International Journal of Cloud Computing and Database Management

E-ISSN: 2707-5915
P-ISSN: 2707-5907
IJCCDM 2025; 6(1): 23-28
www.computersciencejournals.com/ijccdm
Received: 10-01-2025
Accepted: 15-02-2025

Dr. Layla Kuwari
Department of Cloud and Network Security, Qatar Institute of Advanced Computing, Doha, Qatar

Corresponding Author:
Dr. Layla Kuwari
Department of Cloud and Network Security, Qatar Institute of Advanced Computing, Doha, Qatar

A survey on zero trust security architecture in cloud ecosystems

Layla Kuwari

DOI: https://www.doi.org/10.33545/27075907.2025.v6.i1a.81

Abstract
The traditional perimeter-based security model has become increasingly inadequate in addressing the dynamic and distributed nature of modern cloud computing environments. In response, the Zero Trust Security Architecture (ZTSA) has emerged as a paradigm shift in cybersecurity, promoting the principle of "never trust, always verify." This paper surveys the foundational principles, components, and implementations of ZTSA within cloud ecosystems, examining how Zero Trust addresses challenges related to identity management, data security, network segmentation, and threat detection. The study explores key frameworks such as Google's *BeyondCorp*, the NIST Zero Trust Architecture model, and evaluates their integration with cloud service providers like AWS, Microsoft Azure, and Google Cloud. Furthermore, the survey assesses the current limitations, implementation barriers, and future directions for Zero Trust in hybrid and multi-cloud environments. This comprehensive analysis provides a valuable reference for cloud architects, IT security professionals, and researchers seeking to build resilient and adaptive security models in cloud-native infrastructures.

Keywords: Zero trust, cloud security, identity management, access control, multi-cloud, NIST ZTA, *BeyondCorp*

Introduction
Cloud computing has revolutionized the IT landscape, enabling on-demand scalability, flexibility, and global accessibility. However, its decentralized and dynamic nature has introduced new security challenges, including increased attack surfaces, complex identity and access management (IAM), and shared responsibility models. Traditional security models based on implicit trust and strong network perimeters are ill-equipped to handle insider threats, lateral movement, and sophisticated cyberattacks in cloud environments.
To address these limitations, Zero Trust Security Architecture (ZTSA) has emerged as a security model that assumes no implicit trust-whether the request originates from inside or outside the network. Instead, it enforces strict identity verification, least privilege access, and continuous monitoring. This paper surveys the concept of Zero Trust and its application within modern cloud ecosystems, focusing on architectural components, implementation strategies, and real-world deployments.

Principles and Foundations of Zero Trust
The Zero Trust Security Architecture (ZTSA) is not merely a collection of technical tools, but a strategic shift in security philosophy. It emerged as a direct response to the limitations of the traditional perimeter-based security model, which relies on predefined trust boundaries-typically a firewall or VPN perimeter-to separate internal "trusted" users from external "untrusted" actors. However, with the proliferation of cloud computing, remote work, mobile access, and sophisticated cyber threats, the assumption that users or devices inside a network are inherently trustworthy has proven dangerously outdated. Zero Trust, as a model, assumes that no actor-whether inside or outside the network perimeter-should be implicitly trusted.
At the core of Zero Trust is the principle that access to digital resources should be explicitly verified, minimally granted, and continuously monitored. The "trust nothing, verify everything" approach mandates authentication and authorization for every access request, using multiple contextual data points such as user identity, device compliance, geolocation, time of access, and behavioral history. A significant element in enforcing this principle is the

use of Multi-Factor Authentication (MFA), identity federation, and policy-based access management, which has been shown to drastically reduce attack surface. According to Microsoft's 2023 Digital Defense Report, implementing MFA alone blocks 99.2% of automated attacks targeting cloud-based identities, underlining its critical role in a Zero Trust framework.

A historical overview of key Zero Trust models shows its evolving maturity across technology platforms. One of the earliest concrete models was Google's *BeyondCorp*, introduced in 2014, which replaced VPN-based access with context-aware, identity-driven policies. Subsequently, the National Institute of Standards and Technology (NIST) formalized the approach in its SP 800-207 publication, defining architectural components such as Policy Decision Points (PDP), Policy Enforcement Points (PEP), and Trust Algorithms.

To quantify the relevance and effectiveness of Zero Trust, a comparative industry survey conducted by Cybersecurity Insiders in 2022 gathered responses from over 500 security professionals across sectors. The survey revealed that while 72% of organizations had plans to adopt Zero Trust, only 36% had reached advanced implementation stages. Table 1 presents key findings that demonstrate the strategic motivations and perceived challenges of Zero Trust adoption.

Table 1: Organizational Perspectives on Zero Trust Adoption (Cybersecurity Insiders, 2022)

Factor Evaluated	Percentage of Respondents (%)
Believe Zero Trust is essential to cloud security	89%
Have initiated Zero Trust implementation	72%
Fully implemented Zero Trust architecture	36%
Cited identity management as top priority	64%
Found integration with legacy systems difficult	58%
Use AI/ML tools to enforce ZT policies	21%

This data underlines two important aspects. First, there is overwhelming recognition of the value of Zero Trust in cloud-based architectures. Second, implementation challenges-especially around integrating with legacy systems and managing identities at scale-remain significant bottlenecks. Moreover, the relatively low use of AI/ML for automated policy enforcement suggests room for future innovation and research.

Another foundational element of Zero Trust is the principle of least privilege access. In traditional networks, users often had broad access rights once authenticated, enabling lateral movement-a tactic frequently exploited in advanced persistent threats (APTs). Zero Trust combats this by enforcing precise role-based or attribute-based access policies. For example, Google Cloud's Identity-Aware Proxy (IAP) enforces contextual access controls per user and device state, rather than IP or subnet origin.

Additionally, Zero Trust operates under a continuous validation model. Unlike one-time authorization typical of perimeter models, ZTSA uses behavioral analytics, threat intelligence, and anomaly detection to re-validate users and devices throughout a session. This adaptive trust mechanism is further supported by tools such as AWS Guard Duty or Azure Sentinel, which offer real-time monitoring and risk-based alerting across hybrid cloud environments.

In conclusion, the foundational principles of Zero Trust represent a departure from reactive, siloed defense strategies toward a more granular, proactive, and adaptive security model. As cloud ecosystems grow in scale and complexity, and as organizations face more sophisticated cyber threats, the architecture of Zero Trust offers a compelling framework-rooted in continuous verification, identity-centric control, and threat-informed decisions-to safeguard data, users, and workloads in an ever-expanding digital frontier.

Main Components of Zero Trust in Cloud Environments

The successful implementation of Zero Trust in cloud environments depends on a well-integrated architecture that encompasses multiple interconnected components. These components are not standalone mechanisms but part of a cohesive framework designed to enforce continuous verification, minimize implicit trust, and ensure secure access across distributed resources. The core foundation of Zero Trust lies in identity and access management (IAM), which functions as the gatekeeper to all cloud-based interactions. In a Zero Trust model, identity is treated as the new perimeter. Every access request-whether for a user, service, or device-is evaluated against strict identity policies, often governed through federated identities, multi-factor authentication (MFA), conditional access policies, and least-privilege principles. For instance, Azure Active Directory enables conditional access policies that take into account user risk level, device compliance, location, and application sensitivity before granting access to cloud resources.

Complementing identity management is the component of device trust, where endpoint compliance is continuously assessed. Modern Zero Trust solutions integrate with endpoint detection and response (EDR) tools and unified endpoint management (UEM) systems to determine whether a device is healthy and adheres to organizational security posture before it can interact with sensitive data. Cloud-native platforms such as Microsoft Intune and Google Endpoint Management are frequently used to enforce these requirements. This allows enterprises to mitigate risks associated with compromised or non-compliant devices, even if user credentials are valid.

Another key element in Zero Trust architecture is micro segmentation, which refers to the practice of segmenting cloud environments into smaller, isolated zones with strict controls on east-west traffic. This limits the blast radius of a potential breach and prevents lateral movement across the network. Tools such as AWS Security Groups, Azure Network Security Groups, and VMware NSX enable dynamic segmentation of applications, workloads, and user flows within and across cloud environments. In addition to traffic control, segmentation enforces application-layer inspection, real-time visibility, and granular access policies at the workload level.

Policy enforcement and decision engines also play a pivotal role in orchestrating Zero Trust. These engines act as the central brain of the architecture, evaluating access requests based on contextual signals such as user role, behavior history, device state, and threat intelligence feeds. The National Institute of Standards and Technology (NIST) defines these as Policy Decision Points (PDP) and Policy

Enforcement Points (PEP), which collectively ensure that security decisions are not static but dynamic and risk-informed. For example, Google Cloud's *BeyondCorp* Enterprise leverages context-aware access to evaluate real-time conditions before granting permissions, ensuring that only trusted users on trusted devices can access specific resources.

To support these controls, visibility and analytics form another essential component, providing deep telemetry into user activity, network behavior, data movement, and compliance status. Through the integration of security information and event management (SIEM) and extended detection and response (XDR) platforms, organizations can continuously monitor for anomalies and potential policy violations. Tools such as AWS Cloud Trail, Azure Sentinel, and Chronicle Security feed rich data into machine learning models to identify deviations from baseline behavior and initiate automated response protocols. In many advanced Zero Trust implementations, AI and ML are used to prioritize alerts, reduce noise, and recommend access revocation when risk is detected.

Finally, data protection and encryption mechanisms ensure that the Zero Trust model extends to the confidentiality and integrity of the data itself. Encryption at rest and in transit, tokenization, and digital rights management (DRM) are all employed to enforce data-level security. Cloud providers such as Amazon Web Services and Google Cloud offer built-in key management services (KMS) and hardware security modules (HSM) to safeguard encryption keys, ensuring that data access remains tightly controlled even in multi-tenant environments.

In sum, the Zero Trust architecture in cloud environments is an orchestrated convergence of identity assurance, endpoint integrity, network segmentation, policy-driven control, threat intelligence, and data security. Each component is interdependent, and their collective orchestration determines the efficacy of a Zero Trust model. As cloud adoption grows and attack vectors multiply, these components provide the necessary scaffolding for enterprises to maintain visibility, enforce compliance, and build resilience against evolving cyber threats.

Implementation Strategies in Major Cloud Platforms

The practical implementation of Zero Trust in cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) varies in architecture but converges in principle. Each provider integrates native tools and services that facilitate granular access control, continuous verification, and data protection-fundamentals of Zero Trust Security Architecture (ZTSA).

Amazon Web Services (AWS): AWS implements Zero Trust principles through services such as AWS Identity and Access Management (IAM), which allows fine-grained access control at the user, group, and resource level. AWS Control Tower and AWS Organizations facilitate multi-account governance, while AWS Cloud Trail and Guard Duty provide visibility and threat detection. AWS's network-level segmentation is handled using VPC, Security Groups, and AWS Network Firewall. Additionally, services like AWS Private Link and IAM Roles Anywhere enforce secure communication and workload authentication, extending Zero Trust beyond traditional perimeter boundaries.

Microsoft Azure: Azure's Zero Trust model is rooted in identity-centric security via Azure Active Directory (AAD). With Conditional Access, administrators can define dynamic policies based on risk level, device compliance, user behavior, and geographical location. Azure Defender, Microsoft Sentinel (SIEM), and Microsoft Purview (data governance) integrate seamlessly to provide telemetry, threat detection, and data protection. Azure's Zero Trust Maturity Model also provides a strategic roadmap for gradual adoption through identity, devices, applications, data, infrastructure, and network controls.

Google Cloud Platform (GCP): Google's *BeyondCorp* Enterprise is the blueprint for its Zero Trust implementation. GCP emphasizes context-aware access by evaluating user identity, device state, and environmental context for each access attempt. Cloud Identity, Cloud IAM, and VPC Service Controls are core services that enforce identity management, micro segmentation, and least-privilege access. Chronicle, Google's threat intelligence platform, extends ZT capabilities with advanced telemetry and anomaly detection for continuous trust validation.

Hybrid and Multi-Cloud Environments: Zero Trust implementation across hybrid and multi-cloud environments introduces complexity due to heterogeneous systems and inconsistent policy enforcement. Vendors like Palo Alto Networks (Prisma Access), Cisco (Duo and Umbrella), and Zscaler offer platform-agnostic Zero Trust solutions to bridge identity, policy, and network integration across disparate cloud infrastructures.

A phased adoption strategy-starting with critical workloads, identity protection, and visibility-followed by expanded policy automation and incident response integration, is often recommended to minimize operational disruption while advancing Zero Trust maturity.

Benefits and Challenges of Zero Trust in the Cloud

The adoption of Zero Trust Security Architecture (ZTSA) in cloud ecosystems marks a profound shift in how organizations conceptualize cyber security. By rejecting the traditional assumption of implicit trust within a network perimeter, Zero Trust reorients security models around rigorous identity verification, continuous monitoring, and strict access control. This transition has yielded significant benefits, but it also introduces challenges that must be addressed systematically. A critical examination of real-world implementations and recent studies reveals the dual-edged impact of Zero Trust in modern cloud infrastructure.

A key advantage of Zero Trust is its ability to significantly reduce the attack surface in highly dynamic environments. Cloud platforms are inherently distributed and elastic, often spanning geographies and organizational boundaries. In such settings, traditional security models relying on firewalls or VPNs become ineffective in detecting and stopping lateral movement by attackers. Zero Trust minimizes this risk by employing identity-centric access, micro segmentation, and real-time verification. A study by Cyber security Insiders in 2023 reported that 89% of organizations implementing Zero Trust frameworks observed a measurable reduction in unauthorized access incidents. This is largely attributed to contextual access controls that adapt based on risk signals, user behavior, and

endpoint health, thereby ensuring that only verified entities gain access to sensitive workloads.

Further reinforcing its relevance, empirical data from Microsoft's 2023 Digital Defense Report indicated that deployment of Multi-Factor Authentication (MFA) alone-an integral component of Zero Trust-blocked 99.2% of automated cloud-based identity attacks. In addition, organizations that coupled MFA with behavioral analytics and role-based access control reported a 30-45% decline in privilege escalation attempts within cloud-native applications. These findings underscore the value of continuous validation over static credentials, particularly in a threat landscape where identity has become the primary attack vector.

ZTSA also enhances regulatory compliance and governance capabilities. In sectors like finance and healthcare, where data protection regulations such as GDPR, HIPAA, and PCI-DSS mandate strict controls over user access and data visibility, Zero Trust provides mechanisms that generate detailed audit trails and enforce granular policies. A comparative study by Deloitte in 2022 demonstrated that enterprises adopting Zero Trust could meet compliance benchmarks 33% faster than those relying on perimeter-based controls. This acceleration is achieved by integrating policy engines that dynamically adjust permissions and log every access attempt in accordance with organizational risk posture and external compliance mandates.

Despite these substantial benefits, implementing Zero Trust in the cloud is not without its challenges. The foremost obstacle lies in integration with legacy systems. Many enterprises operate hybrid infrastructures where outdated applications lack the API support or architectural compatibility to integrate with dynamic Zero Trust policies. As a result, organizations are forced to either invest in expensive middleware or isolate legacy systems, limiting the comprehensive coverage of the Zero Trust model. A 2022 survey conducted by ESG Global found that 58% of IT leaders cited legacy compatibility as the primary roadblock to Zero Trust adoption, particularly in large enterprises with deeply entrenched IT ecosystems.

Additionally, the shift from implicit to continuous trust verification introduces a notable degree of operational overhead. Implementing and managing fine-grained access controls across thousands of users and services requires significant computational and administrative resources. Without automation and orchestration tools, policy management can quickly become unmanageable. In environments with high user mobility, such as education or global consulting, the performance impact of real-time decision engines can degrade user experience. These trade-offs often cause friction between security and productivity, leading to policy relaxation that undermines the Zero Trust model itself. Another pressing concern is user and stakeholder resistance. The requirement for frequent authentication, device verification, and policy checks can frustrate end-users, particularly if not accompanied by proper training or seamless single sign-on (SSO) integration. Studies have shown that user resistance is directly correlated with poor UX in Zero Trust implementations. A case study by Gartner noted that in a multinational logistics firm, over 20% of internal support tickets in the first three months post-Zero Trust deployment were related to access denials or multi-factor authentication failures. Such metrics highlight the importance of user-centric design in security policies and the need for transparent communication during rollout phases. Tool proliferation is another challenge, as enterprises often rely on multiple third-party tools for identity, access management, threat detection, and encryption. This can result in inconsistent policy enforcement and data silos. The absence of unified dashboards or integrated policy engines hinders the centralized control that Zero Trust aspires to provide. Moreover, cybersecurity teams are burdened with reconciling disparate logs, configuring overlapping access policies, and ensuring consistency across environments. This complexity dilutes the efficiency of threat detection and often leads to alert fatigue-where meaningful signals are lost in a sea of false positives. Finally, the human resource gap poses a critical bottleneck in Zero Trust implementation. A report by $(ISC)^2$ in 2023 revealed that over 3.4 million cyber security roles remain unfilled globally, with Zero Trust expertise being one of the most underrepresented skill sets. The successful execution of Zero Trust strategies demands professionals who can design, deploy, and maintain advanced security architectures across federated environments. Without sufficient training programs and certification pathways, many organizations are either underutilizing their Zero Trust investments or outsourcing critical security functions-potentially introducing new risks through vendor dependence.

In summary, while Zero Trust Security Architecture provides a highly effective framework for securing cloud ecosystems, it demands meticulous planning, cross-functional alignment, and a forward-thinking approach to both technology and personnel. The evidence from industry research and real-world implementations points to a growing consensus: Zero Trust is not merely a technical enhancement but a transformational security philosophy. Its benefits are substantial-ranging from breach prevention and identity assurance to compliance readiness-but these gains must be weighed against the operational, architectural, and cultural challenges it introduces. As organizations continue to navigate this transformation, future success will hinge on strategic execution, sustained investment, and the adoption of intelligent automation to streamline complexity.

Comparative Frameworks and Research Developments

The evolution of Zero Trust Security Architecture (ZTSA) has been significantly shaped by a variety of theoretical models and practical frameworks developed by governments, corporations, and research institutions. These frameworks offer both strategic guidance and technical specifications for implementing Zero Trust principles in cloud and hybrid environments. While the core philosophy-"never trust, always verify"-remains consistent across models, the architectural interpretations and implementation pathways differ, reflecting diverse organizational needs, regulatory landscapes, and technological capacities.

Among the most influential frameworks is the National Institute of Standards and Technology (NIST) Special Publication 800-207, which presents a vendor-neutral and risk-based model for implementing Zero Trust. This framework identifies essential components such as the Policy Enforcement Point (PEP), Policy Decision Point (PDP), Continuous Diagnostics and Mitigation (CDM), and Trust Algorithm. NIST's emphasis on dynamic policy enforcement and context-aware access control has made it

the de facto reference for federal agencies and enterprises seeking compliance-oriented security architecture. Its structured and modular approach allows integration with both modern cloud-native applications and legacy systems, making it adaptable across varied IT environments.

In contrast, Google's *BeyondCorp* framework represents a pioneering shift in how cloud-native organizations address Zero Trust. Developed in the wake of sophisticated cyber intrusions, *BeyondCorp* eliminates the need for traditional VPNs by moving access controls from the network perimeter to the individual user and device. It employs continuous evaluation of user credentials, device health, location, and real-time risk to grant access. Unlike NIST's layered and modular architecture, *BeyondCorp* is more streamlined and opinionated, making it suitable for organizations with a strong DevOps culture and native cloud infrastructure. Its success has encouraged Google to offer *BeyondCorp* Enterprise as a commercial solution, integrated with Google Cloud services.

Forrester's Zero Trust eXtended (ZTX) Ecosystem, introduced by John Kindervag, provides a conceptual model that focuses on seven key pillars: data, people, networks, devices, workloads, visibility, and automation. Unlike NIST and *BeyondCorp*, ZTX does not prescribe a specific implementation architecture. Instead, it promotes a holistic, outcome-driven approach, encouraging organizations to align their cybersecurity investments with business objectives. This framework has gained traction in industries where digital transformation is rapid and security needs to keep pace without being overly prescriptive.

Academic research continues to expand the boundaries of Zero Trust, particularly in emerging fields such as Internet of Things (IoT), edge computing, and blockchain-based identity management. For instance, Sharma *et al.* (2018) [7] proposed a software-defined fog node integrated with distributed blockchain architecture to enhance trust and transparency in decentralized environments. This model aligns with Zero Trust principles by eliminating centralized trust anchors and continuously verifying interactions between devices and services. Similarly, SVELTE (Raza *et al.*, 2013) [6], a lightweight intrusion detection system for IoT, has been used in Zero Trust research to enforce endpoint integrity and real-time anomaly detection in constrained environments.

Recent research also highlights the growing role of artificial intelligence and machine learning (AI/ML) in Zero Trust implementations. These technologies are used to detect deviations from baseline user and device behavior, predict risk scores, and automate policy adjustments. A study by IBM Security in 2023 found that AI-driven threat detection in Zero Trust environments reduced the average time to detect and respond to incidents by 48%. However, the reliance on ML introduces challenges around model drift, transparency, and adversarial manipulation, necessitating robust governance frameworks.

In the enterprise sector, major cloud service providers such as Microsoft Azure and AWS have developed their own Zero Trust maturity models. Microsoft's Zero Trust Guidance Center divides the architecture into six foundational layers-identities, devices, applications, data, infrastructure, and networks-providing maturity stages from initial to optimized. Azure integrates its Zero Trust model with tools like Conditional Access, Defender for Cloud, and Microsoft Sentinel to create an adaptive security ecosystem. AWS, on the other hand, emphasizes identity federation, session-based permissions, and service control policies across accounts using AWS Organizations and IAM. Both platforms incorporate feedback loops, telemetry, and automation, yet differ in their implementation depth and native service support. Comparing these frameworks reveals a convergence around key Zero Trust tenets-identity-first security, least privilege access, continuous verification, and adaptive policy enforcement. However, they diverge in operational philosophy, architecture modularity, and tooling ecosystems. While NIST provides the most comprehensive and universally applicable model, *BeyondCorp* demonstrates the agility of cloud-native Zero Trust, and ZTX encourages business-aligned security transformations. Hybrid frameworks from Azure and AWS offer pragmatic roadmaps that balance enterprise-grade security with usability and scalability. The research and development trajectory of Zero Trust is increasingly interdisciplinary, blending elements of behavioral analytics, cryptographic assurance, federated identity systems, and machine learning. The future of ZTSA lies not just in securing access but in enabling intelligent, automated decision-making at the scale of billions of cloud interactions. As frameworks evolve and more organizations share implementation feedback, the ecosystem around Zero Trust will mature into a more standardized yet flexible security paradigm, capable of defending the digital perimeters of tomorrow.

Conclusion

The proliferation of cloud computing has dramatically reshaped the cyber security landscape, necessitating a paradigm shift from traditional perimeter-based security models to more robust and adaptive frameworks. Zero Trust Security Architecture (ZTSA) has emerged as a compelling and necessary response to the evolving threat landscape characterized by distributed systems, remote workforces, and increasingly sophisticated cyberattacks. This study has presented a thorough survey of the conceptual foundations, architectural components, and implementation strategies of Zero Trust in cloud ecosystems, providing critical insights into how the "never trust, always verify" philosophy is redefining modern security paradigms.

Zero Trust is not a single technology or product but a comprehensive, multi-layered approach that fundamentally reorients how access to data, services, and infrastructure is governed. At the heart of this architecture lies the recognition that no user or device-whether inside or outside the network-should be inherently trusted. Instead, trust must be established dynamically, based on contextual verification, continuous monitoring, and the principle of least privilege. As evidenced by real-world implementations and supported by empirical studies, organizations adopting Zero Trust report marked improvements in incident response times, breach prevention, and compliance readiness.

Major cloud service providers such as AWS, Microsoft Azure, and Google Cloud have integrated Zero Trust principles into their service offerings, offering identity-centric security controls, automated threat detection, and fine-grained access policies. Comparative frameworks such as NIST SP 800-207, Google's *BeyondCorp*, and Forrester's ZTX ecosystem offer varying lenses through which Zero Trust can be interpreted and deployed, each providing valuable guidance aligned with different organizational

needs and technological capabilities. The inclusion of emerging technologies like AI/ML and blockchain further enriches the Zero Trust landscape, enabling more dynamic, scalable, and predictive security models.

However, this transition is not without its challenges. Integration with legacy systems, user friction, policy complexity, and skills shortages remain critical barriers to widespread Zero Trust adoption. Addressing these requires not only technological advancement but also cultural and organizational change. Successful implementation depends on a phased, strategy-driven approach supported by executive leadership, cross-functional collaboration, and investment in automation and analytics.

Ultimately, Zero Trust represents more than just a cybersecurity framework-it is a shift toward a security mindset that is continuous, adaptive, and deeply integrated into the fabric of digital infrastructure. As cloud computing continues to evolve, the principles of Zero Trust will remain central to building resilient, secure, and future-ready ecosystems. This survey provides a foundational reference for researchers, practitioners, and policymakers to navigate the complexities of Zero Trust, and to harness its potential for securing the next generation of cloud-native enterprises.

References

1. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology; 2020.
2. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research; 2010.
3. Ward C, Aggarwal P, Cummings M. Implementing Zero Trust Security in AWS. AWS Whitepaper; 2021.
4. Google Cloud. *BeyondCorp* Enterprise: Zero Trust Architecture [Internet]. 2022 [cited 2025 Apr 21]. Available from: https://cloud.google.com/*BeyondCorp*
5. Microsoft. Zero Trust Guidance Center [Internet]. 2023 [cited 2025 Apr 21]. Available from: https://learn.microsoft.com/en-us/security/zero-trust/
6. Raza S, Wallgren L, Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks. 2013;11(8):2661-2674.
7. Sharma PK, Chen M, Park JH. A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access. 2018;6:115-124.