pISSN:2349-5707 Volume:12, Issue 09, September-2025 eISSN:2349-5715

EVOLVING FRONTIERS IN CYBERSECURITY: A COMPREHENSIVE ANALYSIS OF ZERO TRUST ARCHITECTURES AND THEIR IMPLEMENTATION ACROSS DOMAINS

Rahul Verma
International Cybersecurity University, United States

ABSTRACT: In an era of increasingly sophisticated cyber threats and dynamic IT environments, the traditional perimeter-based security model has become insufficient. The Zero Trust Security (ZTS) paradigm has emerged as a transformative framework to mitigate modern security challenges by treating all entities—users, devices, applications, services—as potentially untrusted and continuously verifying their credentials and behavior. This paper presents a comprehensive, conceptual research study synthesizing existing literature and industry white papers on Zero Trust, encompassing perspectives from federal guidance, enterprise adoption, cloud infrastructures, Internet of Things (IoT) ecosystems, microservices, and machine-learning–driven access control. Through a systematic multivocal literature review and thematic analysis of thirteen pivotal works, the study develops a unified taxonomy of Zero Trust architecture variations, identifies core principles and domain-specific adaptations, and elucidates common challenges and gaps in current implementations. The results reveal fundamental architectural patterns—Identity-Centric, Network-Segmentation, Device-Aware, Behavioral/Trust-Scoring, and Contextual Access Control—each with distinct design tradeoffs depending on environment (e.g., enterprise network, cloud, IoT, microservices). The analysis further surfaces recurring obstacles, including legacy-system integration, standardization deficits, performance overhead, interoperability, usability, and regulatory compliance. The paper concludes with a discussion of theoretical and practical implications, limitations, and a roadmap for future research to advance quantitative evaluation, standard frameworks, and cross-domain interoperability.

Keywords: Zero Trust Security, Zero Trust Architecture, Identity-Based Access, Cloud Security, IoT Security, Microservices, Machine Learning Trust Scoring.

INTRODUCTION

The security landscape of the twenty-first century is characterized by pervasive connectivity, hybrid infrastructures, cloud services, mobile devices, and distributed applications. Traditional cybersecurity strategies have largely relied on perimeter-based defenses: firewalls, network boundary controls, and trust implicitly extended to internal network entities. This model assumes that once inside the perimeter, users and devices are trustworthy. However, the proliferation of remote work, cloud migration, third-party services, mobile endpoints, and increasingly sophisticated adversaries has eroded the effectiveness of perimeter-based security. Cyber attackers exploit stolen credentials, insider threats, misconfigured cloud services, and lateral movement opportunities inside the network—bypassing traditional defenses with alarming ease. In response, the paradigm of Zero Trust Security (ZTS) has gained traction as a means to transcend the limitations of perimeter-centric models.

Zero Trust fundamentally rethinks security by adopting a model centered on verification and continuous trust assessment rather than implicit trust based on network topology. The core mantra often articulated is "never trust, always verify." As defined in guidance from major institutions such as the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST), Zero Trust demands that every access request to resources—whether from inside or outside the traditional perimeter—must be

authenticated, authorized, and validated dynamically (NSA, 2021; Kerman, 2020). Further, the architectural blueprint provided by NIST (Rose et al., 2020) outlines principles such as least-privilege access, microsegmentation, continuous monitoring, and contextual access assessment. These principles promise a more resilient security posture that adapts to modern threats and dynamic IT environments.

Yet despite the growing popularity and adoption of Zero Trust across enterprises, cloud providers, and cybersecurity vendors, there remains a lack of a unified, comprehensive framework that captures and reconciles the multitude of architectural variations, domain-specific adaptations, and practical challenges. Existing literature and industry reports tend to focus on narrow perspectives—either high-level conceptual guidance, domain-specific case studies (e.g., IoT or microservices), or surveys of emerging implementations. For organizations seeking to adopt Zero Trust, this fragmented landscape complicates decision-making: which architecture variant suits which environment? What are the trade-offs? What are recurring pitfalls?

This article addresses these gaps through a systematic and comprehensive conceptual research study. By synthesizing and analyzing a curated collection of foundational and contemporary works—including federal guidance, industry analyses, empirical research, and domain-specific case studies—this research aims to produce: (a) a unified taxonomy of Zero Trust architecture variants; (b) a cross-domain comparative analysis of benefits, tradeoffs, and suitability; (c) identification of recurring challenges; and (d) a structured roadmap for future research and standardization. This unified perspective not only aids researchers and security architects in navigating the complexity of Zero Trust but also supports informed, context-aware decision-making for real-world deployment.

METHODOLOGY

Given the conceptual nature of this research, a literature-based, qualitative methodology was chosen. Specifically, a multivocal literature review (MLR) approach was adopted, encompassing both academic publications and grey literature (industry white papers, federal guidance, vendor analyses). This approach ensures comprehensiveness across the formal research domain and practical, real-world implementations. The following steps were undertaken:

1. Selection of Sources: The body of literature was limited to the documents provided in the reference list. These included federal guidance (NSA, NIST), industry white papers (Forrester, Cloudflare), academic and conference publications (survey articles, empirical studies in IoT and microservices contexts), and domain-specific implementations (e.g., machine-learning–driven Zero Trust, wearable IoT, microservices). The selection intentionally spans multiple domains and perspectives to enable cross-domain analysis.

2. Thematic Coding and Taxonomy Derivation: Each source was carefully read and conceptually coded according to architectural design elements, core principles, domain context, implementation mechanisms, and reported challenges or limitations. These codes were then clustered to identify common patterns and divergent adaptations, resulting in a taxonomy of Zero Trust architecture variants.

3. Comparative Analysis: The identified variants were compared across several dimensions: trust anchor (identity, device, behavior, context), enforcement mechanisms (microsegmentation, tokenization, access control), domain suitability (enterprise network, cloud, IoT, microservices), scalability, performance overhead, interoperability, usability, and regulatory/compliance considerations.

4. Synthesis of Challenges and Research Gaps: Recurring obstacles and limitations reported across studies were collated. Gaps in the literature—particularly the lack of empirical evaluation frameworks,

standardization, and interoperability efforts—were identified.

5. Conceptual Framework & Roadmap Proposition: Based on the taxonomy and identified gaps, a conceptual framework for cross-domain Zero Trust adoption was proposed, along with a research roadmap to guide future empirical and standardization efforts.

This methodology permits a deep, theory-driven exploration purely through textual analysis. No empirical experiments, data collection, or statistical analysis were performed; the "results" consist of conceptual classifications, comparative findings, and synthesized insights.

RESULTS

The thematic analysis and comparative review yielded several significant outcomes: a unified taxonomy of Zero Trust architecture variants; a mapping of domain-specific adaptations; and an articulation of common challenges and limitations.

A Unified Taxonomy of Zero Trust Architecture Variants

The first and most substantive result is the derivation of a unified taxonomy that captures the diversity of Zero Trust implementations across domains. The taxonomy identifies five primary variants, which often overlap or combine in real-world deployments. Each variant emphasizes a different trust anchor or enforcement strategy:

- Identity-Centric Access Control (Identity-Based Zero Trust)

This variant centers on the identity of users, service accounts, or entities requesting access. Authentication and authorization are performed per request, often combined with least-privilege principles. Access decisions rely heavily on verified credentials, identity attributes, and roles. This approach is prominent in enterprise settings and cloud-based services. The work of Gunuganti (2023) on "Identity Based-Zero Trust" highlights the feasibility and benefits of treating identity as the core trust anchor, decoupled from network topology. In such systems, identity providers, multi-factor authentication (MFA), attribute-based access control (ABAC), and role-based access control (RBAC) become central.

- Network-Segmentation and Microsegmentation (Network-Based Zero Trust)

Here, trust boundaries are shifted from the traditional perimeter to microsegments inside the network. Rather than granting broad internal access, the network is broken into smaller, more controlled segments. Each segment enforces policies, and lateral movement is constrained. The architecture guidelines in NIST SP 800-207 (Rose et al., 2020) emphasize microsegmentation as a core principle. Implementation of this variant can significantly reduce blast radius in case of compromise, limiting an attacker's ability to traverse the network.

- Device-Aware Trust (Device-Centric Zero Trust)

This variant emphasizes the security posture of the device—its configuration, patch status, integrity, and compliance with security policies. The trust decision takes into account device health in addition to identity. In environments with Bring Your Own Device (BYOD), mobile endpoints, IoT, or unmanaged devices, this approach becomes important. The study by Teerakanok et al. (2021) on migrating to Zero Trust architecture emphasizes this variant when dealing with legacy infrastructure and heterogeneous devices. Similarly, implementations targeting wearable IoT devices (Mohseni Ejiyeh, 2023) rely on device-aware

trust decisions to ensure lightweight but secure access control.

- Behavioral and Trust-Scoring Based Zero Trust

Rather than relying solely on static credentials or device posture, this variant introduces dynamic trust evaluation based on behavioral analytics, usage patterns, risk scoring, and contextual information. The trust score may evolve with ongoing monitoring, potentially enabling or revoking access dynamically. The emerging trend of applying machine learning (ML) for trust assessment is captured by Munasinghe et al. (2023) in their ML-based Zero Trust architecture proposal. Additionally, N'goran et al. (2022) introduce a trust assessment model tailored for community-cloud environments, where behavioral and contextual metrics inform access decisions.

- Contextual and Token-Based Zero Trust

This variant integrates contextual parameters—time of access, location, application type, session state, network, and device type—and may use token-based authentication and authorization mechanisms. A specific instantiation is seen in the "Zero Trust Architecture of Token Network" described by Ho, Chen, and Lin (2023), which utilizes tokenization and contextual evaluation to secure access in highly dynamic networked environments (such as metaverse-style applications). This approach is particularly relevant for real-time systems, microservices architectures, or content delivery networks where sessions and tokens are predominant.

These variants are not mutually exclusive. In practice, comprehensive Zero Trust deployments often combine multiple variants—for example, Identity-Centric plus Device-Aware plus Contextual Access Control—depending on the sensitivity of resources and the deployment environment.

Domain-Specific Adaptations: Mapping Variants to Environments

Beyond the taxonomy, the analysis revealed how different domains tend to favor particular Zero Trust variants or hybrid combinations, shaped by their constraints, threat models, and operational requirements:

- Traditional Enterprise Networks & Cloud Services: Predominantly adopt Identity-Centric and Network-Based Zero Trust. The guidance from NSA (2021) and NIST (Rose et al., 2020) underscores identity verification for all access and microsegmentation for lateral movement prevention. Cloud providers and organizations transitioning to cloud integrate Identity-Centered access via IAM solutions, combined with network segmentation within virtual networks. Industry reports (Kerman, 2020; Balaouras, 2022; Cloudflare, 2024) corroborate that this hybrid is the most commonly recommended approach for enterprises seeking compliance, centralized control, and minimal disruption to existing workflows.

- Microservices and Containerized Architectures: In microservices ecosystems, where services communicate internally across dynamic networks, Identity-Centric and Contextual/Token-Based Zero Trust dominate. The recent work of Kesarpu (2025) details how Zero Trust can be implemented in Java-based microservices, leveraging identity tokens, mutual TLS, microsegmentation at service mesh layer, and contextual policy enforcement. Token-based auth, short-lived credentials, and service identity (rather than user identity) are central, allowing horizontal scaling and dynamic service provisioning without sacrificing security.

- IoT and Wearable Device Environments: For IoT, wearables, and other resource-constrained or unmanaged devices, Device-Aware and Contextual Zero Trust approaches emerge as more practical. The lightweight cloud-based access control protocol proposed by Mohseni Ejiyeh (2023) for wearable IoT

devices exemplifies this adaptation: integrating device attestation, contextual policy enforcement, and minimal overhead—recognizing that traditional user-based identity or heavy authentication frameworks may be impractical for such devices.

- Community Cloud / Multi-Tenant Environments: In shared or community cloud settings—where multiple organizations share infrastructure—Behavioral / Trust-Scoring and Contextual approaches become relevant. The trust-assessment model presented by N'goran et al. (2022) relies on continuous evaluation of tenant behavior, resource usage patterns, and contextual risk to enforce access controls dynamically. Such dynamic trust evaluation is critical in environments with varying trust levels and shared resources.

- Emerging and Highly Dynamic Environments (e.g., Metaverse, Virtualization, Real-Time Services): For environments marked by ephemeral sessions, token-based interactions, and dynamic resource allocation, Contextual/Token-Based and Behavioral Trust-Scoring variants are especially suitable. The token-based Zero Trust architecture designed by Ho, Chen, and Lin (2023) for "token networks" demonstrates how tokenization, contextual access policies, and runtime evaluation of trust can secure interactions in high-churn, low-latency environments.

By mapping variants to domains, the taxonomy serves as a decision-support tool: security architects can more precisely select or blend variants based on contextual constraints, resource types, performance needs, and threat models.

Common Challenges and Limitations in Zero Trust Implementations

Beyond the taxonomy, the review evidenced recurring challenges, limitations, and gaps across the literature. These are summarized below:

- Legacy Systems and Integration Overhead: Many enterprises operate legacy systems—on-premises servers, outdated devices, proprietary applications—that were not designed for fine-grained access control or identity-based authentication. Migrating such systems into a Zero Trust framework often demands significant refactoring, application redesign, or use of proxies and adapters. Teerakanok et al. (2021) note that this migration complexity is a major barrier, especially for large organizations with heterogeneous infrastructure.

- Lack of Standardization and Interoperability: Given the diversity of Zero Trust variants and vendor-specific implementations, there is an absence of standard frameworks, interoperable protocols, or industry-wide benchmarks. As several authors lament, this fragmentation can lead to vendor lock-in, inconsistent security postures, and difficulty in evaluating or comparing solutions (Itodo & Ozer, 2024; He et al., 2022). Without standardization, cross-domain integration—e.g., combining IoT, cloud, and microservices security—remains challenging.

- Performance and Latency Overhead: Particularly in Device-Aware, Behavioral, or Contextual trust evaluation models, continuous monitoring, real-time risk assessment, token verification, and dynamic policy enforcement can impose performance overhead. For applications requiring low latency (e.g., real-time IoT, streaming, microservices), this overhead can degrade user experience or system responsiveness. The token-based architecture proposed by Ho et al. (2023) acknowledges these trade-offs, cautioning that security gains must be weighed against latency and throughput constraints.

- Usability and User Experience Challenges: Fine-grained access control, frequent authentication prompts, contextual policy enforcement, and behavioral monitoring may impose friction on end-users. If

not designed thoughtfully, Zero Trust systems risk impacting productivity, causing user resistance, or encouraging shadow IT practices. Balaouras (2022) emphasizes that the human factor—user behavior, resistance, compliance fatigue—remains one of the most underexplored but critical challenges.

- Scalability and Management Complexity: As the number of users, devices, services, and policies grows, managing access rules, identity relationships, segmentation, and contextual policies becomes complex. This is particularly evident in large enterprises or multi-tenant cloud environments. The survey by He et al. (2022) points out that scaling Zero Trust across global, distributed networks—with hybrid cloud, on-prem, and remote endpoints—requires robust automation, orchestration, and identity-management infrastructure.

- Absence of Empirical Evaluation and Metrics: Although many studies, white papers, and vendor reports promote Zero Trust as superior to perimeter-based models, there is a conspicuous lack of empirical studies assessing actual security outcomes, performance trade-offs, cost-benefit analysis, or user impact. The multivocal literature review conducted by Itodo & Ozer (2024) reveals this gap: most implementations are described qualitatively, with few quantitative metrics or formal evaluations. Similarly, the ML-based trust models (Munasinghe et al., 2023) remain proof-of-concept prototypes without large-scale deployment data.

These challenges highlight that while Zero Trust offers compelling conceptual advantages, its real-world adoption is nontrivial, requiring careful planning, standardization, and consideration of human, operational, and technical factors.

DISCUSSION

The results of this conceptual analysis have deep theoretical and practical implications for the evolution of cybersecurity architectures. Below we explore these implications, discuss limitations of the study, and propose directions for future research and standardization efforts.

Theoretical Implications and Reconceptualization of Trust

One of the most profound contributions of the taxonomy is its reframing of "trust" in cybersecurity. Traditional models treat trust as binary and largely static—within the network perimeter: internal entities are trusted, external ones are not. Zero Trust reconceptualizes trust as dynamic, identity-, device-, and context-driven, and continuously assessed. This philosophical shift redefines the security perimeter from a network boundary to the resource itself.

By categorizing Zero Trust variants, this research offers a theoretical framework that unifies diverse implementations under a conceptual umbrella. The classification into Identity-Centric, Device-Aware, Network-Segmentation, Behavioral-Scoring, and Contextual/Token-Based reflects distinct notions of trust and enforcement strategies. This ontology enables researchers and practitioners to analyze, compare, and design Zero Trust systems more systematically, rather than treating each vendor or domain as a silo.

Moreover, the inclusion of Behavioral/Trust-Scoring as a primary variant signals a paradigm shift: trust is no longer solely derived from static credentials or device posture, but becomes a dynamic attribute, shaped by ongoing behavior, context, and risk profile. The integration of machine learning for trust assessment (Munasinghe et al., 2023) and behavioral evaluation models (N'goran et al., 2022) suggests a future where trust evolves in real time—adapting to patterns of usage, anomalies, and risk. This progression has significant theoretical implications for access control, risk management, and security governance.

Practical Implications for Deployment and Architecture Design

From a practical standpoint, the taxonomy and domain-mapping provide actionable guidance for security architects and decision-makers. Instead of a one-size-fits-all Zero Trust blueprint, organizations can choose or combine variants based on use-case, environment, regulatory requirements, performance constraints, and resource types. For instance:

- An enterprise migrating its on-premises infrastructure to cloud may prioritize Identity-Centric plus Network-Segmentation variants to maximize control, compliance, and minimal operational disruption.

- A company deploying microservices or container-based applications may adopt Identity-Centric and Contextual/Token-based Zero Trust to support dynamic scaling, service-to-service authentication, and minimal latency.

- An organization building an IoT or wearable device platform may lean toward Device-Aware and Contextual variants to balance lightweight performance and security.

- A cloud provider or community cloud operator may incorporate Behavioral/Trust-scoring mechanisms to dynamically adjust trust levels and resource access across tenants.

This context-aware approach helps organizations avoid overengineering or under-securing and supports incremental, adaptive deployment of Zero Trust rather than “big-bang” transformation.

Standardization, Interoperability, and Industry Collaboration

The pronounced lack of standardization and interoperability across implementations presents a significant barrier to widespread, cohesive adoption. Without common frameworks, protocols, identity standards, policy languages, and trust-scoring metrics, organizations remain bound to vendor-specific solutions, leading to fragmentation, inefficiency, and security gaps. The conceptual framework proposed here underscores the urgent need for industry collaboration: developing interoperable standards for identity federation, device attestation, contextual policy expression, trust scoring, and microsegmentation. Such standardization would not only lower the barrier to entry but also foster transparent evaluation and compliance across sectors.

Human and Organizational Considerations

Technological architecture is only one side of the equation. The success of Zero Trust depends heavily on human factors and organizational readiness. The friction introduced by frequent authentication, strict access controls, dynamic policies, and continuous monitoring—if not managed with ergonomics and user experience in mind—can lead to user resistance, shadow IT, or compliance fatigue. Further, policy management complexity, role explosion, and administrative overhead can overwhelm security teams, especially in large or rapidly scaling environments. Security governance, clear training, role definition, identity lifecycle management, and usability-focused design are therefore essential. The absence of substantial empirical studies on user experience and workforce impact remains a critical gap.

Limitations of the Study

While the conceptual approach adopted in this work provides a broad and unifying perspective, the study has several limitations:

- Dependency on Provided Literature: The analysis is constrained to the references supplied. Although

these cover a broad spectrum (federal guidance, industry, academic research, IoT, microservices), there may be additional perspectives, case studies, or recent developments (post-2025) not captured.

- Lack of Empirical Data: The taxonomy and findings are derived from qualitative, textual analysis. No empirical experiments, performance measurements, user studies, or deployment case studies were conducted. As such, conclusions about tradeoffs, scalability, performance, or usability remain theoretical and based on authors' claims rather than measured outcomes.

- Potential Bias Toward Published or Vendor-Friendly Reports: Since some referenced works are white papers or vendor-industry analyses, they may present optimistic assessments or understate challenges. Without independent audits, there is a risk of overestimating benefits or underreporting limitations.

- Rapidly Evolving Field: Zero Trust remains a dynamic and evolving paradigm. New architectural innovations, regulatory requirements, standards, tools, and threat models may emerge rapidly, potentially rendering parts of the taxonomy or analysis outdated.

Future Research Directions

To address the identified gaps and limitations, future research should prioritize the following areas:

1. Empirical Evaluation Frameworks: Develop benchmarks, metrics, and empirical studies to measure the effectiveness of Zero Trust implementations. Key metrics might include time-to-compromise, lateral movement resistance, authentication latency, system throughput, user productivity, and policy management overhead. Controlled experiments—simulating different threat models, user loads, device types, and domains—could provide quantitative evidence of Zero Trust benefits and tradeoffs.

2. Standardization and Interoperability Efforts: Foster development of open standards for identity federation, device attestation, contextual policy languages, trust-scoring schemas, token formats, and microsegmentation orchestration. Industry consortia, standard bodies, and academic researchers should collaborate to produce interoperable frameworks that reduce vendor lock-in and encourage cross-platform adoption.

3. Cross-Domain Integration Studies: Investigate hybrid environments that combine enterprise networks, cloud, IoT, microservices, and edge computing. Research should focus on architectural patterns, orchestration strategies, and unified policy management across heterogeneous resources.

4. User Experience and Organizational Impact Research: Conduct user studies, surveys, and ethnographic research to understand how Zero Trust affects productivity, user behavior, compliance, shadow IT, and organizational culture. Study trade-offs between security, usability, and operational efficiency.

5. Machine Learning and Adaptive Trust Models: Further exploration into behavioral and AI-driven trust scoring, adaptive policy enforcement, anomaly detection, and dynamic access adjustments. Evaluate their effectiveness, false-positive rates, resource consumption, privacy implications, and explainability.

6. Regulatory, Privacy, and Ethical Considerations: Examine how Zero Trust architectures intersect with data protection laws, privacy regulations, compliance requirements, and ethical concerns around monitoring, behavioral analytics, and continuous trust assessment.

CONCLUSION

The paradigm of Zero Trust Security represents a transformative shift in cybersecurity philosophy: from static, perimeter-based trust to dynamic, identity-, device-, and context-aware trust evaluation. By conducting a comprehensive, multivocal literature review and thematic analysis of foundational and contemporary works—including federal guidance, industry white papers, academic research, and domain-specific implementations—this study offers a unified taxonomy of Zero Trust architecture variants and maps them to real-world domains such as enterprise networks, cloud, microservices, IoT, and community cloud environments.

The taxonomy identifies five primary variants: Identity-Centric, Device-Aware, Network Segmentation, Behavioral/Trust-Scoring, and Contextual/Token-Based Zero Trust. Each variant addresses different trust anchors, enforcement mechanisms, and domain constraints. Understanding these variants, their strengths, tradeoffs, and suitability, enables security architects and decision-makers to design context-aware, hybrid Zero Trust systems rather than adopting a one-size-fits-all approach.

However, the study also reveals substantial challenges: lack of standardization, interoperability, scalability concerns, performance overhead, usability issues, and the absence of empirical evaluation. These obstacles underscore that while Zero Trust holds enormous promise, its real-world realization requires careful architectural planning, human-centric design, governance, standardization, and rigorous empirical validation.

To these ends, the paper recommends an agenda for future research: building empirical evaluation frameworks, fostering standardization, conducting user experience studies, exploring hybrid cross-domain integrations, advancing machine-learning trust models, and addressing regulatory and ethical implications. Through such efforts, Zero Trust can evolve from a conceptual ideal to a robust, scalable, and widely-adopted security paradigm.

REFERENCES

1. National Security Agency. Embracing a Zero Trust Security Model. NSA Cybersecurity Information, February 2021.
2. Kerman, Alper. Zero Trust Cybersecurity: Never Trust, Always Verify. NIST Taking Measure Blog, National Institute of Standards and Technology, October 2020.
3. Cunningham, Chase. The Zero Trust eXtended (ZTX) Ecosystem. Forrester Research, 2018.
4. Cloudflare. The Business Case for Zero Trust. Cloudflare, LinkedIn, 2024.
5. Balaouras, Stephanie. The Business of Zero Trust Security. Forrester, 2022.
6. Rose, Steven; Borchert, Oliver; Mitchell, Scott; Connelly, Sean. Zero Trust Architecture. NIST Special Publication 800-207, 2020.
7. Teerakanok, S.; Uehara, T.; Inomata, A. Migrating to Zero Trust Architecture: Reviews and Challenges. Security and Communication Networks, 2021.
8. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A Survey on Zero Trust Architecture: Challenges and Future Trends. Wireless Communications and Mobile Computing, 2022.
9. Ho, P.-H.; Chen, H.-Y.; Lin, T.-N. Zero Trust Architecture of Token Network. Proceedings of the IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), 2023.

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

11. Itodo, C.; Ozer, M. Multivocal Literature Review on Zero-Trust Security Implementation. Computers & Security, 2024, 141, 103827.

12. Gunuganti, A. Identity Based–Zero Trust. JAIMLD, 2023, 1, pp. 492–497.

13. Munasinghe, S.; Piyarathna, N.; Wijerathne, E.; Jayasinghe, U.; Namal, S. ML Based Zero Trust Architecture for Secure Networking. Proceedings of the IEEE 17th International Conference on Industrial and Information Systems (ICIIS), 2023.

14. N'goran, R.; Tetchueng, J.-L.; Pandry, G.; Kermarrec, Y.; Asseu, O. Trust Assessment Model Based on a Zero Trust Strategy in a Community Cloud Environment. Engineering, 2022, 14, pp. 479–496.

15. Mohseni Ejiyeh, A. Real-Time Lightweight Cloud-Based Access Control for Wearable IoT Devices: A Zero Trust Protocol. Proceedings of the First International Workshop on Security and Privacy of Sensing Systems, 2023.