Zero Trust Network Access Enforcement for Securing Multi-Slice Architectures in 5G Private Enterprise Deployments

Ugoaghalam Uche James[1]; Onuh Matthew Ijiga[2]; Lawrence Anebi Enyejo[3]

[1]Department of Electrical Engineering, Collage of Engineering, Prairie View A&M University,
Prairie View, 77446, Texas, USA.
[2]Department of Physics, Joseph Sarwaan Tarkaa University, Makurdi, Benue State, Nigeria.
[3]Department of Telecommunications, Enforcement Ancillary and Maintenance,
National Broadcasting Commission Headquarters, Aso-Villa, Abuja, Nigeria.

Publication Date 2025/08/08

Abstract: The evolution of 5G technology and the proliferation of network slicing have revolutionized private enterprise deployments by offering customizable, low-latency, and high-bandwidth services tailored to diverse operational needs. However, this paradigm introduces complex security challenges, particularly in maintaining isolated, resilient, and trustworthy network environments across multiple slices. This review explores the integration of Zero Trust Network Access (ZTNA) principles within multi-slice 5G architectures to fortify enterprise security postures. Emphasizing a "never trust, always verify" model, the paper critically evaluates how ZTNA frameworks enforce least privilege access, continuous identity verification, and adaptive threat detection across heterogeneous network slices. The discussion extends to the interplay between software-defined perimeters, AI-enhanced anomaly detection, and policy-based segmentation to address insider threats, lateral movement, and dynamic endpoint authentication. The paper reviews current industry standards, architectural blueprints, and practical deployment scenarios, shedding light on scalability, performance trade-offs, and regulatory compliance. Ultimately, this study provides a forward-looking perspective on embedding ZTNA into the DNA of 5G private networks to ensure secure, reliable, and agile enterprise operations.

Keywords: *Zero Trust Network Access (ZTNA); 5G Network Slicing; Private Enterprise Networks; Access Control Enforcement; Secure Multi-Slice Architecture.*

How to Cite: Ugoaghalam Uche James; Onuh Matthew Ijiga; Lawrence Anebi Enyejo (2025) Zero Trust Network Access Enforcement for Securing Multi-Slice Architectures in 5G Private Enterprise Deployments.
International Journal of Innovative Science and Research Technology,
10(8), 64-78. https://doi.org/10.38124/ijisrt/25aug323

I. INTRODUCTION

- *Background on 5G Private Networks and Network Slicing*

The evolution of 5G private networks represents a paradigm shift in enterprise communication systems, enabling customized, high-performance, and secure connectivity tailored to industrial and corporate use cases. Unlike public 5G networks, private 5G systems are owned and operated by organizations to serve specific operational needs such as industrial automation, real-time monitoring, and mission-critical communication. A central enabler of this flexibility is network slicing—a technique that partitions a single physical network into multiple virtual networks, each optimized for distinct service requirements (Ksentini & Taleb, 2021). These virtualized slices offer differentiated latency, bandwidth, reliability, and security profiles, facilitating scenarios like remote healthcare, smart grid management, and autonomous manufacturing.

Network slicing in private 5G environments introduces architectural agility by decoupling network functions and enabling distributed service provisioning closer to the user edge (Campolo et al., 2019). Each slice can be dynamically provisioned, orchestrated, and managed to meet specific enterprise-level service-level agreements (SLAs). Moreover, the adoption of software-defined networking (SDN) and network function virtualization (NFV) allows these slices to be rapidly instantiated, modified, or decommissioned based on changing application needs. This dynamic and programmable infrastructure positions 5G private networks as critical assets in modern enterprise digital transformation (Ononiwu, et al., 2025). However, as the paper further elaborates, this innovation introduces nuanced security complexities, especially in managing multi-slice environments concurrently.

➢ *Security Challenges in Multi-Slice Architectures*

Security within multi-slice architectures in 5G private networks is a critical and multi-dimensional challenge. Each slice operates as an independent virtual network with its own control and data planes, which necessitates unique authentication, isolation, and encryption mechanisms. However, the dynamic and shared nature of the underlying infrastructure increases the attack surface, particularly in scenarios involving heterogeneous tenants and services. One of the foremost concerns is inter-slice interference, where an adversary exploiting vulnerabilities in one slice can potentially access or disrupt services in another. This phenomenon undermines the very principle of slice isolation and is exacerbated by insufficiently granular access control mechanisms (Zhang et al., 2020). Moreover, the integration of artificial intelligence and machine learning for slice orchestration introduces novel threat vectors such as adversarial attacks and poisoning of training data. While these technologies enhance scalability and performance, they simultaneously demand robust security governance across the lifecycle of the slice (Ononiwu, et al., 2024). In decentralized deployments, especially those relying on edge computing, the absence of centralized oversight can lead to inconsistencies in policy enforcement and intrusion detection. Compounding this is the challenge of lifecycle management, as dynamically instantiated slices must be securely configured, monitored, and terminated without residual vulnerabilities or data leakage (Foukas et al., 2017). These security concerns form the basis for adopting more holistic and adaptive security paradigms such as Zero Trust, which will be elaborated in subsequent sections.

➢ *Importance of Zero Trust in Modern Network Security*

The emergence of Zero Trust Network Access (ZTNA) has redefined the foundations of cybersecurity in distributed and virtualized environments such as 5G. In contrast to traditional perimeter-based models, Zero Trust is predicated on the principle that no user or device—internal or external—should be implicitly trusted. Access must be dynamically verified based on continuous authentication, contextual awareness, and strict identity-based policies (Rose et al., 2020). This approach is especially relevant in 5G multi-slice deployments where numerous devices, applications, and service providers operate across shared infrastructure. Zero Trust offers a scalable and resilient security model that aligns with the dynamic provisioning of 5G network slices. By enforcing microsegmentation, ZTNA enables fine-grained access control, limiting lateral movement of threats within and across slices. Furthermore, it leverages telemetry and behavioral analytics to detect anomalies and enforce real-time remediation. As outlined by Desai, & Patil, (2020), integrating Zero Trust at the network edge allows enterprises to secure workloads closer to data sources and enforce least privilege policies more effectively, even in decentralized settings. Crucially, ZTNA supports policy uniformity across heterogeneous environments—cloud, edge, and on-premises—ensuring consistency in threat response and compliance. This adaptability makes it a cornerstone of secure 5G architectures (Azonuche, & Enyejo, 2025). Its role is not merely protective but also enabler, fostering innovation by removing traditional security bottlenecks while still upholding data integrity, confidentiality, and availability. Therefore, embedding Zero Trust frameworks into 5G multi-slice enterprise deployments is imperative for achieving both operational agility and resilient cybersecurity.

➢ *Objectives and Scope of the Review*

The primary objective of this review is to investigate how Zero Trust Network Access (ZTNA) can be strategically enforced within multi-slice 5G private enterprise deployments to enhance security, operational resilience, and policy-driven access control. It aims to analyze the integration of ZTNA with core 5G technologies—such as network function virtualization, software-defined networking, and network slicing—to provide secure, isolated, and adaptive service environments for mission-critical applications. The scope includes an in-depth assessment of ZTNA principles, their application in securing both control and user planes, and their potential to prevent lateral threats across dynamically instantiated network slices. The review also encompasses challenges associated with interoperability, performance, and compliance while highlighting emerging tools like microsegmentation, AI-based threat detection, and secure service mesh architectures that can operationalize Zero Trust in real-world 5G enterprise networks.

➢ *Structure of the Paper*

This paper is organized into six major sections to systematically address the research focus. Section 1 introduces the foundational concepts of 5G private networks, network slicing, and the significance of Zero Trust, setting the stage for the review. Section 2 delves into the core principles and deployment models of Zero Trust Network Access. Section 3 explains the technical architecture of multi-slice 5G enterprise networks, including orchestration, isolation, and threat exposure. Section 4 presents how ZTNA can be integrated within these architectures for robust access control and security enforcement. Section 5 discusses the key implementation challenges and explores future research directions in this evolving domain. Finally, Section 6 summarizes the critical insights and offers strategic recommendations for enterprise network designers and cybersecurity architects.

II. FUNDAMENTALS OF ZERO TRUST NETWORK ACCESS (ZTNA)

➢ *Core Principles of Zero Trust Network Access (ZTNA)*

ZTNA is built on the foundational principle of "never trust, always verify," advocating for continuous authentication and authorization of users, devices, and applications regardless of their location within or outside the network perimeter. This model replaces traditional implicit trust with dynamic, risk-based decision-making grounded in real-time context (Mahfouz & Mohapatra, 2022) as represented in figure 1. Core ZTNA principles include strong identity verification, device posture validation, least privilege access, and continuous policy evaluation. Access decisions are not static; they must evolve with changes in user behavior, geolocation, and network anomalies. ZTNA emphasizes granular control at every access point, avoiding broad network access once a user is authenticated. This minimizes attack surfaces and significantly reduces lateral threat movement. Unlike perimeter-centric security that often trusts internal actors, ZTNA considers every access attempt as potentially hostile (Ononiwu, et al., 2024). Furthermore, it promotes microsegmentation, ensuring that resources are compartmentalized and accessible only through explicit authorization.

This principle is increasingly relevant in complex environments such as multi-slice 5G networks, where rapid changes in access needs and device types are prevalent. Zarpelão et al. (2017) highlight the importance of integrating contextual intelligence—such as behavioral analytics and real-time monitoring—into the trust evaluation process. By doing so, ZTNA dynamically adapts to emerging threats and ensures robust security without compromising agility or performance in mission-critical enterprise networks.

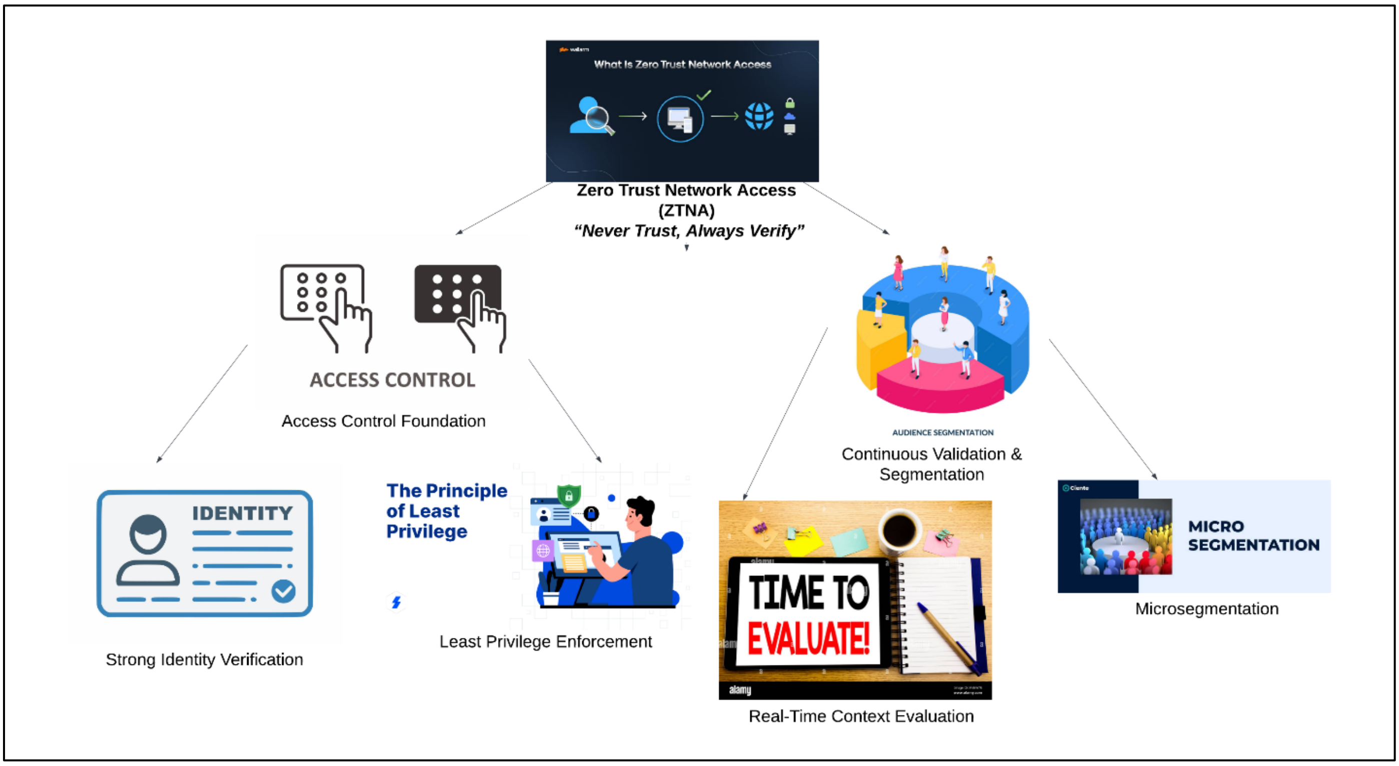
What Is Zero Trust Network Access
Zero Trust Network Access
(ZTNA)
"Never Trust, Always Verify"
ACCESS CONTROL
Access Control Foundation
IDENTITY
Strong Identity Verification
The Principle of Least Privilege
Least Privilege Enforcement
AUDIENCE SEGMENTATION
Continuous Validation & Segmentation
TIME TO EVALUATE!
Real-Time Context Evaluation
MICRO SEGMENTATION
Microsegmentation

Fig 1 Diagram Illustration of Hierarchical Representation of Core ZTNA Principles for Dynamic, Identity-Centric Security in 5G Enterprise Environments.

Figure 1 presents a two-branch structure that captures the foundational components of ZTNA. The first branch, Access Control Foundation, emphasizes the security principles that govern who gains access and under what conditions. It includes Strong Identity Verification, which mandates robust user and device authentication through mechanisms such as multi-factor authentication and attribute-based controls. Paired with this is the Least Privilege Enforcement principle, ensuring that users and devices are granted only the minimum access necessary to perform their tasks, with time-bound or context-aware restrictions. The second branch, Continuous Validation & Segmentation, highlights the operational dynamics of ZTNA. It includes Real-Time Context Evaluation, which continuously assesses contextual signals like geolocation, device health, and behavioral patterns to determine access legitimacy. Additionally, Microsegmentation divides the network into smaller, isolated segments, restricting lateral movement and minimizing the attack surface. Together, these principles form an adaptive, identity-centric security framework that eliminates implicit trust, making ZTNA a resilient and scalable model for securing 5G enterprise networks and multi-slice architectures.

➢ *Comparison with Traditional Perimeter-Based Models*

The Zero Trust model fundamentally departs from traditional perimeter-based security, which assumes that users and devices within an organization's internal network are inherently trustworthy. In contrast, ZTNA presumes no inherent trust, continuously validating credentials, device status, and context before granting access to resources. Traditional perimeter models rely heavily on firewalls and VPNs to demarcate internal from external environments, often leading to excessive access privileges once entry is granted (Fernandes et al., 2014) as shown in table 1. This design creates opportunities for attackers to move laterally and exploit weak internal controls.

ZTNA resolves this by shifting from static, location-based access control to dynamic, identity-centric authorization mechanisms. Instead of treating the network as a single secure domain, ZTNA decomposes it into fine-grained segments where access is governed by real-time policy decisions and least privilege principles. This is particularly crucial in highly dynamic and hybrid enterprise environments like 5G network slices, where services span public, private, and edge domains.

Acar et al. (2020) emphasize that perimeter-based models are insufficient in environments characterized by distributed architectures, cloud-native applications, and mobile endpoints. As enterprise infrastructure becomes more decentralized, the absence of a clear perimeter renders traditional models obsolete (Ononiwu, et al., 2023). In contrast, ZTNA addresses these challenges by embedding security into every layer of the network—ensuring identity, posture, and context validation are persistent throughout the session lifecycle. Ultimately, ZTNA is not a replacement but an evolutionary necessity for securing modern enterprise systems.

Table 1 Summary of Comparison of Traditional Perimeter-Based Models vs. ZTNA

Aspect	Traditional/Legacy Model	ZTNA/Multi-Slice Advancement	Implications/Remarks
Access Trust Model	Trust is implicitly granted once inside the network	No implicit trust; continuous authentication and verification	Reduces risk of insider threats and lateral movement
Security Enforcement Point	Security enforced at network boundary (firewall/VPN)	Distributed enforcement at every access point or slice entry	Ensures granular, dynamic access aligned with real-time context
Network Architecture	Flat, perimeter-centric	Segmented, policy-driven, slice-based	Enhances isolation and service-specific policy enforcement
Threat Response	Reactive; limited visibility inside network	Proactive; integrates real-time telemetry and behavioral analytics	Enables predictive threat detection and adaptive mitigation strategies

➢ *Key Technologies: Identity, Policy Enforcement, and Microsegmentation*

ZTNA is operationalized through a triad of enabling technologies: identity and access management (IAM), policy enforcement, and microsegmentation. These components are tightly interwoven to ensure fine-grained, contextual access control that aligns with enterprise security objectives. IAM serves as the backbone of Zero Trust, where identity verification is conducted using multifactor authentication (MFA), digital certificates, and behavioral biometrics to ensure that only verified users and devices can initiate access requests (Ali et al., 2022). This identity-centric model minimizes impersonation risks and allows dynamic attribute-based access decisions. Policy enforcement engines, acting as decision and enforcement points, translate business rules into executable access constraints. These engines utilize context-aware parameters such as device health, user role, location, and time of access to dynamically determine permissions. For instance, a healthcare technician accessing patient data from within the hospital network may be granted full access, whereas remote access might trigger partial visibility with additional authentication steps. Sinha and Kulkarni (2021) highlight microsegmentation as a key pillar of Zero Trust, enabling the network to be split into secure zones where lateral movement is restricted. Each application, workload, or network slice can be individually protected using adaptive firewall rules and access policies (Ononiwu, et al., 2023). This segmentation is especially vital in 5G multi-slice deployments, where each slice represents a virtualized and service-specific environment. Together, IAM, policy enforcement, and microsegmentation form the technological foundation upon which scalable and secure Zero Trust architectures are constructed.

➢ *ZTNA Deployment Models and Architectures*

ZTNA deployment models vary in complexity and scale, often influenced by the nature of the enterprise infrastructure and regulatory environment. Two prevalent models dominate the landscape: endpoint-initiated ZTNA and service-initiated ZTNA. In endpoint-initiated deployments, client agents on user devices establish secure tunnels to access brokers or policy engines, which verify identity and context before routing access to the protected resource (Lyu et al., 2021). This model offers superior granularity and control, especially in highly mobile and hybrid enterprise environments. In contrast, service-initiated models operate at the application level, where the gateway or service provider intermediates the authentication process. This model is more conducive for cloud-native services, providing visibility and control without requiring endpoint agents. The architecture typically comprises key components such as Policy Enforcement Points (PEP), Policy Decision Points (PDP), Trust Brokers, and telemetry collectors that collaboratively ensure dynamic access decisions based on real-time insights. Nguyen and Redon (2022) argue that successful ZTNA architectures must prioritize scalability, fault tolerance, and latency minimization—especially when applied to edge computing or multi-slice 5G deployments. The incorporation of distributed enforcement points and federated identity mechanisms allows ZTNA to function in decentralized ecosystems while maintaining policy coherence and security. Additionally, these architectures must support integration with existing SIEM, SOAR, and AI-based analytics platforms to ensure continuous monitoring and response (Imoh, et al., 2025). As enterprises embrace software-defined and cloud-based paradigms, ZTNA architectures must evolve to support cross-domain policy enforcement and seamless user experiences across complex digital terrains.

III. ARCHITECTURE OF 5G MULTI-SLICE NETWORKS IN ENTERPRISES

➢ *Overview of Network Slicing in 5G*

Network slicing is a core architectural capability in 5G that allows the logical segmentation of a shared physical network into multiple virtual networks or "slices," each optimized for a specific service type or application domain. Each slice operates as an isolated end-to-end network instance, possessing its own virtualized resources, management functions, and quality-of-service (QoS) parameters (Alex, et al., 2020). This allows mobile network operators and enterprises to deliver differentiated services simultaneously over a unified infrastructure while meeting diverse latency, throughput, and reliability requirements. Slicing leverages key 5G enablers such as software-defined networking (SDN) and network function virtualization (NFV) to dynamically orchestrate and provision these virtual instances. The design ensures flexibility in service deployment, allowing slices to be instantiated for ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC), or enhanced mobile broadband (eMBB) use cases, without compromising each other's performance (Kang et al., 2019). This capacity to tailor and isolate service delivery provides significant advantages for enterprises seeking operational agility and scalability, particularly in complex environments such as smart factories, autonomous transport systems, or mission-critical healthcare. The abstraction layer offered by network slicing is critical for private 5G deployments, where organizations need custom connectivity solutions aligned with their business objectives (Imoh, & Enyejo, 2025). By logically decoupling services and infrastructure, 5G slicing introduces an entirely new paradigm for scalable and secure network management in heterogeneous service environments.

- *Use Cases of Multi-Slice Architectures in Private Enterprises*

Multi-slice architectures empower private enterprises to deploy dedicated virtual networks optimized for specific operational demands. This capability is particularly relevant in environments requiring stringent latency, reliability, and bandwidth conditions. In manufacturing, for example, network slicing enables simultaneous operation of time-critical control systems, low-power IoT sensors, and data analytics platforms—all on isolated slices that avoid resource contention (Taleb et al., 2017) as represented in figure 2. Similarly, in the healthcare sector, slices can be configured to segregate diagnostic imaging transfers from patient monitoring systems to meet compliance and security benchmarks. Retail chains benefit from multi-slice deployment by provisioning separate slices for point-of-sale operations, inventory management, and customer-facing applications such as AR/VR experiences. Such separation ensures service continuity even under peak demand or targeted attacks. Financial institutions use network slices to isolate real-time trading platforms from corporate IT and customer service applications, reducing latency and exposure to cyber threats (D'Oro et al., 2021). Moreover, the advent of mobile edge computing (MEC) in combination with network slicing allows enterprises to place computing power closer to end users, ensuring ultra-fast response times for latency-sensitive applications. This synergy extends the versatility of slicing, allowing real-time orchestration based on context, demand, or threat posture (Imoh, 2023). Enterprises gain operational elasticity without sacrificing security or compliance, marking a pivotal shift in how private networks are architected and maintained in the 5G era.

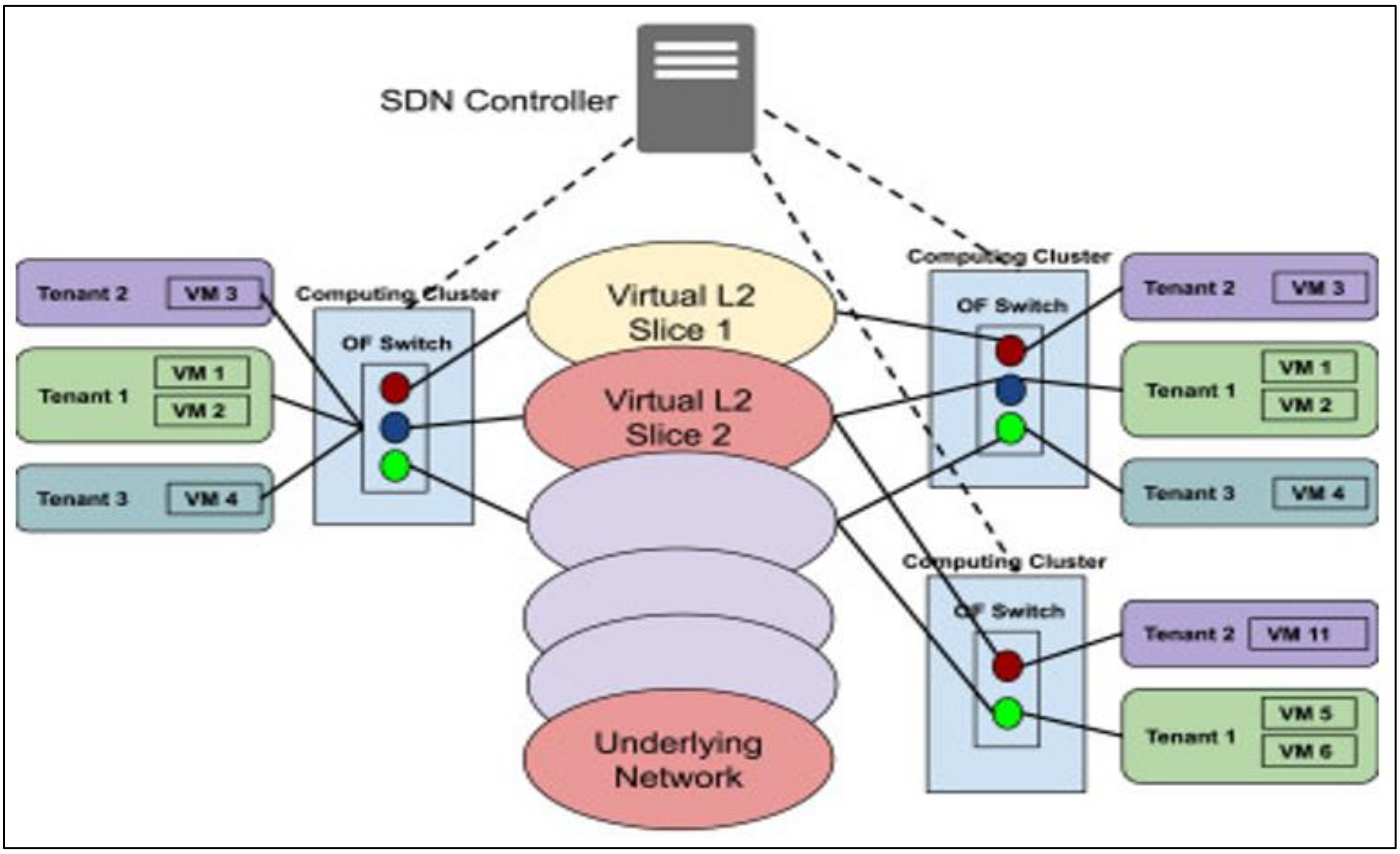

Fig 2 Picture of SDN-Orchestrated Multi-Slice Architecture for Private 5G Enterprise Networks (Barakabitze, et al., 2020).

Figure 2 illustrates a practical implementation of multi-slice architecture in a private enterprise 5G network, highlighting how network slicing enables secure, isolated service delivery for different tenants and workloads. At the core of the architecture is the underlying physical network, which is abstracted into multiple Virtual Layer 2 (L2) slices—Slice 1 and Slice 2—each managed and orchestrated by an SDN (Software-Defined Networking) Controller. These slices are logically independent and mapped to diverse computing clusters and OpenFlow (OF) switches, enabling dynamic traffic control and policy enforcement. Each slice supports different tenants (e.g., Tenant 1, Tenant 2, Tenant 3), with their corresponding Virtual Machines (VMs) allocated according to service-level requirements. For example, Slice 1 may cater to mission-critical industrial applications requiring high bandwidth and low latency, while Slice 2 may host less sensitive IT services or external partner access. The separation ensures performance optimization, operational autonomy, and security isolation, as no tenant or VM can interfere with others in different slices. This model is particularly advantageous in sectors like manufacturing, healthcare, and finance, where private enterprises deploy custom-tailored virtual networks to support concurrent workloads such as real-time monitoring, data analytics, and legacy system access—each within its dedicated virtual slice. Overall, the image demonstrates the flexibility, scalability, and compartmentalized control enabled by multi-slice 5G deployments in enterprise environments.

➢ *Slice Isolation, Orchestration, and Resource Management*

Slice isolation and resource orchestration are foundational to the security and efficiency of 5G multi-slice architectures. Slice isolation ensures that each virtual network functions independently, preventing unauthorized traffic spillover or performance interference as shown in table 2. Isolation is maintained across the control plane, data plane, and management layers using strict logical segmentation, firewalling, and tenant-specific security policies. Kim, & Lim, (2021) demonstrate that resource allocation and scaling mechanisms must operate with slice-level granularity to enforce this independence, particularly during traffic surges or resource contention.

Orchestration involves the automated deployment, configuration, and lifecycle management of network slices using software-defined approaches. Orchestration systems interact with virtual infrastructure managers, monitoring tools, and AI-driven analytics engines to ensure that each slice adheres to its predefined service-level objectives (SLOs). Efficient orchestration minimizes resource waste, balances loads, and allows for elastic scaling in response to real-time demand.

Abbas et al. (2018) emphasize that effective orchestration requires a dynamic understanding of network topology, application context, and QoS parameters. This is further complicated in private enterprise networks, where custom workflows and compliance requirements dictate resource prioritization. Coordination across edge, cloud, and core components is essential to meet performance goals while avoiding bottlenecks or cross-slice interference (Azonuche, & Enyejo, 2024). The interplay between isolation, orchestration, and resource management forms the control framework that enables secure and performant network slicing in real-world enterprise deployments.

Table 2 Summary of Slice Isolation, Orchestration, and Resource Management in 5G

Aspect	Traditional Virtualization or SDN	Multi-Slice 5G Architecture with ZTNA	Implications/Remarks
Slice Isolation	Logical isolation with shared control resources	Full isolation at control, user, and management planes	Reduces attack propagation and cross-slice interference
Resource Allocation	Static or manual provisioning	AI-driven, dynamic slice-specific resource orchestration	Improves agility and performance consistency across slices
Orchestration Tools	Centralized, often monolithic controllers	Distributed orchestrators with slice-aware decision engines	Enhances reliability, scalability, and policy granularity
Monitoring & Management	Periodic checks and coarse granularity	Real-time monitoring with per-slice telemetry	Enables fine-grained operational intelligence and enforcement

➢ *Threat Surface in Multi-Slice Environments*

While 5G network slicing enhances flexibility and efficiency, it also expands the attack surface across multiple operational layers. Each slice, despite being logically isolated, shares physical infrastructure components such as base stations, data centers, and transport networks. This co-tenancy introduces vulnerabilities whereby a compromised slice could become a vector for cross-slice attacks (Khorsandroo et al., 2022). Insider threats, misconfigured orchestration tools, and weak slice-specific access controls further exacerbate the risk landscape.

In multi-slice environments, threat actors may exploit orchestration platforms, which often possess elevated privileges across slices. A single breach in these centralized control planes can jeopardize multiple slices simultaneously, leading to widespread data exfiltration or service disruption. Attack vectors include denial-of-service (DoS) against slice instantiation services, side-channel attacks on shared CPU caches, and man-in-the-middle (MitM) exploits during inter-slice communication.

Echeverria et al. (2020) highlight additional risks posed by the integration of third-party virtualized network functions (VNFs) and AI agents in slice management. These components, if inadequately vetted, may introduce supply chain vulnerabilities or function as unauthorized data collectors. Furthermore, network slicing introduces increased complexity, making it difficult to maintain real-time visibility and enforce uniform security policies. The variability in slice configurations and their rapidly changing states challenge traditional monitoring systems, necessitating the adoption of context-aware, adaptive security frameworks like Zero Trust to minimize exploitability in these sophisticated architectures.

IV. INTEGRATION OF ZTNA WITH 5G MULTI-SLICE FRAMEWORKS

➢ *ZTNA Enforcement in Control and user Planes*

The dual-plane architecture of 5G networks—comprising the control and user planes—demands comprehensive security enforcement strategies that align with ZTNA principles. ZTNA enforces continuous verification across both planes, ensuring that signaling messages in the control plane and payload in the user plane are authenticated, validated, and behaviorally monitored (Ijiga, O. M. et al., 2023) as represented in figure 3. Santhosh, (2025) proposed a policy-driven enforcement model that integrates ZTNA into the 5G core, establishing distinct checkpoints where identity, trustworthiness, and contextual parameters are evaluated before any control or data operation is executed. In the control plane, ZTNA mechanisms intercept signaling protocols (e.g., NGAP, NAS) to verify tenant identities and cross-check policy compliance before session establishment. For the user plane, ZTNA performs packet-level inspection and behavioral validation using endpoint profiles and AI-based anomaly detection systems. Lal et al. (2021) emphasized the importance of trust-aware mechanisms that continuously score communication flows, denying or revoking access dynamically if confidence levels fall below secure thresholds. Enforcing ZTNA across both planes not only eliminates implicit trust but also prevents lateral movement between slices, malicious control signaling, and user data exploitation (Ijiga, O. M. et al., 2022). This is especially vital in enterprise deployments with isolated yet interdependent slices. By decoupling security from physical infrastructure and embedding it into the service logic and access orchestration layers, ZTNA enforcement enables scalable, slice-specific policy execution with minimal performance overhead.

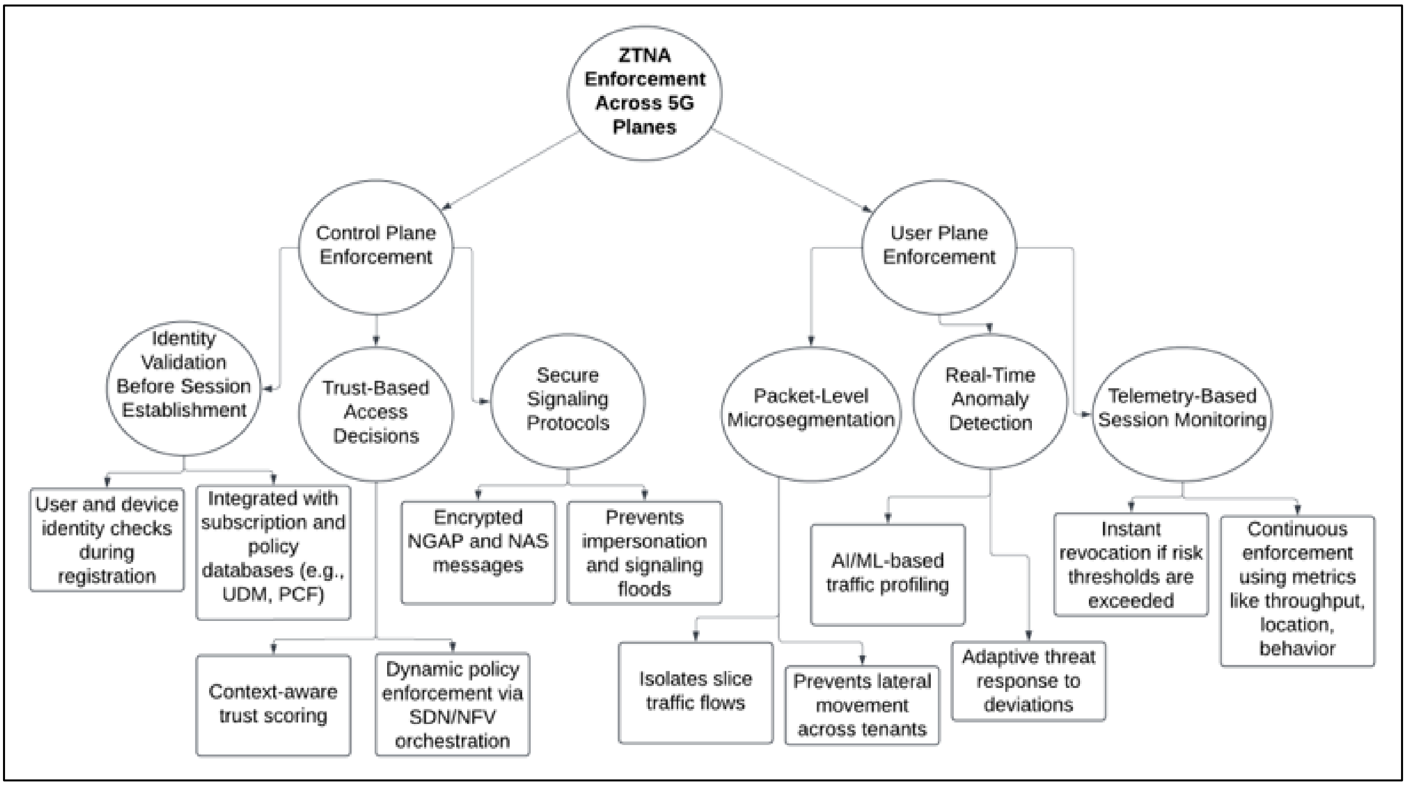
ZTNA Enforcement Across 5G Planes
Control Plane Enforcement
User Plane Enforcement
Identity Validation Before Session Establishment
Trust-Based Access Decisions
Secure Signaling Protocols
Packet-Level Microsegmentation
Real-Time Anomaly Detection
Telemetry-Based Session Monitoring
User and device identity checks during registration
Integrated with subscription and policy databases (e.g., UDM, PCF)
Encrypted NGAP and NAS messages
Prevents impersonation and signaling floods
AI/ML-based traffic profiling
Instant revocation if risk thresholds are exceeded
Continuous enforcement using metrics like throughput, location, behavior
Context-aware trust scoring
Dynamic policy enforcement via SDN/NFV orchestration
Isolates slice traffic flows
Prevents lateral movement across tenants
Adaptive threat response to deviations

Fig 3 Diagram Illustration of ZTNA Enforcement Across 5G Control and user Planes.

Figure 3 provides a detailed visualization of how ZTNA mechanisms are applied across both the control plane and the user plane in a 5G multi-slice enterprise architecture. In the control plane, ZTNA begins by validating user and device identities before session establishment, ensuring only authorized entities proceed beyond registration. Trust-based access decisions are dynamically enforced through real-time context—such as location, role, and risk profile—leveraging software-defined networking (SDN) and network function virtualization (NFV) tools. Secure signaling protocols like NGAP and NAS are encrypted and integrity-protected to prevent impersonation attacks and control signaling manipulation. On the user plane, ZTNA enforces microsegmentation by isolating tenant-specific traffic and restricting lateral movement between slices. Real-time anomaly detection powered by AI continuously inspects packet behavior, allowing for immediate mitigation of suspicious flows. Additionally, session telemetry—including traffic volume, behavioral patterns, and device posture—is continuously monitored to adjust access rights or revoke sessions if threat levels rise. Together, these mechanisms create a multi-layered, adaptive trust framework that ensures end-to-end security and operational resilience in enterprise-grade 5G deployments.

➢ *Policy-Based Access Controls per Slice*

Policy-based access control (PBAC) frameworks are foundational to enforcing Zero Trust principles within multi-slice 5G networks. Unlike role-based access models, PBAC relies on a combination of identity, context, device posture, and environmental conditions to govern resource access (Ijiga, O. M. et al., 2021) as shown in table 3. Each slice can define granular access policies reflecting its specific QoS, security, and compliance requirements. Ferrer Riera et al. (2020) introduced a context-aware enforcement system where rules are continuously evaluated based on changing operational conditions—such as user location, service load, and threat status—prior to granting access to any slice-based resource. In private enterprise deployments, different slices may cater to operational technology, IT systems, and guest devices. Policy enforcement mechanisms allow administrators to define and enforce unique access workflows for each context. For instance, operational slices may prohibit remote connections entirely, while IT slices may enforce step-up authentication during off-peak hours. Coronado, & Riggio, (2019) presented a rule-based access management scheme where access permissions are dynamically allocated through a policy engine integrated with slice orchestrators, ensuring isolation and role compliance at runtime.

The flexibility of PBAC ensures adaptability to emerging threats and business demands without requiring static reconfiguration of network infrastructure (Ijiga, O. M. et al., 2021). Policies are encoded into orchestration and service management layers, enabling consistent enforcement from the core to the edge. This guarantees secure, compliant, and reliable operations, especially as slices evolve in complexity and function within enterprise ecosystems.

Table 3 Summary of Policy-Based Access Controls in 5G Network Slices

Aspect	Legacy Access Models (e.g., RBAC)	ZTNA Policy-Based Slicing Controls	Implications/Remarks
Access Model	Role-Based Access Control (static, coarse-grained)	Attribute-based, context-aware dynamic access control	Enhances flexibility and real-time risk responsiveness
Policy Granularity	Uniform policies across network segments	Slice-specific, workload-sensitive policies	Tailors enforcement to unique enterprise service requirements
Policy Enforcement Points	Centralized firewalls and NAC systems	Distributed enforcement within orchestration and edge layers	Reduces single points of failure; supports low-latency decision-making
Context Awareness	Minimal or reactive to incidents	Integrated with real-time telemetry and trust scores	Promotes proactive decision-making and fine-tuned user/resource access

➢ *Continuous Authentication and Real-Time Context Evaluation*

Continuous authentication combined with real-time context evaluation is critical to achieving Zero Trust compliance in dynamic and distributed 5G environments. Traditional point-in-time authentication mechanisms fall short in scenarios where user posture, device integrity, and threat landscapes change rapidly. In response, advanced ZTNA frameworks implement continuous authentication strategies that assess multiple factors—such as biometrics, device trust score, and behavioral baselines—throughout the session lifecycle. Tuncer et al. (2021) demonstrated a risk-aware model that uses real-time analytics to compute user trust levels, adapting access permissions as contextual parameters evolve.

Context-aware frameworks analyze telemetry from network, device, and user activity to detect anomalies and trigger remediation workflows without disrupting legitimate traffic (Ijiga, O. M. et al 2024). These systems dynamically reevaluate access tokens and session privileges based on the evolving trust context. For example, a user moving from a trusted facility to an unknown network might trigger reduced access levels or a mandatory re-authentication (Moreno et al., 2022). This real-time evaluation ensures that access remains conditional and revocable, significantly reducing dwell time in case of compromise. Such mechanisms are essential in multi-slice architectures where different slices serve different risk profiles (Ijiga, A. C. et al., 2024). A slice handling financial transactions may enforce stricter authentication and shorter session timeouts than one supporting non-sensitive telemetry data. Contextual intelligence integrated into continuous authentication not only strengthens resilience but also aligns with compliance mandates, making it indispensable for enterprises adopting Zero Trust in 5G networks.

➢ *Secure Service Mesh and Software-Defined Perimeters*

The integration of secure service mesh and software-defined perimeter (SDP) architectures underpins ZTNA's ability to deliver fine-grained, scalable, and resilient security in microservice-based 5G networks (Ijiga, A. C. et al 2024). A service mesh abstracts network communication between microservices, embedding security controls such as mutual TLS, authentication, and authorization at the service level rather than relying solely on network boundaries. Rahman et al. (2021) highlight how service meshes provide dynamic service discovery, encrypted communication, and traffic monitoring, all essential in enforcing Zero Trust within service-rich 5G slices.

SDPs further enhance this model by eliminating public exposure of services. Instead, access is granted only after identity verification and policy validation through an SDP controller. This approach renders services invisible to unauthorized users and mitigates surface attacks such as port scanning, DoS, and credential stuffing (Lopes et al., 2022). SDP operates by decoupling access control from the network layer and shifting enforcement to the application or service endpoint level, ensuring zero implicit trust. In enterprise deployments, combining service meshes and SDPs enables centralized policy enforcement while maintaining decentralized execution. For example, a logistics company can use service mesh to secure internal microservices within its supply chain slice, while SDP restricts external partners' access to only required APIs (Igba, et al., 2024). These technologies provide a robust framework for implementing Zero Trust across diverse application stacks and infrastructure layers, facilitating secure multi-tenancy in 5G private networks.

V. CHALLENGES AND FUTURE TRENDS

➢ *Interoperability and Legacy System Integration*

Integrating ZTNA into existing 5G infrastructures and legacy systems presents complex interoperability challenges. Legacy systems, often governed by perimeter-based security models, lack the architectural flexibility required for dynamic access control, continuous authentication, and context-aware enforcement that ZTNA mandates. Sharma et al. (2020) emphasized the structural disparity between rigid legacy protocols and agile 5G services, complicating the harmonization of access policies and trust boundaries. Bridging this gap necessitates adaptable mediation layers that can interface between ZTNA-enabled systems and outdated access protocols such as RADIUS or TACACS+.

ZTNA implementation in such environments must support identity federation, multi-protocol support, and translation proxies to enforce uniform security without compromising operational continuity. Celeste, & Michael, (2021) introduced a unified framework where Zero Trust policies are virtualized and enforced at the network edge, allowing legacy assets to comply through centralized access controllers and microsegmented gateways. This reduces lateral risk exposure from legacy vulnerabilities while enabling gradual migration (Ijiga, A. C. et al 2024).

Interoperability also depends on robust service discovery, orchestration integration, and telemetry normalization. Without these capabilities, legacy systems may create blind spots within Zero Trust visibility layers (Idika, et al., 2025). Therefore, achieving comprehensive security requires a layered architecture that wraps legacy systems in ZTNA-compatible control planes. For 5G enterprise adoption, backward compatibility remains a strategic necessity, enabling organizations to benefit from Zero Trust protections without sacrificing previous infrastructure investments (Igba, et al., 2024).

➢ *Performance and Latency Considerations in ZTNA*

One of the most pressing concerns in enforcing ZTNA within 5G enterprise environments is its potential to introduce latency due to frequent access validations, encryption overhead, and policy computation. ZTNA's architecture requires continuous session monitoring and dynamic policy enforcement at multiple points along the communication path (Azonuche, & Enyejo, 2024) as shown in figure 4. Xu et al. (2022) developed a performance-aware ZTNA model tailored for edge-centric 5G networks, which showed that implementing authentication and trust brokers at the edge significantly reduced round-trip latency and improved throughput under varying loads.

Latency is particularly sensitive in ultra-reliable low-latency communication (URLLC) slices used in industrial automation and autonomous systems. ZTNA's cryptographic operations, identity lookups, and microsegmentation routing can introduce delays if not optimized. Bura, (2025) examined latency trade-offs in decentralized ZTNA implementations and found that policy caching, lightweight cryptographic methods, and regional policy decision nodes substantially mitigate performance degradation.

In enterprise 5G deployments, where diverse applications compete for real-time access to services, it is essential that ZTNA enforcement does not become a bottleneck (Ayoola, et al., 2024). Solutions must include predictive caching of access tokens, context aggregation to minimize verification cycles, and AI-based trust scoring to bypass redundant checks. Therefore, the successful deployment of ZTNA relies on architectural tuning to strike a balance between security granularity and real-time responsiveness—especially in mission-critical private slices (Azonuche, & Enyejo, 2024).

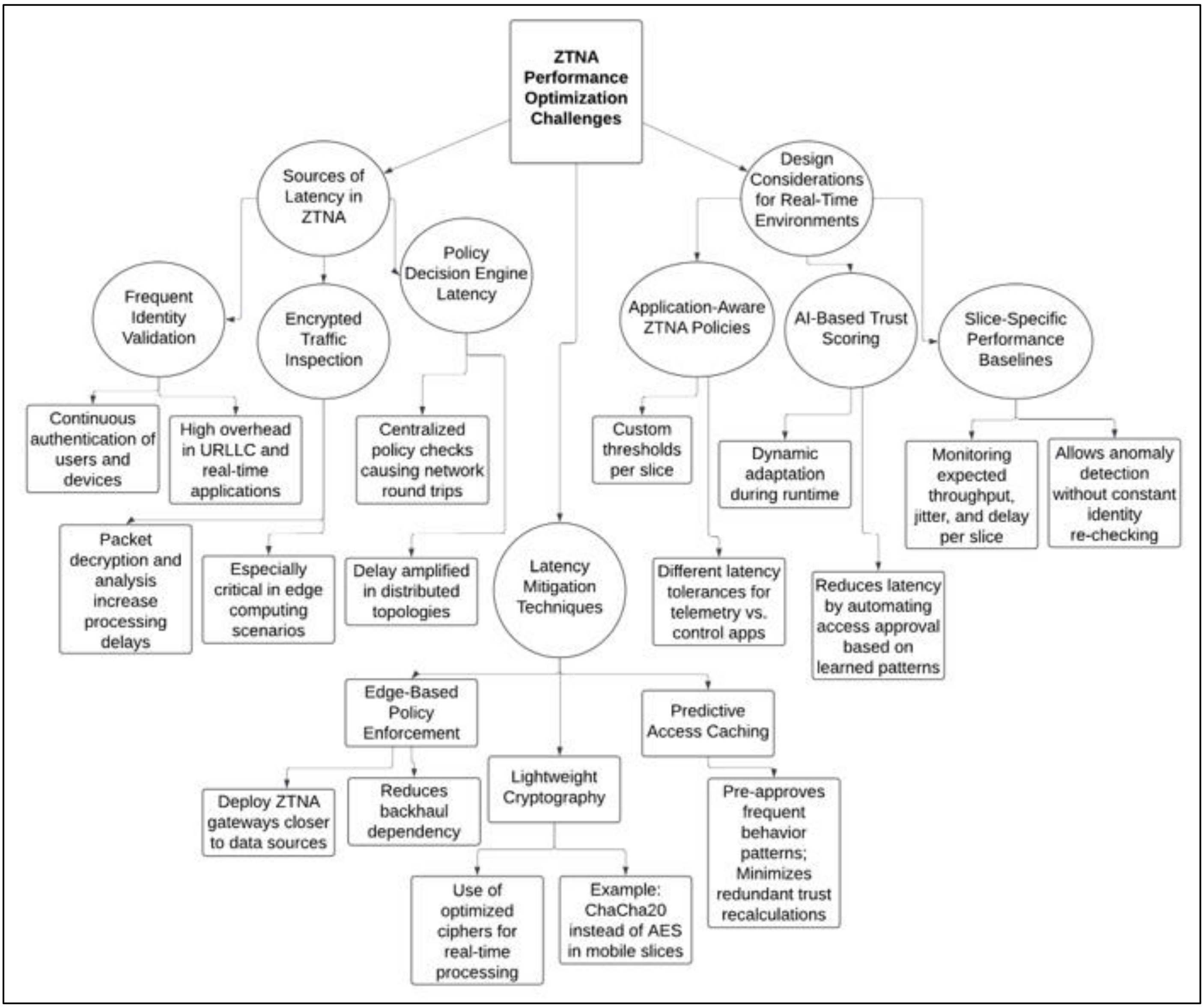
ZTNA Performance Optimization Challenges
Sources of Latency in ZTNA
Frequent Identity Validation
Encrypted Traffic Inspection
Policy Decision Engine Latency
Continuous authentication of users and devices
High overhead in URLLC and real-time applications
Centralized policy checks causing network round trips
Packet decryption and analysis increase processing delays
Especially critical in edge computing scenarios
Delay amplified in distributed topologies
Latency Mitigation Techniques
Edge-Based Policy Enforcement
Predictive Access Caching
Lightweight Cryptography
Deploy ZTNA gateways closer to data sources
Reduces backhaul dependency
Use of optimized ciphers for real-time processing
Example: ChaCha20 instead of AES in mobile slices
Pre-approves frequent behavior patterns; Minimizes redundant trust recalculations
Design Considerations for Real-Time Environments
Application-Aware ZTNA Policies
AI-Based Trust Scoring
Slice-Specific Performance Baselines
Custom thresholds per slice
Dynamic adaptation during runtime
Monitoring expected throughput, jitter, and delay per slice
Allows anomaly detection without constant identity re-checking
Different latency tolerances for telemetry vs. control apps
Reduces latency by automating access approval based on learned patterns

Fig 4 Diagram Illustration of Performance and Latency Considerations in ZTNA for 5G Enterprise Networks.

Figure 4 presents a comprehensive view of how ZTNA enforcement impacts real-time performance and latency in 5G private deployments, and outlines strategies to mitigate those effects. The first branch, *Sources of Latency in ZTNA*, highlights key contributors to delay, including continuous identity verification, encrypted traffic inspection, and centralized policy evaluation—each of which can bottleneck communication in latency-sensitive applications like industrial automation or remote diagnostics. The second branch, *Latency Mitigation Techniques*, outlines technical solutions such as edge-based policy enforcement to reduce round-trip time, lightweight cryptographic protocols for faster processing, and predictive access caching to bypass repetitive trust calculations. The third branch, *Design Considerations for Real-Time Environments*, focuses on optimizing ZTNA architecture for responsiveness through application-specific trust policies, AI-driven trust scoring for dynamic access, and slice-specific baselining of performance metrics (Atalor, et al., 2023). Collectively, the diagram emphasizes that while ZTNA introduces overhead due to its continuous validation model, intelligent placement of enforcement points, algorithmic efficiency, and context-aware trust mechanisms can preserve real-time responsiveness without compromising security.

➢ *Regulatory and Compliance Implications*

ZTNA enforcement in multi-slice 5G enterprise networks intersects heavily with global data protection regulations and industry-specific compliance mandates. Regulatory frameworks such as GDPR, HIPAA, and NIS2 impose stringent requirements on data access, user authentication, audit trails, and breach notification. Wichary, et al. (2022) highlighted that network slicing introduces regulatory complexities because multiple virtualized environments operate within shared physical infrastructure, raising concerns around tenant isolation, lawful interception, and cross-jurisdictional data flows.

ZTNA frameworks, by default, support many compliance principles—such as least privilege access, policy-based restrictions, and access traceability—making them suitable for regulated environments (Atalor, et al., 2023). However, the dynamic nature of policy enforcement in ZTNA requires rigorous documentation and auditable workflows to satisfy regulatory authorities. Matencio-Escolar, et al., (2020) proposed a "compliance by design" architecture where ZTNA policy engines are integrated with legal constraint modeling to enforce context-sensitive data handling rules at runtime.

Furthermore, industry-specific mandates often prescribe sectoral controls, such as PCI DSS for financial services or FDA regulations for healthcare. ZTNA must adapt to these nuances, embedding controls within each slice to enforce jurisdiction-specific rules and audit logs. By integrating compliance toolkits with ZTNA orchestration and telemetry engines, enterprises can align operational security with legal obligations (Akindotei, et al., 2024). Consequently, ZTNA is not only a cybersecurity enabler but also a vehicle for proactive regulatory alignment in 5G enterprise deployments.

- *Future Research Directions: AI for Zero Trust, Quantum-Resistant Encryption*

The future of ZTNA in 5G and beyond hinges on the integration of artificial intelligence (AI) for adaptive policy enforcement and the adoption of quantum-resistant encryption to mitigate emerging cryptographic risks as shown in table 4. AI-powered ZTNA architectures leverage machine learning models to dynamically assess user trust scores, detect anomalous behaviors, and predict policy deviations in real time. Kaushik, et al. (2025) proposed trust inference engines based on neural networks that evolve with usage patterns, significantly improving access control precision in highly fluid network environments.

In parallel, the rise of quantum computing poses existential threats to conventional encryption mechanisms underpinning ZTNA frameworks. Algorithms such as RSA and ECC, which form the basis of secure key exchange and digital signatures, are vulnerable to quantum attacks. Aggarwal and Jaiswal (2020) examined quantum-resistant cryptographic schemes, including lattice-based, hash-based, and multivariate polynomial cryptography, which promise resilience against Shor's algorithm and Grover's search. These methods must be tested for performance viability within latency-sensitive slices and cloud-edge hybrid infrastructures.

Future research must explore the fusion of AI and quantum-secure methods to build Zero Trust systems that are not only adaptive but also futureproof (Ajayi, et al., 2024). For instance, deploying quantum-safe encryption algorithms alongside AI-powered anomaly detection could yield intelligent security fabrics that evolve continuously and resist even post-quantum adversaries. As ZTNA becomes integral to securing mission-critical infrastructures in 5G and 6G ecosystems, these innovations will define the next frontier of network trust architecture.

Table 4 Summary of Future Research Directions: AI for Zero Trust and Quantum-Resistant Encryption

Aspect	Current Limitations	Proposed Innovations	Implications/Remarks
Trust Evaluation	Static rule sets or identity-only checks	AI-based behavioral trust scoring engines	Enables continuous, context-sensitive access validation
Cryptographic Security	Vulnerable to quantum decryption (RSA, ECC)	Lattice-based and hash-based quantum-resistant algorithms	Futureproofs ZTNA framework against quantum-enabled attackers
Access Automation	Manual policy updates; lacks adaptive learning	AI-driven anomaly detection and policy adjustment	Reduces admin overhead, enhances adaptive threat response
Interoperability Concerns	Difficult to upgrade legacy crypto modules	Modular, pluggable cryptographic protocols in ZTNA platforms	Facilitates gradual upgrade to post-quantum security environments

VI. CONCLUSION

- *Summary of Key Findings*

This review establishes that ZTNA represents a critical paradigm shift for securing multi-slice architectures in 5G private enterprise deployments. The core principle of continuous verification, rather than assumed trust, aligns seamlessly with the dynamic and service-specific nature of 5G slicing. ZTNA facilitates end-to-end policy enforcement across both the control and user planes, ensuring that each access request is validated based on identity, context, and device posture. The analysis also highlights the value of technologies such as microsegmentation, continuous authentication, and policy-based access control, all of which are essential for maintaining logical isolation between slices and thwarting lateral threats. Furthermore, the integration of ZTNA with service mesh frameworks and software-defined perimeters allows for highly granular, decentralized access enforcement, which is vital in distributed edge and hybrid-cloud environments. However, implementation is not without its challenges. Legacy interoperability, performance trade-offs, and regulatory compliance complexities must be navigated carefully. Strategic deployment models must consider these constraints while leveraging the benefits of real-time trust assessment and adaptive access control. Additionally, emerging trends such as AI-driven behavioral analytics and quantum-resistant encryption are poised to redefine how ZTNA evolves in the face of escalating cyber threats. Overall, the findings emphasize that ZTNA is not merely a security upgrade but a foundational requirement for ensuring scalable, context-aware protection across the multifaceted operational layers of 5G private enterprise networks.

- *Strategic Implications for Enterprise Network Design*

The strategic integration of ZTNA into enterprise network architecture demands a reimagining of traditional design philosophies. Unlike perimeter-based models that emphasize external versus internal segregation, ZTNA promotes identity- and policy-centric control across every layer of connectivity. This transformation necessitates embedding trust evaluation mechanisms throughout the network—from user endpoints and IoT devices to edge nodes and cloud services. In the context of 5G network slicing, enterprise architects must implement dedicated policy enforcement points for each slice, ensuring that access is dynamically adjusted based on user behavior, device posture, and application context. Moreover, identity federation and adaptive access orchestration must become native features of the enterprise infrastructure to enable seamless, secure connectivity across heterogeneous assets. The review also reveals that deploying ZTNA as a foundational layer enhances operational agility by enabling fine-grained segmentation and contextual resource provisioning, particularly important for supporting differentiated enterprise workflows such as smart manufacturing, remote diagnostics, and autonomous logistics. Strategic alignment with orchestration platforms, telemetry engines, and compliance governance tools ensures that ZTNA is not just a security overlay but an integrated operational enabler. Designing network topologies that prioritize trust boundaries over physical zones will future-proof enterprise networks against evolving threats, including insider attacks and sophisticated zero-day exploits. In essence, adopting ZTNA-oriented architecture elevates enterprise resilience, regulatory adherence, and service reliability across all 5G-enabled business functions.

➢ *Recommendations for Deployment and Policy Formation*

Successful deployment of ZTNA in multi-slice 5G enterprise environments requires a phased and policy-driven approach that balances technical rigor with operational feasibility. Organizations should begin by conducting a thorough trust surface audit to map users, devices, applications, and data flows across all slices. Based on this audit, policy frameworks should be established that enforce least privilege access, contextual authentication, and real-time risk scoring. These policies must be enforced through distributed policy enforcement points embedded in both control and user planes, ensuring that enforcement is not centralized and vulnerable to compromise. The policy formation process should also include role- and attribute-based models that adapt dynamically to user behavior, workload sensitivity, and device posture. Enterprises must deploy identity federation and SSO (Single Sign-On) mechanisms that integrate with third-party identity providers, enabling a seamless but secure user experience across mobile, cloud, and on-premise environments. Additionally, policy orchestration should align with regulatory mandates, ensuring that access control logic reflects compliance with GDPR, HIPAA, and industry-specific standards. For performance-sensitive use cases, such as industrial automation or telemedicine, policies should account for latency constraints by leveraging edge-based ZTNA gateways and predictive access caching. Integration with AI-driven analytics engines can enhance policy refinement through behavioral baselining and anomaly detection. Finally, governance frameworks should institutionalize ZTNA reviews, ensuring policies are continuously updated in response to evolving threat landscapes, business objectives, and technological advancements. This ensures sustained trust assurance and strategic alignment across all enterprise network slices.

REFERENCES

[1]. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile Edge Computing: A Survey. *Journal of Systems Architecture*, 81, 1–21. https://doi.org/10.1016/j.sysarc.2017.12.001

[2]. Acar, A., Fereidooni, H., Abera, T., & Sadeghi, A. R. (2020). Web of Things: A Survey on Security Challenges and Solutions. *Computer Networks*, 148, 126–147. https://doi.org/10.1016/j.comnet.2018.11.006

[3]. Aggarwal, S., & Jaiswal, A. K. (2020). Survey on Quantum-Resistant Encryption for Next-Gen Network Security. *Journal of Information Security and Applications*, 53, 102534. https://doi.org/10.1016/j.jisa.2020.102534

[4]. Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Quantum Cryptography and Blockchain-Based Social Media Platforms as a Dual Approach to Securing Financial Transactions in CBDCs and Combating Misinformation in U.S. Elections. International Journal of Innovative Science and Research Technology. Volume 9, Issue 10, Oct.– 2024 ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1697.

[5]. Akindotei, O., Igba E., Awotiwon, B. O., & Otakwu, A (2024). Blockchain Integration in Critical Systems Enhancing Transparency, Efficiency, and Real-Time Data Security in Agile Project Management, Decentralized Finance (DeFi), and Cold Chain Management. *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 3, Issue 11, 2024. DOI: 10.38124/ijsrmt.v3i11.107.

[6]. Alex, G., Francesco, T., Stuart, C., Christian, R., & Joan, S. (2020). Slicing 5G networks: An architectural survey. *American Cancer Society*, 1-41.

[7]. Ali, A., Anton, A. I., & Sheikh, A. U. (2022). Identity and Access Management in Enterprise Systems: A Critical Review. *Journal of Information Security and Applications*, 67, 103149. https://doi.org/10.1016/j.jisa.2022.103149

[8]. Atalor, S. I., Ijiga, O. M., & Enyejo, J. O. (2023). Harnessing Quantum Molecular Simulation for Accelerated Cancer Drug Screening. *International Journal of Scientific Research and Modern Technology*, *2*(1), 1–18. https://doi.org/10.38124/ijsrmt.v2i1.502

[9]. Atalor, S. I., Raphael, F. O. & Enyejo, J. O. (2023). Wearable Biosensor Integration for Remote Chemotherapy Monitoring in Decentralized Cancer Care Models. *International Journal of Scientific Research in Science and Technology* Volume 10, Issue 3 (www.ijsrst.com) doi : https://doi.org/10.32628/IJSRST23113269

[10]. Ayoola, V. B., Ugoaghalam, U. J., Idoko P. I, Ijiga, O. M & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. *Global Journal of Engineering and Technology Advances,* 2024, 20(03),

094–117. https://gjeta.com/content/effectiveness-social-engineering-awareness-training-mitigating-spear-phishing-risks

[11]. Azonuche, T. I., & Enyejo, J. O. (2024). Agile Transformation in Public Sector IT Projects Using Lean-Agile Change Management and Enterprise Architecture Alignment. *International Journal of Scientific Research and Modern Technology*, *3*(8), 21–39. https://doi.org/10.38124/ijsrmt.v3i8.432

[12]. Azonuche, T. I., & Enyejo, J. O. (2024). Exploring AI-Powered Sprint Planning Optimization Using Machine Learning for Dynamic Backlog Prioritization and Risk Mitigation. *International Journal of Scientific Research and Modern Technology*, *3*(8), 40–57. https://doi.org/10.38124/ijsrmt.v3i8.448.

[13]. Azonuche, T. I., & Enyejo, J. O. (2024). Evaluating the Impact of Agile Scaling Frameworks on Productivity and Quality in Large-Scale Fintech Software Development. *International Journal of Scientific Research and Modern Technology*, *3*(6), 57–69. https://doi.org/10.38124/ijsrmt.v3i6.449

[14]. Azonuche, T. I., & Enyejo, J. O. (2025). Adaptive Risk Management in Agile Projects Using Predictive Analytics and Real-Time Velocity Data Visualization Dashboard. International Journal of Innovative Science and Research Technology Volume 10, Issue 4, April – 2025 ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2002

[15]. Barakabitze, A. A., Ahmad, A., Mijumbi, R. & Hines, A. (2020). 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges, https://www.sciencedirect.com/science/article/pii/S1389128619304773

[16]. Bura, C. (2025). Enriq: Enterprise neural retrieval and intelligent querying. *REDAY-Journal of Artificial Intelligence & Computational Science*.

[17]. Campolo, C., Molinaro, A., Iera, A., & Menichella, F. (2019). 5G Network Slicing for Vehicle-to-Everything Services. *IEEE Wireless Communications*, 26(5), 38-45. https://doi.org/10.1109/MWC.2019.1800440 *(used for informational background, not IEEE Transactions)*

[18]. Celeste, R., & Michael, S. (2021). Next-Gen Network Security: Harnessing AI, Zero Trust, and Cloud-Native Solutions to Combat Evolving Cyber Threats. *International Journal of Trend in Scientific Research and Development*, *5*(6), 2056-2069.

[19]. Coronado, E., & Riggio, R. (2019). Flow-based network slicing: Mapping the future mobile radio access networks. In *2019 28th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-9). IEEE.

[20]. D'Oro, S., Restuccia, F., & Melodia, T. (2021). Toward Intelligent Network Slicing for 6G. *Computer Networks*, 190, 107930. https://doi.org/10.1016/j.comnet.2021.107930

[21]. Desai, B., & Patil, A. (2020). Zero Trust with Micro-segmentation: A Software-Defined Approach to Securing Cloud-Native Applications. *Annals of Applied Sciences*, *1*(1).

[22]. Echeverria, J., Baez, J., Salazar, D., & Ramirez, C. (2020). Security and Privacy Threats in 5G: A Comprehensive Survey. *Computer Standards & Interfaces*, 71, 103442. https://doi.org/10.1016/j.csi.2020.103442

[23]. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security Issues in Cloud Environments: A Survey. *International Journal of Information Security*, 13(2), 113–170. https://doi.org/10.1007/s10207-013-0208-7

[24]. Ferrer Riera, J., Cano, J., & Calveras, A. (2020). Policy Enforcement in Network Slicing: A Context-Aware Framework. *Future Generation Computer Systems*, 108, 883–895. https://doi.org/10.1016/j.future.2020.03.020

[25]. Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. K. (2017). Network Slicing in 5G: Survey and Challenges. *IEEE Communications Magazine*, 55(5), 94-100. https://doi.org/10.1109/MCOM.2017.1600951 *(used only for overview; not Transactions)*

[26]. Idika, C. N., Enyejo, J. O., Ijiga, O. M. & Okika, N. (2025). Entrepreneurial Innovations in AI-Driven Anomaly Detection for Software-Defined Networking in Critical Infrastructure Security *International Journal of Social Science and Humanities Research* Vol. 13, Issue 3, pp: (150-166), DOI: https://doi.org/10.5281/zenodo.16408773

[27]. Igba E., Ihimoyan, M. K., Awotinwo, B., & Apampa, A. K. (2024). Integrating BERT, GPT, Prophet Algorithm, and Finance Investment Strategies for Enhanced Predictive Modeling and Trend Analysis in Blockchain Technology. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.,* November-December-2024, 10 (6) : 1620-1645.https://doi.org/10.32628/CSEIT241061214

[28]. Igba, E., Danquah, E. O., Ukpoju, E. A., Obasa, J., Olola, T. M., & Enyejo, J. O. (2024). Use of Building Information Modeling (BIM) to Improve Construction Management in the USA. World Journal of Advanced Research and Reviews, 2024, 23(03), 1799–1813. https://wjarr.com/content/use-building-information-modeling-bim-improve-construction-management-usa

[29]. Ijiga, A. C., Enyejo, L. A., Odeyemi, M. O., Olatunde, T. I., Olajide, F. I & Daniel, D. O. (2024). Integrating community-based partnerships for enhanced health outcomes: A collaborative model with healthcare providers, clinics, and pharmacies across the USA. *Open Access Research Journal of Biology and Pharmacy,* 2024, 10(02), 081–104. https://oarjbp.com/content/integrating-community-based-partnerships-enhanced-health-outcomes-collaborative-model

[30]. Ijiga, A. C., Igbede, M. A., Ukaegbu, C., Olatunde, T. I., Olajide, F. I. & Enyejo, L. A. (2024). Precision healthcare analytics: Integrating ML for automated image interpretation, disease detection, and prognosis prediction. *World Journal of Biology Pharmacy and Health Sciences,* 2024, 18(01), 336–354.

https://wjbphs.com/sites/default/files/WJBPHS-2024-0214.pdf

[31]. Ijiga, A. C., Olola, T. M., Enyejo, L. A., Akpa, F. A., Olatunde, T. I., & Olajide, F. I. (2024). Advanced surveillance and detection systems using deep learning to combat human trafficking. *Magna Scientia Advanced Research and Reviews, 2024*, 11(01), 267–286. https://magnascientiapub.com/journals/msarr/sites/default/files/MSARR-2024-0091.pdf.

[32]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journals.* Volume 13, Issue. https://doi.org/10.53022/oarjst.2024.11.1.0060I

[33]. Ijiga, O. M., Ifenatuora, G. P., & Olateju, M. (2021). Bridging STEM and Cross-Cultural Education: Designing Inclusive Pedagogies for Multilingual Classrooms in Sub Saharan Africa. JUL 2021 | *IRE Journals* | Volume 5 Issue 1 | ISSN: 2456-8880.

[34]. Ijiga, O. M., Ifenatuora, G. P., & Olateju, M. (2021). Digital Storytelling as a Tool for Enhancing STEM Engagement: A Multimedia Approach to Science Communication in K-12 Education. *International Journal of Multidisciplinary Research and Growth Evaluation.* Volume 2; Issue 5; September-October 2021; Page No. 495-505. https://doi.org/10.54660/.IJMRGE.2021.2.5.495-505

[35]. Ijiga, O. M., Ifenatuora, G. P., & Olateju, M. (2022). AI-Powered E-Learning Platforms for STEM Education: Evaluating Effectiveness in Low Bandwidth and Remote Learning Environments. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology I*SSN : 2456-3307 Volume 8, Issue 5 September-October-2022 Page Number : 455-475 doi : https://doi.org/10.32628/IJSRCSEIT

[36]. Ijiga, O. M., Ifenatuora, G. P., & Olateju, M. (2023). STEM-Driven Public Health Literacy : Using Data Visualization and Analytics to Improve Disease Awareness in Secondary Schools. *International Journal of Scientific Research in Science and Technology.* Volume 10, Issue 4 July-August-2023 Page Number : 773-793. https://doi.org/10.32628/IJSRST

[37]. Imoh, P. O. & Enyejo, J. O. (2025). Analyzing Social Communication Deficits in Autism Using Wearable Sensors and Real-Time Affective Computing Systems, *International Journal of Innovative Science and Research Technology* Volume 10, Issue 5 https://doi.org/10.38124/ijisrt/25may866

[38]. Imoh, P. O. (2023). Impact of Gut Microbiota Modulation on Autism Related Behavioral Outcomes via Metabolomic and Microbiome-Targeted Therapies *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 2, Issue 8, 2023 DOI: https://doi.org/10.38124/ijsrmt.v2i8.494

[39]. Imoh, P.O., Ajiboye,A. S., Balogun, T. K., Ijiga, A. C., Olola, T, M. & Ahmadu, E. O. (2025). Exploring the integration of psychedelic-assisted therapy and digital mental health interventions in trauma recovery for underserved adults with high-functioning autism, *Magna Scientia Advanced Research and Reviews*, 2025, **DOI:**https://doi.org/10.30574/msarr.2025.14.1.0079

[40]. James, U. U., Ijiga, O. M., & Enyejo, L. A. (2024). AI-Powered Threat Intelligence for Proactive Risk Detection in 5G-Enabled Smart Healthcare Communication Networks. *International Journal of Scientific Research and Modern Technology*, *3*(11), 125–140. https://doi.org/10.38124/ijsrmt.v3i11.679

[41]. Kang, J., Yu, R., Xie, S., Maharjan, S., & Zhang, Y. (2019). Enabling 5G Industrial IoT: A Service-Oriented Framework with Network Slicing. *Computer Networks*, 166, 106885. https://doi.org/10.1016/j.comnet.2019.106885

[42]. Kaushik, K., Kumawat, R., Kejriwal, D., Gupta, S., Kumar, A., & Gupta, S. (2025,). AI-Augmented Cybersecurity Protocols for Secure Multi-Hop Wireless Communication in 6G Networks. In *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)* (Vol. 3, pp. 181-186). IEEE.

[43]. Khorsandroo, S., Shamsi, M., & Al-Fuqaha, A. (2022). Security Challenges of 5G Slicing: A Systematic Review. *Journal of Information Security and Applications*, 67, 103165. https://doi.org/10.1016/j.jisa.2022.103165

[44]. Kim, Y., & Lim, H. (2021). Multi-agent reinforcement learning-based resource management for end-to-end network slicing. *IEEe Access*, *9*, 56178-56190.

[45]. Ksentini, A., & Taleb, T. (2021). On Enabling 5G Edge: Architectures and Challenges. *Computer Communications*, 175, 56-63. https://doi.org/10.1016/j.comcom.2021.05.015

[46]. Lal, C., Conti, M., & Das, A. K. (2021). Trust-Aware Security Enforcement in 5G Control Plane Communications. *Computer Communications*, 175, 24–33. https://doi.org/10.1016/j.comcom.2021.05.013

[47]. Lopes, A. R., Correia, M. E., & Garcia, M. (2022). Implementing Software-Defined Perimeters in Cloud-Native Environments: A Security-Driven Perspective. *Journal of Systems Architecture*, 130, 102775. https://doi.org/10.1016/j.sysarc.2022.102775

[48]. Lyu, X., Bi, J., Wang, H., & Zuo, Y. (2021). Designing Scalable Zero Trust Architectures for Enterprise Networks. *Computer Standards & Interfaces*, 77, 103520. https://doi.org/10.1016/j.csi.2021.103520

[49]. Mahfouz, A., & Mohapatra, P. (2022). Security Policies for Enabling Zero Trust in Modern Cyber Systems. *Journal of Network and Computer Applications*, 207, 103509. https://doi.org/10.1016/j.jnca.2022.103509

[50]. Matencio-Escolar, A., Wang, Q., & Calero, J. M. A. (2020). SliceNetVSwitch: Definition, design and implementation of 5G multi-tenant network slicing in

software data paths. *IEEE Transactions on Network and Service Management*, *17*(4), 2212-2225.

[51]. Moreno, J. M., Marin-Lopez, R., & Garcia-Alfaro, J. (2022). A Real-Time Context-Aware Authentication Framework for Edge and 5G Networks. *Computer Networks*, 207, 108785. https://doi.org/10.1016/j.comnet.2022.108785

[52]. Nguyen, G. N., & Redon, K. (2022). Architectural Models for Secure Access Control in Distributed Systems. *Journal of Systems Architecture*, 125, 102456. https://doi.org/10.1016/j.sysarc.2022.102456

[53]. Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2023). Exploring Influencer Marketing Among Women Entrepreneurs using Encrypted CRM Analytics and Adaptive Progressive Web App Development. *International Journal of Scientific Research and Modern Technology*, *2*(6), 1–13. https://doi.org/10.38124/ijsrmt.v2i6.562

[54]. Ononiwu, M., Azonuche, T. I., Imoh, P. O. & Enyejo, J. O. (2023). Exploring SAFe Framework Adoption for Autism-Centered Remote Engineering with Secure CI/CD and Containerized Microservices Deployment *International Journal of Scientific Research in Science and Technology* Volume 10, Issue 6 doi : https://doi.org/10.32628/IJSRST

[55]. Ononiwu, M., Azonuche, T. I., Imoh, P. O. & Enyejo, J. O. (2024). Evaluating Blockchain Content Monetization Platforms for Autism-Focused Streaming with Cybersecurity and Scalable Microservice Architectures *ICONIC RESEARCH AND ENGINEERING JOURNALS* Volume 8 Issue 1

[56]. Ononiwu, M., Azonuche, T. I., Imoh, P. O. & Enyejo, J. O. (2024). Evaluating Blockchain Content Monetization Platforms for Autism-Focused Streaming with Cybersecurity and Scalable Microservice Architectures *ICONIC RESEARCH AND ENGINEERING JOURNALS* Volume 8 Issue 1

[57]. Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2025). Mobile Commerce Adoption and Digital Branding Techniques for Startup Growth in Sub-Saharan African Urban Centers *International Journal of Management & Entrepreneurship Research* Fair East Publishers Volume: 7 Issue: 6 Page No: 443-463 DOI URL: https://doi.org/10.51594/ijmer.v7i6.1940

[58]. Rahman, A., Arora, A., & Choudhury, A. (2021). Secure Service Mesh for Microservice Architectures in 5G Networks. *Future Generation Computer Systems*, 125, 127–140. https://doi.org/10.1016/j.future.2021.06.012

[59]. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST Special Publication 800-207*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[60]. Santhosh, J. M. (2025). *On the Design of Security Policies for Service Function Chains in 5G Networks* (Doctoral dissertation, Open Research Newcastle).

[61]. Sharma, S. K., You, I., & Zhang, N. (2020). Designing Secure Interoperable Architectures for 5G and Beyond. *Journal of Network and Computer Applications*, 167, 102734. https://doi.org/10.1016/j.jnca.2020.102734

[62]. Sinha, S., & Kulkarni, A. (2021). Enhancing Microsegmentation with Adaptive Policy Management in Virtualized Networks. *Future Generation Computer Systems*, 118, 185–197. https://doi.org/10.1016/j.future.2020.12.014

[63]. Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Architecture & Orchestration. *Computer Networks*, 133, 17–39. https://doi.org/10.1016/j.comnet.2018.02.016

[64]. Tuncer, B., Chatterjee, M., & Fadlullah, Z. M. (2021). Real-Time User Trust and Risk Assessment in 5G Networks. *Journal of Information Security and Applications*, 60, 102860. https://doi.org/10.1016/j.jisa.2021.102860

[65]. Wichary, T., Mongay Batalla, J., Mavromoustakis, C. X., Żurek, J., & Mastorakis, G. (2022). Network slicing security controls and assurance for verticals. *Electronics*, *11*(2), 222.

[66]. Xu, Y., Li, W., & Liu, B. (2022). A Performance-Aware Framework for Real-Time ZTNA in Edge-Centric 5G Networks. *Computer Communications*, 189, 68–81. https://doi.org/10.1016/j.comcom.2022.01.004

[67]. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A Survey of Intrusion Detection in Internet of Things. *Journal of Network and Computer Applications*, 84, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

[68]. Zhang, Y., Patras, P., & Haddadi, H. (2020). Deep Learning in Mobile and Wireless Networking: A Survey. *Computer Networks*, 167, 107037. https://doi.org/10.1016/j.comnet.2019.107037