomous Systems," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 11, no. 3, Art. no. 3, June 2024, doi: 10.32628/IJSRSET241487.
72. Didi P.U., Abass, O.S. & Balogun, O., "A Hybrid Channel Acceleration Strategy for Scaling Distributed Energy Technologies in Underserved Regions.." 2024
73. Abass, O.S., Balogun, O. & Didi P.U., "A Patient Engagement Framework for Vaccination and Wellness Campaigns in Resource-Constrained Settings.."
74. RE Dosumu, OO George, CO Makata, "Data-driven customer value management: Developing a conceptual model for enhancing product lifecycle performance and market penetration."
75. M. N. Asata, D. Nyangoma, and C. H. Okolo, "Human-Centered Design in Inflight Service: A Cross-Cultural Perspective on Passenger Comfort and Trust," *Gyanshauryam Int. Sci. Refereed Res. J.*, vol. 6, no. 3, pp. 214–233, 2023.
76. O. O. George, R. E. Dosumu, and C. O. Makata, "Integrating Multi-Channel Brand Communication: A Conceptual Model for Achieving Sustained Consumer Engagement and Loyalty," *Int. J. Manag. Organ. Res.*, vol. 2, no. 1, pp. 254–260, 2023, doi: 10.54660/ijmor.2023.2.1.254-260.
77. A. K. Adeleke, "Ultraprecision Diamond Turning of Monocrystalline Germanium," 2021, [Online]. Available: https://scholar.google.com/scholar?cluster=18034617435016344739&hl=en&oi=scholarr
78. M. AFOLABI, O. A. ONUKOGU, T. O. IGUNMA, A. K. ADELEKE, and Z. Q. S. NWOKEDIEGWU, "Systematic Review of pH-Control and Dosing System Design for Acid-Base Neutralization in Industrial Effluents," 2021
79. R. E. Dosumu, O. O. George, and C. O. Makata, "International Journal of Management and Organizational Research," 2023.
80. Balogun, O., Abass, O.S. & Didi P.U., "Packaging Innovation as a Strategic Lever for Enhancing Brand Equity in Regulation-Constrained Environments
81. MN Asata, D Nyangoma, CH Okolo, "Verbal and Visual Communication Strategies for Safety Compliance in Commercial Cabin Environments."
82. M. N. Asata, D. Nyangoma, and C. H. Okolo, "Verbal and Visual Communication Strategies for Safety Compliance in Commercial Cabin Environments,"

Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 9, no. 3, pp. 823–841, 2023.

83. K. S. Ahmed, O. D. Odejobi, and T. O. Oshoba, "Predictive Model for Cloud Resource Scaling Using Machine Learning Techniques," *J. Front. Multidiscip. Res.*, vol. 1, no. 1, pp. 173–183, 2020, doi: 10.54660/.IJFMR.2020.1.1.173-183.
84. S. E. Aifuwa, T. O. Oshoba, E. Ogbuefi, P. N. Ike, S. B. Nnabueze, and J. Olatunde-Thorpe, "Predictive Analytics Models Enhancing Supply Chain Demand Forecasting Accuracy and Reducing Inventory Management Inefficiencies," *Int. J. Multidiscip. Res. Growth Eval.*, vol. 1, no. 3, pp. 171–181, 2020, doi: 10.54660/.IJMRGE.2020.1.3.171-181.
85. T. O. Oshoba, S. E. Aifuwa, E. Ogbuefi, and J. Olatunde-Thorpe, "Portfolio Optimization with Multi-Objective Evolutionary Algorithms-Balancing Risk, Return, and Sustainability Metrics," *Int. J. Multidiscip. Res. Growth Eval.*, vol. 1, no. 3, pp. 163–170, 2020, doi: 10.54660/.IJMRGE.2020.1.3.163-170.
86. J. Olatunde-Thorpe, S. E. Aifuwa, T. O. Oshoba, and E. Ogbuefi, "Metadata-Driven Access Controls - Designing Role-Based Systems for Analytics Teams in High-Risk Industries," *Int. J. Multidiscip. Res. Growth Eval.*, vol. 1, no. 3, pp. 143–162, 2020, doi: 10.54660/.IJMRGE.2020.1.3.143-162.
87. D. R. E. Ewim *et al.*, "Survey of wastewater issues due to oil spills and pollution in the Niger Delta area of Nigeria: a secondary data analysis," *Bull. Natl. Res. Cent.*, vol. 47, no. 1, p. 116, July 2023, doi: 10.1186/s42269-023-01090-1.
88. C. S. Anyanwu and T. Babawarun, "Shear Stress Distribution in a Fuselage of an Aircraft," *J. Eng. Exact Sci.*, vol. 9, no. 3, pp. 15779–01e, 2023.
89. A. Hamdan, A. Al-Salaymeh, I. M. AlHamad, S. Ikemba, and D. R. E. Ewim, "Predicting future global temperature and greenhouse gas emissions via LSTM model," *Sustain. Energy Res.*, vol. 10, no. 1, p. 21, Dec. 2023, doi: 10.1186/s40807-023-00092-x.
90. O. F. Orikpete, S. Ikemba, and D. R. E. Ewim, "Integration of renewable energy technologies in smart building design for enhanced energy efficiency and self-sufficiency," *J. Eng. Exact Sci.*, vol. 9, no. 9, pp. 16423–01e, 2023.
91. C. C. Okoye *et al.*, "Integrating Business principles in STEM Education: fostering entrepreneurship in students and educators in the US and Nigeria," 2023, [Online]. Available: https://jurnal.narotama.ac.id/index.php/ijebd/article/download/2244/1592
92. O. A. Onukogu *et al.*, "Impacts of industrial wastewater effluent on Ekerekana Creek and policy recommendations for mitigation," *J. Eng. Exact Sci.*, vol. 9, no. 4, pp. 15890–01e, 2023.
93. A. A. Fawole, O. F. Orikpete, N. N. Ehiobu, and D. R. E. Ewim, "Climate change implications of electronic waste: strategies for sustainable management," *Bull. Natl. Res. Cent.*, vol. 47, no. 1, p. 147, Oct. 2023, doi: 10.1186/s42269-023-01124-8.
94. D. R. E. Ewim, S. M. Abolarin, T. O. Scott, and C. S. Anyanwu, "A survey on the understanding and viewpoints of renewable energy among South African school students," *J. Eng. Exact Sci.*, vol. 9, no. 2, pp. 15375–01e, 2023.
95. T. Babawurun, D. R. E. Ewim, T. O. Scott, and C. Neye-Akogo, "A comprehensive review of wind turbine modeling for addressing energy challenges in Nigeria and South Africa in the 4IR context," *J. Eng. Exact Sci.*, vol. 9, no. 2, pp. 15479–01e, 2023.
96. T. S. Mogaji, S. T. Fasasi, A. O. Ogundairo, and I. A. Oluwagbemi, "DESIGN AND SIMULATION OF A PICO HYDROELECTRIC TURBINE SYSTEM," *FUTA J. Eng. Eng. Technol.*, vol. 16, no. 1, pp. 132–139, 2022'
97. S. T. Fasasi, Z. S. Nwokediegwu, and O. J. Adebowale, "Conceptualization of Air Quality Index Performance Metrics for High-Pollution Industrial Zones Under EPA Oversight," 2022, [Online]. Available: https://shisrrj.com/paper/SHISRRJ221227.pdf
98. O. F. Bayeroju, A. N. Sanusi, and Z. Q. S. Nwokediegwu, "Conceptual Framework for Modular Construction as a Tool for Affordable Housing Provision," *Shodhshauryam Int. Sci. Refereed Res. J.*, vol. 5, no. 4, pp. 302–322, 2022.
99. O. F. Bayeroju, A. N. Sanusi, and Z. Q. Sikhakhane, "Conceptual Framework for Green Building Certification Adoption in Emerging Economies and Developing Countries," *Shodhshauryam Int. Sci. Refereed Res. J.*, vol. 5, no. 4, pp. 281–301, 2022.
100. S. T. Fasasi, Z. S. Nwokediegwu, and O. J. Adebowale, "An Engineering Concept for Digital Permit Management Systems to Improve Compliance across Oil and Gas Operations," 2022.
101. Daniel Raphael Ejike Ewim, Modestus O Okwu, Ekene Jude Onyiriuka, Aasa Samson Abiodun, Sogo Mayokun Abolarin, Amr Kaood, "View article."
102. S. A. Adio, T. A. Alo, R. O. Olagoke, A. E. Olalere, V. R. Veeredhi, and D. R. E. Ewim, "Thermohydraulic and entropy characteristics of Al 2 O 3 -water nanofluid in a ribbed interrupted microchannel heat exchanger," Heat Transf., vol. 50, no. 3, pp. 1951–1984, May 2021, doi: 10.1002/htj.21964.
103. S. A. Adio et al., "Thermal and entropy analysis of a manifold microchannel heat sink operating on CuO–

water nanofluid," J. Braz. Soc. Mech. Sci. Eng., vol. 43, no. 2, p. 76, Feb. 2021, doi: 10.1007/s40430-020-02772-x.

104. M. AFOLABI, O. A. ONUKOGU, T. O. IGUNMA, A. K. ADELEKE, and Z. Q. S. NWOKEDIEGWU, "Systematic Review of pH-Control and Dosing System Design for Acid-Base Neutralization in Industrial Effluents," 2021.