GENERATE

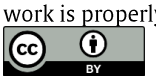
Breakthroughs Information Technology

e-ISSN: 3109-8495

Vol 01 (2) 2025 p. 138-151

Corresponding author:
Sreelatha R
Email : sree.ise@bmsce.ac.in

Received 19 January 2026;
Accepted 5 February 2026;
Published 10 February 2026.



Conflict of interest statement:
Author(s) reported no conflict of interest

DOI: http://doi.org/10.70764/gdpu-bit.2025.1(2)-04

ZERO-TRUST SECURITY CONCEPT AND ITS IMPLEMENTATION IN CLOUD-EDGE ENVIRONMENT

Sreelatha R[1]

[1] *BMS College of Engineering, India*

ABSTRACT

Objective: This study aims to explore high-tech companies' understanding and perceptions of the Zero-Trust Security (ZTS) concept, identify the main challenges of its implementation in cloud–edge architectures, and analyze the security strategies used to effectively implement Zero-Trust in distributed environments.

Research Design & Methods: This study uses a qualitative approach through the Systematic Literature Review (SLR) method on 25 scientific articles obtained from Scopus (18 articles), Google Scholar (7 articles), and additional sources through SciSpace. The analysis process was carried out through identification, screening, and thematic content analysis to map the concepts, challenges, and implementation strategies of Zero-Trust in cloud–edge.

Findings: The results of the study show that Zero-Trust is understood as an identity-based security framework that emphasizes continuous verification, least privilege, and micro-segmentation. Key challenges include edge device heterogeneity, resource constraints, cross-platform policy orchestration, organizational readiness, and the inconsistency of distributed identity standards. Several effective strategies were identified, including adaptive authentication, identity-first architecture, AI-driven anomaly detection, blockchain integration, and policy-as-code for managing cloud–edge policies.

Implications & Recommendations: Implementing Zero-Trust in a cloud-edge environment requires a phased approach that prioritizes identity management, automated policy orchestration, and security control integration tailored to the limitations of edge devices. Organizations are advised to strengthen their technical competencies, improve system interoperability, and adopt a telemetry-based security model.

Contribution & Value Added: This research contributes to the latest conceptual synthesis regarding the implementation of Zero-Trust in cloud-edge architecture and fills the research gap related to the challenges and strategies of its application. The analytical framework can be used by practitioners, researchers, and policymakers in designing adaptive and sustainable Zero-Trust architectures.

Keywords: Zero-Trust, Cloud–Edge, Edge Computing, Implementation, Cloud Security.

JEL codes: O32, M15
Article type: research paper

INTRODUCTION

The digital transformation of high-tech companies in recent years has accelerated, marked by a migration from on-premise infrastructure to distributed computing models such as cloud and edge computing, which offer scalability, efficiency, and operational flexibility. However, this shift

also increases the attack surface and the complexity of cybersecurity (Ahmadi, 2024). Traditional perimeter-based security models that assume internal zones are trusted areas are no longer adequate when data, applications, and users are spread across multiple cloud and edge domains (Lindemulder and Kosinski, 2024; Mushtaq et al., 2025). As the digital ecosystem becomes increasingly open, this security approach fails to address modern challenges such as distributed access, heterogeneous IoT devices, and insider threats.

Responding to these weaknesses, the Zero-Trust Security (ZTS) approach has emerged as a new security paradigm. Zero-Trust emphasizes the principle of never trust, always verify, whereby every entity, including internal users and devices, must be explicitly verified before gaining access (Abdiukov, 2025; R. Wang et al., 2025). This approach utilizes continuous authentication, identity-based access control, and micro-segmentation to minimize risk (Lavanya et al., 2025). Zero-Trust has proven effective in cloud environments for preventing lateral movement, strengthening identity management, and improving network segmentation, making it one of the most relevant security approaches in modern architectures (Ahmadi, 2024; Lavanya et al., 2025; Tanaka, 2024). Although this concept is relatively mature in cloud infrastructure, its application to cloud-edge architecture still requires further in-depth analysis. Edge computing environments have unique characteristics such as limited computing capacity, large numbers of distributed devices, and real-time response requirements, which make Zero-Trust implementation more complex than in the cloud. Continuous authentication policies, device identity verification, and granular encryption are often more challenging in heterogeneous edge nodes (Li et al., 2022; C. Liu et al., 2024; R. Wang et al., 2025). Although literature on Zero-Trust in cloud environments is growing, its implementation in cloud-edge environments presents challenges that have not been analyzed in depth. Edge environments often have dynamic, heterogeneous characteristics and limited resources, making the application of Zero-Trust principles (e.g., continuous authentication, granular access control, micro-segmentation) more difficult than in typical cloud-native environments.

Thus, there is a need to explore how companies, particularly high-tech firms that integrate cloud and edge computing, understand, interpret, and apply Zero-Trust in real-world practice. Factors such as digital identity, dynamic authorization and authentication, security policy orchestration, network segmentation, and performance and scalability warrant further analysis. Based on existing research gaps, this study aims to describe high-tech companies' understanding and perceptions of the Zero-Trust concept in cloud-edge architecture, identify key challenges in its implementation in distributed cloud-edge environments, and analyze the security strategies and practices used to implement Zero-Trust effectively. This research is expected to contribute theoretically by expanding the understanding of Zero-Trust adaptation in modern architecture, while also offering practical implications in the form of implementation recommendations for organizations and a supporting framework for policymakers and service providers to accelerate the adoption of Zero-Trust in cloud-edge environments.

LITERATURE REVIEW

The concept of Zero-Trust Security (ZTS) has emerged as a new approach that rejects the assumption of automatic trust in digital networks, emphasizing the principle of "never trust, always verify" through continuous identity verification, micro-segmentation, and context-based access control (Adamson and Qureshi, 2025). As data and applications increasingly move to the cloud, traditional perimeter-based security models have proven ineffective against threats such as lateral movement, cloud-native malware, and identity abuse, leading to the adoption of ZTS as a more adaptive, risk-based security foundation (Lavanya et al., 2025). Additionally, the integration of artificial intelligence in user and device behavior analysis has led to the emergence of a new generation of ZTS that is more responsive to dynamic threats and capable of automating security policies in multi-cloud environments (Hasan, 2024).

Meanwhile, the development of edge computing adds complexity to security architecture because edge devices are distributed, heterogeneous, and operate in more vulnerable physical conditions, giving rise to threats such as firmware attacks, DDoS, and device manipulation (Roman et al., 2018). Literature studies confirm that traditional security models cannot handle the unique

risks at the edge, so ZTS needs to be implemented to strengthen device authentication, limit granular access, and provide consistent real-time monitoring across cloud–edge (Alwarafy et al., 2020). However, empirical research on the implementation of ZTS in cloud-edge architecture is still minimal, especially in terms of organizational strategy, technological readiness, and security policy integration. Therefore, qualitative studies are needed to bridge the gap between theory and practice in high-tech companies (Hadiningrum et al., 2025).

Cloud-Edge architecture poses complex security challenges due to its distributed and decentralized nature. In distributed database systems, multiple databases may be geographically dispersed, making data consistency across sites a fundamental issue that must be maintained to keep operations synchronized (Grant Thornton International Ltd, 2019). In the context of Zero-Trust, a similar problem arises at the policy level. The consistency of access rules across all enforcement points, both in Cloud infrastructure and thousands of Edge devices, becomes a critical challenge that affects the effectiveness of the security model (Mushtaq et al., 2025; Nzeako and Shittu, 2024). On the other hand, Edge devices such as sensors and IoT generally have limited computing resources, memory, and power, so Zero-Trust mechanisms that require continuous authentication and verification have the potential to cause an excessive burden if not designed efficiently (Balogun and Badi, 2019). Therefore, the implementation of Zero-Trust at the Edge must be adaptive, enabling contextual access control and intelligent threat detection that adjusts to device constraints in distributed environments. Ultimately, Cloud–Edge security integration is key to balancing the need for local autonomy with centralized intelligence, ensuring that security policies can be applied consistently without compromising Edge device performance.

METHODS

This study uses a qualitative approach with the Systematic Literature Review (SLR) method to examine the concept of Zero-Trust Security (ZTS) and its application in cloud–edge architecture. The data were obtained through a structured literature search of two databases, Scopus and Google Scholar, which yielded 25 relevant articles for analysis. The literature was then supplemented with additional articles from SciSpace as supporting sources to reinforce the discussion on organizational perceptions, Zero-Trust implementation challenges, and cloud-edge security strategies. The SLR process is carried out through the stages of identification, screening, and content analysis (thematic analysis) to produce a systematic and targeted qualitative synthesis in accordance with the research objectives. The research results are then organized into four main sections, namely a discussion of the basic concepts of Zero-Trust Security in the cloud-edge environment, a summary of several key findings from previous literature, an in-depth analysis of the application of Zero-Trust in cloud-edge/edge/IoT architecture, identification of challenges in implementing ZTS in distributed ecosystems, and proposed or applied security strategies and practices to effectively realize Zero-Trust. All of these findings are ultimately summarized in conclusions that articulate theoretical and practical implications, including implementation recommendations and directions for further research for organizations and stakeholders seeking to adopt Zero-Trust in modern cloud-edge environments.

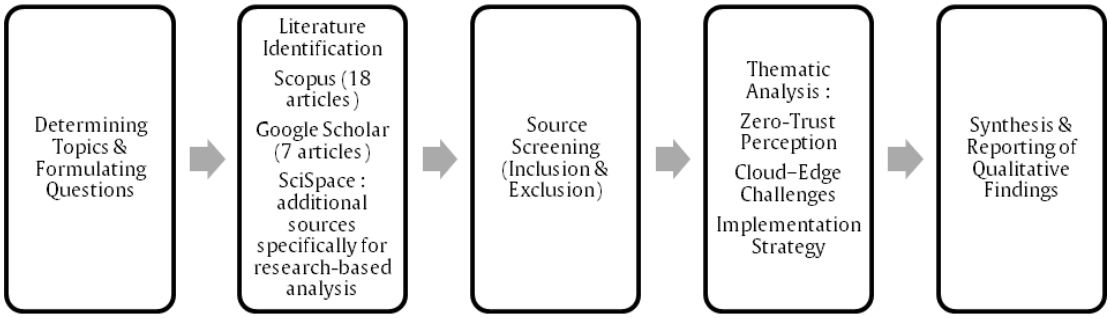


Figure 1. Research Framework

RESULT

Several publications emphasize that companies view Zero Trust as a modern security framework highly relevant to cloud infrastructure and distributed architectures. For example, the study Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities explains that ZTS can significantly reduce the risk of access abuse, lateral movement, and insider threats, thanks to the implementation of identity controls, micro-segmentation, and continuous monitoring (Ahmadi, 2024). Similarly, the Zero-Trust framework is officially recognized in security guidelines by major technology providers. For example, Microsoft's official website explains that ZTS authenticates every user and device before granting access, without relying on internal network trust zones (Microsoft, 2025). This shows that companies tend to view ZTS as the foundation of security architecture, not just an additional feature (Hasan, 2024).

In the context of organizations with cloud-edge infrastructure, literature shows that Zero-Trust is perceived as a strategy that enables flexibility and security. For example, the article Implementing Zero Trust Architecture in Multi-Cloud Environments states that with strong identity and access management (IAM), plus consistent control policies and network segmentation, companies can manage services in multi-cloud/edge environments without compromising security (Manne, 2023). Furthermore, the study Blockchain Implementation in the Development of a Zero Trust-Based Cybersecurity Framework at the Indonesian National Data Center expands on this perception by showing that the integration of Zero Trust with technologies such as blockchain can improve the resilience of national digital infrastructure against modern threats, indicating that for some organizations, Zero Trust is not only technical-operational but also strategic and infrastructural (Khair et al., 2025).

Thus, a combination of global and local literature shows that companies, especially those managing cloud, multi-cloud, or hybrid cloud-edge infrastructure, tend to understand Zero-Trust as a holistic security paradigm, covering identity, access, segmentation, and monitoring; and as a foundation for securing dynamic and distributed modern architectures. This supports the finding that perceptions of Zero-Trust have evolved from merely a security tool to part of a long-term security strategy and cyber risk governance in high-tech companies.

This study analyzes 25 scientific articles that directly focus on the concept and application of Zero-Trust Security (ZTS) in cloud, edge, IoT, and distributed architecture environments. These articles were obtained through a systematic selection process, covering 18 articles from Scopus, 7 articles from Google Scholar, and additional relevant sources that support the mapping of research themes in the discussion section. From the entire collection, 18 articles had complete metadata and could be further processed for thematic analysis. Preliminary statistics showed a strong distribution of research focus on modern computing issues. The term Zero-Trust appeared in 11 articles, cloud in 12, edge in 10, and IoT in 9. Themes related to Identity and Access Management (IAM) and authentication were found in 7 articles, while supporting technologies such as AI/ML and blockchain appeared in 2 and 3 articles, respectively. Although the term micro-segmentation is not captured in the metadata, the concept is likely discussed in the full text of articles not captured by the RIS format. Overall, these findings provide a preliminary overview of current research patterns and focuses and form the basis for the following summary table.

Table 1. Overview of Zero-Trust Implementation in Cloud–Edge/IoT Studies

No	Article Title (source)	Scope / Focus	Zero-Trust Implementation in Cloud–Edge / Edge / IoT
1.	*Data-Centric Zero-Trust Architecture for Edge AI Systems*	Edge AI / IoT / edge distributed systems	ZTS architecture adopts data-flow sensitivity classification, dynamic policy enforcement, hardware-rooted attestation, and micro-segmentation and granular data flow control; suitable for resource-constrained edges (Koshiya, 2025).
2.	*Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and*	Multi-Access Edge Computing (MEC) / edge computing	Proposes a strict device authentication mechanism (identity + biometric + PUF), then only verified and "trusted" devices are allowed to upload tasks to the edge server implementing the Zero-Trust principle

No	Article Title (source)	Scope / Focus	Zero-Trust Implementation in Cloud–Edge / Edge / IoT
	task offloading in Multi-access Edge Computing		for authentication and task allocation in the edge environment (Ali et al., 2024).
3.	*Dissecting zero trust: research landscape and its implementation in IoT*	IoT / edge / distributed sensor network	A systematic review shows that ZTS is considered highly relevant for IoT/edge: many ZTS-based security schemes have been proposed, including segmentation, continuous authentication, and contextual access control to protect IoT/edge devices (C. Liu et al., 2024).
4.	*Zero Trust Security Architecture for Cloud Native Applications*	Cloud-native, multi-cloud, distributed environment/ microservices	Deploying ZTS on cloud-native and multi-cloud environments uses identity-first policies, service mesh/sidecar proxies, continuous access control, and telemetry-based monitoring; this architecture is also relevant when workloads are integrated between cloud and edge (Tanaka, 2024).
5.	*Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities*	Cloud networks (general), literature review	ZTS helps mitigate threats in the cloud, such as lateral movement and insider threats, through micro-segmentation, IAM, and continuous monitoring. These results provide a strong foundation for hybrid cloud-edge implementations (Ahmadi, 2024).
6.	*Analisis Adaptif Zero Trust Architecture (ZTA) Berbasis Machine Learning untuk Deteksi Intrusi pada Jaringan IoT dalam Infrastruktur Kritis*	IoT / critical infrastructure network/ edge-like environment	Presenting an adaptive ZTS model with machine learning for intrusion detection and behavior profiling, plus micro-segmentation and continuous authentication suitable for distributed IoT/edge systems (Darmawan et al., 2025).
7.	*Robust Zero Trust Architecture: Joint Blockchain based Federated learning and Anomaly Detection based Framework*	Decentralized network, IoT / edge, federated learning	Proposing a ZTS + blockchain + anomaly detection framework for distributed systems / IoT/edge that aims to strengthen trust and integrity in decentralized collaboration (Pokhrel et al., 2024).
8.	*Securing edge based smart city networks with software defined Networking and zero trust architecture*	SDN-based smart city security on edge networks	Integration of Zero Trust principles and dynamic trust analysis into the TREN framework for adaptive defense against DDoS and Sybil attacks in edge environments (Iftikhar et al., 2025).
9.	*A lightweight zero-trust authentication architecture for IoT via unified enhanced FAST-SM9 and dynamic re-authentication*	Lightweight authentication for Cloud-Edge-End IoT	Lightweight authentication integration and time-based Zero-Trust re-authentication for defense against session hijacking and credential leakage (Ma et al., 2025).
10.	*Zero Trust Strategies for Cyber-Physical Systems in 6G Networks*	Security of 6G-based Cyber-Physical Systems (CPS)	Zero Trust integration with blockchain and AI for decentralized authentication, real-time anomaly detection, and adaptive access control (Alnaim and Alwakeel, 2025b).
11.	*Emerging Technologies Driving Zero Trust Maturity Across Industries*	The evolution of Zero Trust through new technology (AI, ML, blockchain, edge)	Analysis of the impact of new technologies on the implementation of Zero Trust in hybrid and multi-cloud environments (Joshi, 2025).
12.	*Zero Trust-Driven Collaborative Intrusion Detection in IoT: A Continuous Trust Assessment Approach*	Zero Trust-based collaborative intrusion detection for IoT	Zero Trust architecture with dynamic trust management and anomaly detection for secure communication between cloud-edge-end nodes (X. Wang et al., 2025).
13.	*Securing and Sustaining IoT Edge-Computing Architectures Through Nanoservice Integration*	Energy efficiency and edge computing security	Integration of Zero Trust architecture with micro-segmentation and strict access control on nanoservice services for dynamic security at the edge (Gonzalez et al., 2025).
14.	*Secure Latency-Aware Task Offloading Using Federated Learning and Zero Trust in Edge Computing for IoMT*	Secure offloading for the Internet of Medical Things (IoMT)	Zero Trust integration with federated learning for distributed authentication and secure orchestration between edge servers and cloud (Almuseelem, 2025).
15.	*O-Cloud Security: A Comprehensive Survey of Threats, Mitigation Strategies, and Future Directions*	O-RAN and O-Cloud Security	O-Cloud security survey highlighting the role of ZTA, SASE, blockchain, and AI for next-generation communication network resilience (Shehab et al., 2025).
16.	*SecT: A Zero-Trust Framework for Secure Remote Access in Next-Generation Industrial Networks*	New generation industrial network security	The Zero Trust-based SecT framework replaces traditional VPNs with role-based access control for secure, low-latency connectivity (Asim et al., 2025).

No	Article Title (source)	Scope / Focus	Zero-Trust Implementation in Cloud–Edge / Edge / IoT
17.	*Cloud Edge Integrated Security Architecture of New Cloud Manufacturing System*	Cloud manufacturing system security	Zero Trust-based cloud-edge-terminal architecture with dynamic authorization, attribute-based control, and data protection using blockchain (Zhao et al., 2024).
18.	*An Authentication Mechanism Based on Zero Trust With Radio Frequency Fingerprint for Internet of Things Networks*	Authentication security on IoT & edge networks	Combining Radio Frequency Fingerprint (RFF) and Zero Trust to prevent spoofing, fake AP attacks, and data leaks in IoT (Jing et al., 2024).
19.	*A Review on Blockchain for Fintech using Zero Trust Architecture*	Security and privacy analysis in FinTech	Highlighting security and privacy challenges relevant to the implementation of the Zero Trust concept in cloud-based financial systems (A. Singh et al., 2024).
20.	*Meta Computing*	Cloud-edge resource integration-based meta computing paradigm	Providing full support for Zero Trust environments with continuous authentication and verification between nodes in distributed systems (Cheng et al., 2024).
21.	*Continuous and mutual lightweight authentication for zero-trust architecture-based security framework in cloud-edge computing-based healthcare 4.0*	Cloud-Edge-based Healthcare 4.0 Security	Using Zero Trust with HMAC- and ECC-AES-based lightweight authentication for secure D2D, D2E, and E2C communications (Almuseelem, 2024) .
22.	*Secure and Scalable Cross-Domain Data Sharing in Zero-Trust Cloud-Edge-End Environment Based on Sharding Blockchain*	Sharing data across domains in a Cloud–Edge–End architecture	Zero Trust cross-domain data sharing scheme with blockchain sharding and plaintext-checkable encryption for IoT (Y. Liu et al., 2024).
23.	*Toward a Performance-Based Trustworthy Edge-Cloud Continuum*	Authentication efficiency in the Edge–Cloud Continuum	Performance-based trust assessment mechanism to reduce Zero Trust authentication overhead without compromising security (Dhanapala et al., 2024).
24.	*SysFlow: Toward a Programmable Zero Trust Framework for System Security*	Cross-infrastructure system security control (cloud–edge–IoT)	The SYS FLOW framework extends Zero Trust to the system level with separation of control and data planes and dynamic PDP–PEP (Hong et al., 2023).
25.	*A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing*	Zero Trust Implementation in Multiaccess Edge Computing (MEC)	A Zero Trust-based security maturity framework that divides the implementation stages, starting with Minimum Viable Security (Ali et al., 2022).

DISCUSSION

Implementing Zero Trust in Cloud–Edge / Edge / IoT Architecture

The implementation of Zero-Trust in Cloud-Edge architecture shows significant progress, marked by a combination of continuous verification, adaptive authentication, and dynamic access control tailored to the characteristics of a distributed environment. TREN Framework, for example, demonstrates how Zero-Trust can be implemented through the integration of real-time trust analytics, isolation of risky entities, and automated policy enforcement to improve threat detection by up to 95% while reducing latency and substantially increasing throughput (Iftikhar et al., 2025). Similar efforts can also be seen in the Zero-Trust Dynamic Re-Authentication (zero-trust-DRA) design, which adds an adaptive re-authentication mechanism based on lightweight algorithms such as FAST-SM9, thereby reducing latency by 56% and increasing energy efficiency by more than 60%, making it an ideal solution for edge devices with limited resources (Ma et al., 2025). Another approach combines Adaptive Access Control, blockchain, and AI to deliver continuous authentication and real-time anomaly detection in critical infrastructure such as industry and healthcare, with evidence of increased authentication efficiency and a significant reduction in the success of MITM attacks (Alnaim and Alwakeel, 2025b). Various conceptual studies also emphasize that the evolution of Zero-Trust towards technologically-augmented zero-trust requires continuous adaptation in order to maintain the principles of least privilege and continuous verification in hybrid and multi-cloud environments (Joshi, 2025).

In addition to adaptive authentication, a number of studies highlight the integration of Zero-Trust-based intrusion detection that combines feature-based detection and anomaly detection with dynamic trust management, enabling edge–IoT systems to collaboratively identify internal and external threats (X. Wang et al., 2025). The nanoservice approach also strengthens Zero-Trust through extreme micro-segmentation and on-demand service activation, reducing latency and energy consumption without compromising key security principles (Gonzalez et al., 2025). On the other hand, Zero-Trust in the Edge–Cloud offloading scheme in the IoMT sector combines Federated Learning and trust-based orchestration to ensure secure model training, strict authentication, and reduced risk of data leakage during the offloading process (Almuseelem, 2025). In the telecommunications sector, O-Cloud utilizes ZTA integration with SASE, blockchain, and Proof of Retrievability to strengthen entity verification and data integrity in cloud-native infrastructures such as O-RAN (Shehab et al., 2025). Other studies propose secure UDP-based communication mechanisms with RBAC and continuous verification to replace traditional VPNs, resulting in better performance and security in industrial applications (Asim et al., 2025).

The implementation of Zero-Trust is also increasingly dominant in manufacturing systems (NCMS), where continuous verification, dynamic authorization, and various access control models (ABAC, RBAC, PBAC) as well as blockchain are applied to protect data and prevent device misuse in complex supply chains (Zhao et al., 2024). On IoT–Edge, the combination of ZTA with Radio Frequency Fingerprinting (RFF)-based authentication strengthens security without relying on a trusted center, achieving 99% authentication accuracy and resistance to various forms of network attacks (Jing et al., 2024). Although certain studies do not directly implement ZTA, modern FinTech studies emphasize the need for a non-perimeter approach in line with Zero-Trust principles to protect sensitive data in cloud and mobile environments (A. Singh et al., 2024). In the context of future computing, Meta Computing adopts the Zero-Trust paradigm to unify cloud, edge, and distributed device resources, ensuring continuous authentication in a secure global computing system (Cheng et al., 2024).

The application of Zero-Trust in the Healthcare 4.0 sector demonstrates the effectiveness of efficient two-layer authentication (dynamic HMAC and ECC-AES) for D2D, D2E, and E2C communications, making it suitable for Cloud–Edge-based medical devices that demand high energy efficiency and adaptive security (Almuseelem, 2024). The Zero-Trust system for cross-domain data sharing integrates plaintext-checkable encryption and blockchain sharding architecture, ensuring security, fairness, and scalability of data exchange between IoT and Cloud domains (Y. Liu et al., 2024). In edge-cloud networks with limited resources, the performance-based trust assessment approach provides the flexibility to reduce re-authentication without violating the Zero-Trust principle, thereby reducing communication overhead while maintaining system integrity (Dhanapala et al., 2024). At the system level, the SYS FLOW framework extends the application of Zero-Trust from the network layer to the system layer, using system-flow abstraction, PDP, and dynamic PEP to efficiently enforce policies in large-scale cloud–edge–IoT infrastructure (Hong et al., 2023). Finally, the MEC entity classification framework provides a roadmap for the gradual implementation of Zero-Trust, starting with Minimum Viable Security (MVS), emphasizing that every entity must be continuously verified in a heterogeneous and dynamic edge ecosystem (Ali et al., 2022).

In addition, recent research also reinforces that the implementation of Zero-Trust Security (ZTS) in cloud-edge environments requires an increasingly adaptive and contextual approach. A number of studies emphasize the importance of data-flow sensitivity classification and dynamic policy enforcement to ensure that sensitive data flows at the resource-constrained edge remain protected through micro-segmentation and hardware-rooted attestation mechanisms that maintain device and workload integrity (Koshiya, 2025). This approach is reinforced by a device authentication design based on a combination of identity verification, biometrics, and Physical Unclonable Functions (PUF), so that only truly verified devices can perform task offloading to edge servers, ensuring that no entity gains inherent trust in accordance with the Zero-Trust principle (Ali et al., 2024). Another systematic review also confirms that IoT and edge architectures are the most relevant environments for ZTS implementation, given the increasing need for strict segmentation,

continuous authentication, and dynamic contextual access control in dealing with highly heterogeneous and resource-constrained devices (C. Liu et al., 2024).

Furthermore, several studies highlight the role of cloud-native and multi-cloud architectures that now adopt the Zero-Trust paradigm through identity-first policies, service mesh, sidecar proxies, and continuous telemetry monitoring, all of which are also relevant in cloud–edge workload integration (Tanaka, 2024). This integration helps mitigate threats such as lateral movement, rogue insider access, and identity compromise through a combination of strong IAM, micro-segmentation, and continuous monitoring (Ahmadi, 2024). On the other hand, machine learning-based ZTS design further strengthens threat detection through behavior profiling and adaptive intrusion detection, enabling IoT and edge systems to respond to anomalies more quickly and contextually (Darmawan et al., 2025). Distributed approaches that combine blockchain with anomaly detection are also emerging as a strong trend, especially for maintaining integrity, auditability, and trust in edge–IoT collaboration systems that do not have a single center of trust (Pokhrel et al., 2024).

Challenges Implementing Zero-Trust in Cloud–Edge

Literature analysis shows that although the Zero-Trust concept offers many advantages for cloud-edge environments, its implementation faces a number of significant challenges in terms of technology, resources, and organization.

1. **Device Heterogeneity & Resource Constraints at the Edge**

Edge and IoT devices often have limitations in terms of CPU, memory, and storage capacity, as well as deficiencies in built-in security capabilities such as strong encryption or comprehensive security agents. This makes it difficult to consistently implement heavy authentication or cryptographic controls at edge nodes. Research literature states that in the context of edge/fog/6G networks, traditional ZTS models designed for centralized cloud infrastructure are not suitable when applied to distributed environments with thousands of low-memory nodes; continuous authentication, encryption, and device verification processes can cause heavy loads and are not feasible for many edge devices (Alnaim and Alwakeel, 2025a; C. Liu et al., 2024). As a result, many edge nodes may not be able to fully implement all Zero-Trust pillars, so organizations must choose a subset of controls that can be implemented (e.g., basic identity, lightweight encryption), or entrust some controls to gateways/edge gateways (Alnaim and Alwakeel, 2025a).

2. **Cross-Platform Policy Orchestration (Multi-Cloud and Multi-Vendor)**

In modern cloud-edge environments, many companies use a combination of infrastructure: public/private clouds, edge servers, IoT devices, and third-party services. To implement Zero-Trust effectively, identity and access policies must be consistent across all domains, but differences in policy formats, APIs, identity models, and logging capabilities between vendors/services make synchronization difficult. This leads to policy gaps, blind spots, and inconsistencies in control enforcement. Popular articles discussing the challenges of adopting Zero-Trust in global networks emphasize that infrastructure heterogeneity and diverse cross-cloud–edge tooling make it difficult to enforce identity & access controls uniformly (Dehongi, 2025). This situation is exacerbated when organizations use legacy systems or different vendors for edge, cloud, and applications, making policy automation extremely complex.

3. **Organizational Readiness & Human Resource Skills**

Adopting Zero Trust is not just a matter of technology, but also a change in processes, policies, and security culture. Organizations need to rethink their operating models, staff training, identity consolidation, and ongoing monitoring and auditing. Literature on Zero-Trust practices shows that internal capability gaps in identity management, security operations, and policy orchestration are often the main causes of implementation failure or partial adoption (Sarkar et al., 2022). Additionally, the integration between cloud, network, security, and operations teams often occurs in silos, making coordination and consistency in Zero-Trust implementation difficult.

4. **Lack of Standardization and Interoperability of Distributed Identities**

Zero-Trust in cloud-edge environments requires consistent and trustworthy identities not only for users, but also for devices, services, and edge nodes. However, there is currently no universal standard governing identity management and trust frameworks for the entire cloud-edge/edge-IoT ecosystem. Incompatibility between different vendor identity systems (cloud providers, edge device vendors, third-party services) complicates the implementation of mechanisms such as federated authentication, device attestation, and cross-domain auditing (Alnaim and Alwakeel, 2025a). This situation increases the risk of identity fragmentation and security breaches when data or access moves between cloud and edge domains, or when companies combine services from multiple vendors.

5. **Performance and Latency (Overhead from Zero-Trust Controls)**

Because Zero-Trust requires identity verification, authorization, and security checks (e.g., encryption, device status checks, logging) for every access request, in cloud-edge or IoT architectures, this can add latency and computational overhead. This is crucial especially for real-time, latency-sensitive applications or edge services with strict performance requirements (e.g., industrial IoT, vehicles, smart cities) where even the slightest delay can disrupt user experience or system functionality. Recent studies cite high latency and resource consumption as the main obstacles when implementing Zero-Trust in IoT/edge environments (Alnaim and Alwakeel, 2025a; C. Liu et al., 2024). Furthermore, when heavy security mechanisms (e.g., blockchain-based authentication, AI-driven anomaly detection) are deployed on edge nodes with limited power, the overhead can render the system unresponsive or even fail, forcing organizations to trade off security and performance.

Security Strategies and Practices in Implementing Zero-Trust in Cloud–Edge

1. **Identity-Based Approach**

The implementation of Zero-Trust in cloud-edge environments requires the use of identity as the primary control plane for all types of entities, including humans, services, workloads, and AI agents. Identity must be managed through decentralized provisioning mechanisms, policy-as-code-based policy integration, and continuous verification that evaluates posture, context, and trust scores each time a request occurs (Y. Liu et al., 2025; Prajwalasimha et al., 2025). This approach enables consistent authentication and authorization across cloud-edge nodes without relying on network location as an indicator of trust.

2. **Zero-Trust Architecture Building Blocks**

The core Zero-Trust architecture blocks relevant to cloud–edge include the use of Decentralized Identifiers (DIDs) that eliminate single points of governance and facilitate cross-domain identity portability (Prajwalasimha et al., 2025). Additionally, SPIFFE/SPIRE-based workload identity provides short-term cryptographic identities that enable mutual verification between services and workloads without relying on network topology (Prajwalasimha et al., 2025). Access policies should be implemented as policy-as-code that can be tested, versioned, and automatically adjusted, while continuous verification combines posture, telemetry, and intent to produce more adaptive per-request evaluations (Y. Liu et al., 2025; Prajwalasimha et al., 2025).

3. **Zero-Trust Network Access (ZTNA) Practices**

ZTNA functions as an identity-aware access mechanism that replaces implicit network trust. In this implementation, identity-aware proxies perform context analysis and issue short-lived session tokens before access is granted (Karanam, 2024). Additionally, microsegmentation restricts lateral movement between services through strict east-west segmentation (Y. Liu et al., 2025). The per-session authorization process requires continuous evaluation of access rights and termination of the session if anomalies are detected (Karanam, 2024). To maintain low latency, a regionally based ZTNA gateway strategy is adopted so that policies remain consistent even though edge nodes have different geographic locations (Mubeen, 2024).

4. **Encryption Techniques and Key Management**

Zero-Trust security in the cloud-edge requires the implementation of comprehensive encryption for device-to-cloud, service-to-service, and data at rest communications. The use of mutual TLS (mTLS) through a service mesh provides service identity and cryptographic protection for internal traffic (Bashi and Senan, 2025). Authenticated encryption with rapid key rotation minimizes the risk of compromised credentials being exploited (Bashi and Senan, 2025; Y. Liu et al., 2025). For edge devices with limited computing power, lightweight mutual authentication or delegated attestation schemes are more efficient options (H. P. Singh, 2025). Large scale requires automated PKI and certificate rotation integrated with CI/CD to prevent failures due to expired credentials (Bashi and Senan, 2025).

5. AI Orchestration and Automated Response

AI plays a central role in modern Zero-Trust by supporting continuous contextual verification, anomaly detection, and policy automation. Research shows that Transformer-based behavioral engines improve precision and recall in detecting traffic anomaly patterns and user behavior compared to older methods (Adebowale, 2025). Graph Neural Networks (GNN) enable cross-entity modeling and confidence propagation, providing explainable justifications for contextual decisions. Additionally, LLM-assisted policy automation reduces administrative burdens by automatically generating granular policies. Federated learning supports edge-based learning without sending raw data to the cloud, improving privacy and bandwidth efficiency. The AI system can then support closed-loop responses, such as automatically terminating sessions or reconfiguring microsegmentation based on detection signals (Kaur et al., 2025).

6. Cloud–Edge Integration

Zero-Trust integration in hybrid cloud-edge environments requires identity consistency, policy synchronization, and telemetry orchestration that can operate despite unstable connectivity. The distributed enforcement approach pushes lightweight policy evaluators to edge nodes, while global governance remains in the cloud, reducing latency while maintaining consistency (Bhushan et al., 2025; Mubeen, 2024). Service mesh extension to edge clusters maintains service identity assurance and mTLS despite distributed environment topologies (Bashi and Senan, 2025). Regional brokers or local gateways can issue short-term credentials to accelerate authentication on edge nodes (Mubeen, 2024). Additionally, federated telemetry enables hierarchical aggregation of logs and signals without overloading the network (Adebowale, 2025).

7. Challenges and Mitigation Efforts

Although various strategies have been developed, the implementation of Zero-Trust still faces challenges, especially related to operational complexity and scalability. Architectural complexity is a major obstacle, so organizations are advised to start with high-value assets, enforce policy lifecycle automation, and implement in stages. The heterogeneity of edge devices is also a major issue; mitigation involves using gateways or adapters for older devices rather than forcing full cryptographic implementation (H. P. Singh, 2025). Policy consistency can be maintained through policy-as-code-based CI/CD testing so that configuration changes can be verified before implementation. In addition, operational readiness requires observability, runbooks, playbooks, and human escalation paths to prevent the risks of over-automation.

CONCLUSION

This study concludes that the implementation of Zero-Trust Security (ZTS) in cloud-edge environments has evolved into a comprehensive and strategic security paradigm, encompassing identity, dynamic access control, micro-segmentation, and continuous verification as the main foundations in protecting modern distributed architectures. An analysis of 25 scientific articles shows that organizations no longer view Zero-Trust as an additional feature, but as a holistic security framework capable of reducing the risk of access abuse, lateral movement, and insider threats, while providing operational flexibility in multi-cloud, hybrid cloud, edge, and IoT ecosystems. Various technical approaches such as adaptive authentication, trust-based orchestration, blockchain integration, machine learning-driven anomaly detection, and identity-first architecture further strengthen the effectiveness of Zero-Trust in facing modern threats.

However, Zero-Trust implementation faces significant challenges, including limited edge device resources, cross-platform orchestration complexity, organizational readiness, the lack of distributed identity standards, and the potential for increased latency due to continuous verification.

Implicitly, these findings confirm that organizations need to adopt Zero-Trust gradually through identity-based strategies and policy as code, strengthen cross-domain interoperability, and adjust security controls to the resource-constrained characteristics of edge devices. This approach not only significantly reduces cyber risk but also supports operational efficiency and long-term resilience of digital infrastructure. This research also provides a basis for developing a more adaptive, automated Zero-Trust architecture that is aligned with future computing needs, including cloud-native integration, intelligent edge, and large-scale IoT collaboration.

REFERENCES

Abdiukov, T. (2025). Zero Trust Architecture on Microsegmented Networks: A Cryptographic and Behavior-Based Approach to Adaptive Security Engineering. *International Journal of Innovative Research in Science Engineering and Technology (IJIRSE, 14*(7), 17122–17132. https://doi.org/10.15680/IJIRSET.2025.1407006

Adamson, K. M., & Qureshi, A. (2025). Zero Trust 2.0: Advances, Challenges, and Future Directions in ZTA (pp. 1–46). https://doi.org/10.21203/rs.3.rs-6602547/v1

Adebowale, J. (2025). Zero-Trust Architectures for Secure Cloud-Native Payment Ecosystems. https://www.researchgate.net/profile/Jide-Adebowale/publication/395378991_ZERO-TRUST_ARCHITECTURES_FOR_SECURE_CLOUD-NATIVE_PAYMENT_ECOSYSTEMS/links/68c0048b83031f0e13f34030/ZERO-TRUST-ARCHITECTURES-FOR-SECURE-CLOUD-NATIVE-PAYMENT-ECOSYSTEMS.pdf

Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. *Journal of Engineering Research and Reports, 26*(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083

Ali, B., Gregory, M. A., Li, S., & Dib, O. A. (2024). Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in Multi-access Edge Computing. *Computer Networks, 241*(March), 110197. https://doi.org/10.1016/j.comnet.2024.110197

Ali, B., Hijjawi, S., Campbell, L. H., Gregory, M. A., & Li, S. (2022). A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing. *Security and Communication Networks,* 2022. https://doi.org/10.1155/2022/3178760

Almuseelem, W. (2024). Continuous and Mutual Lightweight Authentication for Zero-Trust Architecture-Based Security Framework in Cloud-Edge Computing-Based Healthcare. *Journal of Theoretical and Applied Information Technology, 101*(1), 66–83. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85182892800&partnerID=40&md5=47f0c99c0002ba7fe7c0e912dd65df3d

Almuseelem, W. (2025). Secure Latency-Aware Task Offloading Using Federated Learning and Zero Trust in Edge Computing for IoMT. *IEEE Access,* 13, 117808–117830. https://doi.org/10.1109/ACCESS.2025.3586730

Alnaim, A. K., & Alwakeel, A. M. (2025a). Zero-Trust Mechanisms for Securing Distributed Edge and Fog Computing in 6G Networks. *Mathematics, 13*(8), 1239. https://doi.org/10.3390/math13081239

Alnaim, A. K., & Alwakeel, A. M. (2025b). Zero Trust Strategies for Cyber-Physical Systems in 6G Networks. *Mathematics, 13*(7). https://doi.org/10.3390/math13071108

Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things. *ArXiv Preprint.* http://arxiv.org/abs/2008.03252

Asim, M., Tariq, N., Awad, A. I., Waheed, F., Ullah, U., & Murtaza, G. (2025). SecT: A Zero-Trust Framework for Secure Remote Access in Next-Generation Industrial Networks. *IEEE Journal on Selected Areas in Communications, 43*(6), 2293–2311. https://doi.org/10.1109/JSAC.2025.3560015

Balogun, F., & Badi, S. (2019). Securing the Edge: AI-Powered Zero-Trust Deployment in Resource-Limited Contexts. https://doi.org/10.13140/RG.2.2.27452.14722

Bashi, Z. S. M. A., & Senan, S. (2025). A Comprehensive Review of Zero Trust Network Architecture (ZTNA) and Deployment Frameworks. *International Journal on Perceptive and Cognitive Computing, 11*(1), 148–153. https://doi.org/10.31436/ijpcc.v11i1.494

Bhushan, B., Rajgopal, P. R., & Sharma, K. (2025). An Intent-Aware Zero Trust Identity Architecture for Unifying Human and Machine Access. *International Journal of Computational and Experimental Science and Engineering, 11*(3). https://doi.org/10.22399/ijcesen.3886

Cheng, X., Xu, M., Pan, R., Yu, D., Wang, C., Xiao, X., & Lyu, W. (2024). Meta Computing. *IEEE Network, 38*(2), 225–231. https://doi.org/10.1109/MNET003.2300092

Darmawan, R. W., Irawan, I., & Petriansyah, S. (2025). Analisis Adaptif Zero Trust Architecture (ZTA) Berbasis Machine Learning untuk Deteksi Intrusi pada Jaringan IoT dalam Infrastruktur Kritis. *RIGGS: Journal of Artificial Intelligence and Digital Business, 3*(4), 36–45. https://doi.org/10.31004/riggs.v3i4.460

Dehongi. (2025, April 28). Implementing Zero Trust Principles Across a Global Network: Key Challenges and Solutions. *Dehongi*.

Dhanapala, I., Bharti, S., McGibney, A., & Rea, S. (2024). Toward a Performance-Based Trustworthy Edge-Cloud Continuum. *IEEE Access*, 12, 99201–99212. https://doi.org/10.1109/ACCESS.2024.3429197

Gonzalez, C. C. T., Ahmad, I., Soderi, S., & Harjula, E. (2025). Securing and Sustaining IoT Edge-Computing Architectures Through Nanoservice Integration. *IEEE Transactions on Cloud Computing, 13*(3), 1026–1037. https://doi.org/10.1109/TCC.2025.3588681

Grant Thornton International Ltd. (2019). Advanced ICT module for Bangladesh Meteorological Department (BMD).

Hadiningrum, T. R., Talasari, R. A. D., Ilham, K. F., & Ijtihadie, R. M. (2025). Survey on Risks Cyber Security in Edge Computing for The Internet of Things Understanding Cyber Attacks Threats and Mitigation. *JUTI: Jurnal Ilmiah Teknologi Informasi, 23*(1), 29–50. https://doi.org/10.12962/j24068535.v23i1.a1210

Hasan, M. (2024). Enhancing Enterprise Security with Zero Trust Architecture. http://arxiv.org/abs/2410.18291

Hong, S., Xu, L., Huang, J., Li, H., Hu, H., & Gu, G. (2023). SysFlow: Toward a Programmable Zero Trust Framework for System Security. *IEEE Transactions on Information Forensics and Security*, 18, 2794–2809. https://doi.org/10.1109/TIFS.2023.3264152

Iftikhar, A., Hussain, F. B., Naseer Qureshi, K. N., Shiraz, M., & Sookhak, M. (2025). Securing edge based smart city networks with software defined Networking and zero trust architecture. *Journal of Network and Computer Applications*, 244. https://doi.org/10.1016/j.jnca.2025.104341

Jing, W., Peng, L., Fu, H., & Hu, A. (2024). An Authentication Mechanism Based on Zero Trust With Radio Frequency Fingerprint for Internet of Things Networks. *IEEE Internet of Things Journal, 11*(13), 23683–23698. https://doi.org/10.1109/JIOT.2024.3385989

Joshi, H. (2025). Emerging Technologies Driving Zero Trust Maturity Across Industries. *IEEE Open Journal of the Computer Society*, 6, 25–36. https://doi.org/10.1109/OJCS.2024.3505056

Karanam, R. (2024). Zero Trust Architecture in DevSecOps: Enhancing Security in Cloud-Native

Environments. *International Journal for Research in Applied Science and Engineering Technology, 12*(8), 1071–1077. https://doi.org/10.22214/ijraset.2024.64045

Kaur, N., Mittal, A., Lilhore, U. K., Simaiya, S., Dalal, S., Saleem, K., & Ghith, E. S. (2025). Securing fog computing in healthcare with a zero-trust approach and blockchain. *EURASIP Journal on Wireless Communications and Networking, 2025*(1), 5. https://doi.org/10.1186/s13638-025-02431-6

Khair, R., Lubis, H. A. S., & Febrian, V. (2025). Blockchain Implementation in the Development of a Zero Trust-Based Cybersecurity Framework at the Indonesian National Data Center. *Jurnal Sistem Komputer dan Informatika (JSON), 7*(1), 105–111. https://doi.org/10.30865/json.v7i1.8932

Koshiya, P. G. (2025). Data-Centric Zero-Trust Architecture for Edge AI Systems. *Journal of Computer Science and Technology Studies, 7*(10), 56–66. https://doi.org/10.32996/jcsts.2025.7.10.6

Lavanya, P., Vidyullatha, P., Kumar, A. P., Manideep, A., Teja, P. S., & Rao, P. P. (2025). Enhancing Cloud Security with Zero Trust Principles: Continuous Authentication and Micro-Segmentation. *Journal of Neonatal Surgery, 14*(28S). https://www.jneonatalsurg.com/index.php/jns/article/view/5862

Li, D., Zhang, E., Lei, M., & Song, C. (2022). Zero trust in edge computing environment: a blockchain based practical scheme. *Mathematical Biosciences and Engineering, 19*(4), 4196–4216. https://doi.org/10.3934/mbe.2022194

Lindemulder, G., & Kosinski, M. (2024). Apa yang dimaksud dengan zero-trust? *Ibm*.

Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y., & Liu, Q. (2024). Dissecting zero trust: research landscape and its implementation in IoT. *Cybersecurity, 7*(1), 20. https://doi.org/10.1186/s42400-024-00212-0

Liu, Y., Xing, X., Tong, Z., Lin, X., Chen, J., Guan, Z., Wu, Q., & Susilo, W. (2024). Secure and Scalable Cross-Domain Data Sharing in Zero-Trust Cloud-Edge-End Environment Based on Sharding Blockchain. *IEEE Transactions on Dependable and Secure Computing, 21*(4), 2603–2618. https://doi.org/10.1109/TDSC.2023.3313799

Liu, Y., Zhang, R., Luo, H., Lin, Y., Sun, G., Niyato, D., Du, H., Xiong, Z., Wen, Y., Jamalipour, A., Kim, D. I., & Zhang, P. (2025). Secure Multi-LLM Agentic AI and Agentification for Edge General Intelligence by Zero-Trust: A Survey. *ArXiv Preprint*. http://arxiv.org/abs/2508.19870

Ma, Z., Wei, H., Jiang, J., Wang, B., Wang, H., & Di, Z. (2025). A lightweight zero-trust authentication architecture for IoT via unified enhanced FAST-SM9 and dynamic re-authentication. *PLOS ONE, 20*(10 October). https://doi.org/10.1371/journal.pone.0332943

Manne, T. A. K. (2023). Implementing Zero Trust Architecture in Multi-Cloud Environments. *International Journal of Computing and Engineering, 4*(3), 1–9. https://doi.org/10.47941/ijce.2754

Microsoft. (2025). Zero Trust adoption framework overview. *Microsoft*.

Mubeen, M. (2024). Zero-Trust Architecture for Cloud-Based AI Chat Applications: Encryption, Access Control and Continuous AI-Driven Verification. https://www.theseus.fi/handle/10024/876662

Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. *Sensors, 25*(19), 6118. https://doi.org/10.3390/s25196118

Nzeako, G., & Shittu, R. A. (2024). Implementing zero trust security models in cloud computing environments. *World Journal of Advanced Research and Reviews, 24*(3), 1647–1660. https://doi.org/10.30574/wjarr.2024.24.3.3500

Pokhrel, S. R., Yang, L., Rajasegarar, S., & Li, G. (2024). Robust Zero Trust Architecture: Joint

Blockchain based Federated learning and Anomaly Detection based Framework. *ArXiv Preprint*. http://arxiv.org/abs/2406.17172

Prajwalasimha, S. N., Pimpalkar, A., Shelke, N., & Bahadur Saini, D. K. J. (2025). Zero Trust Architectures Empowered by AI: A Paradigm Shift in Cloud and Edge Cybersecurity. *2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 328–335. https://doi.org/10.1109/ICSCDS65426.2025.11166875

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78*(2), 680–698. https://doi.org/10.1016/j.future.2016.11.009

Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability, 14*(18), 11213. https://doi.org/10.3390/su141811213

Shehab, M. J., Aly, Y., Badawy, A., Mohamed, A., Barhamgi, M., & Salem, S. (2025). O-Cloud Security: A Comprehensive Survey of Threats, Mitigation Strategies, and Future Directions. *IEEE Open Journal of the Communications Society,* 6, 7037–7074. https://doi.org/10.1109/OJCOMS.2025.3600528

Singh, A., Pareek, V., & Ashish, A. (2024). A Review on Blockchain for Fintech using Zero Trust Architecture. *Journal of Information and Organizational Sciences, 48*(1), 191–213. https://doi.org/10.31341/jios.48.1.11

Singh, H. P. (2025). Beyond Perimeters: Zero Trust security models in distributed cloud architectures. *World Journal of Advanced Research and Reviews, 26*(2), 3545–3553. https://doi.org/10.30574/wjarr.2025.26.2.1909

Tanaka, H. (2024). Zero Trust Security Architecture for Cloud Native Applications. *International Journal of Engineering & Extended Technologies Research (IJEETR), 6*(1), 7484–7487.

Wang, R., Li, C., Zhang, K., & Tu, B. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity, 8*(12), 1–16. https://doi.org/10.1186/s42400-024-00320-x

Wang, X., Yuan, Q., Wang, Y., Teng, J., Tao, J., & Shen, M. (2025). Zero Trust-Driven Collaborative Intrusion Detection in IoT: A Continuous Trust Assessment Approach. *IEEE Internet Computing*. https://doi.org/10.1109/MIC.2025.3610857

Zhao, L., Li, B., & Yuan, H. (2024). Cloud edge integrated security architecture of new cloud manufacturing system. *Journal of Systems Engineering and Electronics, 35*(5), 1177–1189. https://doi.org/10.23919/JSEE.2024.000112