International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Zero Trust Identity Fabric for Multi-Layer Telecom Networks: Implications for Secure and Scalable Digital Infrastructure

Shiva Kumara*

Independent Researcher, University of Washington, USA

Received 01 Dec 2025, Accepted 24 Dec 2025, Available online 26 Dec 2025, **Vol.15, No.6 (Nov/Dec 2025)**

Abstract

The fast change of telecoms to multi-layer, cloud-native, and extremely distributed architectures, in effect, increased the attack surface to a level where the conventional security models that rely on perimeters are no longer effective. Advanced breaches that exploit the identity compromise, lateral movement, and API vulnerability would demand a full shift of the focus of identity-centric to security. how Zero Trust concepts and an Identity Fabric can secure multi-layer telecom networks traversing Radio Access Network, transport, core, service, management, cloud, and edge layers with identity as the primary control plane, the proposed Zero Trust Identity Fabric would permit ongoing authentication, highly detailed authorization, and real-time risk evaluation of users, devices, workloads, and network functions. The study examines the identity requirements of telecom layers and the identity threats, and also represents a conceptual architecture consisting of points of policy decision and enforcement, identity providers, and device posture management. A stable and scalable digital platform, and so, on which the advantages consist of the following: reduced lateral flow, policy enforcement, heterogeneous environment interoperability, and endurance through ongoing monitoring and analytics. Zero Trust Identity Fabric integration is a necessity to ensure that the telecom ecosystems in the present or the future are flexible, scalable, and secure.

Keywords: *Zero trust Architecture, Identity Fabric, Multi-layer Telecom network, Network security, cloud native, Digital infrastructures scalability.*

1. Introduction

The distribution, virtualization, and interconnection of networks have made the issue of cybersecurity very urgent as telecommunication evolves. The presence of advanced threats, which primarily exploit the lateral movement, identity compromise, and API level flaws, means that traditional perimeter-based defenses cannot protect networks [1][2] anymore. Consequently, zero-trust-based cybersecurity is one of the concepts that underlie the notion of distrusting anyone and therefore checking each user, device, and workload unconditionally [3][4]. This paradigm shift preconditions the emergence of more identity-based and dynamic security constructs, which are needed to support complex telecommunication environments.

Zero Trust interoperability with Identity Fabric is a unified, harmonious solution to identity, access, and trust management in decentralized systems [5][6]. The Identity Fabric guarantees perpetual authentication, policy-driven access control, and on-the-fly risk assessment of the entities interacting in the network. Telecom operators may provide comprehensive, context-sensitive, and scalable security by combining the ideas of Zero Trust with identity and access management control. It is a consolidated level where identity is the chief execution point coming straight to the aid of cybersecurity.

As telecom infrastructures change to multi-layer architectures that extend over physical networks, virtualized network functions, cloud-native services, and edge computing platforms, the requirement for identity-driven controls that are consistent and horizontally integrated across the different layers becomes even more evident [7][8]. Previously, telecom networks were secured by perimeter-based security models, also known as trust but verify. These models assumed that services and users were implicitly trustworthy after they had passed through the perimeter. However, these methods are not sufficient in cloud-native environments, which feature dynamic scaling, container orchestration, and multi-tenant environments [9]. The different layers of the network each have distinct security issues, for example, the possibility of an unauthorized user moving across layers, virtual components that have been incorrectly configured, and problems with inter-domain trust

*Corresponding author's ORCID ID: 0009-0009-9906-9561
DOI: https://doi.org/10.14741/ijcet/v.15.6.7

Zero Trust across telecom layers with the broader aim of creating a secure and scalable digital infrastructure of the future. As 5G, IoT, AI-driven orchestration, and edge services progress exponentially, telecom networks have to keep robust data integrity, low latency, and high tolerance [10][11]. These are requirements that can hardly be met by traditional models. A digital infrastructure aligned with Zero Trust provides the means for automated policy enforcement, easy scalability, and strong security across different domains, thus ensuring that the telecom ecosystems of the future are reliable and efficient [12][13]. Therefore, scalability is not only a technical requirement but also a natural consequence of the incorporation of Zero Trust concepts into the multi-layer network and identity fabric.

Structure of the Paper

This paper is organized as follows: Section II Telecom network layer and identity requirement, Section III Zero trust identity fabric in telecom, Section IV Implications for secure and scalable digital infrastructure in telecom in Section V Literature review, Section VI Conclusions and future work.

Telecom Network Layers and Identity Requirements

Modern telecom networks rely on multi-layer architectures spanning RAN, transport, core, service, management, cloud, and edge layers, each having distinct functions and facing different security. Since these layers are progressively getting virtualized and distributed, identity is becoming the most important security factor for access control and trust maintenance. It is absolutely necessary that every user, device, network function, and workload be given a unique identification and that this identification be regularly verified so as not to allow unauthorized access and lateral movement architecture is shown in Figure 1. It is very important to have established consistent identity-driven controls merged with all layers in order to secure the operation, scalability, and resilience of telecom infrastructures.

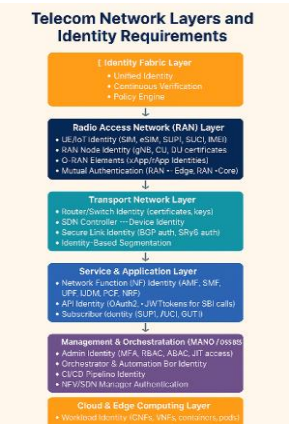

Fig.1 Telecom network layer and identity requirement

Radio Access Network (RAN) Layer

The Radio Access Network (RAN) layer is the front-end part of a telecom network that is directly responsible for connecting the User Equipment (UE) - like smartphones, IoT devices, sensors, and machines - to the core network via radio interfaces. Distributed Units (DU), Central Units (CU), gNB (5G base stations), and, in Open RAN designs, O-RAN components like O-RU, O-DU, O-CU, xApps, and rApps make up the RAN. The RAN is equipped with the capability to perform the central functions of the communication system, such as radio resource management, mobility control, encryption at the air interface, and first device authentication signaling [14]. Due to the RAN's widespread distribution in different locations and sometimes being physically exposed, it is a very vulnerable area that requires tight identity mechanisms to be implemented. These mechanisms include device identities (SIM/eSIM, SUPI, SUCI, IMEI), node identities (certificates for gNB/CU/DU), and a secure mutual authentication between RAN elements and the core or edge systems.

Transport Network Layer

A transport process engages in interactions with other elements. A transport procedure is only a special application procedure [15] that contains RIB, RIB Daemon, and VRM, since its sole purpose is to offer communication services. Figure 2 illustrates how each transport process uses the Transport Process (TP) API to recursively control the utilization of underlying VTNs.

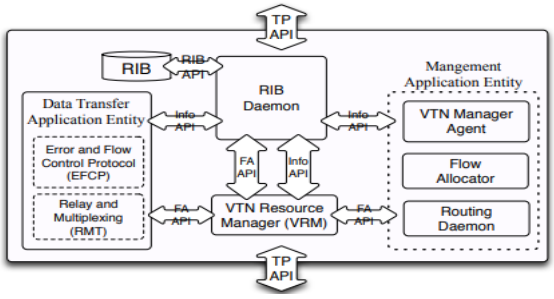

Fig.2 Transport process component layer

The Transport Network Layer is composed of various physical and logical components that together provide high-capacity, secure, and resilient connectivity across the telecom infrastructure. Its major components include:

IP/MPLS Routers

These are the major arteries of the transport network that allow packet-based forwarding, traffic engineering (TE), and Quality of Service (QoS) to be done[16]. The use of MPLS and Segment Routing (SR/SRv6) enables transport operations to be not only scalable but also flexible.

Ethernet and L2/L3 Switches

Listening to Ethernet along with Layer 2 (L2) and Layer 3 (L3) switches continues to be the foundation of the transport network, in which they combine the aggregation and forwarding of the traffic that passes between RAN, edge and core components. These switches are equipped with functionalities, like VLANs, EVPN, and route transport, segmentation, and provide high-speed links that are of great necessity for the expansion of telecom network operations in a cost-efficient way.

Optical Transport Systems (DWDM/OTN)

DWDM and OTN, optical transport systems, are capable of delivering high-capacity transmissions that cover extended transport networks. Simply put, these are wavelength division multiplexing systems that combine several wavelength streams onto one fiber, thus allowing bandwidth to be scaled, minimizing latency, and ensuring a resilient backhaul, which are all factors necessary for the facilitation of 5G, edge, and multi-layer telecom infrastructures.

SDN Controllers

Software-Defined Networking (SDN) controllers handle routing, policy, and traffic engineering in a central manner. As part of the control process, they also verify the identity of devices, permit access, and dictate the overall flow of data to local switching/routing nodes.

Segment Routing (SR/SRv6) Components

Allow smart, on-demand traffic routing that can be controlled by a program. SRv6 brings the features of both the transport and the service layer into a single IPv6 address.

Network Management and Monitoring Tools

There are various tools like NMS, telemetry collectors, and analytics systems, which offer network visibility, configuration, troubleshooting, and performance measurement for the transport networks.

Service and Application Layer

The digital services layer is represented by the Service and Application layer, applications, and network capabilities that are running on top of the telco infrastructure and are the main drivers behind communication, enterprise solutions, and API-driven interactions. This layering detail comprises functions like IMS/VoNR services, IoT platforms, network slicing management, analytics engines, and exposure frameworks such as the Network Exposure Function (NEF). Being the interface layer, it interacts directly with enterprises, developers, and external systems and hence, is the main layer responsible for delivering customized, value-added services [17]. Since it exposes APIs and service interfaces to external users, therefore, proper and strong identity controls, which support applications, slices, and API clients, are very important to avoid unauthorized access, ensure service integrity, and facilitate secure multi-tenancy in modern 5G and cloud-native environments.

Management & Orchestration

The Management & Orchestration (MANO) layer is the top-level managerial layer that handles the entire lifecycle, automation, and governance of the telecom network functions and services. It refers to the NFV MANO components, SDN controllers, OSS/BSS systems, and cloud-native orchestrators such as Kubernetes. This level is the one to actually execute, enlarge, watch, and fine-tune network resources in the RAN, transport, core, and service domains MANO systems are the ones with the most powerful administrative rights, it is very important to secure their characters, e.g. human administrators, automation bots, orchestrators, and CI/CD pipelines, to be able to avert the performing of unauthorized changes or the general network compromising. Strong access controls, continuous verification, and policy-driven automation allow MANO to be a key component of the Zero Trust model in multi-layer telecom networks.

Cloud & Edge Computing Layer

The cloud's remarkable scalability and effective peak activity management are its strongest points [18]. There are several service classifications and types:
Infrastructure as a Service (IaaS): This enables the rental of a virtual machine type infrastructure (VPS—Virtual Private Server) in order to install software such as databases, web servers, and DNS (Domain Name Service), but it requires system administration skills.
Software as a Service (SaaS): This is one of the most often used kinds of cloud solutions [19]. The supplier provides software to do a certain task, and the client is not responsible for the system's installation or hardware/software maintenance (including bug fixes and environmental security issues). Using an API (Application Programming Interface) to interface with the SaaS enables us to use software that is extremely complicated to construct, hence cutting down on development time and expenses. Specifically, SaaS may frequently be acquired through pay-as-you-go options, which significantly lower the upfront cost.
Network as a Service (NaaS): This enables flexible network rental based on user requirements. NaaS has above-average latency but offers noticeably more capacity for transmission.

Identity Requirement Across the Telecom Layer

A telecom network corresponds to different kinds of identities, has different significance for security, and is

differently exposed to attacks. The spectrum of attack surfaces extends from user and device identities in RAN to workload and administrative identities in cloud and MANO layers. These layers can be victimized with threats like spoofing, unauthorized access, API abuse, and privilege escalation. Such security risks can be addressed by implementing Zero Trust Identity Controls, which include continuous authentication, policy-based authorization, and real-time monitoring. The abreast layers, identity types, risks, and controls are reflected in Table I, and explained below.

Table 1 Identity requirement across the telecommunication Layer in zero trust security

Layer	Primary Identity Types	Important	Key Risks: Attack Surface	Zero Trust Identity Controls
RAN (Radio Access Network)	UE identity (SIM/eSIM, SUPI), IoT identities, RAN node certificates, xApp/rApp identities	Secures the most distributed and exposed part of the network	Rogue base stations, device spoofing, air-interface attacks, O-RAN compromise	Mutual authentication, device certificates, continuous UE identity validation, secure onboarding, micro-segmentation
Transport Network	Router/switch identities, SDN controller identity, link/path identity	Prevents route hijacking and unauthorized traffic manipulation	MITM attacks, BGP hijacking, SRv6 spoofing, SDN controller compromise	TLS for control channels, signed routing updates, identity-based segmentation, device attestation
Core Network	NF identities (AMF, SMF, UPF), subscriber identities, API/service identities	Central trust, authentication, mobility and session control	API abuse, NF impersonation, signaling storms, session hijacking	mTLS between NFs, OAuth2/JWT for APIs, identity federation, continuous authorization
Service & Application Layer	Slice identity (NSI, NSSAI), app identity, API consumer identity	Manages enterprise-level and external access	API misuse, slice hopping, tenant isolation failure	API keys + OAuth, per-slice identity policies, service mesh identity enforcement
MANO / Orchestration	Admin identities, automation bot identities, orchestrator identity, CI/CD identities	Highest privilege layer; compromise leads to total control	Privilege escalation, CI/CD pipeline attacks, orchestration takeover	MFA, RBAC/ABAC/JIT access, workload identity for bots, audit logging, privileged access Zero Trust
Cloud & Edge	Workload (CNF/VNF) identity, container/pod identity, node/cluster identity, multi-cloud federation	Ensures secure distributed execution and orchestration	Supply chain attacks, lateral movement, cluster takeover, compromised pods	SPIFFE/SPIRE, workload certificates, node attestation, policy-as-code, identity-aware service mesh

Zero Trust Identity Fabric for Telecom: Architecture and Conceptual Framework

The core of ZTA consists of a policy decision point (PDP) and a policy enforcement point (PEP). The PEP is the first person contacted when someone requests access. When access is granted, a link is established between the requested resource and the subject. The PDP decides whether to provide access with the help of the policy administrator (PA). The decision-making process makes use of all relevant internal and external data on the subject's network assets and security status[20].

Fig.3 Zero-trust architecture for telecom

As shown in Figure 3, the ZTA core establishes and manages a connection using information from many peripheral modules. Sort these modules into two categories: dynamic and static. The static components include identification (ID) management, public key infrastructure (PKI), data access policy, and industry compliance. Together, these modules create the integrity check and secure communication security policy rules. The ZTA core has the ability to dynamically modify the policy rules.

This approach takes into account the fact that threats can either be external or internal to an organization, and access controls are put in place based on identity and situational information. The migration process normally involves several important actions:

Assessment and Planning: To identify vulnerabilities and areas that require improvement, assess the network's present design, security measures, and access controls. Clearly state the objectives, deadlines, and materials needed to use Zero Trust concepts in a migration plan.

Identity and Access Management (IAM): The IAM choices should be expanded to provide high authentication, authorization, and access control mechanisms [21]. To verify user identities and dynamically impose access limitations, employ multi-factor authentication (MFA), least privilege access controls, and continuous monitoring.

Continuous Monitoring and Threat Detection: Utilize cutting-edge security analytics tools to keep an eye on user and application activity as well as network traffic in real time. Utilize ML and AI technologies to keep an eye out for anomalies and security risks and respond appropriately to security-related concerns.

Security Policy Enforcement: Ensure the uniform implementation of security regulations throughout the whole network architecture, including cloud environments, distant endpoints, and IoT devices. Implement policy-driven access restrictions and automate the implementation of security policies to comply with Zero Trust principles.

Regular Evaluation and Improvement: Instruction and Awareness of Employees. Conduct regular audits, track security KPIs, and continuously evaluate the effectiveness of Zero Trust processes to identify weaknesses and areas for improvement.

Core Component of Zero Trust Identity Fabric

The Zero Trust Identity Fabric is based on a collection of tightly interconnected components that, collectively, ensure a perpetual check-up and identity-based access control across the telecom networks. At the heart of the system, an Identity Provider is responsible for authentication and managing the identity lifecycle, along with device and workload identity and posture assessment, and policy-based decision mechanisms. The Policy Decision Point determines what access a request should get based on contextual, risk-based policies, and the Policy Enforcement Point makes sure that the access is granted or denied in real-time at the network, application, and infrastructure levels. To facilitate dynamic trust assessment, thus allowing security that is scalable, adaptive, and consistent across different layers of a telecom environment, is discussed below:

Identity Provider

An Identity Provider (IdP) is a service that creates and manages digital identities and the attributes associated with those identities. IdPs authenticate users through third-party service providers using these identities. IdP workflows typically involve these steps

Requests: Users enter credentials from another service, such as a Google account.

Verification: The IdP checks the user's authorized account against what they should access

Unlocking: After verification, the user is authorized to access specific resources, and the interaction is logged.

Device Identity and Posture Management

Device Identity and Posture Management (DIPM) is the process of making sure that each device that is accessing telecom networks, services, or workloads can be differentiated, is trustworthy, follows the rules, and is constantly checked. Devices in a Zero Trust environment are considered as separate identities.

Key component of device identity and posture management (DIPM)

Unique Device Identification (UDI): Each device is given a single, tamper-resistant, and verifiable identity through UDI by using certificates, hardware root-of-trust, or SIM/eSIM-based identifiers.

Secure Device Registration & Onboarding: After devices are authenticated, validated, and securely enrolled, they are permitted entry to a service or network.

Credential Lifecycle Management: The system that keeps the issuing, changing, renewing, and canceling of the device credentials in a continuous trust environment and also stops the forgery or the illegal use of the identity is the one that handles Credential Lifecycle Management.

Policy Decision Engine (PDP)

A crucial component of an access control system is the Policy Decision Point (PDP). The PDP maintains a set of access control policies articulated in XACML, as seen in Figure 4.

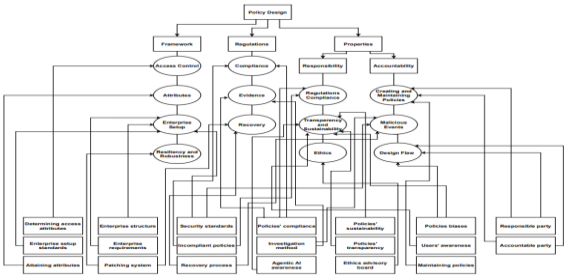

Fig.4 Policy design in Zero Trust

This demonstrates the purchase, development, and maintenance of systems as well as the use of efficient access control and network security management [22]. that demonstrates the organization's risk management.

Policy Enforcement Point (PEP)

This system facilitates, oversees, and ultimately terminates relationships between an individual and an organizational resource [23]. The PEP communicates with the PA to provide requests and/or receive updates to the PA's policies. This is a single logical part of Zero Trust Architecture (ZTA), which can be separated into two separate parts: a unified portal component that serves as a gatekeeper for communication pathways or the client and resource sides (e.g., a gateway component that controls access to resources).

Implications for Secure and Scalable Digital Infrastructure in Telecom

Integrating a Zero Trust Identity Fabric in telecom networks not only makes the system more secure but also more scalable by basically making identity the main control point across all network layers (RAN, transport, core, edge, and cloud). The method employed here is very effective as it keeps checking the authenticity, limits the lateral movement of the intruder, and also allows for very detailed access control [24]. Besides that, it is still very helpful in

meeting the quick scaling needs of 5G/6G, massive IoT, and network slicing by means of automated policy enforcement and cloud-native it offers seamless identity governance, better interoperability, and real-time monitoring; thus, network resilience is enhanced, operational risk is lowered, and there is conformance to regulations. There are some subheadings of digital infrastructure are discussed below:

End-to-end Security Across All Network Layers

Security that is end-to-end and available at every network layer means that every single part of the telecom ecosystem, that is, the radio access network (RAN), transport, core, edge, and cloud, is continuously authenticated, monitored, and protected as per the same security model. Once implicit trust is done away with and identity-based verification is enforced at every interaction point, the network is capable of prohibiting unauthorized access as well as decreasing lateral movements by possible attackers. This integrated, Zero Trust–based solution offering uniform security to a heterogeneous, multi-vendor environment ensures that all users, devices, workloads, and APIs adhere to the same rigorous security policies.

Scalable Access Control for Massive and Dynamic Environment

Telecom networks can maintain security while managing millions of devices, users, workloads, and APIs as they grow through scalable access control for massive and dynamic environments. This is particularly important with the proliferation of 5G, IoT, and cloud-native services [25]. The use of a centralized, identity-driven framework enables access policies to be automated, dynamically changed, and enforced uniformly across distributed network layers without security being compromised as the infrastructure grows. Consequently, the network operator has fewer manual tasks and can rapidly onboard new services, while still being able to respond instantly even in a very dynamic and resource-intensive telecom environment.

Automated identity and policy management allow for real-time access decisions of new devices and services

Policy enforcement is centralized, it is also distributed, thus ensuring that security is maintained at a consistent level in multi-cloud, edge, and on-premise environments.

Dynamic scalability can support sudden traffic changes, new network slices, and massive IoT growth without a threat of security breaches occurring is eves elevated.

Improved Interoperability and Unified Policy Enforcement

Enhanced interoperability and aligned enforcement of policies allow a spectrum of telecom components extending beyond the various vendors, technologies, and cloud environments to be subject to a common and integrated security model. Zero Trust Identity Fabric identities, access policies and security policies become consistent across realms of the network the threat of an inconsistent shield [26]. This unified solution not only exposes the borderless communication capacity of the legacy systems, virtualized network capabilities, APIs, and cloud-native services but also makes the security measures enforced stringent and reliable. As a result, operators receive a more integrated, controllable and secure digital infrastructure, which is appropriate for complex, multi-layer telecom environments.

Enhanced Resilience Through Continuous Monitoring and Analytics

Constant surveillance and analytics resulting in greater resilience is what makes telecom networks secure, stable and highly available. It achieves this through constant monitoring of user behavior and integrity, device and network functionality. Having real-time data collection, anomaly detection and automated threat response, the network can detect the malicious activities at an extremely early stage, preventing the breakdown that extends to the other layers that are interconnected. Such a preventative, intelligence-led approach that concentrates the power of telecom infrastructure of a system failure compromises the operators ' chance of a routine service even when there is an emerging cyber threat or any interruption to service.

Real-time threat detection and anomaly monitoring make it possible to spot odd behavior early on, lowering the risk of the entire network being compromised.

Automated incident response and isolation mechanisms are also key to the instantaneous containment of threats, and therefore, they are the ones that preclude the disruptions that can be propagated to the various layers of interconnected telecom.

Continuous visibility, as well as analytics-oriented insights, is what makes the difference between operational reliability and the operators being more engaged in their task of maintaining the system and the service availability relatively low.

Telecommunication Infrastructure

The conventional telecommunication infrastructure is a sophisticated network consisting of physical components and technologies that enable the transmission of voice, data, and multimedia communications [27]. The fundamental elements of this infrastructure are:

Telecommunication Networks: These networks include of the software and technology that facilitate the transmission of signals and data across various communication channels, including fiber-optic cables,

wireless networks, and satellite linkages. These networks are the basis for the provision of telecommunication services, facilitating the smooth communication of data between devices and users.

Data Centers: Telecommunication companies own specialized data centers that house computers, storage systems, and network devices essential for processing, storing, and managing the substantial data quantities generated by their services [28]. All these data centers are crucial for hosting and delivering telecommunication applications, as well as facilitating the storing and processing of consumer data.

Core Infrastructure: This includes the essential elements of infrastructure that constitute the telecommunication ecosystem, including as switching equipment, signaling devices, and billing and provisioning systems. These components manage the complex functions of telecommunication networks, including routing, switching, service delivery, and customer management.

Literature Review

This section briefly reviews existing studies on Zero Trust, identity management, and AI-enabled security relevant to telecom networks. Table II compares prior work based on focus challenges and future work. The review shows that most approaches address highlighting the need for a secure and scalable multi-layer telecom infrastructure.

Aleisa (2025), post-quantum cryptography and Zero Trust Architecture (ZTA). Secure IoT settings are achieved by the use of a hybrid Reinforcement-Lattice Blockchain Key Generation for quantum-resilient key generation, Deep Q-Network Multi-Factor Secure Key (DQN-MFSK) for dynamic key selection, and Zero-Knowledge Proof for privacy-preserving signatures. This architecture includes resilience against evolving risks, such as potential quantum attacks, auditability and traceability, and data privacy and secrecy. Zero-Knowledge Proofs (ZKP) protect sensitive data from disclosure while offering authentication and verification. QBC-ZKPAF enhances security and privacy for IoT networks through the decentralization of identity management and the implementation of multi-factor authentication [29].

Manuel et al. (2025), Identity management assumes a major role, and in this context, Decentralized Identity Management (DIM) presents a potential option. To protect and enable identifiable transactions throughout the Computing Continuum, it uses decentralized technologies. Implementing the concepts of Self-Sovereign Identity (SSI), which gives distributed, zero-trust infrastructures across the continuum authentication and authorization capabilities, is crucial to enhancing security and privacy. This improves security during the resource sharing and acquisition phases. The system utilizes factors like as decentralization, interoperability, trust management, and privacy-enhancing features. DIM depends on reliability, but also considers privacy through ways that allow individuals to selectively disclose identify traits without compromising sensitive information, utilizing decentralized authentication and authorization mechanisms [30].

Yousseef et al. (2025), AVs Pass the Zero Trust-based Decentralized Identity Management (D-IM) protocol framework by fusing the elements of a blockchain network's decentralization and tamper resistance with the ideas of zero trust architecture, never trust, always verify, removing the utilization of centralized capacity to perform authentication, and ensuring continuous verification of all participants through the implementation of Hyperledger Iroha in support of light weight and safe authentication without a centralized, reliable source, performed on both urban and highway conditions, confirms the pragmatics of the protocol [31].

Manda (2024), The shift to next-generation technologies like cloud computing and 5G, and AI is modernizing telecom companies' current infrastructure and transforming their operational procedures to meet the demands of digital realities as they strive to remain relevant in an increasingly digital world. These technologies not only increase the network's capacity but also foster customer-centricity, flexibility, and operational efficiency. For example, 5G enables telecom operators to provide scalable customer experiences and streamline their IT processes by providing ultra-fast, low-latency connectivity, which is essential for the Internet of Things and cloud computing, and supporting the development of telecom infrastructure and operational strategies. It draws attention to the opportunities and difficulties that telecom firms confront while providing analysis and useful suggestions derived from actual project experiences [32].

Aramide (2024), Zero Trust Architecture (ZTA) employs the idea of "never trust, always verify" to alter the security paradigm by mandating that everything be constantly authorized and confirmed by everyone. Zero Trust is revolutionizing identity management by doing away with role-based access and static credentials and replacing them with behavior-based, real-time verification. Using contextual data, including device posture, user behavior, geolocation, access patterns, identity lifecycle, threat detection, and risk-aware access control, artificial intelligence (AI) makes it easier to continuously assess trust. protection, scalability, and privacy of integrating identity verification procedure with AI Zero Trust ideas that provide next-generation networks with robust, scalable, and context-aware defense against identity-based threats [33].

Gharib and Afghah (2023) By providing improved subscriber identity protection, 5G significantly improved cellular network security. However, a security architecture that implements user-network mutual authentication is necessary to provide security services that are independent of any trusted authority

in the 5G network. SCC5G Critical-mission Security. This study proposes communication over a 5G network in a ZT context. SCC5G is a post-quantum cryptography (PQC) security solution that implants an integrated hardware root of authentication (HRA), such as physically unclonable functions (PUF), onto users' devices to enable tamper-resistant and unclonable authentication capabilities [34].

Table 2 Comparative analysis of zero trust in identity fabric for multi-layer telecom network implication for digital infrastructure

Author	Study On	Key Findings	Application	Challenges	Future Work
Aleisa (2025)	Zero Trust Architecture with Post-Quantum Cryptography for IoT using Reinforcement Learning, Lattice-based Blockchain Key Gen, DQN-MFSK, and ZKP	Demonstrates a quantum-resilient IoT security framework combining Zero Trust, blockchain, reinforcement learning, and ZKP. Achieves confidentiality, auditability, traceability, and resistance to quantum attacks through decentralized identity and multi-factor authentication.	Secure IoT environments, quantum-resilient identity and key management	High computational overhead, scalability in large IoT deployments, integration complexity of PQC and RL mechanisms	Optimization for lightweight IoT devices, real-world deployment validation, energy-efficient PQC and RL-based security models
Manuel et al. (2025)	Self-Sovereign Identity (SSI) and Decentralized Identity Management (DIM) along the Computing Continuum	Proposes DIM with SSI principles to enhance security, privacy, and trust in zero-trust distributed infrastructures. Enables selective disclosure, decentralized authentication, and authorization across	Computing Continuum (edge–fog–cloud), distributed systems, resource sharing	Interoperability across platforms, trust governance, and usability of SSI for end-users	Standardization of SSI protocols, performance evaluation at scale, seamless integration with Zero Trust frameworks
Yousseef et al. (2025)	Decentralized Identity Management (D-IM) for Autonomous Vehicles with Zero Trust	a blockchain-enabled Zero Trust identity framework using Hyperledger Iroha. Eliminates centralized authorities and ensures continuous verification with lightweight authentication	Autonomous Vehicles (AVs), intelligent transportation systems	Latency constraints, blockchain scalability, and mobility-related authentication overhead	Large-scale AV network testing, integration with V2X security, adaptive trust models for dynamic mobility
Manda (2024)	Digital Transformation of Telecom Infrastructure using 5G, Cloud, and AI	5G, cloud computing, and AI modernize telecom operations by improving scalability, efficiency, and customer-centricity. Provides practical insights from real-world telecom projects.	Telecom networks, 5G infrastructure, cloud-based services	Legacy system integration, security risks during transformation, skills gap	Deeper integration of Zero Trust security, AI-driven network automation, resilience against emerging cyber threats
Aramide (2024)	Zero Trust Architecture and AI-driven Identity Management	Zero Trust replaces static credentials with continuous, behavior-based authentication using AI. Enhances risk-aware access control, identity lifecycle management, and threat detection.	Next-generation networks, enterprise identity systems	Privacy concerns with AI-driven monitoring, scalability, and explainability of AI decisions	Privacy-preserving AI models, federated learning for identity trust evaluation, and standardized AI-ZTA frameworks
Gharib & Afghah (2023)	Post-Quantum Secure Critical Mission Communication FOR 5G (SCC5G) in Zero Trust Environments	a PQC-based ZT security architecture for 5G using hardware root of authentication (PUF). Achieves tamper resistance, unclonability, and mutual authentication without relying on trusted authorities.	5G critical mission communications, defense and public safety networks	Hardware deployment cost, integration with the existing 5G infrastructure	Lightweight PQC schemes, broader PUF adoption, real-world trials in large-scale 5G networks

Conclusion and Future Work

A Zero Trust Identity Fabric is essential for securing and scaling next-generation multi-layer telecom networks. With telecom infrastructures turning cloud-native, virtualized, and highly distributed, the old perimeter-based security models cannot deal with threats like identity compromise, lateral movement, API misuse, and orchestration-layer attacks anymore. Thus, by making the identity the main security control point, the Zero Trust Identity Fabric allows telecoms to do continuous authentication, fine-grained authorization, and real-time risk evaluation at any layer, i.e., RAN, transport, core, service, MANO, and cloud-edge. The research demonstrates that consistent identity governance and policy-driven access control help decrease the operational risk while facilitating the enormous scalability needed for 5G, IoT, network slicing, and new digital services. Moreover, the support for the multi-vendor and multi-cloud ecosystems through automated policy enforcement and continuous monitoring leads to improved network resilience and reliability. Hence, the security paradigm thus created, besides being more secure in an end-to-end fashion, is also in sync with the operational tactical skills of telecom operators, thereby enabling the rapid

onboarding of new services without trust being compromised. Therefore, a Zero Trust Identity Fabric is a consolidated, scalable and anticipatory security infrastructure that assists secure digital transformation in telecom networks. Next, the research could shed light on AI-driven adaptive trust models, decentralized and self-sovereign identity frameworks, and post-quantum cryptographic techniques to advance security, privacy, and scalability in telecom infrastructures of the future.

References

[1] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and A maturity assessment framework," Comput. Secur., vol. 133, Oct. 2023, doi: 10.1016/j.cose.2023.103412.

[2] K. Sowjanya, D. Saha, and B. Lall, "Zero-Trust Security in 5G and Beyond Networks: An Overview," in 2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS), IEEE, Jan. 2025, pp. 1230–1234. doi: 10.1109/COMSNETS63942.2025.10885674.

[3] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis: A Comparative Study," TIJER – Int. Res. J., vol. 11, no. 12, pp. 922–928, 2024.

[4] K. B. Thakkar and H. P. Kapadia, "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model," in 2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST), IEEE, Apr. 2025, pp. 1–6. doi: 10.1109/ICTEST64710.2025.11042822.

[5] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," Int. J. Sci. Res. Mod. Technol., vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[6] S. Thangavel, K. C. Sunkara, and S. Srinivasan, "Software-Defined Networking (SDN) in Cloud Data Centers: Optimizing Traffic Management for Hyper-Scale Infrastructure," Int. J. Emerg. Trends Comput. Sci. Inf. Technol., vol. 3, no. 1, pp. 29–42, 2022, doi: 10.63282/3050-9246.IJETCSIT-V3I3P104.

[7] S. R. Kurakula, "Designing Enterprise Systems for the Future of Financial Services: The Intersection of AI, Cloud-Native Microservices, and Intelligent Data Processing," Eur. J. Comput. Sci. Inf. Technol., vol. 13, no. 20, pp. 91–103, Apr. 2025, doi: 10.37745/ejcsit.2013/vol13n2091103.

[8] D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 454–464, Jan. 2024, doi: 10.48175/IJARSCT-11900D.

[9] P. Srikanth and S. Patchamatla, "Design and Implementation of Zero-Trust Microservice Architectures for Securing Cloud-Native Telecom Systems," Int. J. Res. Appl. Innov., vol. 4, no. 6, pp. 6169–6177, 2021, doi: 10.15662/IJRAI.2021.0406008.

[10] S. Amrale, "Proactive Resource Utilization Prediction for Scalable Cloud Systems with Machine Learning," Int. J. Res. Anal. Rev., vol. 10, no. 4, 2023.

[11] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," Int. J. Res. Anal. Rev., vol. 11, no. 4, pp. 901–907, 2024.

[12] G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," ESP J. Eng. Technol. Adv., vol. 4, no. 3, pp. 209–218, 2024, doi: 10.56472/25832646/JETA-V4I3P122.

[13] S. B. Karri, C. M. Penugonda, S. Karanam, M. Tajammul, S. Rayankula, and P. Vankadara, "Enhancing Cloud-Native Applications: A Comparative Study of Java-To-Go Micro Services Migration," Int. Trans. Electr. Eng. Comput. Sci., vol. 4, no. 1, pp. 1–12, Apr. 2025, doi: 10.62760/iteecs.4.1.2025.127.

[14] S. Singh, "Open Radio Access Networks in Multi - Vendor Environments: A Survey of Interoperability Solutions and Best Practices," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 2, pp. 57–65, 2025.

[15] Y. Wang and I. Matta, "Multi-layer Virtual Transport Network management," Comput. Commun., vol. 130, pp. 38–49, Oct. 2018, doi: 10.1016/j.comcom.2018.08.011.

[16] V. Shah, "Next-Gen Emergency Communication Using Low-Power Wide-Area and Software-Defined WANS," Int. J. Adv. Res. Sci. Commun. Technol., vol. 2, no. 1, pp. 600–609, Sep. 2022, doi: 10.48175/IJARSCT-8349M.

[17] R. Patel, "Security Challenges in Industrial Communication Networks: A Survey on Ethernet/Ip, Controlnet, and Devicenet," Int. J. Recent Technol. Sci. Manag., vol. 7, no. 8, pp. 54–63, 2022, doi: 10.10206/IJRTSM.2025171772.

[18] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge Computing and Cloud Computing for Internet of Things: A Review," Informatics, vol. 11, no. 4, Sep. 2024, doi: 10.3390/informatics11040071.

[19] B. R. Cherukuri, "Edge Computing vs. Cloud Computing: A Comparative Analysis for Real-Time AI Applications," Int. J. Multidiscip. Res., vol. 6, no. 5, pp. 1–17, Oct. 2024, doi: 10.36948/ijfmr.2024.v06i05.29316.

[20] N. Nahar, K. Andersson, O. Schelén, and S. Saguna, "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks," IEEE Access, vol. 12, pp. 94753–94764, 2024, doi: 10.1109/ACCESS.2024.3425350.

[21] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security: Challenges and Solutions," Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 3, pp. 6–18, Mar. 2025, doi: 10.48175/IJARSCT-23902.

[22] F. R. Sandjaja, A. A. Majeed, A. Abdullah, G. Wickremasinghe, K. Rafferty, and V. Sharma, "Policy Design in Zero-Trust Distributed Networks: Challenges and Solutions," pp. 1–10, 2025.

[23] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," CRC Press, Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[24] S. K. Davuluri, V. Challagulla, V. Mudapaka, and U. Konka, "AI-Driven DevOps in Telecommunications: Bridging Predictive Analytics with Continuous Delivery for Network Agility," in 2025 IEEE International Conference and Expo on Real Time Communications at IIT (RTC), IEEE, Oct. 2025, pp. 1–4. doi: 10.1109/RTC66985.2025.11211551.

[25] J. W. Sajja and N. Kolli, "Towards a Unified Framework for Enterprise Data Transformation: Cloud Architecture, Governance, and Intelligent Automation," J. Inf. Syst. Eng. Manag., vol. 9, no. 4, pp. 1–20, 2024.

[26] P. R. Marapatla, "Intelligent APIs: AI-Powered Ecosystem for Nonprofit Digital Transformation," J. Inf. Syst. Eng. Manag., vol. 10, no. 60s, pp. 605–618, Sep. 2025, doi: 10.52783/jisem.v10i60s.13174.

[27] A. Egon, "Cloud Computing and Its Impact on Telecommunication Infrastructure," pp. 1–23, 2024.

[28] S. K. N. S. Biswal, S. S. Jain, S. Phalke, and S. K. Ulaganathan, "Methods and apparatus for datacenter monitoring," 2024.

[29] M. A. Aleisa, "Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments," IEEE Access, vol. 13, pp. 18660–18676, 2025, doi: 10.1109/ACCESS.2025.3529309.

[30] J. M. B. Murcia, E. Cánovas, J. García-Rodríguez, A. M. Zarca, and A. Skarmeta, "Decentralised Identity Management solution for zero-trust multi-domain Computing Continuum frameworks," Futur. Gener. Comput. Syst., vol. 162, Jan. 2025, doi: 10.1016/j.future.2024.08.003.
[31] A. Yousseef, S. Satam, B. S. Latibari, M. Abdel-malek, S. Salehi, and P. Satam, "Zero Trust-based Decentralized Identity Management System for Autonomous Vehicles," IEEE Open J. Veh. Technol., pp. 1–14, 2025.
[32] J. K. Manda, "Digital Transformation Impact on Telecom Infrastructure: Analyzing the implications of digital transformation initiatives on telecom infrastructure and operational strategies, based on your experience in digital transformation projects," vol. 5, no. 8, pp. 5–17, 2024.
[33] O. O. Aramide, "Zero-trust identity principles in next-gen networks: AI-driven continuous verification for secure digital ecosystems," World J. Adv. Res. Rev., vol. 23, no. 3, pp. 3304–3316, Sep. 2024, doi: 10.30574/wjarr.2024.23.3.2656.
[34] M. Gharib and F. Afghah, "SCC5G: A PQC-Based Architecture for Highly Secure Critical Communication Over Cellular Network in Zero-Trust Environment," in 2023 57th Asilomar Conference on Signals, Systems, and Computers, IEEE, Oct. 2023, pp. 11–18. doi: 10.1109/IEEECONF59524.2023.10477078.