IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

Zero-Trust Technology and Industry Development: Architecture, Key Technologies, Opportunities and Challenges

Rohit Bhausaheb Jarhad[1], Prof. Y. G. Suryavanshi[2], Dr. H. B. Jadhav[3]
[1] Student,[2] Assistant Professor,[3] Head of Department
Department of Computer Engineering,
Adsul's Technical Campus, Chas, India

Abstract: *Zero-trust is a network security architecture built on the principle of "never trust, always verify." It replaces the traditional assumption that everything inside a network perimeter is trustworthy with continuous verification, dynamic authorization and least-privilege access. This paper presents a structured review based on the IEEE SA Industry Connections Report IC24-08, "Zero-Trust Technology and Industry Development" (Mu and Chai, CAICT). It reorganizes the report's findings into a review format covering the history and strategic value of zero-trust, the three key industry players (producers, consumers and market managers), the eight key technologies of the overall architecture, and the opportunities and challenges of zero-trust in five scenarios: 5G, Internet of Vehicles, Internet of Things, Industrial Internet and Computing Power Network. The review shows that zero-trust offers strong security benefits in all five scenarios, while cost, processing latency, operational complexity, legacy equipment and cross-domain trust remain the main obstacles. The paper can help students and researchers understand the current landscape of zero-trust and identify areas for further study.*

Keywords: Zero-Trust, Network Security, Never Trust Always Verify, Micro-Segmentation, 5G, Internet of Vehicles, Internet of Things, Industrial Internet, Computing Power Network

I. INTRODUCTION

Zero-trust is a network security paradigm centered on resource protection. It was first introduced in 2010 by Forrester analyst John Kindervag, who argued that all network traffic is untrustworthy and that every request for any resource needs security control [1][2]. This idea challenged the traditional border (perimeter) security model and attracted wide attention from the network security industry.

Standardization followed. In 2014 the Cloud Security Alliance (CSA) released the SDP Specification v1.0, an early step in one of the three major technology routes of zero-trust, the software-defined perimeter. CSA later published the SDP Architecture Guide v2 (2019), a white paper on SDP and Zero Trust, and SDP Specification v2.0 (2022). In 2019 the U.S. National Institute of Standards and Technology (NIST) released the draft Zero Trust Architecture, later published as NIST SP 800-207 [3], which marked the formal start of zero-trust standardization.

Zero-trust protects modern digital environments by segmenting networks, preventing lateral movement, providing threat prevention and simplifying fine-grained user access control. It integrates cloud-native technology, software-defined security, identity management, data security and micro-isolation to move from passive "patching" defense to native, continuous security. Together with progress in cloud, networking, artificial intelligence (AI) and big data, it has become a mainstay of the network security guarantee system.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-40459

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

II. PROBLEM STATEMENT AND RESEARCH GAP

Problem statement: Digital transformation, 5G, cloud computing, the Internet of Things (IoT), connected vehicles and industrial networks have dissolved the clear boundary between "inside" and "outside" the network. Traditional perimeter-based defense assumes that internal assets can be trusted, so a single breach allows attackers to move laterally and the attack surface keeps growing.

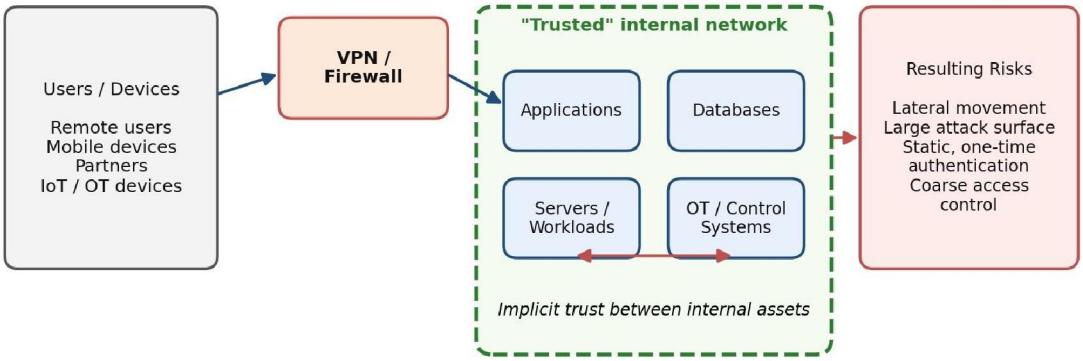
Research Gap: Zero-trust market is fragmented. Technical standards, security concepts and implementation solutions differ widely between vendors, and most current zero-trust schemes are simple integrations of discrete security modules. Their suitability for latency-sensitive, cost-sensitive and legacy environments is not yet fully settled.

Research Questions: (1) What are the key technologies of a zero-trust architecture? (2) What opportunities does zero-trust create in 5G, IoV, IoT, Industrial Internet and Computing Power Network scenarios? (3) What challenges must be solved for its large-scale adoption?

III. EXISTING SYSTEM

The diagram below shows the existing, perimeter-based security model. Users and devices reach internal applications through a VPN or firewall. Once access is granted, internal assets are implicitly trusted, which creates risks such as lateral movement, a large attack surface and static, one-time authentication.

Existing System: Traditional Perimeter-Based Security



Once the perimeter is crossed, an attacker can move freely inside the network.

Fig 1: Existing System – Traditional Perimeter-Based Security Model.

Working of existing system:

1. User Request: Users, partners and devices request access to applications and data, often through a VPN.
2. Perimeter Check: A firewall or VPN authenticates the user once at the network edge.
3. Implicit Trust: After entry, the user or device can reach many internal systems because the internal network is treated as trusted.
4. Limited Visibility: Security monitoring is mostly concentrated at the border, so internal movement is hard to detect.
5. Impact: One compromised account or device can expose applications, databases and control systems. The model also struggles with cloud, mobile and IoT access.

IV. PROPOSED SYSTEM

The proposed system is a zero-trust architecture that strictly follows the principle "never trust, always verify." Every access request, whether from inside or outside the network, is authenticated, authorized and encrypted. Trust is

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

evaluated continuously using identity, device state, network condition and real-time risk, and access is limited to the minimum privilege needed.

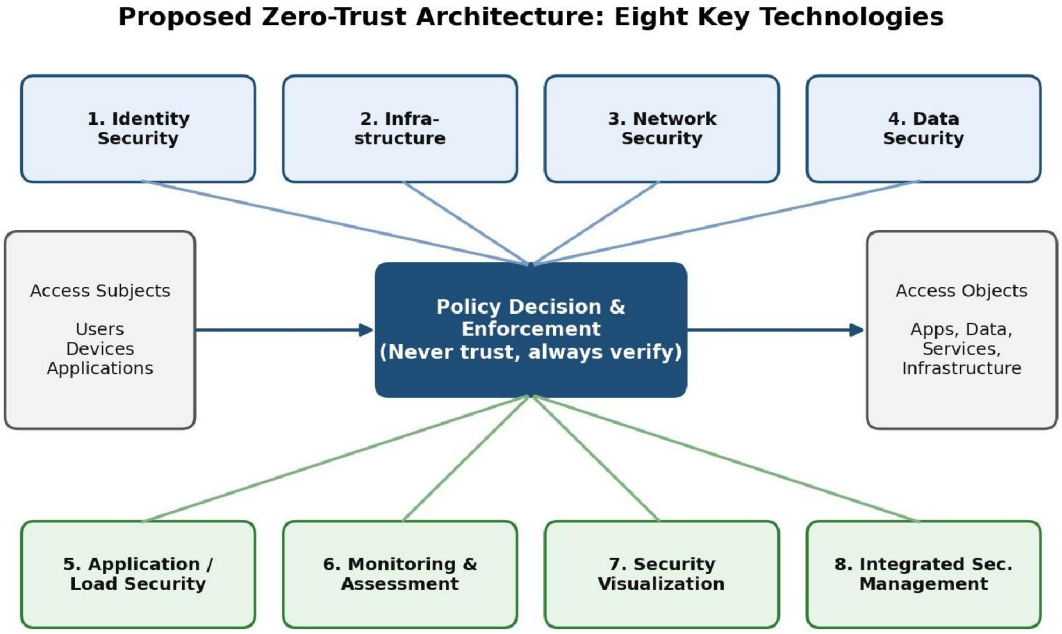


Fig 2: Proposed Zero-Trust Architecture with Eight Key Technologies.

The architecture contains eight key technologies: identity security, infrastructure, network security, data security, application/load security, security monitoring and assessment, security visualization, and integrated security management. A successful deployment is a systematic project; the organization should also upgrade its information security management and personnel management together with the technical measures.

Key players in the zero-trust industry

The report identifies three key players. Zero-trust product producers integrate resources, design and deliver solutions and promote large-scale production. Zero-trust product consumers are enterprise users who order products, solutions and services from the industry marketplace to protect their digital assets. Zero-trust market managers build the standard system, standardize product capabilities, improve evaluation schemes and provide supply–demand exchange platforms. The current market is fragmented, and Security as a Service (SECaaS) is the mainstream delivery model internationally, while solution-based delivery dominates in China in the short term.

V. PROPOSED ZERO-TRUST FRAMEWORK

Working of Proposed System

Sr. No.	Module	Description
1	Identity Security	Unified authentication, authorization and auditing of all entities (people, devices, applications, networks); continuous identity evaluation.
2	Infrastructure	Network, computing and business-system base that hosts access control and security audit; must be stable, inclusive and scalable.
3	Network Security	Network control mechanism, data security, access, defense and threat protection to enforce flexible access control.
4	Data Security	Collection, classification, grading, isolation, encryption, control and monitoring of data regardless of its location.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

5	Application / Load Security	Application access control, load management, dynamic trust assessment and dynamic privilege control.
6	Monitoring and Assessment	Continuous acquisition and analysis of security events, risk-model based judgement and response advice.
7	Security Visualization	Identity, terminal, application, network and data/breach visibility with event analysis and automated response.
8	Integrated Security Management	Coordination of all technologies with security management, personnel management and operations.

Table 1: Key technologies of the proposed zero-trust framework.

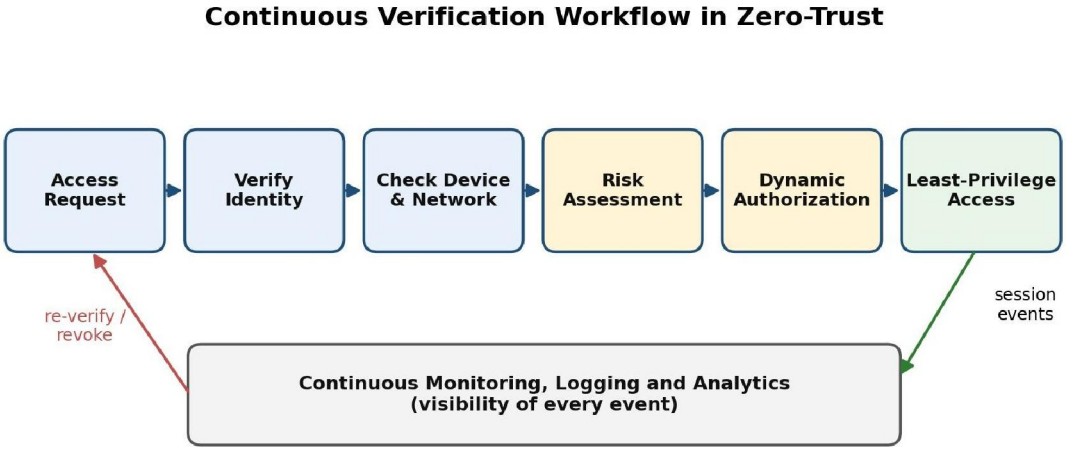


Fig 3: Continuous Verification Workflow in Zero-Trust.

Fig 3 shows the working flow. A request is verified for identity, then for device and network state. A risk assessment feeds a dynamic authorization decision and least-privilege access is granted. Monitoring continues during the session, and access can be re-verified or revoked when risk changes.

VI. RESULTS AND DISCUSSIONS

This review examines zero-trust in five application scenarios. The results are qualitative findings of the source report; no new experiments were conducted. Fig 4 shows adoption indicators reported in the cited sources: Gartner forecast that by 2022, 80% of new digital business applications opened to ecosystem partners would be accessed through zero-trust network access, and that by 2023, 60% of enterprises would replace most remote-access VPNs with zero-trust [4]. A Palo Alto Networks survey found that 44% of IT decision-makers in mainland China believed they should use network micro-segmentation to isolate IoT devices [5].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

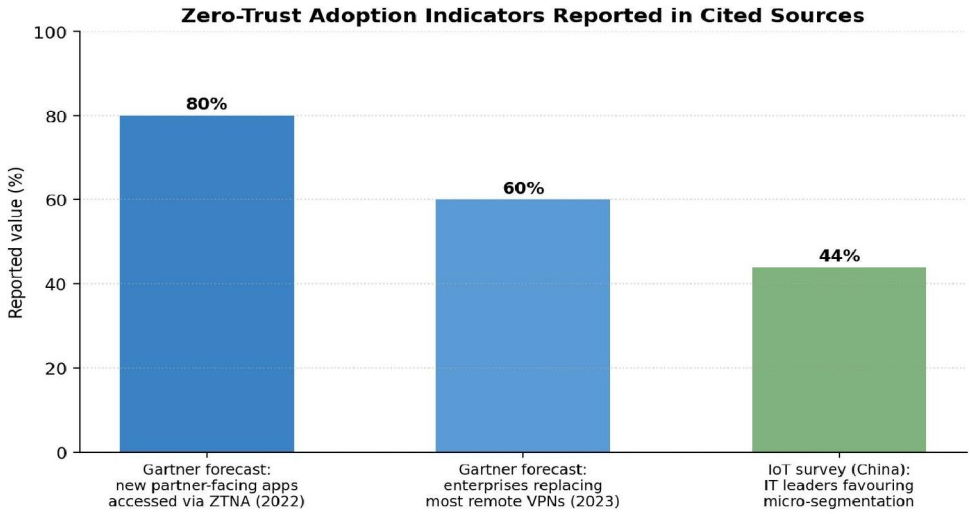


Fig 4: Zero-Trust Adoption Indicators Reported in Cited Sources.

A. 5G Scenario

The 5G core network is built on the 3GPP Service-Based Architecture, in which network functions (NFs) communicate through service-based interfaces. As NFs grow and interact in more complex ways, the attack surface expands. In containerized deployments, NF containers within a Pod trust each other by default, which is a risk under zero-trust thinking. Zero-trust can remove this default trust through authentication, micro-isolation and continuous monitoring, and can support vulnerability scanning and compliance checks over the container lifecycle. Challenges are higher construction cost, added processing delay (especially for uRLLC and mMTC services) and harder operation and maintenance when IP/port rules are replaced by identity- and application-based rules; distributed security schemes and automated operations are suggested.

B. Internet of Vehicles (IoV) Scenario

Smart vehicles have frequent vulnerability reports, including one in widely used open-source software that allowed remote control of vehicle functions. Zero-trust can improve IoV security through micro-isolation of cloud platforms, supply-chain security management of open-source and commercial software, and terminal security for T-Boxes. The main challenge is latency: at 120 km/h a vehicle moves about 33 meters per second, so delay can be critical. The report states that the processing delay added by zero-trust checks should be kept between 1 ms and 10 ms to keep pace with 5G.

C. Internet of Things (IoT) Scenario

IoT devices blur the boundary between the physical and digital worlds and enlarge the attack surface. Zero-trust can use AI for automated device discovery, automatic security baselines, recommended security rules and continuous monitoring for abnormal behavior. The main challenge is cost: the value of one device is small, and the security investment per device should not exceed about 10% of its value.

D. Industrial Internet Scenario

Integration of IT and operational technology (OT) has broken the closed, trusted environment of traditional industrial networks. Zero-trust enables authentication, authorization and encryption for all access requests and real-time risk assessment across the industrial intranet, edge, cloud platform and Internet layers. Challenges include networks that cannot be fully isolated, legacy OT systems on which endpoint security software cannot be installed, high-availability requirements that limit online monitoring devices, and future IoT-style OT devices that no longer follow the Purdue model.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

E. Computing Power Network Scenario

A computing power network integrates distributed computing nodes, networks and services. Zero-trust (strong identity governance, micro-segmentation, ZTNA, continuous monitoring and dynamic application authorization) can support its overall security system and raise the risk awareness of operation staff. Open challenges include securing transactions, billing and settlement without reducing efficiency, new threats such as algorithm poisoning, uncontrollable ubiquitous nodes, zero-trust across multiple computing power networks, and the need to converge discrete security modules into a SaaS-style offering.

Scenario	Key Opportunity	Key Challenge
5G Network	Remove implicit trust between NF containers	Cost, added delay, operation complexity
Internet of Vehicles	Micro-isolation, supply-chain & T-Box security	Delay budget of 1-10 ms
Internet of Things	AI-based discovery, baselines & monitoring	Per-device security cost (<=10% of value)
Industrial Internet	Authenticate all requests; dynamic risk-based control	Legacy OT, high availability, non-isolated networks
Computing Power Network	Identity governance, ZTNA, continuous monitoring	Cross-network trust, algorithm poisoning

Fig 5: Summary of Zero-Trust Opportunities and Challenges by Scenario.

F. Discussion

Across all scenarios the same trade-off appears: zero-trust adds verification, monitoring and policy management, which improves security but increases cost, latency and operational complexity. Distributed security, automation, AI-assisted policy generation and SaaS delivery are the main directions to reduce this burden.

VII. LIMITATIONS OF THIS REVIEW

This paper is a structured review and synthesis based primarily on the supplied IEEE SA Industry Connections Report IC24-08. It does not independently test or implement a zero-trust system, and the reported figures (such as adoption forecasts, the 1–10 ms delay target and the 10% cost guideline) are those of the source report and its cited sources. The review also inherits the report's limitations, including its focus on selected scenarios and the fact that the report is not an IEEE standard. Fig 1–3 and Fig 5 are conceptual illustrations prepared from the report's text.

VIII. CONCLUSION

Zero-trust, based on "never trust, always verify," gives a practical security model for the digital economy. Its eight key technologies work together to provide continuous identity verification, micro-segmentation, dynamic authorization and visibility. It offers clear benefits in 5G, Internet of Vehicles, IoT, Industrial Internet and Computing Power Network scenarios. However, cost, added latency, operation complexity, legacy OT equipment and cross-network trust still need to be addressed. Future work should focus on lightweight and distributed zero-trust schemes, automated operations, standardization of the fragmented market and measurable evaluation methods.

IX. ACKNOWLEDGMENT

I would like to express my sincere gratitude to everyone who helped and supported me in completing this project on "Zero-Trust Technology and Industry Development." I especially thank my project guide for the valuable guidance, support and suggestions throughout the work.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

REFERENCES

1. Y. Mu and Y. Chai, "Zero-Trust Technology and Industry Development," IEEE SA Industry Connections Report IC24-08, Computing and Network Convergence Initiative, IEEE, New York, NY, USA, 2025.
2. J. Kindervag, "No more chewy centers: the zero trust model of information security," Forrester Research, 2016.
3. NIST, "Zero Trust Architecture," NIST Special Publication 800-207.
4. S. Riley, N. MacDonald, and L. Orans, "Market Guide for Zero Trust Network Access," Gartner Report, 8 Jun. 2020.
5. Palo Alto Networks, "The Connected Enterprise: IoT Security Report 2021," Santa Clara, CA, USA, 2021