INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 7,854 Volume 12, issue 08 (2025)

TOWARD A UNIFIED FRAMEWORK FOR ZERO TRUST ADOPTION IN INDUSTRIAL AND CLOUD ENVIRONMENTS

Raghav Verma
Global Institute of Technology and Research, London, United Kingdom

Abstract: The increasing frequency and sophistication of cyberattacks across both traditional IT infrastructures and emerging industrial control, cloud, and Internet-of-Things (IoT) environments demand a paradigm shift in network security. Zero Trust Architecture (ZTA) has emerged as a powerful design philosophy purporting to eliminate implicit trust and enforce continuous verification. However, existing literature often treats cloud, enterprise, and industrial IoT deployments in isolation, resulting in fragmented adoption strategies and limited cross-domain applicability. This article synthesizes key theoretical and empirical insights from foundational works and recent advances to propose a comprehensive, unified framework for Zero Trust deployment spanning enterprise IT, critical infrastructure, and industrial IoT ecosystems. Through a rigorous integrative literature review, we identify core architectural principles, domain-specific challenges, and emergent threats such as ransomware targeting industrial control systems. We then articulate an abstract, extensible Zero Trust model that accounts for identity-centric access management, micro-segmentation, dynamic trust evaluation, continuous monitoring, and policy orchestration. Our framework also embeds adaptive mechanisms to address latency, legacy systems, and resource constraints common in industrial and edge deployments. We conclude by elucidating limitations, paths for future empirical validation, and recommendations for stakeholders seeking a holistic security posture across heterogeneous environments.

Keywords: Zero Trust, Industrial IoT, Cloud Security, Critical Infrastructure, Micro-segmentation, Ransomware, Continuous Monitoring.

Introduction

In the contemporary cybersecurity landscape, traditional perimeter-based security models increasingly fail to protect against advanced persistent threats, insider attacks, and lateral movement within networks. Historically, enterprises relied on the notion of a secure internal network shielded by firewalls and guarded entry points. Yet, in a world where remote access, cloud services, third-party integrations, and interconnected devices — especially in industrial IoT infrastructures — are ubiquitous, the assumption that anything "inside the perimeter" is implicitly trustworthy is dangerously outdated. Recognizing this deficiency, the concept of Zero Trust Architecture (ZTA) has gained traction, arguing for a fundamental redesign of network security predicated on the maxim "never trust, always verify" (Kindervag, 2010).

The formalization of ZTA by standardization bodies further validated its significance; for instance, the National Institute of Standards and Technology (NIST) articulated a comprehensive model encompassing identity, device, network, and data flows (Rose et al., 2020). Simultaneously, the ascendancy of cloud and collaboration-based computing—once the frontier of enterprise efficiency—introduced new vectors and complexities for access management (Almorsy, Grundy & Ibrahim, 2011). Meanwhile, critical infrastructure sectors such as oil and gas pipelines, energy grids, and manufacturing face not only conventional cyber threats but also operational and physical safety implications (Kilovaty, 2023; Elete, 2024).

The growing body of research reflects a proliferation of ZTA adaptations: focused studies on cloud environments, surveys of Zero Trust for IoT, theoretical expositions, and limited case studies in industrial contexts (Kang et al., 2023; He et al., 2022; Zanasi, Russo & Colajanni, 2024; Kesarpu, 2025). However, these efforts remain largely siloed. Few works endeavor to integrate disparate domains into a unified conceptual architecture, while practical guidance to reconcile the divergent requirements of enterprise IT, cloud, industrial IoT, and critical infrastructure remains scattered. In particular, there exists a lack of a coherent framework that simultaneously addresses identity, device posture, network segmentation, continuous monitoring, threat detection (including ransomware and insider threats), and operational constraints (e.g., latency, legacy systems, resource limitations) across all domains.

Therefore, this article seeks to fill the gap by systematically synthesizing the state of the art across domains and proposing a unified, extensible framework for Zero Trust adoption. In doing so, we aim to support organizations navigating hybrid environments — where cloud services, industrial control systems, IoT devices, and traditional enterprise networks coexist — and to provide a conceptual foundation for holistic security strategies.

Methodology

This research adopts an integrative literature review methodology, complemented by conceptual synthesis and cross-domain analytical reasoning. The integrative review process proceeds as follows:

1. Selection of Sources: We examine seminal works that laid the foundation for Zero Trust — notably, Kindervag (2010) — and subsequent formalizations by standardization bodies (Rose et al., 2020). We further include domain-specific studies reflecting cloud security management (Almorsy, Grundy & Ibrahim, 2011), industrial IoT adaptation (Zanasi, Russo & Colajanni, 2024), and critical infrastructure implementations (Adapa, 2024), alongside recent surveys and critical analyses (Kang et al., 2023; He et al., 2022; Fernandez & Brazhuk, 2024). Threat-specific literature — including insider threat detection via honeypots (Spitzner, 2003) and ransomware impact on industrial control systems (Elete, 2024) — is also incorporated to ground the threat model in realistic adversarial contexts. Finally, we consider broader perspectives on IoT security (Alaba et al., 2017) and emerging edge/fog computing security concerns (Rapuzzi & Repetto, 2018).

2. Analytical Framework: Each source is critically analyzed with respect to its contributions to architectural principles, domain constraints, threat models, and proposed mitigations. We map these contributions onto a conceptual template delineating: identity and access control, device posture and health, network segmentation, data protection, monitoring and visibility, policy orchestration, and domain-specific constraints (e.g., latency, legacy devices).

3. Synthesis: Through iterative comparison and cross-referencing, we derive a set of core principles applicable across domains, and identify variations necessary to accommodate domain-specific constraints. Contradictions, limitations, and areas lacking maturity are highlighted.

4. Framework Design: Based on the synthesis, we propose a unified, high-level Zero Trust framework. While abstract, it is sufficiently detailed to guide thinking about concrete deployment across varied environments. We also discuss possible extensions and adaptation strategies for different domains.

5. Validation via Scenario Analysis: To assess the applicability and robustness of the proposed framework, we apply it to conceptual scenarios — e.g., securing a hybrid cloud–industrial IoT environment controlling an oil pipeline — drawing on insights from domain-specific threat literature (Elete, 2024; Kilovaty, 2023).

Given the conceptual and literature-based nature of the study, no empirical deployment or original data collection is reported. Rather, the focus is on theoretical integration and practical guidance grounded in existing evidence.

Results

The integrative literature review and synthesis yield a set of foundational principles, domain-agnostic architectural tenets, and domain-specific adaptations which together inform a unified Zero Trust framework. The results are presented as (a) core Zero Trust principles, (b) challenges and constraints across domains, and (c) the outline of a unified conceptual architecture with domain-specific adaptations.

Core Zero Trust Principles

1. Identity-Centric Access Control and Least-Privilege

At the heart of ZTA lies the reorientation of security away from the network perimeter toward identity and resource-level access. Rather than assuming trust based on network location, each request must be authenticated, authorized, and audited. This identity-centric model — first articulated in foundational work (Kindervag, 2010) — demands rigorous authentication procedures, robust identity management, and continuous verification. NIST formalizes this by mandating that actors (users, devices, services) be identified and their credentials validated for every access attempt, with policies enforcing least-privilege (Rose et al., 2020).

This principle ensures that even if an attacker breaches the perimeter — for example, through phishing or compromised credentials — they cannot traverse the network arbitrarily; lateral movement is constrained by identity-based segmentation and minimal privileges.

2. Device and Workload Posture Verification

Beyond identity, Zero Trust posits that devices and workloads accessing resources must present assurance of their security posture. The assurance may include device health, patch levels, configuration compliance, and workload trustworthiness. Rose et al. (2020) emphasize the need for device compliance checks as part of access policy enforcement. This prevents compromised or unmanaged devices from acting as pivot points.

In contexts such as cloud, industrial IoT, and edge computing, where devices vary widely in capability and lifecycle, posture verification becomes especially critical.

3. Micro-Segmentation and Least-Privileged Network Access

A major departure from traditional flat networks is the granular segmentation of network flows — often termed "micro-segmentation." In ZTA, network segmentation is dynamic and policy-driven, enforcing minimal connectivity: only the required communication paths are allowed, avoiding "all-to-all" trust (Kindervag, 2010; Rose et al., 2020).

Micro-segmentation limits the "blast radius" of breaches — even if an attacker compromises one segment, lateral movement is hampered by enforcement of narrow, context-dependent connectivity. This segmentation can be especially important in cloud and hybrid environments where services and workloads are distributed.

4. Continuous Monitoring and Adaptive Trust Evaluation

Zero Trust rejects one-time authentication at session initiation: instead, access decisions and trust should be continuously evaluated during the lifecycle of connections and resource usage. NIST calls for continuous visibility, telemetry collection, and policy-based re-evaluation (Rose et al., 2020).

Continuous monitoring enables detection of anomalous behavior, privilege escalation, or device compromise — including insider threats or post-exploitation lateral spread. It also allows dynamic revocation of access if trust diminishes.

5. Policy Orchestration and Centralized Governance

Implementing ZTA effectively requires a centralized mechanism to define, manage, and enforce access policies across identities, devices, workloads, and network flows. This governance layer coordinates authentication, authorization, compliance, segmentation, logging, and revocation. In hybrid and heterogeneous environments — cloud, enterprise, industrial IoT — policy orchestration ensures consistent security posture without manual intervention (Almorsy, Grundy & Ibrahim, 2011).

Challenges and Constraints Across Domains

While the core principles provide a foundation, deploying Zero Trust in real-world environments surfaces significant challenges, some common across domains and others domain-specific.

1. Legacy Infrastructure and Resource Constraints

Many industrial control systems, IoT devices, and critical infrastructure components were designed without modern security in mind. They often operate on legacy protocols, lack identity or authentication mechanisms, and may not support patching or encryption. This severely complicates both identity-based access control and device posture verification (Alaba et al., 2017; Zanasi, Russo & Colajanni, 2024). Resource constraints — limited CPU, memory, or bandwidth — make continuous monitoring and encryption computationally expensive, sometimes infeasible.

2. Latency and Real-Time Constraints

In industrial and control systems, operations may require real-time or near-real-time responsiveness. Adding layers of authentication, encryption, segmentation, and monitoring — if not optimized — can impair performance or even violate operational constraints. Edge and fog computing paradigms further complicate this, as they distribute computation across constrained devices (Rapuzzi & Repetto, 2018).

3. Heterogeneity of Devices and Protocols

Industrial IoT and critical infrastructure often involve a wide array of devices — sensors, actuators, legacy PLCs (programmable logic controllers), SCADA systems — using proprietary or specialized protocols. Integrating these into a unified identity-based, segmented, policy-driven architecture is non-trivial (Alaba et al., 2017; Zanasi, Russo & Colajanni, 2024).

4. Operational Culture and Organizational Resistance

Transitioning from perimeter-based security to Zero Trust often requires fundamental changes in operations, mindset, and administration. Legacy organizational practices, lack of skilled personnel, and resistance to change impede adoption (He et al., 2022). In mission-critical environments — e.g., oil and gas, water utilities — administrators may be averse to modifications that risk downtime or disruption.

5. Threat Complexity: Insider Threats, Ransomware, and Advanced Persistent Threats (APTs)

The nature of threats continues evolving. While ZTA mitigates many threats via segmentation and least privilege, it also demands comprehensive threat detection mechanisms. Insider threats, for instance, may bypass identity checks by using legitimate credentials; detection often requires behavioral analysis and deception mechanisms such as honeypots (Spitzner, 2003). Meanwhile, ransomware attacks targeting industrial control systems are increasingly common (Elete, 2024), exploiting legacy vulnerabilities, weak segmentation, or lack of monitoring.

6. Regulatory and Compliance Challenges

Critical infrastructure and industrial sectors are often subject to regulatory requirements, compliance standards, and high uptime demands. Introducing new security architectures may require regulatory approval, interoperability validation, and adherence to safety standards — constraints sometimes at odds with ideal Zero Trust implementations.

A Unified Conceptual Zero Trust Framework with Domain-Specific Adaptations

Based on the synthesis, we propose a unified conceptual Zero Trust framework composed of modular layers, each mapping to core principles while allowing domain-specific instantiation. The layers are:

- Identity & Credential Layer
- Device/Workload Posture Layer
- Network Segmentation & Access Layer
- Data and Resource Protection Layer
- Monitoring & Telemetry Layer
- Policy Orchestration & Governance Layer

Below, we outline each layer, its functions, and considerations for cloud, enterprise, and industrial/critical infrastructure deployments.

1. Identity & Credential Layer

○ Maintain a centralized identity and access management system (IAM), supporting users, services, devices, and workloads.

○ Employ strong authentication mechanisms (e.g., multi-factor authentication) for human users; for devices, use certificates, device identity tokens, or hardware-based identities where feasible.

○ For industrial IoT and legacy devices unable to support modern identity mechanisms, deploy identity proxies or gateways that abstract device identity and mediate access. For example, an edge gateway can represent a legacy device, performing translation and enforcing identity-based access on its behalf (Zanasi, Russo & Colajanni, 2024).

○ Enforce least-privilege role-based or attribute-based access control (RBAC or ABAC), minimizing permissions to only what is strictly necessary (Kindervag, 2010; Rose et al., 2020).

2. Device/Workload Posture Layer

○ Continuously assess device posture: patch status, configuration compliance, firmware version, known vulnerabilities, and health metrics.

○ For virtual workloads in cloud or containerized environments: integrate with orchestration platforms to enforce compliance before deployment or runtime.

○ For industrial control systems and IoT devices: where continuous posture assessment is impossible due to constraints, implement compensating controls such as network isolation, gateway-based filtering, or scheduled device health audits.

○ Maintain a device registry and posture history repository to enable visibility, auditing, and anomaly detection.

3. Network Segmentation & Access Layer

○ Implement dynamic micro-segmentation: segments defined not by physical network topology but by policy, identity, and workload attributes. This can be realized via software-defined networking (SDN), overlay networks, virtual LANs (VLANs), or next-generation firewalls depending on context.

○ In cloud environments: utilize virtual network constructs (e.g., subnets, security groups) and software-defined policies to isolate workloads.

○ In industrial IoT and critical infrastructure: where SDN may not be feasible, use edge gateways, data diodes, and network-level proxies to segregate zones (e.g., supervisory control networks vs. business networks), ensuring only necessary communications are permitted.

○ Enforce network-level access control lists (ACLs), flow controls, and default-deny rules; all allowed flows must be explicitly permitted.

4. Data and Resource Protection Layer

○ Encrypt data at rest and in transit where possible; for resource-constrained devices, use lightweight encryption protocols or gateway-based encryption.

○ For critical operational data (e.g., control commands, telemetry), apply strict access controls, audit logging, and integrity verification.

○ Apply data classification and labeling to identify sensitive data requiring stricter protections — especially relevant in cloud and enterprise contexts where regulatory compliance is critical.

5. Monitoring & Telemetry Layer

○ Deploy continuous monitoring mechanisms across identity usage, network flows, device health, workload behavior, and data access.

○ Collect logs, metrics, and telemetry centrally to allow for correlation, anomaly detection, behavioral analysis, and forensic readiness.

○ Use adaptive trust evaluation: based on observed behavior, posture changes, or suspicious activity, the

system recalculates trust and can revoke or restrict access dynamically (Rose et al., 2020).

○ In industrial environments, where bandwidth may be limited and devices constrained, prioritize critical telemetry (e.g., control command logs, access attempts, anomalous flows) — possibly using sampling, aggregation, or gateway-based summarization to reduce overhead (Rapuzzi & Repetto, 2018).

6. Policy Orchestration & Governance Layer

○ Maintain a central policy engine that defines and enforces access rules across identity, device posture, network flow, data access, and resource usage.

○ Provide administrative interfaces for policy definition, review, audit, and exception management.

○ Ensure that policy definitions remain consistent across hybrid environments (cloud, on-premise, industrial) to avoid gaps or policy conflicts — especially critical in organizations managing diverse infrastructure.

○ Support dynamic policy updates to respond to evolving threats (e.g., new ransomware variants) or operational changes (e.g., device onboarding, IoT expansion).

Domain-Specific Adaptations: Illustrative Scenarios

To illustrate how the unified framework adapts to different contexts, consider the following scenarios:

● Hybrid Cloud–Enterprise Deployment: An organization uses a public cloud provider for application hosting, maintains on-premise legacy servers for sensitive data, and offers remote access to employees. In this environment, the identity layer binds user identities across on-premise and cloud resources; micro-segmentation isolates workloads; encryption protects data in transit; continuous monitoring tracks access and detects suspicious behavior. Policy orchestration ensures that users accessing from unmanaged devices or untrusted networks are restricted or blocked.

● Industrial IoT Environment: A manufacturing plant leverages IoT sensors and actuators, connecting legacy PLCs, SCADA systems, and edge devices. Many of these devices lack modern security. A Zero Trust gateway at the edge represents legacy devices to the rest of the infrastructure, mediating authentication, enforcing segmentation, and encrypting communication. Workload posture verification may be limited; instead, network isolation and gateway-based controls reduce risk. Telemetry focuses on control commands and access logs.

● Critical Infrastructure (Oil & Gas Pipeline): Such systems face risks from cyberattacks, including ransomware that can disrupt operations, cause environmental damage, or endanger human safety (Elete, 2024; Kilovaty, 2023). Here, the unified framework enforces strict identity and device control, segments the pipeline control network from business networks, applies encryption and resource-level controls, and continuously monitors for anomalous commands or unauthorized access. In the event of a detected breach, the centralized governance layer can automatically revoke access, isolate segments, and alert operators.

Through these domain-specific instantiations, the unified framework demonstrates flexibility: it preserves core Zero Trust principles while accommodating constraints arising from legacy devices, resource limitations, real-time requirements, and regulatory demands.

Discussion

The unified framework outlined above offers several important conceptual and practical implications for organizations aiming to transition toward Zero Trust across heterogeneous environments. Nonetheless, deploying such a framework in real-world systems involves formidable challenges, trade-offs, and areas requiring further research.

1. Implications and Advantages

○ Holistic Security Posture: By integrating identity, device, network, and data controls under a unified architecture, stakeholders avoid fragmentation or silos — a common issue when adopting domain-specific solutions in cloud, enterprise, and industrial contexts. This reduces complexity, ensures policy consistency, and closes visibility gaps.

○ Resilience Against Advanced Threats: The layered defensive approach — identity verification, micro-segmentation, continuous monitoring — significantly raises the bar for attackers. Even if credentials are compromised or a device is infiltrated, lateral movement, privilege escalation, and data exfiltration become far more difficult. The model particularly strengthens defense against insider threats (Spitzner, 2003) and ransomware attacks on critical infrastructure (Elete, 2024).

○ Adaptability and Scalability: The modular layer design allows organizations to deploy Zero Trust incrementally. For instance, starting with identity and micro-segmentation for enterprise IT, then extending coverage to cloud workloads, and finally integrating industrial IoT devices via edge gateways. Such phased adoption is more manageable and less disruptive.

2. Limitations and Challenges

○ Absence of Empirical Evaluation: As a conceptual framework derived from literature synthesis, this article does not provide empirical performance measurements, quantitative risk reduction data, or operational case studies. Real-world deployment may expose unexpected issues such as performance degradation, false positives, or administrative overhead.

○ Legacy and Resource-Constrained Devices: Many industrial IoT and control systems may be incapable of supporting even lightweight security mechanisms. Gateway-based abstractions or proxies may partially mitigate, but ultimately may not guarantee device-level security. Complete coverage may be impossible without device upgrade or replacement — which may be cost-prohibitive or operationally infeasible.

○ Operational and Cultural Barriers: Implementing this framework requires organizational commitment, investment, and possibly retraining of staff. In critical infrastructure settings where uptime is paramount, administrators may resist changes due to fear of unintended downtime or system instability.

○ Policy Complexity and Management Overhead: As the number of identities, devices, workloads, and segments grows, policy management becomes complex. Ensuring consistency, avoiding conflicts, and maintaining up-to-date policy definitions demand rigorous governance processes, which may impose administrative burden.

○ Performance and Latency Concerns: Continuous monitoring, encryption, and traffic inspection — especially in edge or real-time control environments — may introduce latency or affect real-time performance. Packet inspection, logging, and policy enforcement must be carefully optimized to avoid system degradation.

3. Future Research and Development Directions

- Empirical Implementation and Benchmarking: Future work should involve deploying the proposed architecture in real-world pilot environments — e.g., a manufacturing plant retrofitted with Zero Trust gateways, or a hybrid cloud–on premise enterprise — to evaluate performance, overhead, latency, usability, and security effectiveness. Metrics such as time to detect compromise, mean time to isolate, system performance degradation under load, and rate of false positives would provide valuable empirical validation.

- Automation and Orchestration Tools: As policy complexity grows, human management becomes unsustainable. Research is needed into automation frameworks, policy orchestration tools, and AI-driven adaptive policy engines that can learn from behavior, detect anomalies, and dynamically adjust access privileges. Incorporating machine learning for behavioral baselining and anomaly detection may strengthen defense against insider threats and advanced persistent threats.

- Lightweight Security Mechanisms for Constrained Devices: For industrial IoT, edge, and legacy control systems, development of lightweight authentication, encryption, and monitoring protocols tailored to limited-resource devices is critical. Research into efficient cryptographic protocols, lightweight identity tokens, and adaptive telemetry is vital.

- Standards and Compliance Frameworks: As adoption grows, industry standards and regulatory compliance frameworks tailored to Zero Trust in industrial and critical infrastructure contexts are needed. Collaboration between security researchers, industry stakeholders, and regulatory bodies can help define best practices, audit mechanisms, and compliance requirements.

- Human Factors and Governance Models: Effective Zero Trust adoption depends not just on technology, but on human processes, policy governance, and organizational culture. Research into human factors, usability, policy governance models, change management strategies, and training frameworks will be essential to facilitate real-world transitions.

Conclusion

The shifting threat landscape — propelled by the proliferation of cloud services, IoT, industrial control systems, and remote connectivity — necessitates a departure from traditional perimeter-based security models. The Zero Trust paradigm offers an appealing and fundamentally different approach: one centered on identity, verification, segmentation, and continuous trust evaluation. While prior research has explored ZTA in isolated domains — enterprise, cloud, industrial IoT — there has been limited work toward a holistic, unified architecture capable of spanning heterogeneous environments.

This article has attempted to bridge that gap by synthesizing foundational and contemporary literature to propose a unified, modular Zero Trust framework. By delineating core architectural layers — identity, device posture, network segmentation, data protection, monitoring, and governance — and mapping them to domain-specific adaptations, the framework aims to guide organizations managing hybrid environments: cloud and on-premises enterprise, industrial IoT, and critical infrastructure.

While the proposed model offers theoretical robustness and flexibility, its conceptual nature underscores urgent need for empirical evaluation. Real-world deployments, performance testing, governance tooling, and lightweight security mechanisms for constrained devices remain open challenges. Nonetheless, we argue that the framework provides a valuable blueprint for future research, adoption strategies, and policy development — ultimately supporting a more resilient, unified, and proactive cybersecurity posture across today's complex and interconnected digital environments.

References

1. Kindervag, J. (2010). Build security into your network's DNA: The Zero Trust network architecture. Forrester Research.

2. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207.

3. Spitzner, L. (2003). Honeypots: Catching the insider threat. In Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC), 170–179.

4. Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011). Collaboration-based cloud computing security management framework. In 2011 IEEE 4th International Conference on Cloud Computing, 364–371.

5. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc Networks, 156, 103414.

6. Adapa, V. R. K. (2024). Zero Trust Architecture Implementation in Critical Infrastructure: a Framework for Resilient Enterprise Security. International Journal of Advanced Research in Engineering & Technology, 15(6), 76–89.

7. Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. Entropy, 25(12), 1595.

8. Kesarpu, S. (2025). Zero-Trust Architecture in Java Microservices. International Journal of Networks and Security, 5(01), 202–214.

9. Kilovaty, I. (2023). Cybersecuring the Pipeline. Houston Law Review, 60.

10. Elete, N. T. Y. (2024). Impact of ransomware on industrial control systems in the oil and gas sector: Security challenges and strategic mitigations. Computer Science & IT Research Journal, 5(12), 2664–2681.

11. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on Zero Trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 1–13.

12. Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces, 89, 103832.

13. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28.

14. Rapuzzi, R., & Repetto, M. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. Future Generation Computer Systems, 85, 235–249.