Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Zero-Trust Security Architecture for AI-Integrated Private 5G Networks

Vijayakumar Venganti
Jawaharlal Nehru Technological University, Hyderabad, India
Corresponding Author: Vijayakumar Venganti, **E-mail**: vijayvenganti@gmail.com

| ABSTRACT

Private 5G networks represent a transformative evolution in enterprise connectivity, blending reliability, ultra-low latency, and customizability for diverse applications. As organizations deploy these networks in manufacturing facilities and university campuses, integrating artificial intelligence creates both opportunities and security challenges. Traditional perimeter-based security models prove inadequate in these dynamic environments where devices move across network slices and workloads shift between edge and cloud. This article proposes an innovative Zero-Trust Security Architecture for AI-integrated private 5G networks, operating on the principle of "never trust, always verify" while leveraging AI for continuous authentication, behavioral analysis, and automated policy enforcement. The architecture's four-layer framework—Access, Transport & Segmentation, Policy & Intelligence, and Control & Orchestration—addresses the unique challenges of securing these environments. Key components include AI-powered identity management, micro-segmentation through network slicing, predictive threat detection, and a centralized governance layer. This comprehensive article enables organizations to maintain security integrity while fully leveraging the transformative potential of AI-integrated private 5G networks in critical infrastructure settings.

| KEYWORDS

Zero-Trust Architecture, Private 5G Security, AI-Enhanced Cybersecurity, Network Slicing, Behavioral Authentication

| ARTICLE INFORMATION

ACCEPTED: 20 October 2025 **PUBLISHED:** 05 November 2025 **DOI:** 10.32996/jcsts.2025.7.11.21

1. Introduction

Private 5G networks have become the backbone for enterprise digital transformation in several verticals. Unlike public deployments, enterprise 5G offers an end-to-end spectrum, core services, and security policy control to enterprises, therefore, endorsing deterministic performance of mission-critical workloads. According to industry research, the adoption of a private 5G is still growing in popularity as companies require greater control over their connectivity infrastructure to support more data-intensive workloads. The industrial and manufacturing sectors head this adoption curve, propelled by the demand for ultra-reliable low-latency communications (URLLC) in support of real-time control systems. Niral Networks' exhaustive analysis of private 5G deployments indicates that companies that deploy dedicated private cellular networks achieve up to three times higher levels of operational reliability and much less downtime than those dependent on public infrastructure, especially in scenarios with high electromagnetic interference or physical barriers [1]. Two sectors specifically ready to take advantage are manufacturing plants—where robotics, automated guided vehicles (AGVs), and industrial IoT are the norm—and university campuses, where AR/VR classrooms, high-bandwidth research networks, and telemedicine training demand high-performance, secure connectivity.

The addition of AI in network operations brings opportunities, but also threats. As AI algorithms help classify traffic, predict network maintenance, and detect anomalies, they at the same time become new attack surfaces in case they are compromised. Current research by Palo Alto Networks' threat intelligence groups shows that AI-boosted private 5G networks can detect potential security breaches ahead of time through advanced pattern recognition features constantly monitoring network activity

for anomalies across huge numbers of connected devices. Their deployments in industrial environments have demonstrated the capability of AI-based intrusion detection systems at the network edge to analyze patterns of traffic from tens of thousands of sensors in real-time, recognizing subtle anomalies imperceptible to conventional rule-based systems. But these same systems are confronted by complex threats specifically aimed at disrupting their learning mechanisms. Security researchers have reported growing examples of adversarial methods that intentionally manipulate input streams of data to trigger AI misclassifications. In testing environments, well-crafted adversarial examples in a high percentage of test cases were able to successfully make security algorithms misclassify hostile traffic as legitimate, demonstrating the double-edged nature of AI integration [2]. For example, adversarial ML inputs can misclassify malicious traffic as legitimate, so attacks can evade security controls.

Legacy perimeter-based security models, which were intended for static LAN or VPN topologies, are inadequate in dynamic 5G environments where devices travel at speeds across slices, workloads migrate from edge to cloud and back, and user mobility dissolves legacy trust boundaries. Niral Networks' longitudinal research monitoring device movement behavior within private 5G installations proves that industrial mobile robots and autonomous systems regularly move between distinct network zones as they traverse production environments, necessitating ongoing security validation instead of point-in-time authentication. Their observations of manufacturing deployments in the real world indicate that in cutting-edge plants, each device is connected to dozens of various endpoints every day, forming intricate trust relationships that no traditional security models can handle well [1]. Such models, which presume traffic and devices within the network boundary are secure, have inherent flaws in such a scenario. Palo Alto Networks' threat intelligence indicates that in contemporary industrial settings, the interconnectivity complexity of devices offers exponentially more lateral movement opportunities following the initial compromise. Their Industrial IoT security audits routinely discover that conventional network segmentation cannot provide for the dynamic nature of contemporary industrial processes, where ad hoc trust relationships are created between once-separate systems on a regular basis. Based on their incident response groups, the complexity of supply chain attacks has matured precisely to compromise these trust assumptions, with tainted firmware or software updates as primary access vectors bypassing traditional security screening [2]. Malicious insiders, compromised IoT devices, or supply chain attacks can readily compromise these defenses to reach valuable assets. Zero-trust strategies in this setting become not best practice but a necessity.

Aspect	Challenges	Zero-Trust Solutions
Network Architecture	Dynamic environment with fluid perimeters	Continuous verification regardless of connection status
Device Connectivity	Frequent transitions between network zones	Micro-segmentation through network slicing
AI Integration	New attack surfaces are vulnerable to adversarial inputs	AI-powered anomaly detection and behavioral analysis
Manufacturing Sector	Operational technology/IT convergence risks	Real-time security verification for robotics and AGVs
Education Sector	Complex digital ecosystems with bandwidth spikes	Dynamic policy enforcement for research networks
Traditional Security	Inadequate monitoring of internal traffic	East-west traffic analysis and lateral movement prevention
Authentication	Point-in-time verification insufficient	Continuous behavioral authentication
Threat Response	Reactive detection after compromise	Predictive security with simulation-based threat modeling

Table 1: Security Paradigm Shift: Challenges and Solutions for AI-Integrated Private 5G Networks [1, 2]

2. Problem Statement

2.1 Manufacturing Challenges

Manufacturing facilities that adopt Private 5G for industrial automation have serious security concerns. Production facilities are especially exposed environments, given their intricate mesh of operational technology with information technology systems. Research found in the Science Direct Journal of Industrial Networks, the merging of OT/IT in intelligent manufacturing has introduced unprecedented security threats, and industrial connected systems produce immense operational data daily. Control

messages with ultra-low latency are exchanged between robots and AGVs, with industrial communications research reporting that ultra-reliable low-latency communication is needed by collaborative robotic systems to ensure safe operation [3]. If the attackers laterally take control of an AGV, they may be able to manipulate its path to induce collisions or production loss. Industrial sensors gathering operational data may be compromised, causing predictively incorrect maintenance results. In addition, firmware-based attacks on robots or PLCs may go on undetected for months if security models are based on static perimeters.

2.2 Campus Challenges

Universities implementing immersive technologies have distinctive security challenges. Boldyn Networks' analysis of higher education connectivity shows that contemporary university campuses have become highly sophisticated digital ecosystems blending research networks, administrative systems, student services, and education technology platforms. AR headsets are bandwidth-intensive, and when several devices are used together in classrooms, network requirements skyrocket [4]. Malicious actors hacking AR traffic flows would be able to crash classes or spread malicious content. In research, cross-border collaboration involves the secure transfer of sensitive data, for example, genomic information or defence projects. The conventional VPN firewalls do not offer adequate protection when workloads are dynamically redistributed across slices and Multi-access Edge Computing nodes.

2.3 Drawbacks of Classic Security

Classic perimeter security uses gateways and firewalls to establish a "moat" around networks. In AI-integrated private 5G, this model is insufficient for the following reasons: Dynamic perimeters make fixed security impractical, as most IoT devices are unshielded by their nature. Lateral movement attacks arise when classic defense mechanisms are incapable of scanning internal traffic. AI models themselves become targets of data poisoning or model stealing. Current security mechanisms depend on static rules with no real-time context adaptation. The larger attack surface of many connected devices provides exponential vulnerability proliferation. Latency requirements of manufacturing and educational use cases introduce security versus performance tradeoffs. Insecure authentication in multifarious device ecosystems poses unauthorized access risks, particularly in open campus networks where user populations change wildly during academic cycles [3][4].

Sector	Vulnerability Type	Impact	Zero-Trust Mitigation
Manufacturing	Lateral Movement	AGV trajectory manipulation	Continuous authentication
	Firmware Attacks	Extended undetected presence	Device integrity verification
	Sensor Tampering	Incorrect maintenance predictions	Real-time data validation
	OT/IT Convergence	Expanded attack surface	Micro-segmentation
Education	AR/VR Traffic Hijacking	Classroom disruption	Traffic isolation through slicing
	Research Data Protection	Sensitive information exposure	Dynamic access control
	Dynamic User Population	Authentication challenges	Behavioral analytics
	Cross-border Collaboration	Data sovereignty issues	Context-aware policy enforcement

Table 2: Sector-Specific Vulnerabilities in Private 5G Networks [3, 4]

3. Related Work

3.1 3GPP Standards

Release 16/17 of 3GPP added network slicing security features and MEC platform integration. These standards define minimum security requirements for 5G network elements, such as authentication mechanisms, encryption algorithms, and procedures for slice isolation. The GSMA's detailed security evaluation framework for mobile networks states that, whereas 3GPP standards offer solid security features for core network operations, they are more concerned with threats particular to telecommunications than enterprise security issues. The GSMA structure points out that 3GPP security controls were conceived with public network architectures in mind and focus on subscription authentication and radio interface protection [5]. These are foundation controls but do not prescribe enterprise-class zero-trust models, with key implementation questions left to organizations rolling out private 5G networks to critical infrastructure environments.

3.2 NIST Zero-Trust

NIST SP 800-207 defines Zero-Trust as zero trust, detect and validate, and concentrates on the controls that are identity-based and continuous risk evaluation. It is one of the greatest changes in relation to traditional perimeter-based security paradigms because it requires continuous authentication regardless of the location or network connectivity. The NIST model categorically mentions that "a zero trust architecture is designed to prevent data breaches and limit internal lateral movement" through the adoption of micro-segmentation and detailed perimeter enforcement on the basis of users, assets, and resources [6]. Nonetheless, it delivers abstract principles instead of 5G implementations, and it needs much adjustment to wireless environments where connection state, mobility, and radio interface characteristics add security concerns not treated by the abstract model.

3.3 AI in 5G Security

There has been shown ML capability for anomaly detection, especially for Distributed Denial of Service (DDoS) traffic and botnets within 5G networks. Current security research has discussed a range of machine learning techniques for monitoring network traffic behavior, detecting potential attacks, and implementing automated response procedures. The GSMA security risk assessment framework recognizes the emerging use of AI to augment threat detection capability, observing that advanced analytics can detect nuanced attack patterns that signature-based systems may fail to detect [5]. However, most research is devoid of integration with slice-aware policies or URSP-based routing, which leaves a gap between theoretical studies and real-world applications in production 5G networks. This research gap hampers organizations from exploiting AI capabilities in full within their security framework.

3.4 Research Gaps

There are some crucial gaps in research presently that restrict the practical application of end-to-end security frameworks to AI-integrated private 5G networks. Zero-Trust research does not usually take into account the special topology of 5G slices, which are logical network isolations with independent security needs and trust domains. NIST SP 800-207 recognizes that its abstract model has to be tailored to particular technology environments and explains that "there are several logical components that make up a zero trust architecture deployment" without actually detailing how these would correspond to 5G network functions or slices [6]. AI security research tends to overlook integration into enterprise Identity and Access Management (IAM) and Zero Trust Network Access (ZTNA) policies, developing silos among AI-based security elements and organization-wide security systems. Furthermore, there is no common architecture that covers both manufacturing and campus environments, and organizations are left patching together different approaches instead of having cohesive security strategies for various deployment scenarios [5].

Domain	Current State	Limitations	Research Needs
3GPP Standards	Network slicing security mechanisms	Telecommunications-focused rather than enterprise-oriented	Enterprise-grade zero-trust implementation guidelines
3GPP Standards	MEC platform integration	Public network architecture emphasis	Critical infrastructure adaptation frameworks
NIST Framework	"Never trust, always verify" principle	Abstract guidelines only	5G-specific implementation models
NIST Framework	Identity-centric controls	Limited wireless environment considerations	Adaptation for mobility patterns and radio interfaces
AI Security	Anomaly detection capabilities	Lacks integration with network slicing	Slice-aware policy implementation
AI Security	DDoS and botnet traffic analysis	Theoretical models without practical deployment	Production environment integration methods
Zero-Trust Research	General security frameworks	Ignores 5G slice topology	Slice-specific trust boundary models
Enterprise Integration	Separate security components	Siloed AI and IAM/ZTNA policies	Unified security architecture

Table 3: Critical Gaps in Private 5G Security Standardization [5, 6]

4. Innovative Solutions

To counter these challenges, this article suggests a new Zero Trust (ZT) security architecture for AI-integrated private 5G networks with AI-driven mechanisms for more robust verification and threat mitigation. This architecture is based on existing ZT frameworks but is innovative in its use of AI at various layers to develop a self-adaptive system. Ericsson's AI/ML security in telecommunications research identifies that the security of next-generation networks needs "automated, intelligent and adaptable solutions that can identify and respond to threats in real-time," especially as networks are increasingly software-defined and disaggregated [7].

The framework has four layers:

- Access Layer – where User Equipment (UEs) like robots, AGVs, AR/VR headsets, IoT sensors, and laptops connect to the 5G Radio Access Network (RAN). This layer enforces constant device verification regardless of connection or prior authentication state.
- Transport & Segmentation Layer – where traffic is segmented into logical network slices, each controlled by strict policies. Robust segmentation secures traffic being in the right places within the correct trust boundaries while preserving required performance properties.
- Policy & Intelligence Layer – wherein AI/ML engines resident at the MEC constantly evaluate traffic behavior, apply risk scores, and engage with policy enforcement capabilities. This layer is a quantum leap ahead of conventional rule-based security insofar as it employs real-time threat intelligence-based dynamic policy updates.
- Control & Orchestration Layer – where the Zero-Trust Controller applies enterprise-defined policies, integrates with Identity and Access Management (IAM), and dynamically updates User Rule Selection Policy (URSP) rules. This orchestration function provides consistent policy enforcement over heterogeneous network environments [8].

This layer-based structure ensures that in case one system segment is compromised (for instance, a hacking IoT device), lateral spread is instantly restricted by micro-segmentation and risk-adaptive routing.

4.1 The Core Elements of the Architecture

4.1.1 AI-Driven Identity and Access Management (IAM)

Conventional ZT is based on multi-factor authentication (MFA), but in this architecture, machine learning is used to examine behavioral patterns in real-time, dynamically adapting access rights. Anomaly detection software keeps tabs on user activity in 5G slices, detecting deviations like uncharacteristic data requests from AI agents. Ericsson's research on telecommunications security highlights that "AI and ML can significantly enhance the precision of anomaly detection by defining behavioral baselines for users, devices, and applications, then detecting deviations that can be indicative of compromise." Their examination further suggests that machine learning models can handle enormous volumes of network telemetry data to detect subtle patterns that would be impossible to detect by human analysts [7]. This predictive methodology enhances ZT by anticipating threats and mitigating false positives via contextual learning.

4.1.2 Micro-Segmentation with AI-Augmented Network Slicing

Private 5G's network slicing feature is utilized for ZT segmentation, where every slice has isolated policies in place. AI comes in here to optimize slice assignment based on threat intelligence, employing graph neural networks for modeling inter-slice dependencies and lateral movement prevention. IEEE 5G security architecture research highlights dynamic micro-segmentation as a key driver for zero-trust deployments in mobile networks, citing that "network slicing provides a natural enforcement point for policy-based access controls when augmented with continuous monitoring and verification" [8]. Static models would be different because this dynamic segmentation is AI workload-specific, causing minimal interference during peak-traffic conditions.

4.1.3 Predictive Threat Detection and Response

The architecture also includes generative AI in simulation-based threat modeling, predicting possible attacks on AI elements like model tampering on edge nodes. AI-fortified Extended Detection and Response (XDR) platforms include automated remediation, including isolating infected slices. As Ericsson's security research states, "predictive security is the new frontier in telecommunications defense where AI-based systems can model possible attack vectors and proactively adapt defenses prior to threats being realized." Their study proves that this method of operation can drastically shorten response times and reduce damages compared to classical reactive security patterns [7]. This advancement applies ZT concepts to offensive defense, merging security into the network fabric.

4.1.4 Hybrid Governance and Compliance Layer/Zero-Trust Controller

A unified AI-orchestrated dashboard imposes compliance throughout the ecosystem, correlating security boundaries and duties. This layer employs blockchain-inspired ledgers to provide immutable audit trails to ensure traceability in AI-driven decisions. IEEE zero-trust architecture research for telecommunications underscores that "centralized policy orchestration with distributed enforcement embodies the best model for ensuring consistent security posture across varied 5G deployment environments." The study also points out that "auditability and transparency in security decisioning procedures are critical to regulatory compliance and incident response in critical infrastructure deployments" [8].

It serves as the security ecosystem's brain, with some duties being:

- Aligning policies between IAM, slices, MEC AI engines, and the 5G core
- Orchestrating dynamic updates of URSP
- Integration with SIEM/SOAR systems for end-to-end visibility
- Feedback loop to enable AI-driven risk insights to update security posture directly

Layer	Components	Functions	AI Enhancement
Access Layer	UEs (robots, AGVs, sensors)	Continuous device verification	Real-time behavioral authentication
	RAN connectivity	Connection state monitoring	Device legitimacy validation
Transport & Segmentation	Network slices	Traffic isolation	Graph neural networks for dependency modeling

	Trust boundaries	Preventing lateral movement	Dynamic slice allocation
Policy & Intelligence	AI/ML engines at MEC	Traffic behavior assessment	Risk scoring based on pattern recognition
	Policy enforcement	Dynamic rule application	Contextual adaptation to threat landscape
Control & Orchestration	Zero-Trust Controller	Enterprise policy enforcement	Integration with IAM systems
	Blockchain-inspired ledgers	Immutable audit trails	AI-driven decision traceability

Table 4: Four-Layer Zero-Trust Framework for Private 5G [7, 8]

Conclusion

The Zero-Trust Security Architecture represents a pioneering approach to securing AI-integrated private 5G networks through principles that fundamentally reimagine cybersecurity for next-generation wireless environments. By embedding AI-driven security mechanisms throughout the network fabric, this architecture addresses the complex challenges facing both manufacturing and educational deployments, including expanded attack surfaces, lateral movement threats, and the protection of AI systems themselves. The layered framework enables dynamic policy adaptation, behavioral analytics, and proactive threat mitigation while maintaining the performance characteristics essential for mission-critical applications. Through continuous verification, micro-segmentation, and centralized orchestration, organizations can establish trusted operations in inherently untrusted environments. While current implementations remain nascent, this approach provides a blueprint for security that evolves alongside the rapidly advancing capabilities of both AI and private cellular networks. The fusion of zero-trust principles with cutting-edge AI security represents not merely an incremental improvement but a fundamental paradigm shift necessary to protect the increasingly intelligent and interconnected infrastructure underpinning enterprise digital transformation.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Niral Networks, "Transforming Enterprise Connectivity: The Strategic Advantage of Zero-Trust Security in Private 5G Networks," 2025. [Online]. Available: https://niralnetworks.com/transforming-enterprise-connectivity-the-strategic-advantage-of-zero-trust-security-in-private-5g-networks/
[2] Mitch Rappard and Andre Ferreira, "Enhance Private 5G Security for Industrial Deployments," Palo Alto Networks, 2025. [Online]. Available: https://www.paloaltonetworks.com/blog/2025/03/enhance-private-5g-security/
[3] Adel Alqudhaibi et al., "Securing industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management," Cyber Security and Applications, Volume 3, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S277291842400033X
[4] Boldyn Networks, "The Zero Trust Model in Higher Education – A Necessary Shift,". [Online]. Available: https://www.boldyn.com/blog/the-zero-trust-model-in-higher-education-a-necessary-shift
[5] GSMA, "5G Security Guide," 2024. [Online]. Available: https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/07/FS.40-v3.0-002-19-July.pdf
[6] Scott Rose et al., "Zero Trust Architecture," NIST Special Publication 800-207, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
[7] Andrey Shorov et al., "AI/ML security in mobile telecommunication networks," Ericsson Technology Blog, 2024. [Online]. Available: https://www.ericsson.com/en/blog/2024/4/ai-ml-security-in-mobile-telecommunication-networks
[8] Nurun Nahar et al., "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks," IEEE Access, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10589640