International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 12, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i12.1050

Implementing Zero Trust Architecture: Principles, Models and Challenges

Raghuvar Karthik Durga[1]

Publication Date: 2025/12/30

Abstract

The combination of cloud adoption, mobile workforces, and advanced cyber threats has rendered traditional perimeter-based security models ineffective, as they no longer effectively protect networks. This paper examines Zero Trust Architecture (ZTA), a strategic security model that operates based on the fundamental concept of "never trust, always verify." The research investigates ZTA fundamentals through explicit verification and least privilege access and micro-segmentation while demonstrating how Identity and Access Management (IAM) functions as the essential foundation of this architecture. The research presents a functional deployment approach based on NIST SP 800-207 standards, which starts with protecting surface identification, followed by transaction flow mapping and implementation of detailed access controls. The research examines three major obstacles organizations encounter when implementing Zero Trust, which include user resistance to change, system integration difficulties with existing infrastructure, and challenges in maintaining user convenience. The implementation of Zero Trust represents an absolute necessity for organizations, as it creates a robust security system that protects against contemporary threats in today's distributed digital landscape.

Keywords: *Zero Trust Architecture, Never Trust Always Verify, Micro-Segmentation, Identity and Access Management (IAM), Least Privilege Access, NIST SP 800-207.*

I. INTRODUCTION

Organizations used the "castle-and-moat" model for decades to protect their systems by creating strong perimeter defenses through firewalls and virtual private networks (VPNs), which trusted all internal elements. The digital environment has undergone a complete transformation, rendering the previous security model entirely ineffective. The digital environment has undergone significant changes, driven by the rapid adoption of cloud computing, the widespread use of mobile devices, the increasing standardization of remote work, and the rapid expansion of the Internet of Things (IoT) (Stafford, 2020). Built on the premise of a fortified perimeter and unexamined internal trust, the castle-and-moat model fails to meet the security demands of today's distributed and cloud-centric enterprise landscape. The modern network environment has evolved into a complex system of interconnected devices, as data and applications are now located outside of data centers. Users can access resources from any location worldwide, and connected devices operate within the network. The network has evolved into a vulnerable system because the traditional perimeter defense model no longer applies, as threats can enter from both external and internal network sources (He, 2022).

Modern cyber threats use the network perimeter vulnerabilities to launch sophisticated phishing attacks and ransomware assaults and exploit insider threats. The network connection trust assumption enables attackers to easily access vital assets through the wide range of attack possibilities that exist within the network (Bertino, 2021). The growing security threats have led to the development of Zero Trust Architecture (ZTA) as a new security philosophy. Zero Trust functions as a strategic initiative that implements an architectural framework based on the fundamental principle of "never trust, always verify." The system requires continuous verification of every access request through context-based evaluation, which includes user identity, device health, location, and application sensitivity, regardless of the request origin. As illustrated in Table .1, the two models differ radically in their core assumptions, controls, and approach to access, necessitating a fundamental shift in security strategy and architecture (Moruff, 2024).

Durga, R. K. (2025). Implementing Zero Trust Architecture: Principles, Models, and Challenges. *International Journal of Scientific Research and Modern Technology*, *4*(12), 162–170. https://doi.org/10.38124/ijsrmt.v4i12.1050

Table 1 Castle-and-Moat v/s Zero Trust Security Models (Moruff, 2024).

Aspect	Castle-and-Moat (Traditional) Model	Zero Trust Model
Trust Assumption	Everything inside the network perimeter is trusted.	Nothing is trusted by default, regardless of location.
Security Perimeter	Hard, Fixed Boundary.	Fluid, Identity-Centric
Primary Control	Network Location	Identity & Context.
Access Approach	Broad Network Access	Least Privilege Access
View of Threats	Primarily designed to keep threats out. Vulnerable to insider threats.	Assuming threats exist both inside and outside. Focuses on containment.
Best For	Static environments where all users and data are within a confined network.	Hybrid environments with cloud services, remote work, and mobile devices.

The research investigates Zero Trust Architecture through its fundamental concepts and technological elements, as well as the evaluation of the NIST SP 800-207 framework and the organizational challenges encountered during implementation. The paper demonstrates that Zero Trust represents a fundamental security transformation that organizations need to establish as part of their modern digital security foundation.

II. BACKGROUND AND EVOLUTION OF ZERO TRUST

The zero-trust security model introduces a new security paradigm that moves away from traditional perimeter-based security systems, which depend on firewalls and VPNs to control access through network location and perimeter trust boundaries. Conventional security methods have lost their effectiveness because cloud services, mobile devices, and advanced cyber-attacks have become more prevalent (Bertino, 2021). The security approach depends on predetermined network areas, which prove insufficient for stopping internal threats and perimeter-evading attacks (Edo et al., 2022; Kumar, 2024). John Kindervag, a Forrester Research employee, introduced the term "Zero Trust" in 2010. According to Kindervag's research, "never trust, always verify" became the core principle of his security model, which grants no automatic trust to users or devices regardless of their network position (Teerakanok et al., 2021). The security model BeyondCorp, which Google developed under zero-trust principles, became widely known after the company implemented it. The system enables users to access services through secure connections without requiring a VPN, as it verifies each request as if it came from an open network (Ajish, 2024; Edo et al., 2022). Figure .1 shows the adoption percentage of ZTA among organizations is being raised from 2020 to 2024.

The National Institute of Standards and Technology (NIST) established zero-trust standards through Special Publication 800-207, which presents complete zero-trust principles and architectural frameworks. The NIST guidelines serve as fundamental standards for zero-trust deployment across various organizational environments, providing specific implementation strategies for complex systems (Borchert et al., 2025; Chandramouli & Butcher, 2023).

Fig 1 Percentage of Organizations Adopting Zero Trust (2020-2024) (Bradbury, n.d.)

III. CORE PRINCIPLES OF ZERO TRUST ARCHITECTURE

Zero Trust Architecture represents a complete change in cybersecurity principles, which goes beyond being a collection of security technologies. The framework consists of multiple core principles that direct its development process. The security posture of Zero Trust Architecture emerges through the combined operation of its fundamental principles, which provide dynamic protection against contemporary threats (Lund, 2024) (Azad, 2024).

➢ *Never Trust, Always Verify:*

The core principle of Zero Trust eliminates all implicit trust relationships. The traditional security approach depended on the belief that all resources located within the corporate network boundaries were trustworthy. ZTA rejects this notion entirely. The "Never Trust, Always Verify" principle requires all entities, including users, devices, applications, and services, to prove their identity before receiving any form of trust. Every access request, from public internet connections to internal corporate LANs, requires strict authentication, authorization, and encryption before access becomes available. The system demands that trust must be proven through explicit actions for every transaction and session (Azad, 2024). The foundational principles of Zero Trust Architecture (ZTA) are best understood as a cohesive philosophy, visually summarized in Figure 1.

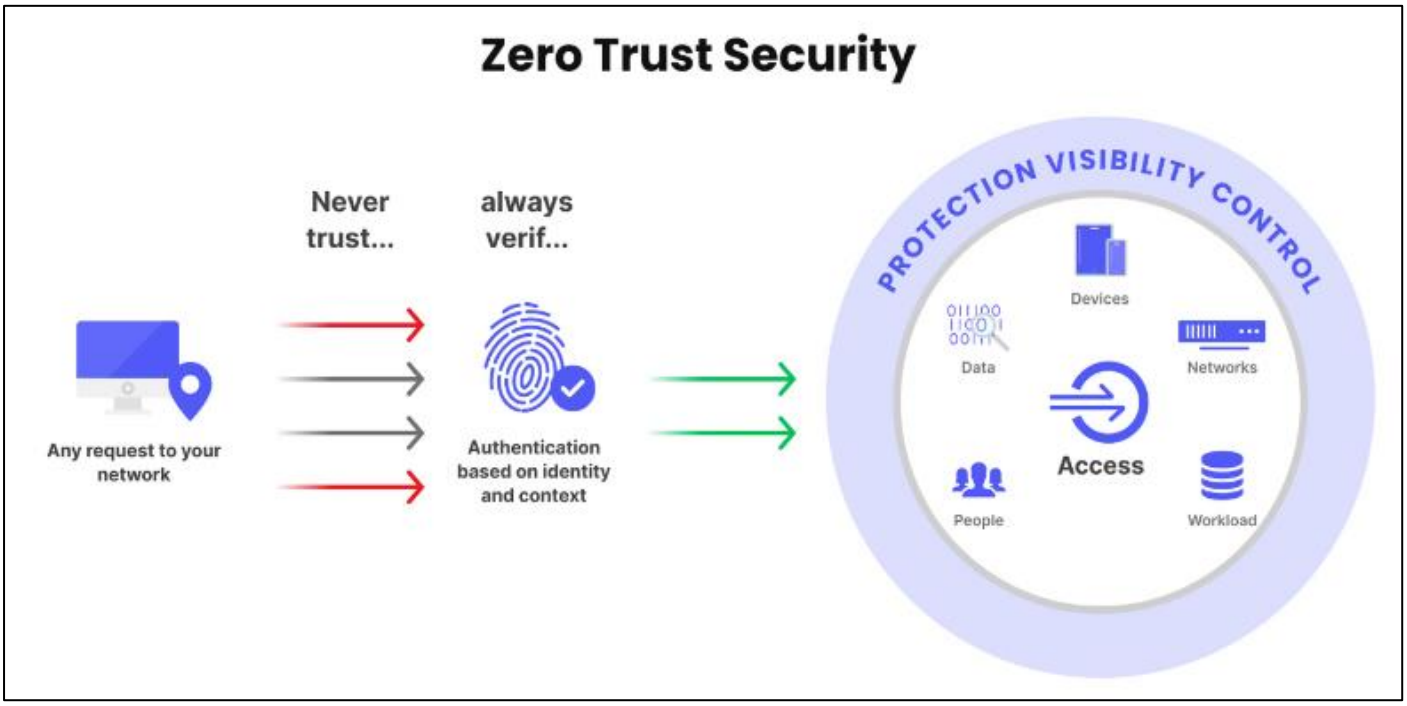

Fig 2 The Core Philosophy of Zero Trust.

➢ *Assume Breach*

Zero Trust security depends on the fundamental principle that network breaches will happen or are already underway. The security approach relies on breach detection and impact reduction through continuous monitoring and swift response systems to stop attackers from spreading through the network (Ahn et al., 2024).

➢ *Principle of Least Privilege (PoLP)*

The "Never Trust" principle gets its practical implementation through Least Privilege, which functions as an enforcement mechanism. The principle requires all users, devices, and applications to receive only the essential permissions that match their authorized roles and responsibilities (Hammad, 2017). The principle extends to all entities, including human operators and system processes. The process of PoLP requires organizations to create detailed access control rules, which specify that developers should not access HR documents, and database servers should prevent internet connection initiation. The attack surface decreases significantly because attackers who gain access to credentials can only reach restricted resources (Basta, 2022).

➢ *Micro-Segmentation*

The network infrastructure implements the "Assume Breach" and "Least Privilege" principles through technical means, which is known as Micro-segmentation. The network gets divided into multiple secure areas through micro-segmentation, which extends down to individual workloads and applications. Each segment operates with its own strict access controls, and policy-based enforcement ensures their maintenance. The strategy enables the management of east-west traffic flow between data center segments, while abandoning traditional flat network designs. The security system prevents attackers who gain access to web servers in one segment from moving to database servers in different segments, thereby limiting the spread of the threat (Sheikh, 2021) (Ejiofor, 2025).

➢ *Continuous Verification and Validation*

The security posture remains dynamic through continuous verification and validation because this principle conducts ongoing assessments of user security states and network environments. Organizations can identify security threats through real-time monitoring of user activities and network health because this approach delivers current information about system behavior (Ejiofor et al., 2025; Azad et al., 2024).

Organizations that follow these principles will achieve a better security posture, which results in improved defense capabilities against contemporary cyber threats.

IV. KEY PILLARS AND TECHNOLOGY COMPONENTS

The implementation of Zero Trust principles depends on multiple technological pillars that form its operational foundation. The modern digital enterprise relies on these integrated components to enforce policies, evaluate trust levels, and safeguard its resources.

➢ *Identity and Access Management (IAM): The Cornerstone*

IAM functions as the core element of ZTA because it implements the "Never Trust, Always Verify" principle. The system grants authorized users and services access to resources based on established conditions.

- Multi-Factor Authentication (MFA): The implementation of Multi-Factor Authentication (MFA) stands as an essential requirement for ZTA. The combination of three verification elements (something you know, something you have, and something you are) through MFA makes it nearly impossible for attackers to use stolen credentials to gain unauthorized access (Anderson, 2022).
- Single Sign-On (SSO): Single Sign-On (SSO) enables users to handle strict authentication through an easy-to-use interface. Users authenticate only once to access multiple applications, but subsequent requests undergo verification checks from the central identity provider against active policy settings to ensure continuous verification requirements are met (Anderson, 2022).
- Privileged Access Management (PAM): PAM solutions under This Framework enforce minimum permission levels for users who require administrative access and high-level system privileges. The security of privileged credentials depends on PAM solutions, which implement just-in-time access and session monitoring and vaulting to protect against insider threats and stop attackers from moving laterally (Anderson, 2022).

➢ *Device Trust and Health:*

Secure networks depend on the trustworthiness of devices that attempt to access them. The process of device health assessment, security requirement verification, and ongoing device behavior tracking is necessary for network protection. The implementation of device trust protocols prevents untrusted devices from entering the network, thereby protecting its security (Prajapati, 2025; Azad et al., 2024).

➢ *Network Segmentation:*

Network segmentation through micro-segmentation divides networks into smaller segments to achieve better access control and reduce the potential spread of breaches across networks. The practice of segmenting networks into smaller areas through micro-segmentation enhances security by restricting the movement of threats and providing detailed access restrictions for each network segment (Dhiman et al., 2024; Syed et al., 2022).

➢ *Data Security:*

The protection of sensitive information depends on Zero Trust security, which requires encryption, data masking, and access control systems. The protection of data confidentiality and integrity throughout transfer operations is a core requirement for ZTA, according to Daah et al. (2024) and He et al. (2022).

➢ *Workload Security:*

ZTA requires organizations to protect their workloads through continuous security monitoring and policy enforcement for all network applications and services. Protection of applications against real-time operating environment vulnerabilities and attacks becomes possible through this approach (Adamson & Qureshi, 2025).

➢ *Visibility and Analytics:*

The implementation of Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), and User and Entity Behavior Analytics (UEBA) systems delivers complete visibility to organizations. The technologies produce log data for analysis while detecting irregularities to deliver fast incident response capabilities (Prajapati, 2025; Kumar, 2024).

➢ *Automation and Orchestration:*

Implementing Zero Trust requires these components to achieve scalability and immediate threat response. The implementation of zero trust policies across various dynamic environments becomes possible through automation, which enables fast security measure deployment and minimizes human mistakes (Dhiman et al., 2024).

V. CONCEPTUAL MODELS AND FRAMEWORKS

- NIST SP 800-207: The NIST Special Publication 800-207 defines Zero Trust Architecture (ZTA) through three essential elements, which include the Policy Engine (PE), Policy Administrator (PA), and Policy Enforcement Point (PEP). The Policy Engine determines access authorization through policy evaluation using user identity information, device status, and operational context data. The Policy Administrator implements policies by sending PE

decisions to suitable PEPs. The Policy Enforcement Point functions as a security checkpoint that enforces resource access restrictions according to administrative decisions. The ZTA model operates by transitioning from traditional perimeter security to establish identity-based access controls, which verify both people and systems before granting access (Chandramouli & Butcher, 2023; Borchert et al., 2025).

- Forrester Zero Trust Extended (ZTX) Ecosystem framework: The Forrester Zero Trust Extended (ZTX) Ecosystem framework extends this method by adding seven essential pillars, which include Workforce, Device, Workload, Network, Data, Visibility & Analytics, and Automation & Orchestration. Each security pillar needs its own specific protection plan. The security approach for Workforce protects user identities through access control systems, Device security protects endpoints through protection measures, and Workload security defends applications from threats. Network security protects data during its movement, and Data security handles encryption and protection functions. The combination of Visibility & Analytics provides real-time threat detection and continuous monitoring. At the same time, Automation & Orchestration enables fast security incident responses through automated processes that minimize human errors and accelerate threat elimination (Borchert et al., 2025).
- CISA Zero Trust Maturity Model: The CISA Zero Trust Maturity Model enables organizations to follow a structured path for moving away from conventional security systems toward complete Zero Trust implementation. The model consists of five distinct pillars, which include Identity and Device, Network/Environment, Application Workload, and Data. Organizations use pillars to evaluate their Zero Trust development stage, which helps them establish strategic directions for future development and resource allocation. The model focuses on identity-based security methods, requiring organizations to continuously assess and manage access permissions throughout their networks and systems (Azad et al., 2024).

The frameworks demonstrate that organizations should replace implicit trust with strong authentication and authorization systems to achieve adequate cyber threat protection.

VI. IMPLEMENTATION STRATEGY AND MIGRATION PATH

A Zero Trust Architecture (ZTA) implementation strategy for practical deployment requires a step-by-step approach because Zero Trust functions as an ongoing process instead of a single deployment. This method enables organizations to transition smoothly while maintaining operational continuity and employee productivity (Vanickis, 2018).

➢ *Identify Protect Surface*

The first step requires organizations to identify their most important data assets and applications and services (DAAS) that need maximum protection. Use specialized tools to perform a detailed resource assessment, which evaluates each item based on its business worth and vulnerability level. The list includes customer databases together with proprietary intellectual property and payment processing systems (Vanickis, 2018) (Shipman, 2024).

➢ *Map Transaction Flows*

The document tracks the movement of traffic between the protected surface and all other identified areas. Network traffic analysis (NTA) tools help organizations visualize application, user, and device dependencies and intersections through flow analysis. The analysis shows security weaknesses and unneeded access rights, which help determine optimal control positions (Shipman, 2024).

➢ *Architect a Zero Trust Environment*

The protected surface should be the foundation for environmental design through micro segmentation, which creates separate network zones for detailed access management. The environment should use VLANs, SDN, and next-generation firewalls to limit network traffic between zones. The system requires integration of identity providers and device management platforms to achieve enhanced access control (Bertino, 2021).

➢ *Create and Enforce Policies*

Each transaction flow requires specific "allow" policies that define exact permissions for authorized operations. The Zero Trust Policy Engine requires policies to exist in both human-readable and machine-readable formats for integration purposes. The real-time enforcement and adaptive controls of Azure AD, Okta, and Zscaler tools allow for immediate policy application (Bertino, 2021).

➢ *Monitor and Maintain*

The system requires ongoing monitoring of all financial transactions, access attempts, and policy enforcement activities to ensure compliance. The system depends on SIEM, log review, and automated alerts to provide continuous feedback for adjusting. The system requires periodic updates to its policies, informed by threat analysis, operational requirements, and regulatory compliance needs (Bertino, 2021).

➢ *Use Cases:*

The first step for organizations to start their Zero Trust implementation involves solving particular high-impact security requirements.

- Securing Remote Access: The implementation of Zero Trust Network Access (ZTNA) solutions should replace traditional VPN systems for remote access security. ZTNA enables users to access specific applications securely through a system that denies

them complete network access, thus minimizing the attackable network areas (Syed, 2022).

- Protecting Cloud Migrations: Organizations should implement Zero Trust Architecture principles during their initial public cloud (IaaS/PaaS) workload deployments. The new environment requires cloud-native tools for identity-based access, workload segmentation, and data encryption within the cloud platform (Syed, 2022).
- Securing DevOps Pipelines: The CI/CD process requires security integration through three essential steps, which include vulnerability scanning of workloads, identity policy definition, and least privilege access deployment. DevSecOps implements Zero Trust principles through application development, starting from the initial creation phase (Taskin, 2025).

This approach helps organizations move steadily from legacy perimeter defenses toward a dynamic, resilient, and adaptive Zero Trust security posture, with incremental steps and ongoing policy refinements.

VII. CHALLENGES AND LIMITATIONS

The implementation of Zero Trust Architecture (ZTA requires organizations to address multiple obstacles, which need detailed planning and strategic execution.

- Cultural and Organizational Change: The adoption of Zero Trust security necessitates significant cultural transformations within organizations, as they must transition away from traditional perimeter-based security systems. The adoption of "never trust, always verify" faces challenges because employees resist new security approaches that differ from their established practices and lack familiarity with modern security principles. The transition to Zero Trust security affects both technological systems and business operations and employee attitudes, so organizations need to develop strong management approaches (Ogundipe et al., 2024).
- Implementation Complexity: Implementing Zero Trust principles with existing legacy systems poses significant challenges due to the complexity of their integration. The integration of Zero Trust principles with legacy systems becomes challenging because these systems often lack modern security features and require significant updates to achieve compatibility, which can result in system disruptions and increased expenses during the transition period. Zero Trust solutions must operate alongside existing systems without introducing security risks or performance degradation, according to Vermeeren et al. (2015).
- Cost and Resource Intensity: Implementing Zero Trust Architecture requires significant financial resources, as it necessitates advanced technology systems and specialized personnel to operate these complex systems. Organizations need to budget for training expenses and technology purchases to establish an effective Zero Trust environment (Micu et al., 2019).
- User Experience (UX): A Zero Trust system requires designers to create an optimal user experience by striking a balance between security measures and user-friendly interfaces. The implementation of multiple security checks for MFA and other authentication methods should be carefully managed, as excessive security requests can lead to user dissatisfaction and performance decline. The system needs to achieve minimal user resistance through secure design elements, which will enhance both user satisfaction and system compliance (Law et al., 2008).
- Performance Overhead: Implementing Zero Trust security through continuous validation and encryption can create system performance delays due to its inherent operational overhead. The performance overhead from Zero Trust security becomes most problematic when organizations need to process data in real-time. Organizations need to optimize their network infrastructure to manage increased system load while preserving service quality standards (Sharma et al., 2016).

Organizations need to implement a complete solution that combines technical answers with educational programs and cultural development initiatives to achieve Zero Trust adoption while preserving operational efficiency and user contentment.

VIII. FUTURE TRENDS AND THE EVOLVING LANDSCAPE

The development of Zero Trust Architecture (ZTA) depends on multiple emerging trends and technological developments, which shape its current state. Zero Trust implementations receive essential support from Artificial Intelligence (AI) and Machine Learning (ML) technologies, which deliver advanced behavioral analytics, automated policy enforcement, and anomaly detection capabilities. AI/ML technologies process extensive data collections to detect abnormal patterns, which leads to improved security through immediate threat identification and response systems (Balcıoğlu, 2024; Ssetimba et al., 2024). AI-driven solutions help organizations meet regulatory requirements efficiently in complex sectors like fintech through their ability to perform real-time data analysis and automate compliance processes (Saiyed, 2025). The implementation of Zero Trust principles in Internet of Things (IoT) and Operational Technology (OT) networks becomes essential for protecting these quickly expanding environments. The numerous connected devices in IoT and OT networks create extensive attack surfaces because of their large number of entry points. Organizations can minimize security risks through Zero Trust implementation by requiring strict verification of all devices and network transactions (Akhter et al., 2025; Dada et al., 2024). Identity-Centric Security represents an ongoing development that shifts security operations from network-based controls to identity-based protection systems. Identity and access management stands as the central security element that verifies all entities before they can access protected systems and data. The approach gains its significance because organizations need to protect their data in hybrid and cloud environments where traditional

perimeter defenses become ineffective (Marengo, 2023). The adoption of Zero Trust strategies depends on regulatory compliance because ZTA frameworks have become mandatory for different industries. Organizations must adhere strictly to Zero Trust principles because regulatory bodies have established guidelines for implementing AI technology in compliance processes, which require digital operations to maintain transparency and accountability (Singhal, 2024; Torens et al., 2022). The evolving nature of Zero Trust security stems from its ability to address modern security threats that exist across various technological environments.

IX. CONCLUSION

The modern security perimeter has become obsolete because organizations have adopted cloud computing and mobile devices, and as a result, they have encountered increasingly advanced cyber threats (Stafford, 2020) (Basta, 2022). The paper demonstrates that Zero Trust Architecture (ZTA) represents the essential strategic security approach that protects contemporary digital business operations. ZTA establishes a robust defense system against both external and internal threats by eliminating outdated network-based trust assumptions in today's borderless digital environment. The research supported the paper's central argument through its explanation of Zero Trust fundamentals, which include the "never trust, always verify" principle and the defensive approach of "assuming breach," least privilege access rules, micro-segmentation, and continuous verification (Hammad, 2017). The research showed how these principles become operational through identity management, device security, data protection, and pervasive visibility technologies, which can be deployed through a structured migration process starting with essential assets (Micu et al., 2019). The path to complete Zero Trust implementation faces significant obstacles, which include cultural transformation, high implementation costs, and system complexity, yet organizations must adopt this model. The rising number of destructive cyberattacks makes it impossible for organizations to maintain their current security status. Zero Trust Architecture has evolved from an optional security measure into the essential framework that organizations must adopt to create a future-proof cybersecurity system that adapts to changing digital environments (Azad, 2024).

REFERENCES

[1]. Borchert, O., Souppaya, M., Kerman, A., Rose, S., & Howell, G. (2025). Implementing zero-trust architecture: National Institute of Standards Technology. https://doi.org/10.6028/nist.sp.1800-35

[2]. Ajish, D. (2024). The significance of artificial intelligence in zero trust technologies: a comprehensive review. Journal of Electrical Systems and Information Technology, 11(1). https://doi.org/10.1186/s43067-024-00155-z

[3]. Edo, O. C., Etu, E.-E., Ayuwu, A., Emakhu, J., Tenebe, T., & Adebiyi, S. (2022). Zero Trust Architecture: Trend and Impact on Information Security. International Journal of Emerging Technology and Advanced Engineering, 12(7), 140–147. https://doi.org/10.46338/ijetae0722_15

[4]. Kumar, R. (2024). An Extensive Analysis on Zero Trust Architecture. International Journal of Innovative Science and Research Technology (IJISRT), 1056–1061. https://doi.org/10.38124/ijisrt/ijisrt24may1225

[5]. Teerakanok, S., Inomata, A., & Uehara, T. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges. Security and Communication Networks, 2021, 1–10. https://doi.org/10.1155/2021/9947347

[6]. Chandramouli, R., & Butcher, Z. (2023). A zero-trust architecture model for access control in cloud-native applications in multi-location environments. National Institute Of Standards Technology. https://doi.org/10.6028/nist.sp.800-207a

[7]. Lund, B. D., Mannuru, N. R., Lee, T.-H., Wang, Z., & Wang, T. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. Encyclopedia, 4(4), 1520–1533. https://doi.org/10.3390/encyclopedia4040099

[8]. Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. Internet of Things, 27, 101227. https://doi.org/10.1016/j.iot.2024.101227

[9]. Ahn, G., Choi, S., Jang, J., & Shin, D. (2024). Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model with the MITRE ATT& CK Matrix. IEEE Access, 12, 89291–89309. https://doi.org/10.1109/access.2024.3417182

[10]. Hammad, M., Bagheri, H., & Malek, S. (2017). Determination and Enforcement of Least-Privilege Architecture in Android. 59–68. https://doi.org/10.1109/icsa.2017.18

[11]. Basta, N., Walker, A., Kaafar, M. A., & Ikram, M. (2022). Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework. 1–7. https://doi.org/10.1109/noms54207.2022.9789888

[12]. Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation. 1–6. https://doi.org/10.1109/infocomwkshps51825.2021.9484645

[13]. Ejiofor, O., Olusoga, O., & Akinsola, A. (2025). Zero trust architecture: A paradigm shift in network security. Computer Science & IT Research Journal, 6(3), 104–124. https://doi.org/10.51594/csitrj.v6i3.1871

[14]. Anderson, J., & Nguyen, A. (2022). The Role of Identity and Access Management (IAM) in Securing Cloud Workloads. ResearchGate December.

[15]. Prajapati, V. (2025). Role of Identity and Access Management in Zero Trust Architecture for Cloud

Security: Challenges and Solutions. International Journal of Advanced Research in Science, Communication and Technology, 6–18. https://doi.org/10.48175/ijarsct-23902

[16]. Kumar, R. (2024). An Extensive Analysis on Zero Trust Architecture. International Journal of Innovative Science and Research Technology (IJISRT), 1056–1061. https://doi.org/10.38124/ijisrt/ijisrt24may1225

[17]. Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. Internet of Things, 27, 101227. https://doi.org/10.1016/j.iot.2024.101227

[18]. Dhiman, P., Hamid, Y., Kaur, A., Saini, N., Nisa, K. U., Gulzar, Y., & Turaev, S. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors, 24(4), 1328. https://doi.org/10.3390/s24041328

[19]. Daah, C., Awan, I., Konur, S., & Qureshi, A. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. Electronics, 13(5), 865. https://doi.org/10.3390/electronics13050865

[20]. Adamson, K. M., & Qureshi, A. (2025). Zero Trust 2.0: Advances, Challenges, and Future Directions in ZTA. Springer Science Business Media Llc. https://doi.org/10.21203/rs.3.rs-6602547/v1

[21]. He, Y., Ma, X., Chen, L., Ni, Y., & Huang, D. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. Wireless Communications and Mobile Computing, 2022, 1–13. https://doi.org/10.1155/2022/6476274

[22]. Syed, N. F., Shah, S. W., Doss, R., Shaghaghi, A., Anwar, A., & Baig, Z. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access, 10, 57143–57179. https://doi.org/10.1109/access.2022.3174679

[23]. Vanickis, R., Dehghanzadeh, S., Lee, B., & Jacob, P. (2018). Access Control Policy Enforcement for Zero-Trust-Networking. 1–6. https://doi.org/10.1109/issc.2018.8585365

[24]. Shipman, M. E., Millwater, N., Smith, S., & Owens, K. (2024, April 9). A Zero Trust Architecture for Automotive Networks. https://doi.org/10.4271/2024-01-2793

[25]. Bertino, E. (2021). Zero Trust Architecture: Does It Help? IEEE Security & Privacy, 19(5), 95–96. https://doi.org/10.1109/msec.2021.3091195

[26]. Torens, C., Dauer, J. C., & Durak, U. (2022, January 3). Guidelines and Regulatory Framework for Machine Learning in Aviation. https://doi.org/10.2514/6.2022-1132

[27]. Singhal, S. (2024). Data Privacy, Compliance, and Security Including AI ML (pp. 111–126). Igi Global. https://doi.org/10.4018/979-8-3693-2909-2.ch009

[28]. Balcıoğlu, Y. S. (2024). Revolutionizing Risk Management AI and ML Innovations in Financial Stability and Fraud Detection (pp. 109–138). Igi Global. https://doi.org/10.4018/979-8-3693-4382-1.ch006

[29]. Dada, M., Daraojimba, O., Oliha, J., Nwokediegwu, Z., Majemite, M., & Obaigbena, A. (2024). Review of smart water management: IoT and AI in water and wastewater treatment. World Journal of Advanced Research and Reviews, 21(1), 1373–1382. https://doi.org/10.30574/wjarr.2024.21.1.0171

[30]. Akhter, S., Arefin, J., Zishan, M. S. R., Amanul Islam, M., Bhuyan, M. H., Hossen, M. S., & Taslim, S. M. B. (2025). Neuro-Symbolic AI for IoT-Driven Smart Cities: A Next-Generation Framework for Urban Intelligence. Journal of Computer Science and Technology Studies, 7(2), 36–55. https://doi.org/10.32996/jcsts.2025.7.2.4

[31]. Ssetimba, I., Nakayenga, H., Pinyi, E., Kato, J., Twineamatsiko, E., & Muhangi, E. (2024). Advancing electronic communication Compliance and fraud detection Through Machine Learning, NLP and Generative AI: A Pathway to Enhanced Cybersecurity and Regulatory Adherence. World Journal of Advanced Research and Reviews, 23(2), 697–707. https://doi.org/10.30574/wjarr.2024.23.2.2364

[32]. Marengo, A. (2023). The Future of AI in IoT: Emerging Trends in Intelligent Data Analysis and Privacy Protection. Mdpi Ag. https://doi.org/10.20944/preprints202312.2184.v1

[33]. Saiyed, A. (2025). AI-Driven Innovations in Fintech: Applications, Challenges, and Future Trends. International Journal of Electrical and Computer Engineering Research, 5(1), 8–15. https://doi.org/10.53375/ijecer.2025.437

[34]. Ogundipe, D., Edunjobi, T., & Odejide, O. (2024). Agile methodologies in digital banking: Theoretical underpinnings and implications for customer satisfaction. Open Access Research Journal of Science and Technology, 10(2), 021–030. https://doi.org/10.53022/oarjst.2024.10.2.0045

[35]. Sharma, M., Tiwari, P., & Chaubey, D. S. (2016). Summarizing Factors of Customer Experience and Building a Structural Model Using Total Interpretive Structural Modelling Technology. Global Business Review, 17(3), 730–741. https://doi.org/10.1177/0972150916630825

[36]. Law, E., Roto, V., Hassenzahl, M., Vermeeren, A. P. O. S., & Kort, J. (2008). Towards a shared definition of user experience. 2395–2398. https://doi.org/10.1145/1358628.1358693

[37]. Vermeeren, A. P. O. S., Roto, V., & Väänänen, K. (2015). Design-inclusive UX research: design as a part of doing user experience research. Behaviour & Information Technology, 35(1), 21–37. https://doi.org/10.1080/0144929x.2015.1081292

[38]. Micu, A. E., Bouzaabia, R., Bouzaabia, O., Micu, A., & Capatina, A. (2019). Online customer experience in e-retailing: implications for web entrepreneurship. International Entrepreneurship and Management Journal, 15(2), 651–675. https://doi.org/10.1007/s11365-019-00564-x

[39]. It's official: Zero Trust is now favored by 96% of organizations. (n.d.). https://www.okta.com/blog/industry-insights/its-

official-zero-trust-now-favored-by-96-of-organizations/
[40]. Stafford, V. (2020). Zero trust architecture. NIST special publication, 800(207), 800-207.
[41]. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 2022(1), 6476274.
[42]. Bertino, E. (2021). Zero trust architecture: does it help? IEEE Security & Privacy, 19(05), 95-96.
[43]. Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces, 89, 103832.
[44]. Moruff, O. A. (2024). ON THE EMERGENCE OF ZERO TRUST ARCHITECTURE IN ENTERPRISE NETWORKS-A SURVEY ON IMPLEMENTATION METHODS, STRENGTHS AND OPEN PROBLEMS. In International Conference on Technological Solutions for Smart Economy| SmartEco (p. 299).
[45]. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. IEEE access, 10, 57143-57179.
[46]. Taskin, E. (2025). Transitioning from Individual Implementation of Zero Trust Architecture to AI-driven Tools: Reducing Manual Workloads and Increasing Efficiency through AI in ZTA.